1

Syllabus Algebra I

voorlopige versie

Prof. Dr G. van der Geer

Faculteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
Versie: 2002

Het woord *algebra* is afgeleid van de arabische uitdrukking *al-jabr wa'l muqabala* in de titel van een boek van Al-Khwarizmi uit de negende eeuw opgedragen aan de kalief Al Ma'mum. De perzische dichter en wiskundige Omar Khayyam (10??-ca. 1126) geeft de volgende omschrijving van algebra:

Een van de wiskundige theorieën die nodig zijn in dat deel van de filosofische wetenschappen dat bekend staat als de wiskunde is de kunst van de algebra die zich richt op de bepaling van onbekende getalsmatige of meetkundige grootheden.

Van Dale, het woordenboek van de nederlandse taal, geeft de volgende omschrijving:

> **al′gebra** (< Ar.). v. (*m.*), letterrekening, stelkunde, deel der wiskunde dat zich bezighoudt met de betrekkingen van grootheden die voorgesteld worden door symbolen (letters); —(zegsw.) *dat is algebra voor mij*, daar begrijp ik niets van; — (bij overdr.) les in algebra: *van 9-10 hebben wij algebra*; — leerboek over algebra: *ik heb mijn algebra vergeten*; —(fig.) abstract stelsel.

De inleiding van 'Algeba', van N. Bourbaki, een encyclopedisch compendium van de moderne algebra, begint met de omschrijving:

"Algebra heeft voornamelijk van doen met 'berekenen', d.w.z. met het uitvoeren van " algebraïsche operaties" op de elementen van een verzameling, waarvan het bekendste voorbeeld wordt gegeven door de 'vier bewerkingen' van de elementaire rekenkunde.

1. Gehele Getallen

Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk.
(L. Kronecker*)

De *natuurlijke getallen* $1, 2, 3, \ldots$ zijn wellicht de meest fundamentele wiskundige objecten en behoren tot het oudste culturele erfgoed van de mensheid. De oudste ons bekende archeologische sporen hiervan zijn inkepingen in botten uit de Aurignac-periode (30.000-20.000), waarin de zogenaamde Cro-Magnon-mens voorkwam.

We noteren de verzameling van de natuurlijke getallen met $\mathbb{N}$. Dus

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Het is een kwestie van smaak of men de 0 ook tot de natuurlijke getallen rekent. De nul is blijkbaar niet zo natuurlijk, want zij dateert pas van later datum en komt bijvoorbeeld bij de klassieke Grieken nog niet voor. De nul komt voor bij de laat-Babylonische wiskunde (3de eeuw voor het begin van de jaartelling) en bij de Indische wiskunde in de 3de tot 5de eeuw. Een verzamelingstheoretische definitie van de natuurlijke getallen is als volgt.

De natuurlijke getallen vormen een verzameling waarin een element $1 \in \mathbb{N}$ aangegeven is en die een afbeelding $S : \mathbb{N} \to \mathbb{N}$ (opvolgerfunctie) bezit met de volgende eigenschappen:

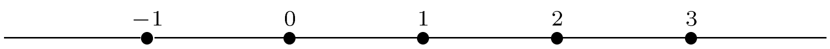
i) S is injectief;
ii) $1 \notin S(\mathbb{N})$;
iii) Als een deelverzameling $M \subseteq \mathbb{N}$ het element 1 bevat en voldoet aan $S(M) \subseteq M$ dan $M = \mathbb{N}$.

De drie axioma's corresponderen met ons welbekende eigenschappen van tellen: ieder natuurlijk getal heeft een opvolger ($S(1) = 2$, $S(2) = 3, \ldots$). Het eerste axioma zegt ons dat we daarbij een gegeven natuurlijk getal niet meer dan een keer tegenkomen. Het derde is equivalent met twee andere 'principes', het wel-ordeningsprincipe en het principe van volledige inductie, zie na (1.13). Het eerste, dat we vaak zullen hanteren, luidt (voor $\mathbb{N} \cup \{0\}$) als volgt.

(1.1) Principe. *Iedere niet-lege verzameling van niet-negatieve gehele getallen bevat een kleinste element.*

De uitbreiding van $\mathbb{N}$ tot de verzameling $\mathbb{Z}$ van de gehele getallen

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$



die men krijgt door 0 en de negatieve getallen toe te voegen, mag voor ons heel vanzelfsprekend zijn, maar dateert ook pas van later. Naar het schijnt komen negatieve getallen het eerst voor in het oude China. Indiase wiskundigen stuitten op negatieve getallen toen

* L. Kronecker, Duits wiskundige, 1823–1891

ze een algoritme voor het oplossen van kwadratische vergelijkingen probeerden te formuleren. Ook Diofantos** gebruikte negatieve getallen. De term 'negatief' getal komt voor het eerst voor in een manuscript van Petrus Ramus in 1569. Pas in de zeventiende eeuw wordt het gebruik hiervan algemeen geaccepteerd onder wis- en natuurkundigen.

De gehele getallen spelen een fundamentele rol in de gehele wiskunde, en dus ook in de algebra. In dit hoofdstuk bespreken we een paar fundamentele eigenschappen van gehele getallen, in het bijzonder deelbaarheid en de hoofdstelling van de rekenkunde.

Eerst leiden we nu de mogelijkheid van 'deling met rest' af.

(1.2) Stelling. (Deling met Rest.) *Laat a en b gehele getallen zijn met $b > 0$. Dan bestaan er twee eenduidig bepaalde gehele getallen q en r zodat*

$$a = qb + r \quad \text{met} \quad 0 \leq r < b.$$

Bewijs. Het idee van het bewijs is simpel: trek b net zolang van a af totdat er een rest over is die kleiner is dan b. Meer precies gaat dat zo. Beschouw de verzameling

$$V = \{\ldots, a - 2b, a - b, a, a + b, a + 2b, \ldots\} = \{a - xb : x \in \mathbb{Z}\}.$$

Deze verzameling bevat niet-negatieve elementen: bijv. als $a \geq 0$ nemen we $x = 0$ en $x = a$ als $a < 0$. Volgens bovenstaand principe is er dan een kleinste niet-negatief getal, zeg $r = a - qb$, in $V \cap \{0, 1, 2, \ldots\}$ voor zekere q. Dan kunnen we schrijven

$$a = qb + r \qquad \text{met} \quad r \geq 0.$$

Wanneer $r \geq b$, dan is $r - b$ weer een element van $V \cap \{0, 1, 2, \ldots\}$, want $r - b \geq 0$ en $r - b = a - (q + 1)b$. Wegens $r - b < r$ weerspreekt dit de minimaliteit van r. Dus concluderen we $0 \leq r < b$.

Nu we een q en een r met de gevraagde eigenschappen gevonden hebben moeten we nog laten zien dat q en r eenduidig bepaald zijn. Als q', r' een ander paar is, dan geldt

$$a = qb + r,$$
$$a = q'b + r'$$

met $0 \leq r, r' < b$. Stel nu dat $q \neq q'$. Na eventueel verwisselen van q en q' mogen we veronderstellen dat $q > q'$. Aftrekken van bovenstaande vergelijkingen en gebruikmaken van $q - q' \geq 1$, dus $(q - q')b \geq b$, levert

$$b \leq (q - q')b = r' - r \leq r' < b.$$

Deze tegenspraak leert ons dat $q = q'$, dus dat $r = a - qb = a - q'b = r'$. Dit bewijst de eenduidigheid en daarmee de gehele uitspraak.

Het getal q in de stelling heet het *quotiënt* en r heet de *rest* van a na deling door b. Bijvoorbeeld voor $a = -27$ en $b = 6$ vinden we $-27 = -5 \cdot 6 + 3$, d.w.z. $q = -5$, $r = 3$.

(1.3) Definitie. Laat a, b gehele getallen zijn. We zeggen: *a deelt b* als er een geheel getal c bestaat met

$$b = a\,c.$$

** wiskundige uit Alexandrië, derde eeuw

Dus bijvoorbeeld 7 deelt 35 omdat $35 = 7 \cdot 5$. Als a het getal b deelt zeggen we ook dat *a een deler is van b* of dat *b deelbaar is door a*. De notatie hiervoor is:

$$a \mid b.$$

Merk op dat ieder getal een deler is van 0, terwijl 1 ieder getal deelt. Verder geldt dat wanneer a zowel b als b' deelt, dan deelt a ook $b \pm b'$ en ook iedere gehele lineaire combinatie $xb + yb'$ met $x, y \in \mathbb{Z}$.

(1.4) Definitie. Laat a en b gehele getallen zijn, niet beide gelijk aan 0. De *grootste gemene deler* van a en b, geschreven $\mathrm{ggd}(a, b)$, is het grootste gehele getal dat zowel a als b deelt. Verder definiëren we $\mathrm{ggd}(0, 0) = 0$. We zeggen dat a en b *onderling ondeelbaar* zijn als $\mathrm{ggd}(a, b) = 1$.

Als d een deler is van x en $x \neq 0$ dan $|d| \leq |x|$. Daarom gaat het hier om het grootste element van een eindige verzameling gehele getallen en heeft bovenstaande definitie zin.

(1.5) Lemma. *Laat a en b gehele getallen zijn. Dan geldt:*
i) $\mathrm{ggd}(a, b) = \mathrm{ggd}(b, a)$*;*
ii) $\mathrm{ggd}(a, b) = \mathrm{ggd}(-a, b)$*;*
iii) $\mathrm{ggd}(a, b + xa) = \mathrm{ggd}(a, b)$ *voor alle* $x \in \mathbb{Z}$.

Bewijs. We laten het bewijs van i) en ii) aan de lezer over. Voor iii) merken we op dat iedere deler d van a en b ook de lineaire combinatie $b + xa$ deelt. Omgekeerd, iedere deler van a en $b + xa$ deelt ook de lineaire combinatie $b = (b + xa) - xa$. Dus de verzameling van gemeenschappelijke delers van a en b is gelijk aan de verzameling van gemeenschappelijke delers van a en $b + xa$. Dit bewijst iii).

(1.6) Stelling. *Laat a en b gehele getallen zijn, niet beide gelijk aan 0. Dan is de grootste gemene deler van a en b gelijk aan het kleinste positieve element van de verzameling*

$$L = \{ax + by : x, y \in \mathbb{Z}\}.$$

Bewijs. De verzameling L bevat a, $-a$, b en $-b$ zoals men ziet door $x = \pm 1, y = 0$ of $x = 0, y = \pm 1$ te nemen. Dus L bevat positieve elementen.

Laat $d = ax_0 + by_0$ het kleinste positieve element van L zijn. Omdat alle elementen van L sommen van veelvouden van a en b zijn, zijn ze allemaal door $\mathrm{ggd}(a, b)$ deelbaar, in het bijzonder is ook d deelbaar door $\mathrm{ggd}(a, b)$. We vinden

$$\mathrm{ggd}(a, b) \leq d. \tag{1}$$

Van de andere kant, als $c = ax_1 + by_1$ een element van L is, dan levert deling door d met rest: $c = md + r$ met $0 \leq r < d$. Maar r is een lineaire combinatie van a en b want

$$r = c - md = a(x_1 - mx_0) + b(y_1 - my_0).$$

Omdat d het kleinste positieve getal in L is moet r nul zijn. Dus concluderen we dat d ieder getal c in L deelt. Dus d deelt in het bijzonder a en b, dus

$$d \leq \mathrm{ggd}(a, b). \tag{2}$$

De twee ongelijkheden (1) en (2) tezamen impliceren $d = \operatorname{ggd}(a, b)$, zoals te bewijzen was.

(1.7) Gevolg. *De grootste gemene deler van twee gehele getallen a, b kan geschreven worden als een lineaire combinatie van a en b, d.w.z. er bestaan $x, y \in \mathbb{Z}$ zodat*

$$\operatorname{ggd}(a, b) = ax + by.$$

Bewijs. Dit is duidelijk uit de voorgaande stelling voor a, b niet beide nul. Wanneer $a = b = 0$ dan is het ook direct duidelijk.

(1.8) Gevolg. *Als d een deler van a en b is, dan ook van $\operatorname{ggd}(a, b)$.*

(1.9) Propositie. *Laat $a, b, c \in \mathbb{Z}$. Stel $\operatorname{ggd}(a, b) = 1$ en $a|bc$. Dan geldt $a|c$.*

Bewijs. Het gegeven $\operatorname{ggd}(a, b) = 1$ impliceert dat er x en y zijn met

$$1 = ax + by.$$

Na vermenigvuldiging met c geeft dit $c = cax + cby$. Omdat a het product bc deelt is er een $z \in \mathbb{Z}$ met $bc = za$, en dus vinden we $c = cax + zay = a(cx + zy)$, d.w.z. a deelt c.

(1.10) Definitie. Een geheel getal p heet een *priemgetal* (of simpelweg *priem*) als $p > 1$ en als de enige positieve delers van p de getallen 1 en p zijn. Een geheel getal $n > 1$ dat niet priem is heet *samengesteld.*

Voorbeelden van priemgetallen zijn:

$$\begin{aligned} 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17\ 19,\ 23,\ \ 29,\ 31,\ 37,\ 41, 43, \ldots, \\ 101, 103, 107, 109, 113, 127, 131, 137, 139, \ldots, \\ 1009, 1013, 1019, 1021, 1031, \ldots, \\ 10007, 10009, 10023, 10037, \ldots, \\ 100003, 100019, 100049, \ldots, \\ 10000019, 10000079, \ldots, \end{aligned}$$

maar ook bijvoorbeeld

$$2^{127} - 1 = 170141183460469231731687303715884105727.$$

We noteren de verzameling van priemgetallen met $\mathcal{P}$. De priemgetallen zijn de ‘atomen’ van de wiskunde.

Hoe verder we op de getallenrechte komen, des te minder priemgetallen treffen we aan; alle veelvouden van eerdere priemgetallen vervallen als mogelijke kandidaat. Blijft er op den duur nog iets over? Het antwoord is van Euclides:

(1.11) Stelling. *(Euclides*) Er zijn oneindig veel priemgetallen.*

Bewijs. Stel dat $\mathcal{P}$ eindig is, zeg $\mathcal{P} = \{p_1, \ldots, p_r\}$. Beschouw dan $N = p_1 p_2 \cdots p_r + 1$. Laat p de kleinste deler > 1 van N zijn. Omdat een deler van p tenslotte ook een deler van N is moet p een priemgetal zijn. Dus geldt $p = p_i$ voor zekere i. Maar dan deelt p zowel $p_1 p_2 \cdots p_r$ als N, dus ook het verschil $N - p_1 p_2 \cdots p_r = 1$. Deze tegenspraak bewijst dat $\mathcal{P}$ niet eindig is.

Dit bewijs heeft sinds Euclides nog niets van zijn charme verloren!

(1.12) Lemma van Euclides. *Laat a en b gehele getallen zijn en p een priemgetal. Als p het product ab deelt, dan deelt p ofwel a ofwel b (of beide).*

Bewijs. Omdat p priem is geldt $\mathrm{ggd}(p, a) = 1$ of $\mathrm{ggd}(p, a) = p$. Als p geen deler is van a, dan $\mathrm{ggd}(p, a) = 1$. Uit propositie (1.9) volgt dan dat $p|b$.

(1.13) Hoofdstelling van de Rekenkunde. *Ieder geheel getal $n > 1$ kan geschreven worden als product van priemgetallen: er bestaan priemgetallen $p_1, \ldots, p_r$ zodat*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r. \tag{3}$$

Deze schrijfwijze is eenduidig op de volgorde na.

Bewijs. We bewijzen eerst het bestaan van een schrijfwijze (3). We doen dit met inductie naar n. Als $n = 2$ hebben we zo een schrijfwijze met $r = 1$ en $p_1 = 2$. Stel dat het bestaan van zo een schrijfwijze bewezen is voor alle getallen x met $1 < x < n$. Nu is n òf priem, òf samengesteld. Als n priem is hebben we de gezochte schrijfwijze $n = p$. Stel nu dat n samengesteld is, zeg $n = ab$ met $1 < a, b < n$. Volgens de inductieveronderstelling kunnen zowel a als b als product van priemgetallen geschreven worden:

$$a = p_1 \cdot \ldots \cdot p_s \quad \text{en} \quad b = q_1 \cdot \ldots \cdot q_t.$$

Dan is $n = p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t$ de verlangde schrijfwijze.

Om de eenduidigheid te bewijzen nemen we aan dat er geen uniciteit geldt en beschouwen we het kleinste gehele getal $n > 1$ dat twee zulke schrijfwijzen heeft:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s. \tag{4}$$

Het priemgetal p_1 deelt dan het product $q_1 \cdot \ldots \cdot q_s$. Met herhaald toepassen van het Lemma van Euclides volgt dat p_1 een priemgetal q_i deelt voor een $1 \leq i \leq s$. Omdat zowel p_1 als q_i priem zijn volgt $p_1 = q_i$. Deling door $p_1 = q_i$ levert

$$n/p_1 = p_2 \ldots \cdot p_r = q_1 \cdot \ldots q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_s. \tag{5}$$

Omdat n/p_1 kleiner is dan n is de schrijfwijze (5) eenduidig op volgorde na. Maar daaruit volgt direct dat ook de schrijfwijze (4) eenduidig is op volgorde na. Dit weerspreekt onze aanname en bewijst de stelling.

---

* Wiskundige uit Alexandrië die rond 330 v. C. leefde en daar een wiskundige school stichtte tijdens de regering van Ptolemeus I.

We kunnen de stelling ook geldig maken voor $n = 1$ door het lege product gelijk te stellen aan 1. Voor negatieve gehele getallen n levert toepassing van de stelling op $-n$ een schrijfwijze

$$n = -p_1 \cdot \ldots \cdot p_r$$

op, wederom eenduidig op volgorde na.

In het bewijs is gebruik gemaakt van het Principe van Volledige Inductie.

(1.1 a) Principe van Volledige Inductie. *Laat V een verzameling gehele getallen zijn met $1 \in V$. Stel dat V de eigenschap heeft dat wanneer $n \in V$ ook $n+1 \in V$. Dan is ieder positief geheel getal in V bevat.*

Dit principe is equivalent met het principe (1.1). In het bewijs van (1.13) bestaat V uit alle getallen die eenduidig te factorizeren zijn.

Voor een gegeven geheel getal n en een priemgetal p kunnen we kijken hoe vaak p in de schrijfwijze (3) voorkomt.

(1.14) Definitie. Laat n een positief geheel getal zijn en p een priemgetal. Dan is de orde van n bij p, genoteerd $\mathrm{ord}_p(n)$, het aantal factoren $p_i = p$ in de schrijfwijze (3). Voor negatieve n stellen we $\mathrm{ord}_p(n) = \mathrm{ord}_p(-n)$.

Voor een geheel getal $n \neq 0$ is $\mathrm{ord}_p(n)$ een niet-negatief geheel getal. Voor $n = 0$ is $\mathrm{ord}_p(0)$ niet gedefiniëerd. Een positief geheel getal n laat zich dan schrijven als

$$n = \prod_{p \in \mathcal{P}} p^{\mathrm{ord}_p(n)},$$

waarbij het product over de verzameling

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, \ldots\}$$

van priemgetallen loopt. Alhoewel dit product over *alle* priemgetallen loopt is maar voor eindig veel p de exponent $\mathrm{ord}_p(n)$ ongelijk 0. Voor negatieve n hebben we de schrijfwijze $n = -\prod_p p^{\mathrm{ord}_p(n)}$.

De functie $\mathrm{ord}_p : \mathbb{Z} - \{0\} \to \mathbb{Z}_{\geq 0}$ voldoet aan de eigenschap

$$\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b). \tag{6}$$

Immers, als $a = \prod p^{\mathrm{ord}_p(a)}$ en $b = \prod p^{\mathrm{ord}_p(b)}$ dan levert $ab = \prod p^{\mathrm{ord}_p(a)+\mathrm{ord}_p(b)}$. Omdat de schrijfwijze uniek is, volgt (6).

(1.15) Lemma. *Een geheel getal $a \neq 0$ deelt b dan en slechts dan als $\mathrm{ord}_p(a) \leq \mathrm{ord}_p(b)$ voor elk priemgetal p.*

Bewijs. Als a een deler is van b volgt uit (6) dat

$$\mathrm{ord}_p(b) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b/a) \quad \text{voor alle } p \in \mathcal{P}.$$

Omdat $\mathrm{ord}_p(b/a) \geq 0$ volgt $\mathrm{ord}_p(a) \leq \mathrm{ord}_p(b)$.

Omgekeerd, als voor iedere priem p geldt $\mathrm{ord}_p(a) \leq \mathrm{ord}_p(b)$ kunnen we schrijven

$$b = a \cdot c \quad \text{met} \quad c = \prod p^{\mathrm{ord}_p(b) - \mathrm{ord}_p(a)}.$$

Dit bewijst de bewering.

(1.16) Opgave. Bewijs de volgende formule voor de grootste gemene deler:

$$\operatorname{ggd}(a,b) = \prod_{p\in\mathcal{P}} p^{\min(\operatorname{ord}_p(a),\operatorname{ord}_p(b))}.$$

We geven nu een recept om de grootste gemene deler van een tweetal gegeven gehele getalen uit te rekenen. Deze methode heet het Euclidisch algoritme. Gezien Lemma (1.5) is het geen serieuze beperking van de algemeenheid als we veronderstellen dat a en b positief zijn.

(1.17) Euclidisch algoritme. Laat $a, b \in \mathbb{Z}$. We definiëren nu een rij niet-negatieve gehele getallen r_k voor $k = 0, 1, 2, \ldots$ door $r_0 = |a|$ en $r_1 = |b|$. Als $r_1 \neq 0$ delen we r_0 door r_1 met quotiënt q_1 en rest r_2 waarbij $0 \leq r_2 < r_1$. Als $r_2 \neq 0$ dan delen we r_1 door r_2 met quotient q_2 en rest r_3 die voldoet aan $0 \leq r_3 < r_2$. We herhalen dit als r_k niet nul is door r_{k-1} te delen door r_k met quotiënt q_k en rest r_{k+1}:

$$r_{k+1} = \text{rest van } r_{k-1} \text{ bij deling door } r_k \text{ als } r_k \neq 0.$$

Er geldt $0 \leq r_{k+1} < r_k$. De r_i vormen dan een dalende rij niet-negatieve gehele getallen: $r_1 > r_2 > \ldots$. Omdat de r_i niet-negatief zijn wordt r_k nul bij een bepaalde index k en dan stoppen we. De rest r_{k-1} is dan de $\operatorname{ggd}(a,b)$.

(1.18) Voorbeeld. We berekenen de ggd van 246810 en 13579.

$$\begin{aligned}
246810 &= 18 \times 13579 + 2388\\
13579 &= 5 \times 2388 + 1639\\
2388 &= 1 \times 1639 + 749\\
1639 &= 2 \times 749 + 141\\
749 &= 5 \times 141 + 44\\
141 &= 3 \times 44 + 9\\
44 &= 4 \times 9 + 8\\
9 &= 1 \times 8 + 1\\
8 &= 8 \times 1 + 0
\end{aligned}$$

Dus de grootste gemene deler is volgens dit voorschrift 1. We moeten echter nog nagaan dat dit voorschrift ook echt het gewenste resultaat levert.

(1.19) Propositie. *Het Euclidisch algoritme is een correct algoritme: het stopt na eindig veel stappen en levert als uitkomst de grootste gemene deler.*

Bewijs. Omdat het algoritme een rij getallen r_k levert die niet-negatief zijn en steeds kleiner worden moet het algoritme na eindig veel stappen stoppen (principe (1.1)).

Uit de relatie $r_{k-1} = q_k r_k + r_{k+1}$ volgt met (1.5) dat

$$\operatorname{ggd}(r_{k-1}, r_k) = \operatorname{ggd}(r_k, r_{k+1}).$$

Dus we vinden

$$\operatorname{ggd}(a,b) = \operatorname{ggd}(r_0,r_1) = \operatorname{ggd}(r_1,r_2) = \ldots = \operatorname{ggd}(r_{k-1},r_k) = \ldots.$$

Wanneer nu bij stap k de rest $r_k = 0$ dan geldt $\operatorname{ggd}(r_{k-1},r_k) = \operatorname{ggd}(r_{k-1},0) = r_{k-1}$ zoals verlangd.

Door de boekhouding tijdens het uitvoeren van het algoritme beter bij te houden kunnen we niet alleen de grootste gemene deler $\operatorname{ggd}(a,b)$ berekenen, maar ook een schrijfwijze

$$\operatorname{ggd}(a,b) = xa + yb$$

vinden. We doen dit als volgt. Kies hiervoor

$$x_0 = \pm 1, y_0 = 0, \qquad x_1 = 0, y_1 = \pm 1$$

zodat aan de volgende vergelijkingen voldaan is

$$\begin{aligned} x_0 a + y_0 &= r_0 (= |a|) \\ x_1 + y_1 b &= r_1 (= |b|) \end{aligned}$$

Als $r_1 \neq 0$ trekken we de tweede vergelijking q_1 keer van de eerste af en vinden dan

$$x_2 a + y_2 b = r_2.$$

Algemener voor $i < k$ krijgen we de $i+1$-ste vergelijking door q_i maal de i-de van de $(i-1)$-de af te trekken. Dan voldoen de x_i en y_i aan de vergelijking

$$x_{i-1} = q_i x_i + x_{i+1} \quad y_{i-1} = q_i y_i + y_{i+1}.$$

Bij de stap k waarbij r_k nul wordt levert dit

$$x_{k-1} a + y_{k-1} b = r_{k-1} = \operatorname{ggd}(a,b).$$

(1.20) Voorbeeld. We doen het bovenstaande voorbeeld nu met de uitgebreide boekhouding. Laat dus $a = 246810$ en $b = 13579$.

$$\begin{aligned}
246810 &= 1 \times a + 0 \times b \\
\text{(18 keer aftrekken)} \quad 13579 &= 0 \times a + 1 \times b \\
\text{(5 keer aftrekken)} \quad 2388 &= 1 \times a - 18 \times b \\
1639 &= -5 \times a + 91 \times b \\
749 &= 6 \times a - 109 \times b \\
141 &= -17 \times a + 309 \times b \\
44 &= 91 \times a - 1654 \times b \\
9 &= -290 \times a + 5271 \times b \\
8 &= 1251 \times a - 22738 \times b \\
1 &= -1541 \times a + 28009 \times b
\end{aligned}$$

Dit levert de schrijfwijze van de ggd als lineaire combinatie

$$1 = -1541 \times 246810 + 28009 \times 13579.$$

Opgaven

1) Laat a en b gehele getallen zijn met $\operatorname{ggd}(a,b) = d \neq 0$. Bewijs dat a/d en b/d onderling ondeelbaar zijn.

2)
 i) Laat c een positief geheel getal zijn. Bewijs dat $\operatorname{ggd}(ac, bc) = c \operatorname{ggd}(a,b)$.
 ii) Laat $a, b, c \in \mathbb{Z}$. Bewijs dat $\operatorname{ggd}(a, \operatorname{ggd}(b,c)) = \operatorname{ggd}(\operatorname{ggd}(a,b), c)$.

3)
 i) Bepaal de grootste gemene deler $d := \operatorname{ggd}(666, 2003)$ en geef gehele getallen x en y aan met $666 \cdot x + 2003 \cdot y = d$.
 ii) Bepaal alle oplossingen $(x,y) \in \mathbb{Z}^2$ van de vergelijking $666 \cdot x + 2003 \cdot y = d$.

4) Voor ieder priemgetal $p > 3$ is $p^2 - 1$ deelbaar door 24. Bewijs dit.

5) Laat zien dat een geheel getal $n > 1$ priem is dan en slechts dan als n geen positieve gehele delers d heeft met $1 < d \leq \sqrt{n}$.

6) Laat n een positief geheel getal zijn en p een priemgetal.
 (i) Bewijs met volledige inductie dat

$$\operatorname{ord}_p(n!) = \sum_{j=1}^{n} \operatorname{ord}_p(j).$$

 (ii) Laat verder zien dat

$$\operatorname{ord}_p(n!) = \sum_{r=1}^{\infty} \lfloor \frac{n}{p^r} \rfloor = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots,$$

 waarbij $\lfloor a \rfloor$ voor $a \in \mathbb{R}$ het grootste gehele getal m is met $m \leq a$.
 (iii) Op hoeveel nullen eindigt 1000! ?

7) Laat n een positief geheel getal zijn en beschouw de binomiaalcoëfficiënt $\binom{2n}{n}$. Bewijs dat $\operatorname{ord}_p(\binom{2n}{n}) = 1$ voor alle priemgetallen p met $n < p < 2n$.

8) Laat $a, b, c \in \mathbb{Z}$. Als $x = r/s$ met $r, s \in \mathbb{Z}$ en $\operatorname{ggd}(r,s) = 1$ een oplossing is van $aX^2 + bX + c = 0$ dan is r een deler van c en is s een deler van a. Bewijs dit. Laat zien dat als $X^2 + bX + c$ een oplossing x in de rationale getallen heeft dan $x \in \mathbb{Z}$.

9) Laat $a \in \mathbb{Z}_{>0}$ en $n \in \mathbb{Z}_{\geq 2}$. Bewijs dat als $a^n - 1$ priem is dat $a = 2$ en n een priemgetal is. Geldt ook het omgekeerde? De getallen $2^p - 1$ met p priem heten de *Mersenne* getallen*. Het is niet bekend of er oneindig veel Mersenne-priemen onder de Mersenne-getallen zijn. De grootste bekende Mersenne-priem op dit moment (dec. 99) heeft $p = 6972593$ en is een getal met 2 098 960 cijfers.

---

* Marin Mersenne, een Franse monnik, 1588–1648

10) Bepaal alle priemgetallen tussen 1000 en 1100; idem voor de twee intervallen $[10\,000, 10\,100]$ en $[100\,000, 100\,100]$.

11) Het *kleinste gemene veelvoud* (*kgv*) van twee gehele getallen a en b, niet beide gelijk aan 0, is het kleinste positieve getal dat een veelvoud van a en van b is. Notatie: $\mathrm{kgv}(a, b)$. Geef het analogon van Opgave (1.16) in de tekst voor het kgv. Bewijs: $\mathrm{kgv}(a, b) \times \mathrm{ggd}(a, b) = |ab|$. Geef een algoritme aan om het kgv te berekenen.

12) Laat zien dat als m en n onderling ondeelbare gehele getallen zijn dat

$$\frac{1}{mn} = \frac{x}{m} + \frac{y}{n}$$

voor zekere gehele getallen x en y.

13) Laat zien dat het positieve reële getal $\sqrt{2}$ geen rationaal getal is.

14)* Bewijs: de reeks

$$\sum_{p \in \mathcal{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots$$

divergeert (*lastig*).

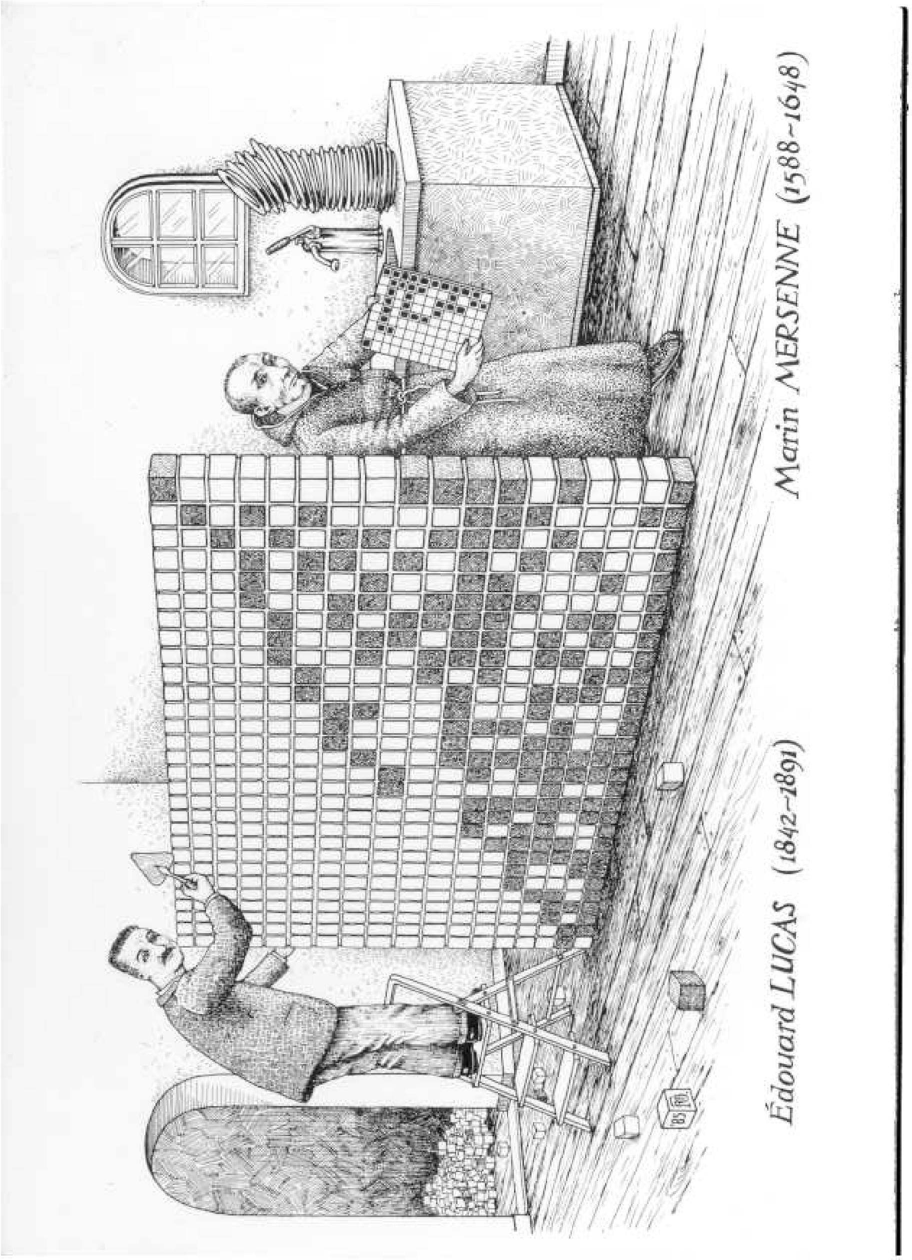
15) Het product van n opeenvolgende natuurlijke getallen is deelbaar door $n!$. Bewijs dit.

16) Bewijs dat voor alle $n \in \mathbb{Z}_{\geq 2}$ de som $1 + 1/2 + 1/3 + \ldots + 1/n$ niet geheel is.

17) Interpreteer de prent die hierna volgt.

Suggesties voor verdere literatuur

Het volgende artikel over priemgetallen kan zeer worden aanbevolen.
D. Zagier: The first 50 Million Prime Numbers. *Mathematical Intelligencer* **0** (1977). p. 7–19.



2. Equivalentie-relaties

Twee figuren zijn gelijkvormig of equivalent als ze op zich beschouwd niet onderscheiden kunnen worden omdat ze iedere denkbare eigenschap of objectieve betekenis gemeen hebben.
(G.W. Leibniz*)

Het komt vaak voor in de wiskunde dat we bepaalde dingen als gelijk willen zien terwijl ze het niet zijn. Bijvoorbeeld beschouwen we $3-4$ en -1 als gelijk. Ook gelijkvormige driehoeken worden soms als gelijk beschouwd. Om verschillende objecten toch als gelijk te kunnen beschouwen voeren we het begrip *equivalentierelatie* in. Dit berust op de observatie dat het gelijkteken $=$ de volgende eigenschappen heeft:
i) $a = a$;
ii) als $a = b$ dan ook $b = a$;
iii) als $a = b$ en $b = c$ dan $a = c$.

(2.1) Definitie. *Een equivalentierelatie op een verzameling V is een deelverzameling R van $V \times V$ zodat voor alle a, b, $c \in V$ geldt*
i) $(a, a) \in R$*;*
ii) als $(a, b) \in R$ *dan ook* (b, a)*;*
iii) als $(a, b) \in R$ *en* $(b, c) \in R$ *dan* $(a, c) \in R$*.*

De drie eigenschappen heten (in deze volgorde) *reflexiviteit, symmetrie en transitiviteit.* We schrijven in plaats van $(a, b) \in R$ vaak eenvoudig $a \sim b$ en we zeggen: a is equivalent met b als $(a, b) \in R$. Ook andere symbolen worden soms gebruikt, bijvoorbeeld $\equiv$ en $\cong$, zoals we later zullen zien.

(2.2) Definitie. Als $\sim$ een equivalentierelatie is op een verzameling V en $v \in V$ een element, dan heet de deelverzameling

$$\{w \in V : w \sim v\}$$

de *equivalentieklasse* van v.

De equivalentieklasse van v wordt vaak gedefinieerd met $[v]$ of $\bar{v}$. We geven nu een aantal voorbeelden.

(2.3) Voorbeeld. Beschouw het complexe vlak $\mathbb{C}$. Elementen hiervan, de complexe getallen, hebben een schrijfwijze $a + b\,i$ met $a, b \in \mathbb{R}$. Hierbij geldt $i^2 = -1$. De norm $|z| \in \mathbb{R}_{\geq 0}$ van een complex getal $z = a + b\,i$ wordt gedefinieerd door

$$|z|^2 = a^2 + b^2.$$

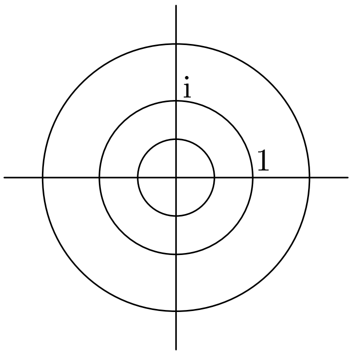
We definiëren nu een equivalentierelatie op $\mathbb{C}$ door

$$z \sim w \quad \text{dan en slechts dan als} \quad |z| = |w|.$$

Meetkundig zegt dit: de afstand van z en w tot de oorsprong is gelijk. Omdat $=$ reflexief, symmetrisch en transitief is volgt dit nu ook voor onze $\sim$. De equivalentieklasse van $z \in \mathbb{C}$ is de cirkel met straal $|z|$ en met de oorsprong als middelpunt.

---

* G.W. Leibniz, Duits wiskundige, 1646–1716



(2.4) Voorbeeld. Beschouw de verzameling van gehele getallen $\mathbb{Z}$. Definieer hierop een equivalentierelatie $\sim$ door

$$a \sim b \qquad \text{dan en slechts dan als} \quad 2|(a-b).$$

Dit is een equivalentierelatie: i) $2|(a-a)$; ii) als $2|(a-b)$ dan ook $2|(b-a)$; iii) als $2|(a-b)$ en $2|(b-c)$ dan $2|(a-b)+(b-c)$, dus $2|(a-c)$ zoals gewenst.

De equivalentieklasse van 0 bestaat uit alle *even* getallen; de equivalentieklasse van 1 bestaat uit alle *oneven* getallen. We schrijven

$$a \equiv b (\bmod 2) \qquad \text{voor} \qquad a \sim b.$$

(2.5) Voorbeeld. Beschouw weer de verzameling van gehele getallen $\mathbb{Z}$. Laat n een gegeven positief geheel getal zijn. Definieer op $\mathbb{Z}$ een equivalentierelatie $\sim$ door

$$a \sim b \qquad \text{dan en slechts dan als} \quad n|(a-b).$$

Dit is ook weer een equivalentierelatie. (Ga dit na!) We schrijven nu om verwarring te voorkomen $a \equiv b\,(\bmod n)$ in plaats van $a \sim b$ en zeggen* *a is congruent met b modulo n* De equivalentieklasse van a wordt genoteerd als $a(\bmod n)$ of kortweg met $\bar{a}$.

De equivalentieklasse van een getal a is gelijk aan die van zijn rest r bij deling door n. Er geldt $0 \le r < n$. We zien dus in dat er precies n equivalentieklassen zijn, namelijk

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}.$$

Deze equivalentieklassen heten ook wel *restklassen* modulo n. De notatie voor deze verzameling equivalentieklassen is $\mathbb{Z}/n\mathbb{Z}$. Dus

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

met

$$\bar{0} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$\bar{1} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$

etc.

---

* Deze notatie stamt van C.F. Gauss, e en van de belangrijkste wiskundigen, 1777–1855

We zien in deze voorbeelden dat onze verzameling V opgedeeld wordt in disjuncte equivalentieklassen. Dat geldt algemeen:

(2.6) Definitie. Een verdeling of partitie van een verzameling V is een collectie niet-lege disjuncte deelverzamelingen $V_i : i \in I$ (met I een of andere indexverzameling) van V zodat hun vereniging gelijk is aan V.

(2.7) Propositie. *Laat V een verzameling zijn met een equivalentierelatie $\sim$. Dan geven de equivalentieklassen een verdeling van V.*

Bewijs. Neem een element $x \in V$. Noteer de equivalentieklasse van x met $\bar{x}$. Wegens eigenschap i) geldt $x \in \bar{x}$. Dus een equivalentieklasse $\bar{x}$ is niet leeg. Ook volgt hieruit dat de vereniging van de equivalentieklassen gelijk is aan V. Neem nu twee equivalentieklassen $\bar{x}$ en $\bar{y}$. Stel dat hun doorsnede niet leeg is, zeg $z \in \bar{x} \cap \bar{y}$. Dan geldt $x \sim z$ en $y \sim z$ en wegens de symmetrie en transitiviteit geldt dus ook $x \sim y$. Dus als $v \sim x$ geldt wegens transitiviteit $v \sim y$. Maar dat betekent $\bar{x} = \bar{y}$.

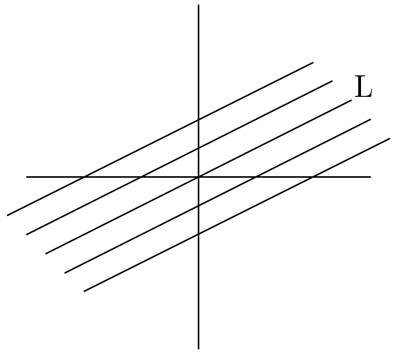
(2.8) Voorbeeld. Beschouw het platte vlak $\mathbb{R}^2$. Kies een lijn L in $\mathbb{R}^2$ door de oorsprong. Definieer een equivalentierelatie op $\mathbb{R}^2$ via

$$v_1 \sim v_2 \quad \text{dan en slechts dan als} \quad v_1 - v_2 \in L.$$

Omdat $0 \in L$ en met $w \in L$ ook $-w \in L$ volgen de reflexiviteit en de symmetrie. Verder geldt dat als $v_1 - v_2 \in L$ en $v_2 - v_3 \in L$ dat ook $(v_1 - v_2) + (v_2 - v_3) \in L$, waaruit de transitiviteit volgt. De equivalentieklasse van een element $x \in \mathbb{R}^2$ bestaat uit alle vectoren van de vorm $x + v$ met $v \in L$:

$$\bar{x} = \{x + v : v \in L\} = x + L.$$

Dus de equivalentieklasse is een lijn die evenwijdig is met L. Door ieder punt $x \in \mathbb{R}^2$ gaat precies één lijn evenwijdig met L. De verdeling of partitie van $\mathbb{R}^2$ wordt verkregen door $\mathbb{R}^2$ te schrijven als disjuncte vereniging van alle lijnen evenwijdig met L.



We kunnen een equivalentierelatie vaak gebruiken om nieuwe wiskundige objecten te definiëren. We geven een paar voorbeelden.

(2.9) Voorbeeld. We gaan uit van de verzameling $\mathbb{N} = \{1, 2, 3, \ldots\}$ van natuurlijke getallen en gaan nu de verzameling $\mathbb{Z}$ van de gehele getallen daaruit construeren. Beschouw de verzameling $V = \mathbb{N} \times \mathbb{N}$ van geordende paren natuurlijke getallen. We definiëren een equivalentie $\sim$ op V door:

$$(a, b) \sim (c, d) \quad \text{dan en slechts dan als} \quad a + d = c + b.$$

Het is niet moeilijk na te gaan dat dit een equivalentierelatie is. In het bijzonder is (a,b) equivalent met $(a+x, b+x)$ voor iedere $x \in \mathbb{N}$. Denk gewoon aan de klasse van (a,b) als het verschil $a-b$. We noteren het paar (a,b) ook wel met $a-b$. We noteren de verzameling van equivalentieklassen voor het moment even met $\mathbb{G}$. We kennen $\mathbb{G}$ al: het zijn de gehele getallen.

We kunnen nu een afbeelding maken $\mathbb{N} \to \mathbb{G}$ via $n \mapsto \overline{(n+1,1)}$. We kunnen dit uitbreiden tot een bijectie $\mathbb{Z} \to \mathbb{G}$ via $n \mapsto \overline{(n+x,x)}$ waarbij $x = x_n > 0$ zo gekozen is dat $n + x > 0$.

(2.10) Voorbeeld. In het tweede voorbeeld construeren we de rationale getallen ('breuken') uit de gehele getallen. Beschouw de verzameling $V = \{(a,b) \in \mathbb{Z}\times\mathbb{Z} : b \neq 0\}$ van paren gehele getallen met $b \neq 0$. We definiëren een equivalentie $\sim$ op V door:

$$(a,b) \sim (c,d) \quad \text{dan en slechts dan als} \quad ad = bc.$$

Het is niet moeilijk na te gaan dat dit een equivalentierelatie is. We controleren de transitiviteit. Als $(a,b) \sim (c,d)$ en $(c,d) \sim (e,f)$ dan geldt $ad = bc$ en $cf = de$. Dit betekent dat $adcf = bcde$. Als $c = 0$, dan volgt $a = 0$ en $e = 0$ en geldt $af = be$. Als $cd = dc \neq 0$ volgt ook $af = be$ dus $(a,b) \sim (e,f)$.

In het bijzonder is (a,b) equivalent met (ax, bx) voor iedere $x \in \mathbb{Z}$, $x \neq 0$. Denk gewoon aan de klasse van (a,b) als het quotiënt a/b. We noteren de equivalentieklasse van (a,b) ook als a/b. Er geldt dus

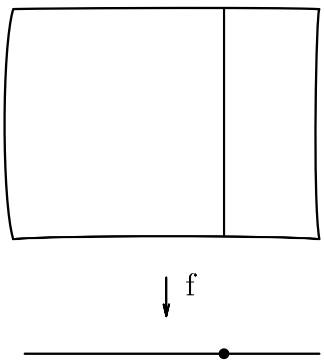
$$a/b = c/d \iff ad = bc.$$

De verzameling equivalentieklassen kan geïdentificeerd worden met de verzameling $\mathbb{Q}$ van breuken. Iedere equivalentieklasse van een paar (a,b) met $a \neq 0$ bevat precies één paar (a',b') waarbij $\mathrm{ggd}(a',b') = 1$ en $b' > 0$.

Een ander voorbeeld van een equivalentierelatie komt van een afbeelding $f : X \longrightarrow Y$. Laat X, Y twee verzamelingen zijn en laat $f : X \longrightarrow Y$ een afbeelding zijn. We definiëren een equivalentierelatie op X via

$$x \sim y \quad \text{dan en slechts dan als} \quad f(x) = f(y).$$

Dit is een equivalentierelatie. Een equivalentieklasse heet een *vezel* van de afbeelding f.



(2.11) Voorbeeld. i) Laat $f : \mathbb{C} \to \mathbb{C}$ de afbeelding $f(z) = z^n$ zijn. De vezels van f zijn van de vorm $\{x, \zeta x, \zeta^2, x, \ldots, \zeta^{n-1}x\}$ met $\zeta = e^{2\pi i/n}$ een n-de machts eenheidswortel.

ii) Laat $f : \mathbb{C} \to \mathbb{R}_{\geq 0}$ de afbeelding zijn met $f(z) = |z|$. De vezels zijn de cirkels met middelpunt $0 \in \mathbb{C}$, vgl. voorbeeld (2.3).

Vaak is het handig om uit iedere equivalentieklasse één element te kiezen waarmee we dan werken. Welk element dit is, doet dan meestal niet terzake. Bijvoorbeeld zouden we uit de verzameling equivalentieklassen $\mathbb{Z}/5\mathbb{Z}$ van de relatie $a \equiv b(\mathrm{mod} 5)$ de elementen $0, 1, 2, 3, 4$ kunnen kiezen.

(2.12) Definitie. Laat R een equivalentierelatie op de verzameling V zijn. Een *volledig representanten-systeem* voor R (ook wel volledig stelsel van representanten) is een deelverzameling W van V die uit iedere equivalentieklasse precies één element bevat.

(2.13) Voorbeelden. De verzameling $\{0, 1, 2, 3, 4\}$ is een volledig representantensysteem voor de equivalentierelatie $a \equiv b(\mathrm{mod} 5)$ op de gehele getallen $\mathbb{Z}$. De verzameling $\{15, 26, -8, 18, 104\}$ is dat ook. Een lijn die niet evenwijdig is aan L in Voorbeeld (2.8) snijdt iedere lijn evenwijdig aan L in één punt en vormt dus zo een volledig representantensysteem voor de equivalentierelatie in (2.8). Geef zelf een volledig representantensysteem voor het voorbeeld van (2.3).

Opgaven

1) Een *relatie* op een verzameling V is een deelverzameling van de verzameling $V \times V$. Geef een voorbeeld van een relatie de reflexief en symmetrisch is, maar niet transitief. Geef een voorbeeld van de relatie die symmetrisch en transitief is, maar niet reflexief.

2) Is de volgende relatie op de reële getallen $\mathbb{R}$ een equivalentierelatie? $x \sim y \iff xy \geq 0$

3) Bewijs dat een partitie van V aanleiding geeft tot een equivalentierelatie. Concludeer dat equivalentierelaties en partities gelijkwaardige begrippen zijn.

4) Laat F de verzameling van reëelwaardige differentieerbare functies van een reële variabele zijn:

$$F = \{f : \mathbb{R} \to \mathbb{R} : f \quad \text{differentieerbaar}\}.$$

Definiëer een relatie: $f \sim g \iff f' = g'$, waarbij f', g' de afgeleide aangeeft. Ga na dat dit een equivalentierelatie is en bepaal de equivalentieklassen.

5) Geef een volledig representantensysteem voor de equivalentierelatie van voorbeeld (2.11).

6) Bewijs de volgende beweringen over getallen $n \in \mathbb{N}$ in het tientallig stelsel. i) n is deelbaar door 3 dan en slechts dan als de som van de cijfers van n deelbaar is door 3; ii) n is deelbaar door 9 dan en slechts dan als de som van de cijfers van n deelbaar is door 9; iii) n is deelbaar door 11 dan en slechts dan als de alternerende som van de cijfers deelbaar is door 11.

7) Bewijs dat $a \sim b \iff a - b \in \mathbb{Z}$ een equivalentierelatie op de verzameling van reële getallen $\mathbb{R}$ definieert. Geef een volledig stelsel representanten aan.

8) Geldt het Principe (1.1) ook voor de verzameling $\mathbb{Q}$ van de rationale getallen?

9) Laat zien dat voor $a, b \in \mathbb{Z}$ geldt $(a + b)^p \equiv a^p + b^p(\mathrm{mod} p)$ voor ieder priemgetal p.

10) Laat $n, x \in \mathbb{N}$ met $1 < x < n$. Bewijs dat n geschreven kan worden als

$$n = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$$

voor een zekere k en gehele getallen a_i met $0 \leq a_i < x$ en dat k en de a_i éénduidig door n en x bepaald zijn.

11) Laat zien dat als $a, b \in \mathbb{Z}$ dan $(a-b)|a^n - b^n$. Laat verder zien dat $a+b$ het getal $a^n + b^n$ deelt als n oneven is.

3. Groepen

Après cela, il y aura, j'espère, des gens qui trouveront
leur profit à dechiffrer tout ce gâchis
É. Galois

Een centraal begrip in de algebra is het begrip "groep". Het begrip komt voor het eerst voor een in artikel van Galois* uit 1831, maar het heeft vrij lang geduurd voordat dit begrip gemeengoed onder wiskundigen was geworden.

We vallen maar met de deur in huis en geven de definitie en een aantal voorbeelden.

Een *bewerking* op een verzameling G is een afbeelding

$$G \times G \longrightarrow G \qquad (x, y) \mapsto x \circ y$$

ofwel, een voorschrift dat aan ieder geordend paar elementen x, y een element van G toevoegt. We hebben dit element hier met $x \circ y$ genoteerd. Vaak noemen we $x \circ y$ het *product*.

(3.1) Definitie. Een *groep* is een verzameling G voorzien van een bewerking

$$\circ : G \times G \to G$$

en van een element $e \in G$, zodat aan de volgende eisen is voldaan:

(G1) *Associativiteit* Voor iedere $x, y, z \in G$ geldt

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

(G2) *Eenheidselement* Voor iedere $x \in G$ geldt

$$x \circ e = e \circ x = x.$$

(G3) *Inverse* Voor iedere $x \in G$ is er een element $x^* \in G$ zodat

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

In plaats van $x \circ y$ worden vaak andere symbolen gebruikt, zoals $x * y$, $x + y$ of $x \cdot y$, of we laten het tussensymbool geheel weg en schrijven gemakshalve kortweg xy.

Vanwege de associatieve eigenschap G1 zijn de twee uitdrukkingen $x \circ (y \circ z) = (x \circ y) \circ z$ gelijk voor alle $x, y, z \in G$. Dat maakt het mogelijk de haakjes weg te laten en eenvoudigweg $x \circ y \circ z$ voor $x \circ (y \circ z) = (x \circ y) \circ z$ te schrijven, of nog eenvoudiger xyz. We kunnen dit ook uitbreiden naar producten van meer dan drie elementen.

Het element x^* bepaald door axioma G3 heet de *inverse* van x en wordt meestal genoteerd met x^{-1}. Dit element is eenduidig bepaald: laat x' een ander element zijn dat voldoet aan $x \circ x' = x' \circ x = e$. Dan vinden we

$$x^* \overset{(G2)}{=} e \circ x^* \overset{(G3)}{=} (x' \circ x) \circ x^* \overset{(G1)}{=} x' \circ (x \circ x^*) \overset{(G3)}{=} x' \circ e \overset{(G2)}{=} x'.$$

dus $x^* = x'$. Dit rechtvaardigt de naam *de inverse* van x voor x^*.

---

* Évariste Galois, Frans wiskundige, 1811–1832

Een groep wordt gegeven door een drietal $(G, \circ, e)$. Wanneer het duidelijk is wat de bewerking en het eenheidselement op de verzameling G zijn, spreken we vaak van de groep G zonder expliciet $\circ$ en e te noemen.

Voordat we nu voorbeelden geven nog wat notatie. Voor een natuurlijk getal n noteren we

$$g^n = \underbrace{g \circ g \circ \ldots \circ g}_{n \text{ keer}}$$

Verder stellen we nog $g^0 = e$. Het n-voudig product $g^{-1} \circ \ldots \circ g^{-1}$ wordt genoteerd met g^{-n}. Dan geldt voor alle $g \in G$ en alle $n, m \in \mathbb{Z}$ de identiteit

$$g^m \circ g^n = g^{m+n}.$$

Verder zal het handig blijken om het *lege product* (met nul factoren) gelijk te stellen aan het eenheidselement e. Een product $g_1 g_2 \ldots g_n$ wordt ook wel als $\prod_{i=1}^n g_i$ geschreven. Hierbij is de volgorde van groot belang. In het algemeen zal *niet* gelden dat $x \circ y = y \circ x$. Wanneer dit wel geldt hebben we te maken met speciale groepen.

(3.2) Definitie Een groep G heet *commutatief* of *abels*** als in G het volgende axioma geldt:

(G4) *Commutativiteit* $x \circ y = y \circ x$ voor alle $x, y \in G$.

Voor commutatieve groepen wordt in plaats een 'multiplicatieve notatie' vaak een additieve notatie gebruikt. In plaats van xy schrijven we dan $x + y$; in plaats van x^{-1} schrijven we $-x$ en voor het eenheidselement schrijven we 0.

(3.3) Voorbeeld. *De additieve groep* $\mathbb{Z}$.

De gehele getallen vormen een groep met als bewerking $+$ en met 0 als eenheidselement e. Het is welbekend dat aan de axioma's G1, G2 en G3 voldaan is. De inverse van een element n is $-n$. Deze groep is commutatief. De deelverzameling $\mathbb{N} \subset \mathbb{Z}$ vormt niet een groep onder de optelling, omdat de inverse niet bestaat.

(3.4) Voorbeeld. *De additieve groepen* $\mathbb{Q}$ en $\mathbb{R}$.

Ook voor de rationale getallen en de reële getallen met bewerking de optelling $(+)$ en eenheidselement 0 gaat men gemakkelijk na dat de axioma's G1, G2 en G3 gelden. Verder geldt ook weer G4: deze groepen zijn commutatief.

(3.5) Voorbeeld. *De multiplicatieve groepen* $\mathbb{Q}^*$ *en* $\mathbb{R}^*$

Laat

$$\mathbb{Q}^* := \{x \in \mathbb{Q} : x \neq 0\} = \mathbb{Q} - \{0\},$$

de verzameling van de rationale getallen ongelijk nul zijn. Onder de gebruikelijke vermenigvuldiging van rationale getallen is het product van twee rationale getallen $\neq 0$ weer een rationaal getal $\neq 0$. Het element $e = 1$ voldoet aan G2 en ieder rationaal getal $a/b \neq 0$ heeft als inverse b/a. Dus $\mathbb{Q}^*$ wordt zo een groep. Deze groep is commutatief. Omdat $0 \cdot x = 0$ voor elk rationaal getal x kan 0 geen multiplicatieve inverse hebben; daarom moeten we 0 verwijderen om met deze bewerking een groep te kunnen definiëren.

** naar Niels Henrik Abel, Noors wiskundige, 1802–1829

Op een dergelijke manier kunnen we ook van de verzameling

$$\mathbb{R}^* := \{x \in \mathbb{R} : x \neq 0\} = \mathbb{R} - \{0\},$$

van reëele getallen ongelijk nul een groep maken. Weer is 1 het eenheidselement en voor ieder reëel getal $x \neq 0$ is er een inverse $x^{-1} \neq 0$ met $xx^{-1} = 1 = x^{-1}x$. Ook $\mathbb{R}^*$ is een commutatieve groep.

(3.6) Voorbeeld. *De additieve groep van de complexe getallen* $\mathbb{C}$. De verzameling $\mathbb{C}$ van de complexe getallen bestaat uit alle uitdrukkingen van de vorm $a + b\,i$ met $a, b \in \mathbb{R}$ en waarbij i een symbool is. Voor $a + 0\,i$ schrijven we vaak a. We definiëren een optelling $+$ van complexe getallen als volgt: als $z = a + b\,i$ en $z' = c + d\,i$ dan definiëren we

$$z + z' = (a + c) + (b + d)i$$

Hier wordt de gewone optelling van reële getallen gebruikt. Men gaat nu snel na dat uit de eigenschappen G1, G2 en G3 van $\mathbb{R}$ deze eigenschappen voor $\mathbb{C}$ volgen. Ook G4 volgt. Dus $\mathbb{C}$ is een commutatieve groep met als eenheidselement $0 = 0 + 0\,i$.

(3.7) Voorbeeld *De multiplicatieve groep van complexe getallen* $\mathbb{C}^*$.
Op $\mathbb{C}$ kunnen we ook een vermenigvuldiging definiëren:

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

In het bijzonder volgt $i^2 = -1$. Maar het is voldoende $i^2 = -1$ als uitgangspunt te nemen en verder het product uit te rekenen door $(a+bi)(c+di)$ gewoon te ontwikkelen (haakjes wegwerken). Men ziet snel dat $1 \in \mathbb{C}$ de eigenschap heeft dat $1 \cdot (a + bi) = (a + bi) \cdot 1 = a + bi$. We definiëren

$$\mathbb{C}^* = \mathbb{C} - \{0\}.$$

We beweren nu dat $\mathbb{C}^*$ een groep wordt met de vermenigvuldiging als bewerking en 1 als eenheidselement. We moeten daarvoor G1, de associativiteit, verifiëren. Dit is wat bewerkelijk, maar gaat rechttoe rechtaan:

$$\begin{aligned}
((a + bi)(c + di))(e + fi) &= ((ac - bd) + (ad + bc)i)(e + fi) \\
&= ((ac - bd)e - (ad + bc)f) + ((ac - bd)f + (ad + bc)e)i \\
&= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i; \\
(a + bi)((c + di)(e + fi)) &= (a + bi)((ce - df) + (cf + de)i) \\
&= ((a(ce - df) - b(cf + de)) + (a(cf + de) + (b(ce - fd))i \\
&= (ace - adf - bcf - bde) + (acf + ade + bce - bfd)i,
\end{aligned}$$

waaruit volgt dat in $\mathbb{C}^*$ axioma G1 geldt. Ook geldt G4. Om in te zien dat er ook voor ieder $z \in \mathbb{C}^*$ een inverse bestaat gebruiken we de identiteit

$$(a + bi)(a - bi) = a^2 + b^2.$$

Verder geldt

$$a + b\,i = 0 \quad \text{dan en slechts dan als} \quad a^2 + b^2 = 0.$$

Dus

$$(a+bi)(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}\,i)=1=(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}\,i)(a+bi)$$

en we zien dat $a+b\,i\in\mathbb{C}^*$ een inverse heeft.

(3.8) Voorbeeld. *De Viergroep V_4 van Klein*.*

De Viergroep V_4 van Klein bestaat uit vier elementen $V_4=\{e,a,b,c\}$. De vermenigvuldiging wordt gegeven door de volgende tabel (het product xy is het element uit rij x maal het element uit kolom 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

Het eenheidselement is e. Merk op dat $a^2=b^2=c^2=e$, dus ieder element is zijn eigen inverse. De verificatie van het axioma G1 van de associativiteit van de bewerking kan met dit diagram gedaan worden; het vergt enig werk, maar het aantal gevallen dat men moet onderscheiden valt mee als men de symmetrie van het diagram gebruikt.

(3.9) Voorbeeld *De groep $\mathbb{Z}/n\mathbb{Z}$ van restklassen modulo n*

Laat $n\in\mathbb{Z}$. In Hoofdstuk 2 hebben we op $\mathbb{Z}$ de equivalentierelatie

$$a\equiv b(\mathrm{mod} n)\quad\text{dan en slechts dan als}\quad n|(a-b)$$

ingevoerd. Een equivalentieklasse heet een restklasse modulo n en is van de vorm

$$\overline{k}=\{a\in\mathbb{Z}:\text{de rest van }a\text{ bij deling door }n\text{ is }k\ \}\qquad\text{met }0\le k<|n|$$

en we vinden zo een verdeling

$$\mathbb{Z}=\overline{0}\sqcup\overline{1}\sqcup\ldots\sqcup\overline{|n-1|}.$$

Beschouw nu de verzameling $\mathbb{Z}/n\mathbb{Z}$ bestaande uit deze $|n|$ restklassen:

$$\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}.$$

We gaan nu van deze $|n|$ restklassen een groep van $|n|$ elementen maken door de volgende optelling

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

We moeten nagaan dat deze definitie in orde is, d.w.z. dat de definitie niet van de keuze van a en b afhangt, maar alleen van de *klassen* $\overline{a}$ en $\overline{b}$. Als a_1 en b_1 zo zijn dat $\overline{a}=\overline{a_1}$ en $\overline{b}=\overline{b_1}$ dan moeten we inzien dat $\overline{a+b}=\overline{a_1+b_1}$. Maar n deelt $a-a_1$ en $b-b_1$, dus n deelt ook $(a+b)-(a_1+b_1)$, m.a.w. $\overline{a+b}=\overline{a_1+b_1}$.

De bewerking is associatief omdat de bewerking $+$ in $\mathbb{Z}$ associatief is:

$$(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+(\overline{b}+\overline{c}).$$

* Felix Klein, Duits wiskundige, 1849–1925

Het eenheidselement is $\overline{0}$ omdat

$$\overline{0}+\overline{a}=\overline{0+a}=\overline{a}=\overline{a+0}=\overline{a}+\overline{0}.$$

De inverse van een element $\overline{a}$ is $\overline{-a}$:

$$\overline{-a}+\overline{a}=\overline{(-a)+a}=\overline{0}=\overline{a+(-a)}=\overline{a}+\overline{-a}.$$

Dus we concluderen dat $\mathbb{Z}/n\mathbb{Z}$ een groep is met deze optelling. Het is een commutatieve groep.

(3.10) Voorbeeld. *De multiplicatieve groep* $(\mathbb{Z}/n\mathbb{Z})^*$ *van restklassen modulo* n.
Neem een geheel getal $n \neq 0$ en definieer

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \operatorname{ggd}(a,n)=1\}.$$

Als $\overline{a_1}=\overline{a}$ dan $a-a_1=kn$ voor een zekere $k \in \mathbb{Z}$. Maar dan

$$\operatorname{ggd}(a,n)=\operatorname{ggd}(a_1+kn,n)=\operatorname{ggd}(a_1,n)$$

wegens (1.5). Omdat de $\operatorname{ggd}(a,n)$ niet van de speciale keus van a afhangt is de verzameling $(\mathbb{Z}/n\mathbb{Z})^*$ goed gedefinieerd.

We voorzien deze verzameling nu van een bewerking:

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

Omdat ook deze definitie a priori weer afhangt van de keus van de representanten a en b moeten we nagaan dat dit goed gedefinieerd is. Laat daarom a_1 en b_1 andere representanten zijn zodat $a-a_1$ en $b-b_1$ deelbaar zijn door n, zeg $a-a_1=kn$, $b-b_1=\ell n$. Dan vinden we

$$a\cdot b=(a_1+kn)\cdot(b_1+\ell n)=a_1b_1+(a\ell+kb+kln)\cdot n.$$

Dus het verschil $ab-a_1b_1$ is deelbaar door n, m.a.w. $\overline{ab}=\overline{a_1b_1}$. Dus de vermenigvuldiging is goed gedefinieerd.

De associativiteit van deze bewerking wordt, analoog aan die van de optelling, op de associativiteit van de vermenigvulding op $\mathbb{Z}$ teruggevoerd. Het eenheidselement is $\overline{1}$. We moeten nu nog nagaan dat ieder element een inverse heeft voor deze bewerking. Laat $\overline{a}$ zo een element zijn. Dan weten we dat $\operatorname{ggd}(a,n)=1$. Dus volgens (1.6) zijn er $x,y\in\mathbb{Z}$ zodat

$$ax+ny=1.$$

Dus $\overline{ax}=\overline{1}$ en omdat $\overline{ax}=\overline{a}\cdot\overline{x}=\overline{x}\cdot\overline{a}$ zien we dat $\overline{x}$ de gevraagde inverse is. Dus we concluderen dat $(\mathbb{Z}/n\mathbb{Z})^*$ een groep is.

(3.11) Definitie. De Euler* ϕ-functie $\phi(n)$ wordt voor $n\in\mathbb{Z}, n\neq 0$ gedefinieerd door

$$\phi(n)=\#(\mathbb{Z}/n\mathbb{Z})^*.$$

---

* L. Euler, 1707–1783, wiskundige afkomstig uit Basel die in St. Petersburg en in Berlijn gewerkt heeft

Expliciet:

$$\phi(n) = \#\{k \in \{1,2,\ldots,n\} : \mathrm{ggd}(k,n) = 1\}.$$

Dus geldt bijvoorbeeld $\phi(1) = 1$, $\phi(11) = 10$, $\phi(21) = 12$, $\phi(101) = 100$, $\phi(1001) = 720$.

Laten we in het speciale geval dat $n = 12$ kijken wat voor groep we aantreffen: $(\mathbb{Z}/12\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ met de volgende vermenigvuldigingstabel:

	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

We zien dat dit 'dezelfde' vermenigvuldigingstabel is als voor de Viergroep van Klein door $e = \overline{1}, a = \overline{5}, b = \overline{7}, c = \overline{11}$ te stellen. Omdat de bewerking op $(\mathbb{Z}/12\mathbb{Z})^*$ commutatief is volgt dat ook nog eens voor de bewerking van de viergroep van Klein.

We geven nu een voorbeeld van een niet-commutatieve groep.

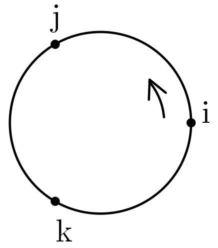
(3.12) Voorbeeld. *De quaterniongroep Q van orde* 8.*

Beschouw de verzameling $Q = \{1, -1, i, -i, j, -j, k, -k\}$ van 8 elementen. We definiëren de vermenigvuldiging door $1 \cdot x = x$ en $-1 \cdot x = -x$ en $-1 \cdot -x = x$ voor $x = 1, i, j, k$ en

$$i^2 = j^2 = k^2 = -1$$
$$ij = k, \quad jk = i \quad ki = j$$
$$ji = -k, \quad kj = -i, \quad ik = -j.$$

Het eenheidselement is 1. We laten de verificatie van G1, G2 en G3 aan de lezer over. Dit is een groep, maar ten duidelijkste een niet-commutatieve groep.

De rekenregel laat zich gemakkelijk onthouden door de elementen i, j, k bij een cirkel te zetten.



Vermenigvuldiging van twee met de richting mee levert het derde element; tegen de richting in levert het min dat element.

(3.13) Voorbeeld. *De vectorruimten $\mathbb{R}^n$ en $\mathbb{C}^n$.*

---

* De quaternionen zijn ontdekt (uitgevonden) door William Rowan Hamilton op 16 oktober 1843.

Reële en complexe vectorruimten leveren voorbeelden van (additief geschreven) commutatieve groepen. Neem bijvoorbeeld de vectorruimte $\mathbb{R}^n$. Twee kolomvectoren $\mathbf{v}$ en $\mathbf{w}$ worden coordinaatsgewijs bij elkaar opgeteld:

$$\mathbf{v}+\mathbf{w} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1+w_1 \\ \vdots \\ v_n+w_n \end{pmatrix}.$$

Idem dito voor complexe vectorruimten als $\mathbb{C}^n$.

(3.14) Voorbeeld. *De algemene lineaire groep* $\mathrm{GL}_2(\mathbb{R})$ *van reële* 2×2*-matrices.* Beschouw de verzameling van reële 2×2-matrices

$$\mathrm{GL}_2(\mathbb{R}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R}, ad-bc \neq 0\}.$$

De uitdrukking $ad-bc$ heet de *determinant* van de matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, en wordt genoteerd met $\det(M)$. De vermenigvuldiging wordt gedefinieerd door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

Men gaat na dat $\det(M)\det(N) = \det(M\cdot N)$, waaruit volgt dat het product weer een element van $\mathrm{GL}_2(\mathbb{R})$ is. Met enig rekenwerk laat men ook zien dat deze bewerking op 2×2-matrices associatief is. Het eenheidselement is de matrix

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

Verder heeft iedere matrix met determinant $ad-bc \neq 0$ een inverse, namelijk

$$\begin{pmatrix} d/(ad-bc) & -b/(ad-bc) \\ -c/(ad-bc) & a/(ad-bc) \end{pmatrix}.$$

Daarmee wordt de verzameling $\mathrm{GL}_2(\mathbb{R})$ een groep, de algemene lineaire groep (Eng.: **g**eneral **l**inear group). Deze groep is niet commutatief! Zo laat bijvoorbeeld de berekening

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

zien dat deze matrices niet commuteren als $a+c \neq a$.

(3.15) Definitie. Laat G_1 en G_2 groepen zijn. Laat $G_1\times G_2$ de verzameling van paren (x_1,x_2) zijn met $x_1\in G_1$ en $x_2 \in G_2$. We definiëren nu de bewerking $(x_1,x_2)\circ(y_1,y_2) = (x_1y_1, x_2y_2)$, waarbij in de eerste factor het product in G_1 en in de tweede factor het product in G_2 bedoeld wordt. Het wordt aan de lezer overgelaten te verifiëren dat aan de axioma's G1, G2 en G3 voldaan is. Op deze manier wordt $G_1 \times G_2$ een groep, het *directe product* van G_1 en G_2.

Zoals bovenstaande voorbeelden laten zien kan een groep G zowel eindig veel als oneindig veel elementen hebben. Het aantal elementen van de groep heet *de orde* van de groep. Notatie: $\#G$. De *triviale groep* is de groep die alleen uit het eenheidselement bestaat en heeft dus $\#G = 1$.

(3.16) Definitie. De *orde* van een element $a \in G$ is het kleinste positieve getal n waarvoor $a^n = e$ geldt. Is er niet zo een n, dan zeggen we dat de orde van a oneindig is.

(3.17) Voorbeelden. De elementen i, j en k van de quaterniongroep uit voorbeeld (3.12) zijn alledrie van orde 4. In de groep

$$\mathrm{SL}_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1\}$$

van geheeltallige 2×2-matrices met determinant 1 hebben de elementen

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

orde 4 en 6. Het element

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

heeft oneindige orde. Ga na dit zelf na! In de groep $\mathbb{Z}$ heeft het element 1 oneindige orde.

(3.18) Propositie. *Zij G een groep en $x \in G$ een element.*

i) Als de orde van x oneindig is dan zijn alle elementen in de rij $(x^k)_{k\in\mathbb{Z}}$ van machten van x verschillend.

ii) Als het element x eindige orde n heeft, dan zijn er precies n verschillende machten van x en er geldt $x^{n+m} = x^m$ voor alle $m \in \mathbb{Z}$.

Bewijs. Stel dat $x^i = x^j$ met $i > j$. Dan vinden we door vermenigvuldiging met x^{-j} dat $x^{i-j} = x^0 = e$, dus x heeft een eindige orde. Daaruit volgt i) en het feit dat als x eindige orde heeft de machten $x^0, x^1, \ldots, x^{n-1}$ allemaal verschillend zijn. Verder geldt voor alle $m \in \mathbb{Z}$ dat $x^{n+m} = x^n x^m = ex^m = x^m$ zoals verlangd.

(3.19) Propositie. *In een groep G is de vergelijking $ax = b$ bij gegeven $a, b \in G$ altijd oplosbaar en heeft precies één oplossing: $x = a^{-1}b$. Ook de vergelijking $xa = b$ is altijd oplosbaar en heeft precies één oplossing $x = ba^{-1}$.*

Bewijs. Door de vergelijking $ax = b$ van links met a^{-1} te vermenigvuldigen vinden we $x = a^{-1}b$. Het element $x = a^{-1}b$ is een oplossing en is bovendien eenduidig bepaald.

(3.20) Gevolg. *Laat G een groep zijn en g een willekeurig element. Dan is de afbeelding $\lambda_g : G \to G$, $x \mapsto gx$ (linksvermenigvuldiging met g) een bijectie. Ook is de afbeelding $\rho_g : G \to G$, $x \mapsto xg$ (rechtsvermenigvuldiging met g) een bijectie.*

Ter afsluiting nog een opmerking over de inverse. De inverse van een product xy is

$$(xy)^{-1} = y^{-1}x^{-1}$$

(let op de volgorde) zoals door uitvermenigvuldigen direct te zien is. Als een element x orde twee heeft, dan is de inverse van x gelijk aan x.

Opgaven

1) Laat zien dat $\{+1, -1\} \subset \mathbb{R}^*$ een abelse groep vormt onder de vermenigvuldiging.

2) Wat is het eenheidselement van het directe product $G_1 \times G_2$ (Voorbeeld (3.15)) ? En wat is de inverse van $(x_1, x_2) \in G_1 \times G_2$?

3) Ga na dat de verzameling van 3×3-matrices

$$\{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R}\}$$

een groep vormen onder matrixvermenigvuldiging. Deze groep is een zogenaamde Heisenberg-groep*.

4) Als G_1 en G_2 eindige groepen zijn van orde m en n, wat is dan de orde van $G_1 \times G_2$?

5) Laat zien dat in een abelse groep G voor alle $x, y \in G$ geldt: $(xy)^n = x^n y^n$. Laat met een tegenvoorbeeld zien dat dit niet altijd juist is voor niet-abelse groepen.

6) Laat $x_1, \ldots, x_n \in G$ elementen van een groep G zijn. Bewijs:

$$(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}.$$

7) Bewijs: een groep G is abels dan en slechts dan als $(xy)^{-1} = x^{-1}y^{-1}$ voor alle $x, y \in G$.

8) Bewijs dat $(x^{-1})^{-1} = x$ voor alle elementen x van een groep G.

9) Zij G een eindige abelse groep en $\gamma \in G$ een element. Bewijs dat $\prod_{g \in G} g = \prod_{g \in G} \gamma\, g$. Bewijs hiermee dat de orde van γ de orde van G deelt. (Pas dit toe op $(\mathbb{Z}/p\mathbb{Z})^*$ met p priem en concludeer $a^{p-1} \equiv 1 (\operatorname{mod} p)$ als $\operatorname{ggd}(a, p) = 1$.)

10) Bewijs de formule

$$\phi(n) = n \prod_p (1 - \frac{1}{p}),$$

waarbij het product over de priemdelers van n wordt genomen.

11) Bewijs dat in een groep G een identiteit $xy = xz$ impliceert dat $y = z$.

* W. Heisenberg, Duits natuurkundige, 1901–1976

12) Laat G een groep zijn en x, g elementen van G. Bewijs dat de orde van gxg^{-1} gelijk is aan de orde van x.

13) Laat G een groep zijn en $x, y \in G$ elementen van orde 2. Bewijs dat $xyxyxyx$ orde 2 heeft.

14) Bewijs dat de orde van een element x in een groep gelijk is aan de orde van zijn inverse.

15) Laat G een groep zijn en g een element van eindige orde, zeg n. Bewijs dat voor alle $r \in \mathbb{Z}$ geldt: $\text{orde}(g^r) = n/\text{ggd}(n, r)$.

16) Doe voor alle groepen in de onderstaande lijst het volgende. Maak een lijst van alle elementen en geef voor elk element de inverse en de orde.

i) $G = \mathbb{Z}/11\mathbb{Z}$;
ii) $G = \mathbb{Z}/12\mathbb{Z}$;
iii) $G = (\mathbb{Z}/11\mathbb{Z})^*$;
iv) $G = (\mathbb{Z}/12\mathbb{Z})^*$;
v) $G = Q$, de quaterniongroep als in (3.12).

17) Geef een voorbeeld van een groep G waarin de vergelijking $x^n = e$ met $n \geq 2$ meer dan n oplossingen heeft.

18) Laat G een groep zijn met een element x waarvoor geldt dat $xyx = y^3$ voor alle $y \in G$. Bewijs dat $x^2 = e$ en $y^8 = e$ voor alle $y \in G$.

4. SYMMETRIEGROEPEN

Beauty is bound up with symmetry
H. Weyl,*

In de voorbeelden van groepen van het vorige hoofdstuk lag de nadruk op getalsystemen als $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ en matrices. We zagen dat het begrip optreedt als unificerend begrip voor de vele voorbeelden. Maar het belang en ook de oorsprong van het begrip groep liggen elders: bij het begrip symmetrie. Vele groepen komen in de 'natuur' voor als groep van symmetrieën van een figuur of ander wiskundig object. Het begrip groep speelt een sleutelrol bij onderwerpen als kristallen, elementaire deeltjes, getallenlichamen, algebraïsche krommen en vele andere.

In zijn meest algemene vorm nemen we een willekeurige verzameling X en bekijken de verzameling van alle bijecties $f : X \to X$.

Als X_i voor $i = 1, 2, 3, 4$ verzamelingen zijn en f, g en h afbeeldingen daartussen

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

dan geldt de identiteit

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

voor de samenstellingen van deze afbeeldingen. Daaruit blijkt dat samenstelling van afbeelding aan de eigenschap G1 (associativiteit) voldoet. Nemen we nu $X_i = X$ en de afbeeldingen bijectief dan vinden we een voorbeeld van groep.

(4.1) Stelling. *Laat X een verzameling zijn. Dan is de verzameling $S(X)$ van bijecties $X \to X$ met als bewerking de samenstelling van afbeeldingen en als eenheidselement de identieke afbeelding een groep.*

Bewijs. De samenstelling van twee bijecties $X \to X$ is weer een bijectie. Verder geldt zoals we zojuist zagen de associatieve eigenschap. De identieke afbeelding $\mathrm{id}_X : X \to X, x \mapsto x$ fungeert als eenheidselement. De 'afbeelding terug' f^{-1}, de inverse van een bijectie $f \in S(X)$, voldoet aan de eigenschap $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$ en levert de inverse voor de bewerking.

Door voor X een eindige verzameling te nemen vinden we de zogenaamde *permutatiegroepen* die we nog uitgebreid zullen bestuderen. Als $X = \{1, 2, \ldots, n\}$ dan noteren we S_n voor $S(X)$. Deze groep heet de *symmetrische groep* op n symbolen.

We kunnen aan de bijecties f die we beschouwen nog allerlei beperkende eigenschappen opleggen die interessante voorbeelden van groepen leveren.

(4.2) Voorbeeld. *De orthogonale groep $O_2(\mathbb{R})$.*

Beschouw het platte vlak $\mathbb{R}^2$. Hierop hebben we een afstandsfunctie

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \qquad \text{voor} \quad x = (x_1, x_2),\ y = (y_1, y_2)$$

---

* Herman Weyl, Duits en later Amerikaans wiskundige, 1885–1955

Een *isometrie* van $\mathbb{R}^2$ is een afbeelding $f : \mathbb{R}^2 \to \mathbb{R}^2$ met de eigenschap dat $d(x,y) = d(f(x), f(y))$ voor alle $x, y \in \mathbb{R}^2$. Zo een isometrie is een bijectie. (Ga na.) Beschouw nu de verzameling van isometrieën die de oorsprong vastlaten:

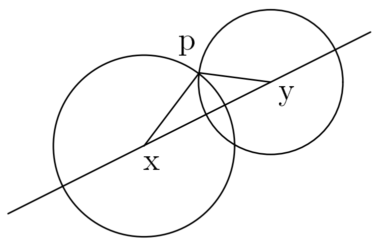
$$O_2(\mathbb{R}) = \{ f : f \text{ is een isometrie en } f((0,0)) = (0,0) \}.$$

De identitieke afbeelding $\mathrm{id}_{\mathbb{R}^2}$ is een element van $O_2(\mathbb{R})$. De samenstelling van twee elementen is weer een element van $O_2(\mathbb{R})$. Verder geldt zoals we in het bewijs van bovenstaande stelling zagen de associativiteit. De inverse f^{-1} van een element in $O_2(\mathbb{R})$ bewaart afstanden en laat de oorsprong vast. Daarmee is $O_2(\mathbb{R})$ een groep.

Voorbeelden van elementen in $O_2(\mathbb{R})$ zijn draaiingen r_α om de oorsprong over een hoek α. Verdere voorbeelden zijn spiegelingen s_ℓ in een lijn ℓ door de oorsprong. Ga na dat een spiegeling determinant -1 heeft. We noemen de elementen van $O_2(\mathbb{R})$ orthogonale afbeeldingen.

(4.3) Propositie. *Een isometrie die twee verschillende punten vastlaat is de identiteit of de spiegeling in de lijn door deze twee punten.*

Bewijs. Als een isometrie f twee punten x en y vastlaat dan moeten voor een willekeurig punt p de afstanden van p en van $f(p)$ tot x en y hetzelfde zijn. Dat betekent dat $f(p)$ ligt op de doorsnede van de cirkel C_1 met middelpunt x en straal $d(x,p)$ en de cirkel C_2 met middelpunt y en straal $d(y,p)$. Als p niet op de lijn $\ell = \overline{x\,y}$ door de middelpunten ligt dan hebben deze twee cirkels precies twee snijpunten: p en $s_\ell(p)$ (zie de figuur); als p op ℓ ligt is er één snijpunt. We concluderen dat $f(p) = p$ voor alle $p \in \ell$ en dat $f(p) = p$ of $f(p) = s_\ell(p)$ voor alle p. Als f nu ook een punt q buiten ℓ vastlaat, dan geldt voor een punt p buiten ℓ dat $d(p,q) = d(f(p), f(q)) = d(f(p), q)$, maar $d(p,q) \neq d(s_\ell(q), p)$, dus we kunnen niet $f(p) = s_\ell(p)$ hebben en dan is f de identiteit. Als f geen enkel punt buiten ℓ vastlaat dan moet $f(p) = s_\ell(p)$ gelden en f is de spiegeling in ℓ.



(4.4) Gevolg. *Een orthogonale afbeelding is een draaiing r_α om de oorsprong of een spiegeling s_ℓ in een lijn ℓ door de oorsprong.*

Bewijs. Laat $f \in O_2(\mathbb{R})$. Kies een punt $p \in \mathbb{R}^2$ met $p \neq (0,0)$. Omdat f afstanden bewaart moet $f(p)$ op de cirkel om de oorsprong met straal $d(p,0)$ liggen. Na samenstelling met een geschikte draaiing r_α voert $r_\alpha \circ f$ het punt p in zich over. De isometrie $r_\alpha \circ f$ laat twee punten vast: p en de oorsprong; dit is dus de identiteit of een spiegeling om de lijn ℓ door p en de oorsprong. Als het de identiteit is, dan is $f = r_{-\alpha}$ een draaiing. Als $r_\alpha \circ f$ een spiegeling s_ℓ is, dan voert f de lijn ℓ' die een hoek van $\alpha/2$ met ℓ maakt in zich over en geldt $f = s_{\ell'}$.

(4.5) Gevolg. *Een orthogonale afbeelding is een lineaire afbeelding. Als de determinant $+1$ is, dan is het een draaiing; is de determinant -1, dan is het een spiegeling.*

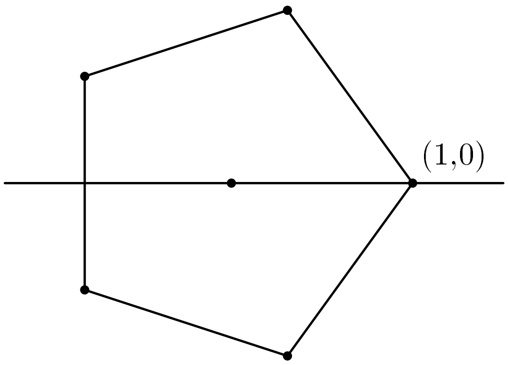
Voor verder gebruik merken we op dat voor iedere draaiing r en iedere spiegeling s in $O_2(\mathbb{R})$ geldt

$$rs = sr^{-1}. \tag{1}$$

Immers, de spiegeling rs heeft orde 2 en is dus gelijk aan zijn eigen inverse $(rs)^{-1} = rs$. Maar $(rs)^{-1} = s^{-1}r^{-1} = sr^{-1}$. Ieder element van $O_2(\mathbb{R})$ is ofwel van de vorm r_α of van de vorm $r_\alpha\sigma$ met $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. De rekenregels $\sigma^2 = 1$ en (1) beschrijven de vermenigvuldiging in $O_2(\mathbb{R})$ volledig.

(4.6) Voorbeeld. *De dihedrale groep D_n.*

Laat n een geheel getal ≥ 2 zijn. Beschouw de regelmatige n-hoek in $\mathbb{R}^2$ met centrum de oorsprong en een hoekpunt in $(1,0)$. Dus Δ_2 is het interval $[-1,1]$, Δ_3 is een gelijkzijdige driehoek, Δ_4 is een vierkant, enz.



Δ_5

We definiëren nu de *dihedrale* of *diëdergroep* van orde $2n$ als de symmetriegroep van deze figuur in de volgende zin

$$D_n = \{t \in O_2(\mathbb{R}) : t(\Delta_n) = \Delta_n\}.$$

Men gaat gemakkelijk na dat dit een groep is. Deze groep bevat de draaiing $r = r_\alpha$ met $\alpha = 2\pi/n$ en alle machten r^k hiervan. Merk op dat dit element r van orde n is. Daarnaast bevat D_n bepaalde spiegelingen in lijnen door de oorsprong. Allereerst zijn er de spiegelingen in een lijn door de oorsprong en een hoekpunt. Dit zijn er n voor n oneven en $n/2$ voor n even. Voor even n zijn er ook nog de $n/2$ spiegelingen in een lijn door de oorsprong en het midden van een zijde. In totaal zijn er dus n spiegelingen. Laat s de spiegeling in de x-as zijn. Dan kunnen we de $2n$ elementen van D_n schrijven als

$$D_n = \{r^k : k = 0, 1, \ldots, n-1\} \cup \{sr^k : k = 0, 1, \ldots, n-1\}.$$

We kunnen nu de relaties $s^2 = 1$ en (1) gebruiken om te rekenen in deze groep.

Gemakshalve definiëren we nog $D_1 = \{e, s\}$.

De beschouwing over symmetrieën van vlakke figuren kunnen gemakkelijk worden uitgebreid tot symmetrieën van ruimtelijke figuren. Laat $\mathbb{R}^3$ de drie-dimensionale Euclidische ruimte zijn met de gebruikelijke afstandsfunctie

$$d(x,y) = \sqrt{\sum_{i=1}^{3}(x_i - y_i)^2}.$$

Een *isometrie* is net als voor dimensie 2 een afstandsbewarende bijectie van $\mathbb{R}^3$ naar $\mathbb{R}^3$. Voor een deelverzameling F (voor 'figuur') van $\mathbb{R}^3$ kunnen we dan de verzameling van isometrieën beschouwen die F in zich voeren. Die vormen een groep, de *symmetriegroep* van de figuur F.

Net als in dimensie 2 hebben we een orthogonale groep:

$$O_3(\mathbb{R}) = \{f : \mathbb{R}^3 \to \mathbb{R}^3 : \ f \text{ is een isometrie en } \quad f((0,0,0) = (0,0,0)\}$$

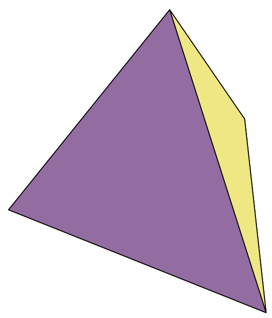
Omdat zo een f een orthogonale basis van $\mathbb{R}^3$ in een orthogonale basis overvoert is de matrix A die f representeert een *orthogonale matrix*. Dat kan uitgedrukt worden met de voorwaarde

$$A^t\, A = I$$

met A^t de getransponeerde matrix. Binnen de groep $O_3(\mathbb{R})$ vinden we de *rotaties*: dat zijn de elementen met determinant 1. Deze transformaties vormen de *speciale orthogonale groep*:

$$SO_3(\mathbb{R}) = \{A \in GL_3(\mathbb{R}) : A^t\, A = I, \det(A) = 1\}.$$

We vinden interessante voorbeelden van groepen door de symmetriegroepen van de regelmatige n-vlakken in $\mathbb{R}^3$ te bekijken. Deze regelmatige veelvlakken zijn: regelmatig viervlak of tetraeder, kubus, regelmatig achtvlak of octaeder, regelmatig twaalfvlak of dodecaeder en het regelmatige twintigvlak of icosaeder. Deze veelvlakken heten de Platonische veelvlakken en waren al aan de klassieke Grieken bekend.



tetraeder

Laat T een tetraeder zijn met hoekpunten a, b, c, d. Een symmetrie van T voert hoekpunten in hoekpunten over en geeft aanleiding tot een permutatie van de verzameling $\{a, b, c, d\}$ van hoekpunten. Zo een symmetrie is volledig bepaald door wat hij met de hoekpunten doet. (Ga na.) De spiegeling van $\mathbb{R}^3$ in het vlak dat door cd gaat en loodrecht staat op ab is een symmetrie van T en laat c en d vast, maar verwisselt a en b. De rotatie rond de lijn door d en het midden van de gelijkzijdige driehoek abc is ook een symmetrie van T. Het is niet moeilijk in te zien dat we zo alle permutaties van de verzameling $\{a, b, c, d\}$ kunnen krijgen. Zo zien we in dat de symmetriegroep van een tetraeder uit 24 elementen bestaat. We komen hier later nog uitgebreid op terug.

Opgaven

1) Laat zien dat de elementen van $O_2(\mathbb{R})$ ofwel in de gedaante

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

ofwel in de gedaante

$$r_\alpha s = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}.$$

te schrijven zijn.

2) Bewijs de volgende rekenregels in de diëdergroep D_n:

$$(r^i s^j)(r^k s^\ell) = \begin{cases} r^{i+k} s^\ell & \text{als } j = 0 \\ r^{i-k} s^{\ell+1} & \text{als } j = 1. \end{cases}$$

3) Beschouw de verzameling van afbeeldingen $\mathbb{R} \to \mathbb{R}$ van de vorm (affiene transformatie)

$$x \mapsto a\,x + b \qquad a \in \mathbb{R}^*, b \in \mathbb{R}.$$

Laat zien dat deze afbeeldingen onder samenstelling een groep vormen. Is deze groep commutatief?

4) Een translatie $t = t_a$ van $\mathbb{R}^2$ is een afbeelding van de vorm $t(x) = x + a$ voor vaste $a \in \mathbb{R}^2$ en alle $x \in \mathbb{R}^2$. Laat zien dat een isometrie eenduidig geschreven kan worden als product van een translatie t en een orthogonale afbeelding.

5) Bewijs dat de symmetriegroep van de kubus uit 48 elementen bestaat.

6) Markeer op een regelmatig viervlak de middens van de zijden. Verbind nu de middens van twee zijden met een lijnstuk als de twee zijden een gemeenschappelijke ribbe hebben, anders niet. Welke figuur ontstaat zo? Voer dit ook uit voor het regelmatig zes-, acht-, twaalf- en twintigvlak. Hoeveel symmetrieën heeft een regelmatig achtvlak?

7) Beschrijf de groep van symmetriën van de verzameling $\mathbb{Z} \subset \mathbb{R}$. Deze groep heet de *oneindige diëdergroep* D_∞.

5. Ondergroepen en homomorfismen

A mathematician, like a painter or a poet, is a maker of patterns
G.H. Hardy*

In de vele voorbeelden van groepen die we hebben gezien trad regelmatig het verschijnsel op dat bepaalde deelverzamelingen van een groep zelf weer een groep vormden, bijvoorbeeld $\mathbb{Z} \subset \mathbb{R}$. Dit leidt tot de volgende definitie.

(5.1) Definitie. Zij G een groep. Een deelverzameling H van G heet een *ondergroep van* G als H met de bewerking van G en hetzelfde eenheidselement als G een groep vormt.

We geven nu een eenvoudig kriterium waarmee men kan toetsen of een deelverzameling H van een groep G een ondergroep is.

(5.2) Stelling. *Laat G een groep zijn en H een deelverzameling van G. Dan zijn de volgende beweringen equivalent.*

i) H is een ondergroep van G.
ii) H is niet leeg en met ieder tweetal elementen $x, y \in H$ zitten ook xy en x^{-1} in H.
iii) H is niet leeg en met ieder tweetal elementen $x, y \in H$ zit ook xy^{-1} in H.

Bewijs. Als H een ondergroep van G is, dan is H niet leeg (want H bevat e) en met ieder tweetal elementen x, y moet ook het product xy en de inverse x^{-1} in H bevat zijn, dus ii) volgt. Ook de implicatie ii) $\Longrightarrow$ iii) is triviaal. Neem nu iii) aan. Dan bevat H tenminste één element, zeg x. Passen we nu iii) toe op x en $y = x$ dan volgt dat $e = x\,x^{-1}$ in H zit. Passen we iii) toe op e en x dan volgt dat ook $x^{-1} = e\,x^{-1}$ in H zit. Dus met ieder element zit de inverse van dat element ook in H. Met een tweetal elementen x en y van H zit dan ook y^{-1} en dus ook $xy = x(y^{-1})^{-1}$ in H. Dus de bewerking van G definieert een bewerking op H. Deze bewerking op H voldoet aan de associativiteit omdat daaraan op G voldaan is. Daarmee zijn de groepsaxiomas voor H gecontroleerd en volgt i). Dit beëindigt het bewijs.

(5.3) Voorbeelden.

i) $\mathbb{Z}$ is een ondergroep van $\mathbb{R}$; $\mathbb{Q}$ is een ondergroep van $\mathbb{R}$ en ook van $\mathbb{C}$ etc.
ii) De even getallen $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ vormen een ondergroep van $\mathbb{Z}$. De verzameling van de oneven getallen vormt geen ondergroep want 0 zit daar niet in.
iii) De positieve reële getallen $\mathbb{R}_{>0}$ vormen een ondergroep van de multiplicatieve groep $\mathbb{R}^*$.
iv) De verzameling $\{\pm 1, \pm i\}$ vormt een ondergroep van de quaterniongroep Q van orde 8.
v) $SO_2(\mathbb{R})$, de groep van de rotaties, is een ondergroep van $O_2(\mathbb{R})$.
vi) Laat S_n de groep van permutaties van $\{1, 2, \ldots, n\}$ zijn. Laat $k \in \{1, 2, \ldots, n\}$. De verzameling
$$H = \{\sigma \in S_n : \sigma(k) = k\}$$
is een ondergroep van S_n.

---

* G.H. Hardy, Engels wiskundige, 1877–1947

Laat nu $S \subset G$ een deelverzameling van een groep G zijn. In de regel zal S geen ondergroep zijn. We kunnen wel de 'kleinste' ondergroep van G die S bevat bekijken. Met ieder element x moet ook x^{-1} in deze ondergroep zitten en ook alle producten van elementen van S en hun inversen. Dit levert een groep:

(5.4) Lemma. *Laat S een deelverzameling van een groep G zijn. Dan vormt de verzameling $\langle S \rangle$ die bestaat uit alle eindige producten van elementen $x \in G$ met $x \in S$ of $x^{-1} \in S$ een ondergroep van G.*

Bewijs. Het lege product is gelijk aan e en dus is $\langle S \rangle$ niet leeg. Als g, h twee elementen van G zijn die als product van elementen $x \in G$ met $x \in S$ of $x^{-1} \in S$ geschreven kunnen worden, dan kan het product gh ook zo geschreven worden. Verder kan ook de inverse zo geschreven worden (vgl. Opgave (3.6)). Dus $\langle S \rangle$ is een ondergroep

De ondergroep $\langle S \rangle$ heet de *ondergroep voortgebracht door S*. De elementen van S heten *voortbrengers* van $\langle S \rangle$. Een groep met eindig veel voortbrengers heet een *eindig voortgebrachte groep.*

Als een groep door één element wordt voortgebracht dan heet G een *cyclische groep.* Een cyclische groep $\langle x \rangle$ bestaat dus uit de machten (positieve en negatieve) van een element x. Als dat element eindige orde heeft, zeg n, dan zijn dat er n. Zo niet dan is G een oneindige groep. Bijvoorbeeld geldt voor $S = \{1\} \subset \mathbb{Z}$ dat $\langle 1 \rangle = \mathbb{Z}$.

Ter illustratie bepalen we nu eerst de ondergroepen van $\mathbb{Z}$ en van $\mathbb{Z}/n\mathbb{Z}$.

(5.5) Stelling. *i) De ondergroepen van $\mathbb{Z}$ zijn $\{0\}$ en de cyclische groepen*

$$d\,\mathbb{Z} = \{\ldots, -2d, -d, 0, d, 2d, \ldots\}$$

met d een positief geheel getal. ii) De ondergroepen van $\mathbb{Z}/n\mathbb{Z}$ zijn de cyclische groepen $\langle\, \bar{d} \,\rangle$ met d een positieve deler van n.

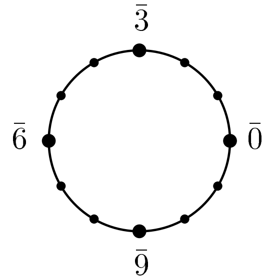
Bewijs. Laat H een ondergroep van $\mathbb{Z}$ zijn. Dan zit 0 in H. Als H verder geen elementen bevat dan $H = \{0\}$. Is dit niet zo, dan bevat H een element $x \neq 0$ en dus ook $-x \in H$. Dus H bevat positieve getallen. Zij d het kleinste positieve getal dat bevat is in H. Dan is ook $d\mathbb{Z}$ bevat in H.

We gaan nu na dat ieder element x van H een veelvoud van d is. Deel x door d: laat $x = qd + r$ met $0 \leq r < d$. Omdat H een groep is moet ook het verschil $x - qd = r$ bevat zijn in H. Omdat $0 \leq r < d$ en d het kleinste positieve getal in H is volgt $r = 0$. Daarmee volgt $H = d\mathbb{Z}$. Merk op dat al deze ondergroepen $d\mathbb{Z}$ verschillend zijn want d is het kleinste positieve element van $d\mathbb{Z}$. Daarmee is deel i) van de stelling bewezen.

ii) Laat nu H een ondergroep van $\mathbb{Z}/n\mathbb{Z}$ zijn. Bekijk dan de verzameling

$$\tilde{H} = \{x \in \mathbb{Z} : \bar{x} \in H\}.$$

We beweren dat $\tilde{H}$ een ondergroep van $\mathbb{Z}$ is. Ten eerste zit 0 in $\tilde{H}$ omdat $\bar{0} \in H$. Als $x, y \in \tilde{H}$ dan $\bar{x}, \bar{y} \in H$, en dus $\overline{x - y} \in H$ waaruit volgt dat $x - y \in \tilde{H}$, zodat $\tilde{H}$ een ondergroep is. Omdat $\tilde{H}$ ook n bevat volgt $\tilde{H} \neq \{0\}$. Uit het eerste deel van deze stelling volgt dan dat $\tilde{H} = d\mathbb{Z}$ voor een positieve d. Omdat $n \in \tilde{H} = d\mathbb{Z}$ moet d een deler zijn van n. Dus H bestaat uit alle veelvouden van $\bar{d}$. Verder zijn de ondergroepen $\langle \bar{d} \rangle$ met $0 < d | n$ allemaal verschillend. Dit bewijst de stelling.



$\langle \bar{3} \rangle \subset \mathbb{Z}/12\mathbb{Z}$

In Hoofdstuk 3 kwamen we twee groepen tegen met dezelfde vermenigvuldigingstabel, de viergroep van Klein en de groep $(\mathbb{Z}/12\mathbb{Z})^*$. Eigenlijk zijn deze groepen hetzelfde: er is een bijectie van de ene groep naar de andere zodat de bewerkingen overeenstemmen. Afbeeldingen tussen groepen die 'verdraagzaam' zijn met de bewerkingen vormen een geschikt middel om groepen met elkaar te kunnen vergelijken.

(5.6) Definitie. Laat G en G' twee groepen zijn. Een afbeelding $f : G \to G'$ heet een *homomorfisme* als

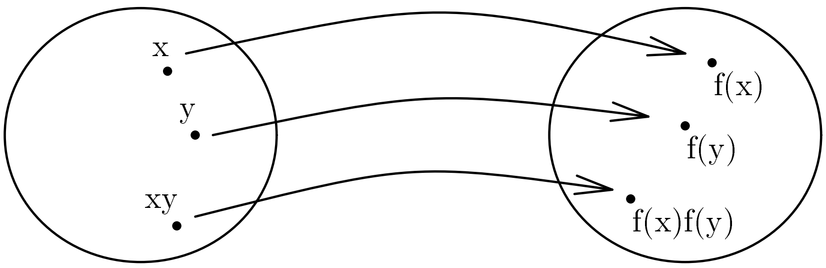
$$f(x\,y) = f(x)\,f(y) \text{ voor alle } \quad x, y \in G.$$

Een homomorfisme heet een *isomorfisme* als f bijectief is.

Merk op in deze definitie dat $x\,y$ het product in G is, terwijl het product $f(x)f(y)$ in G' genomen wordt.

Voor een isomorfisme $f : G \to G'$ wordt vaak $f : G \xrightarrow{\sim} G'$ geschreven. We zeggen dan: de groepen G en G' zijn isomorf en schrijven $G \cong G'$.

Een homomorfisme $f : G \to G$ heet een *endomorfisme* van G. Een bijectief endomorfisme heet een *automorfisme van* G.



(5.7) Voorbeelden.

i) Het *triviale* homomorfisme $f : G \to G'$ met $f(x) = e'$, het eenheidselement van G', voor alle x is een homomorfisme.

ii) De afbeelding $f : \mathbb{R}^* \to \mathbb{R}^*$, $\quad x \mapsto x^2$ is een homomorfisme. Dit is ook een endomorfisme, maar geen automorfisme want het is niet surjectief.

iii) De afbeelding $\det : GL_2(\mathbb{R}) \to \mathbb{R}^*$ die aan een matrix zijn determinant toevoegt is een homomorfisme.

iv) Laat G een groep zijn en $x \in G$ een element. De afbeelding $f : \mathbb{Z} \to G$ met $f(n) = x^n$ is een homomorfisme.

v) Laat $\mathbb{R}_{>0}$ de ondergroep van $\mathbb{R}^*$ van positieve reële getallen zijn. De afbeelding

$$\log : \mathbb{R}_{>0} \longrightarrow \mathbb{R}, \quad x \mapsto \log(x)$$

is een homomorfisme. Dit volgt uit de regel $\log(xy) = \log(x) + \log(y)$. De afbeelding

$$\exp : \mathbb{R} \longrightarrow \mathbb{R}_{>0}, \quad x \mapsto e^x$$

is ook een homomorfisme en bovendien de inverse afbeelding van log. Dus zowel log als exp zijn bijectief en dus isomorfismen. Blijkbaar is de multiplicatieve groep $\mathbb{R}_{>0}$ niets anders dan een vermomde versie van de additieve groep $\mathbb{R}$.

vi) De afbeelding $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ gegeven door $x \mapsto \bar{x}$ is een homomorfisme.

vii) Voor $n|m$ is de afbeelding $f : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ gegeven door $x(\operatorname{mod} m) \mapsto x(\operatorname{mod} n)$ een homomorfisme.

We bewijzen nu eerst twee eenvoudige eigenschappen van homomorfismen.

(5.8) Propositie. *Laat G (resp. G') een groep zijn met eenheidselement e (resp. e'). Dan geldt voor ieder homomorfisme $f : G \to G'$:*

i) $f(e) = e'$.

ii) $f(x^{-1}) = f(x)^{-1}$ *vor alle* $x \in G$.

Bewijs. Wegens $f(e) = f(e \cdot e) = f(e)f(e)$ volgt

$$e' = f(e) \cdot f(e)^{-1} = (f(e)f(e))f(e)^{-1} = f(e) \cdot e' = f(e).$$

Daaruit volgt $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$. Dus is $f(x^{-1})$ de rechtsinverse van $f(x)$. Zo ook volgt $f(x^{-1})f(x) = e'$. Dit bewijst de propositie.

Net als in de lineaire algebra een lineaire afbeelding een kern en beeld heeft die beide weer vectorruimten zijn, bepaalt een homomorfisme twee groepen, de kern en het beeld, die als volgt gedefinieerd zijn.

(5.9) Definitie. Laat $f : G \to G'$ een homomorfisme zijn van twee groepen G en G'. Dan is de *kern* van f de deelverzameling van G

$$\ker(f) = \{x \in G : f(x) = e'\}.$$

Het *beeld* van f is de deelverzameling van G'

$$f(G) = \{f(x) : x \in G\}.$$

Het beeld wordt ook wel genoteerd met $\operatorname{Im}(f)$.

(5.10) Stelling. *Laat $f : G \to G'$ een homomorfisme zijn. Dan geldt:*

i) De kern $\ker(f)$ *van f is een ondergroep van G.*

ii) Het beeld van f is een ondergroep van G'.

iii) De afbeelding f is injectief dan en slechts dan als $\ker(f) = \{e\}$, *het eenheidselement van G.*

Bewijs. i) Vanwege Propositie (5.8) is e element van $\ker(f)$ en dus $\ker(f) \neq \emptyset$. Als $x, y \in \ker(f)$ dan $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e'{e'}^{-1} = e'$. Dus (5.2) impliceert i).

ii) Vanwege (5.8) is e' element van $f(G)$ en $f(G)$ is dus niet leeg. Laat $x = f(\xi)$ en $y = f(\eta)$ elementen van $f(G)$ zijn. Dan geldt $xy^{-1} = f(\xi)f(\eta)^{-1} = f(\xi)f(\eta^{-1}) = f(\xi\eta^{-1}) \in f(G)$.

iii) Stel f is injectief. Er geldt altijd $e \in \ker(f)$. Laat $x \in \ker(f)$. Dan geldt $f(x) = e' = f(e)$. Omdat f injectief is moet dan $x = e$, dus $\{e\} = \ker(f)$. Omgekeerd, stel $f(x) = f(y)$, dan $f(xy^{-1}) = f(x)f(y)^{-1} = e'$ en dus $xy^{-1} \in \ker(f)$. Als $\ker(f) = \{e\}$ volgt $xy^{-1} = e$, dus $x = y$. Dus f is injectief. Dit bewijst de stelling.

Isomorfe groepen willen we als 'hetzelfde' beschouwen. Om dat te rechtvaardigen volgt nu een propositie.

(5.11) Propositie. *i) De samenstelling van twee isomorfismen is weer een isomorfisme. ii) De inverse afbeelding $f^{-1} : G' \to G$ van een isomorfisme $f : G \to G'$ is een isomorfisme.*

Bewijs. De samenstelling van twee bijecties is een bijectie. De samenstelling van twee homomorfismen is een homomorfisme. Dit bewijst i). Om ii) in te zien merken we eerst op dat een bijectieve afbeelding een inverse afbeelding heeft. Er geldt nu

$$f(f^{-1}(xy)) = xy = f(f^{-1}(x))\, f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y)).$$

Uit de injectiviteit van f volgt dan $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Hiermee volgt het gevraagde.

Met deze propositie zien we dat de relatie $G \cong G'$ een equivalentierelatie op de klasse van alle groepen is. De reflexiviteit ($G \cong G$) volgt uit het feit dat de identieke afbeelding $G \to G$ een isomorfisme is. Deel ii) van de propositie impliceert de symmetrie ($G \cong H \Rightarrow H \cong G$) en deel i) geeft de transitiviteit ($G \cong H,\ H \cong K \Rightarrow G \cong K$). Isomorfe groepen kunnen we dus als 'gelijk' beschouwen.

We sluiten dit hoofdstuk af met een toepassing: de Chinese reststelling.

(5.12) Stelling. *(Chinese reststelling) Laat m en n twee onderling ondeelbare positieve gehele getallen zijn. Dan is de afbeelding*

$$f : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad x(\operatorname{mod} mn) \mapsto (x(\operatorname{mod} m), x(\operatorname{mod} n))$$

een isomorfisme.

Bewijs. De afbeelding f is welgedefinieerd en een homomorfisme, zoals de lezer snel kan nagaan. Laat nu $x(\operatorname{mod} mn) \in \ker(f)$. Dan moet gelden $x \equiv 0(\operatorname{mod} m)$ en $x \equiv 0(\operatorname{mod} n)$, wat wil zeggen dat zowel m als n delers zijn van x, zeg $x = am$ en $x = bn$. omdat de ggd van m en n gelijk is aan 1 zijn er ξ en η met $\xi m + \eta n = 1$. Vermenigvuldig dit met x:

$$x = x \cdot 1 = x\xi m + x\eta n = bn\xi m + an\eta m = (b\xi + a\eta)\, mn.$$

Derhalve is x deelbaar door mn en dus $x \equiv 0(\operatorname{mod} mn)$. Dit laat zien dat f injectief is. Omdat zowel $\mathbb{Z}/mn\mathbb{Z}$ als $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ cardinaliteit mn hebben moet f een bijectie, dus een isomorfisme zijn. Dit bewijst de stelling.

(5.13) Gevolg. *Laat m en n positieve gehele getallen zijn die onderling ondeelbaar zijn. Laat verder a en $b \in \mathbb{Z}$ gegeven zijn. Dan heeft het stelsel vergelijkingen*

$$x \equiv a \,(\operatorname{mod} m)$$
$$x \equiv b \,(\operatorname{mod} n)$$

een éénduidige oplossing modulo mn.

Bewijs. De existentie van een oplossing volgt uit de surjectiviteit van de afbeelding f uit stelling (5.12). De injectiviteit bewijst de eenduidigheid.

Om de oplossing expliciet te bepalen gebruiken we eerst het Euclidisch algoritme om een representatie

$$1 = \xi m + \eta n$$

te bepalen. Dan nemen we $x = b\,\xi m + a\,\eta n$. Dit element (of liever zijn restklasse) voldoet. Merk op dat $\xi m \equiv 0(\operatorname{mod} m)$ en $\xi m \equiv 1(\operatorname{mod} n)$ terwijl $\eta n \equiv 1(\operatorname{mod} m)$ en $\eta n \equiv 0(\operatorname{mod} n)$.

De stelling dankt zijn naam aan het feit dat oplossingen van lineaire congruenties als in (5.13) voorkomen in de Chinese wiskunde, bijv. in het Rekenleerboek van Meester Sun (Sun Tzu Suan Ching) dat gedateerd wordt ergens in de periode 280–473.

Opgaven

1) Bewijs: een ondergroep van een abelse groep is abels. Geef een niet-triviaal voorbeeld van een abelse ondergroep van een niet-abelse groep.

2) Laat $f : G \to G'$ een homomorfisme zijn. Laat H' een ondergroep van G' zijn. Bewijs: het inverse beeld $f^{-1}(H') = \{x \in G : f(x) \in H'\}$ is een ondergroep van G.

3) Bepaal alle ondergroepen van de Viergroep van Klein.

4) Laat H_1 en H_2 twee ondergroepen van een groep G zijn. Bewijs dat als $G = H_1 \cup H_2$ dan $G = H_1$ of $G = H_2$. Geldt iets dergelijks ook voor drie ondergroepen?

5) Bewijs dat $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$.

6) Ga na dat de volgende afbeeldingen homomorfismen zijn. Bepaal kern en beeld.
i) $\mathbb{R}^* \to \mathbb{R}^*, \quad x \mapsto |x|$.
ii) $\mathbb{C} \to \mathbb{C}, \quad x + i\,y \mapsto x - i\,y$.
iii) $\mathbb{C}^* \to \mathbb{C}^*, \quad z \mapsto z^n$ voor $n \in \mathbb{Z}$.
iv) $\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}, \quad x(\operatorname{mod} 12) \mapsto x(\operatorname{mod} 4)$.
v) $(\mathbb{Z}/12\mathbb{Z})^* \to (\mathbb{Z}/4\mathbb{Z})^*, \quad x(\operatorname{mod} 12) \mapsto x(\operatorname{mod} 4)$.
vi) $\mathbb{R} \to \mathbb{C}^*, \quad \phi \mapsto \cos(\phi) + i\,\sin(\phi)$.
vii) $\mathbb{Z}/12\mathbb{Z} \to (\mathbb{Z}/13\mathbb{Z})^*, \quad x(\operatorname{mod} 12) \mapsto 2^x(\operatorname{mod} 13)$.

7) Zij G een groep en $g \in G$. Laat zien dat de afbeelding $G \to G$ met $x \mapsto gxg^{-1}$ een automorfisme is.

8) Zij G een groep. Bewijs dat de afbeelding $x \mapsto x^{-1}$ een homomorfisme is dan en slechts dan als G abels is. Bewijs dat $x \mapsto x^2$ een homomorfisme is dan en slechts dan als G abels is.

9) Bewijs dat twee groepen van orde 2 isomorf zijn. Bewijs dat twee groepen van orde 3 isomorf zijn. Bewijs: een groep van orde 4 is isomorf met de Viergroep van Klein of cyclisch van orde 4.

10) Bewijs i) $\mathbb{R}^* \cong \mathbb{R}_{>0} \times \{\pm 1\}$. ii) $\mathbb{R}^* \cong \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$.

11) Bewijs dat de deelverzameling $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ van $\mathbb{C}^*$ een ondergroep is van $\mathbb{C}^*$. Bewijs $\mathbb{C}^* \cong S^1 \times \mathbb{R}_{>0}$.

12) Bewijs dat voor oneven $n \in \mathbb{N}$ geldt $D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$.

13) Vind een $x \in \mathbb{Z}$ met $0 \leq x \leq 1000$ zodat $x \equiv 2 (\bmod 7)$, $x \equiv 3 (\bmod 11)$, $x \equiv 4 (\bmod 13)$. Idem met $x \equiv 6 (\bmod 7)$, $x \equiv 10 (\bmod 11)$ en $x \equiv 12 (\bmod 13)$.

14) Zij G een cyclische groep van orde 8. Hoeveel elementen van G zijn een voortbrenger van G?

15) Bepaal het aantal elementen van orde 2 in de symmetrische groep S_4, de symmetriegroep van een tetraëder.

16) Zij G een abelse groep. Laat zien dat de elementen van eindige orde een ondergroep van G vormen. (Deze ondergroep heet de *torsieondergroep* van G.) Geldt dit ook voor niet-abelse groepen? (Bekijk bijv. D_∞ of $\mathrm{SL}_2(\mathbb{Z})$.)

17) Laat G een groep zijn en H een ondergroep van G. Laat zien dat de relatie $a \sim b \iff ab^{-1} \in H$ een equivalentierelatie op G is.

18) Zij $x \in G$ een element van orde n (resp. orde ∞) in een groep G. Bewijs dat $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$ (resp. $\cong \mathbb{Z}$).

19) Bewijs de doorsnede van een stelsel ondergroepen van een groep is weer een ondergroep. Laat $S \subset G$ een deelverzameling van een groep zijn. Bewijs: $\langle S \rangle$ is de doorsnede van alle ondergroepen van G die S bevatten.

20) Laat H een niet-lege eindige deelverzameling van een groep G zijn. Bewijs: H is een ondergroep $\iff$ H is gesloten onder de vermenigvuldiging (d.w.z. als $a, b \in H$ dan $ab \in H$).

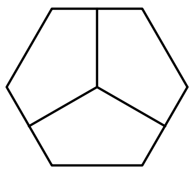
21) Laat zien dat de additieve groep $\mathbb{Q}$ met de bewerking $+$ niet isomorf is met de multiplicatieve groep $\mathbb{Q}^*$ met de bewerking $\times$. Bewijs ook dat $\mathbb{Q}^*_{>0}$ niet isomorf is met $\mathbb{Q}$.

22) Bewijs de volgende beweringen:

i) $\mathbb{Q}[i] = \{a + b\, i : a, b \in \mathbb{Q}\}$ is een ondergroep van $\mathbb{C}$.

ii) De groepen $\mathbb{Q}[i]$ and $\mathbb{Q}$ zijn niet isomorf.

23) Bepaal de symmetriegroep van de volgende figuur



24) Bewijs: een eindige symmetriegroep van een vlakke figuur is isomorf met een cyklische groep of een diëdergroep.

6. Permutatiegroepen

stapel spatel pastel slapte
plaste laspet telpas taples
petsla petlas patles pletas
*

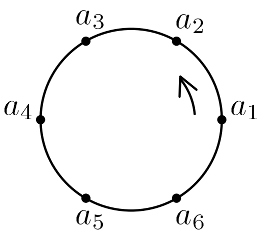
De groep van permutaties van n objecten heet de *symmetrische groep* en wordt genoteerd als S_n. Voor deze n objecten nemen we vaak de getallen $1, 2, \ldots, n$. Deze groep heeft orde $n!$. Immers om een element σ vast te leggen hebben we voor $\sigma(1)$ precies n mogelijkheden, voor $\sigma(2)$ dan nog maar $n-1$, etc. De complexiteit van deze groepen neemt snel toe als n groter wordt.

(6.1) Definitie. Een element $\sigma \in S_n$ heet *cykel* als er k verschillende elementen $a_1, \ldots, a_k$ in $\{1, \ldots, n\}$ zijn met $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k$ en $\sigma(a_k) = a_1$ en bovendien $\sigma(a) = a$ als $a \notin \{a_1, \ldots, a_k\}$. De notatie voor deze cykel is

$$\sigma = (a_1\, a_2\, \ldots\, a_k).$$

Het getal k heet de *lengte* van de cykel. We zeggen ook wel dat σ een k-cykel is. De 2-cykels heten *transposities* of *verwisselingen*. Het eenheidselement wordt ook wel als (1) genoteerd. De lengte daarvan is 1.

Merk op dat de notatie voor een k-cykel niet eenduidig is. Er geldt $(a_1\, a_2\, \ldots\, a_k) = (a_2\, a_3, \ldots\, a_k\, a_1)$ etc. Onder een k-cykel worden de a_i cyclisch verwisseld.



We noemen twee cykels $(a_1\, a_2\, \ldots\, a_k)$ en $(a'_1\, a'_2\, \ldots\, a'_\ell)$ *disjunct* als geen van de a_i gelijk is aan een a'_j.

(6.2) Voorbeeld. i) Laat $n = 4$. Het element $\sigma \in S_4$ gegeven door

$$1 \mapsto 4, \qquad 2 \mapsto 1, \qquad 3 \mapsto 3, \qquad 4 \mapsto 2$$

is een 3-cykel: $\sigma = (1\,4\,2)$.

ii) Laat $n = 7$. Het element $\rho \in S_7$ gegeven door

$$1 \mapsto 5, \qquad 2 \mapsto 4, \qquad 3 \mapsto 1, \qquad 4 \mapsto 7, \qquad 5 \mapsto 3, \qquad 6 \mapsto 6, \qquad 7 \mapsto 2$$

kan geschreven worden als product van twee disjuncte 3-cykels en een 1-cykel:

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

* vgl. Battus: *Opperlandse Taal- en Letterkunde*

(6.3) Opmerking. *Twee disjuncte cykels commuteren.*

Met behulp van disjuncte cykels kunnen we alle elementen van S_n beschrijven:

(6.4) Stelling. *Iedere permutatie $\sigma \in S_n$ is te schrijven als product van disjuncte cykels. Deze schrijfwijze is eenduidig op de volgorde na.*

Bewijs. Het idee van het bewijs is simpel: neem een willekeurig element a en volg dat onder σ tot we weer bij a terug zijn. Dan hebben we een cykel gevonden. Ga dan verder met een ander element dat niet in deze cykel zit. Meer formeel: We voeren het bewijs met inductie naar n. Voor $n = 1$ kunnen we σ schrijven als (1). Stel dat de stelling geldt voor S_m met $m < n$. Kies nu een element $\sigma \in S_n$ en een willekeurig element $a \in \{1, \ldots, n\}$. Beschouw dan de deelverzameling

$$\{a, \sigma(a), \sigma^2(a), \sigma^3(a), \ldots\}.$$

Dit is een eindige verzameling want zij is bevat in $\{1, \ldots, n\}$. Dus zijn er verschillende i, j met $\sigma^i(a) = \sigma^j(a)$. We mogen aannemen dat $i > j \geq 0$. Toepassen van σ^{-j} geeft $\sigma^{i-j}(a) = a$ met $i - j > 0$. Zij nu k het kleinste positieve getal met $\sigma^k(a) = a$. Dan zijn de elementen van de verzameling

$$A = \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{k-1}(a)\}$$

allemaal verschillend en σ werkt hierop als k-cykel. Omdat σ een bijectie is beeldt σ het complement

$$A^c = \{1, \ldots, n\} - A$$

bijectief op zich af en σ is vanwege de inductie aanname te schrijven als product van disjuncte cykels, zeg $\sigma|A^c = \tau_1 \cdots \tau_r$. Dan kan σ geschreven worden als

$$(a\,\sigma(a)\,\ldots\sigma^{k-1}(a))\tau_1 \cdots \tau_r.$$

Daarmee is de existentie bewezen. De eenduidigheid volgt direct met inductie uit het feit dat σ een bijectie is. Einde bewijs.

Het bewijs levert ons een procédé om een gegeven permutatie ρ te schrijven als disjunct product van cykels, bijv. als ρ een gegeven product van twee cykels is. We geven een voorbeeld. Laat $\sigma = (1\,2\,3\,4\,5)$ en $\tau = (1\,3\,5\,7)$ in S_7. We berekenen het product

$$\rho = \sigma\tau = (1\,2\,3\,4\,5)\,(1\,3\,5\,7).$$

De notatie betekent: eerst τ toepassen, daarna σ. Onder τ gaat 1 naar 3 en onder σ gaat 3 naar 4, dus $\rho(1) = 4$. Nu geldt $\tau(4) = 4$ en $\sigma(4) = 5$, dus $\rho(4) = 5$. We zien $5 \xrightarrow{\tau} 7 \xrightarrow{\sigma} 7$, dus $\rho(5) = 7$. Zo ook $7 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2$, dus $\rho(7) = 2$. Verder $2 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3$, dus $\rho(2) = 3$. Tenslotte $3 \xrightarrow{\tau} 5 \xrightarrow{\sigma} 1$, dus $\rho(3) = 1$. Verder blijft 6 op zijn plaats. We zien dus

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

In de notatie van Stelling (5.3) kunnen we 1-cykels net zo goed weglaten en dat zullen we meestal doen. Hierbij wordt het lege product gedefinieerd als het eenheidselement.

Als een permutatie σ het disjuncte product is van r disjuncte cykels van lengte ℓ_1, $\ell_2, \ldots, \ell_r$, waarbij we de 1-cykels ook meetellen, dan heet de verzameling $\{\ell_1, \ldots, \ell_r\}$ het *cykeltype* van σ. Er geldt $\sum_{i=1}^r \ell_i = n$. De cykeltypes corresponderen zo met de 'partities' van n. Bijvoorbeeld, het element

$$(27)(345) \in S_7$$

correspondeert zo met

$$1 + 1 + 2 + 3 = 7.$$

We gaan nu aan ieder element $\sigma \in S_n$ een 'teken' $\epsilon(\sigma) \in \{+1, -1\}$ toekennen. Daarvoor beschouwen we de verzameling F van afbeeldingen $f : \mathbb{Z}^n \to \mathbb{Z}$. Zo een afbeelding of functie kan geschreven worden als $f(x_1, \ldots, x_n)$. Met $\sigma \in S_n$ en $f \in F$ verkrijgen we een nieuwe afbeelding $\sigma(f)$ gedefinieerd door

$$\sigma(f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Merk op dat $\sigma(f)$ de samenstelling is van

$$\mathbb{Z}^n \longrightarrow \mathbb{Z}^n, \quad (x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

met f.

In het bijzonder kunnen we voor f de functie ('discriminant')

$$d = \prod_{1 \le i < j \le n} (x_i - x_j).$$

nemen. Omdat afgezien van het teken ieder verschil $x_i - x_j$ precies één keer voorkomt in $\sigma(d)$ geldt

$$\sigma(d) = \pm d$$

(6.5) Definitie. Voor $\sigma \in S_n$ definiëren we het teken $\epsilon(\sigma) \in \{\pm 1\}$ door

$$\sigma(d) = \epsilon(\sigma)\, d.$$

De permutaties met $\epsilon(\sigma) = 1$ heten *even*, die met $\epsilon(\sigma) = -1$ heten *oneven*.

Als voorbeeld nemen we de 4-cykel $(1\,2\,3\,4) \in S_4$. Er geldt

$$\begin{aligned} \sigma(d) &= (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) \\ &= -(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4), \end{aligned}$$

dus $\epsilon(\sigma) = -1$. Ga zelf na dat een verwisseling $(a_1\, a_2)$ teken -1 heeft.

(6.6) Propositie. *Het teken definieert voor $n \ge 2$ een surjectief homomorfisme*

$$\epsilon : S_n \longrightarrow \{+1, -1\},$$

m.a.w. $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$ *voor alle* $\sigma, \tau \in S_n$.

Bewijs. Voor een functie $f \in F$ geldt $(\sigma\tau)(f) = \sigma(\tau(f))$. Immers, $(\sigma\tau)(f)$ is de samenstelling

$$(x_1, \ldots, x_n) \mapsto (x_{\tau(1)}, \ldots, x_{\tau(n)}) \mapsto (x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(n))})$$

gevolgd door f. Maar dit is gelijk aan σ toegepast op de functie $\tau(f)$

$$(x_1, \ldots, x_n) \mapsto (x_{\tau(1)}, \ldots, x_{\tau(n)}) \mapsto f(x_{\tau(1)}, \ldots, x_{\tau(n)})).$$

Dus in het bijzonder vinden we $(\sigma\tau)(d) = \sigma(\tau(d))$, waaruit $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$ volgt. Een verwisseling $(i\,j)$ heeft teken -1. Dit bewijst de propositie.

Uit (6.6) volgt direct dat een product van een even aantal verwisselingen teken $+1$ heeft, terwijl het product van een oneven aantal verwisselingen teken -1 heeft. Als σ een k-cykel is dan hebben we $\epsilon(\sigma) = (-1)^{k-1}$. Dit volgt uit de relatie

$$(a_1\, a_2\, a_3\, \ldots\, a_k) = (a_1\, a_2)\,(a_2\, a_3)\,(a_3\, a_4)\ldots(a_{k-1}\, a_k) \tag{1}$$

die eenvoudig te controleren is en het feit dat ϵ een homomorfisme is.

Een natuurlijk voorbeeld waar de tekens van permutaties optreden zijn determinanten. Laat $A = (a_{ij})$ een $n \times n$-matrix zijn, zeg met coëfficiënten uit de reële getallen. Dan is de determinant $\det(A)$ gelijk aan de uitdrukking

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\,\sigma(1)} a_{2\,\sigma(2)} \cdots a_{n\,\sigma(n)}.$$

Ga na dat dit voor $n = 2, 3$ de gebruikelijke formule geeft. Ga verder na dat de getransponeerde matrix $A^t = (a_{ji})$ dezelfde determinant heeft als A.

(6.7) Propositie. *Ieder element uit* S_n *is een product van verwisselingen.*

Bewijs. Dit volgt direct uit de relatie (1) en Stelling (6.4).

Een andere manier om dit te verwoorden is: de verwisselingen zijn voortbrengers van de groep S_n.

(6.8) Definitie. De kern van het tekenhomomorfisme $\epsilon : S_n \to \{+1, -1\}$ heet de *alternerende groep* en wordt genoteerd met A_n:

$$A_n = \{\sigma \in S_n : \epsilon(\sigma) = 1\}.$$

Omdat verwisselingen teken -1 hebben bevat A_n geen verwisselingen. Daarmee kan de orde van de groep A_n bepaald worden. Laat $n \geq 2$. Als $\tau = (1\,2)$ dan levert de afbeelding

$$S_n \longrightarrow S_n \qquad \sigma \mapsto \sigma\tau = \sigma\,(1\,2)$$

een bijectie van S_n op zichzelf waarbij even elementen in oneven elementen overgaan en omgekeerd. Dus:

$$\#A_n = \frac{n!}{2} \qquad (n \geq 2).$$

Daarentegen liggen alle 3-cykels in A_n. De volgende stelling zegt dat deze elementen de groep A_n voortbrengen.

(6.9) Stelling. *De groep A_n wordt voortgebracht door de 3-cykels.*

Bewijs. Voor $n \leq 2$ is de uitspraak ten duidelijkste waar want A_1 en A_2 bestaan uit het eenheidselement en dat is gelijk aan het lege product van 3-cykels. Laat nu $n \geq 3$. Volgens (6.6) en (6.7) is ieder element van A_n te schrijven als product van een *even* aantal verwisselingen. Om de stelling in te zien is het dus voldoende te bewijzen dat een product $\rho = (a\,b)\,(c\,d)$ van twee verwisselingen een product van 3-cykels is. We onderscheiden twee gevallen:

i) de twee verwisselingen zijn disjunct. Dan volgt de bewering direct uit de betrekking:

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

ii) de verwisselingen zijn niet disjunct. Dan geldt $(a\,b) = (c\,d)$ en ρ is het eenheidselement (leeg product van 3-cykels) of we hebben een product van het type $(a\,b)\,(b\,c)$ met a, b, c verschillend. Maar dan gebruiken we

$$(a\,b)(b\,c) = (a\,b\,c).$$

Daarmee is het bewijs volledig.

De S_n leveren ons veel interessante voorbeelden van eindige groepen die allemaal niet commutatief zijn als $n \geq 3$. De volgende stelling zegt dat deze groepen heel algemeen zijn.

(6.10) Stelling van Cayley*. *Ieder eindige groep G is isomorf met een ondergroep van een symmetrische groep S_n.*

Bewijs. We gaan laten zien dat er een injectief homomorfisme is van G naar de symmetrische groep van bijecties $S(G)$ van de verzameling G. We doen dit door aan g de linksvermenigvuldiging met g toe te voegen. Definieer $j : G \longrightarrow S(G)$ door

$$g \mapsto \lambda_g \quad \text{met} \quad \lambda_g(h) = gh \quad \text{voor alle } h \in G.$$

We weten al uit (3.18) dat λ_g een bijectie is op de verzameling G. We gaan nu na dat j een homomorfisme is. Uit $(gg')h = g(g'h)$ volgt

$$\lambda_g(\lambda_{g'}(h)) = (\lambda_g \circ \lambda_{g'})(h),$$

dus

$$j(gg') = j(g) \circ j(g').$$

Uit $\lambda_g(e) = g$ volgt $\lambda_g \neq \lambda_{g'}$ voor $g \neq g'$ en dus de injectiviteit van j. We zien dus dat $G \cong j(G)$ en $j(G)$ is een ondergroep van $S(G)$. De groep $S(G)$ is isomorf met S_n met $n = \#G$. Met (5.11) is de stelling nu bewezen.

* A. Cayley, Engels wiskundige, 1821–1895

De oorsprong van de groepentheorie ligt in het werk van Lagrange**, Ruffini*** en Galois over de oplosbaarheid van veeltermvergelijkingen. Zij bestudeerden groepen van permutaties van de wortels van een polynoom. Als

$$f = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n = (X - \alpha_1)\cdots(X - \alpha_n)$$

een polynoom is met wortels $\alpha_1 \ldots, \alpha_n$ dan zijn de coëfficiënten $a_1, \ldots, a_n$ symmetrische uitdrukkingen in de wortels

$$a_1 = -\sum_{i=1}^{n}\alpha_i, \quad a_2 = \sum_{1\le i<j\le n}\alpha_i\alpha_j, \quad \ldots, \quad a_n = (-1)^n\alpha_1\cdots\alpha_n$$

en blijven onveranderd onder permutaties van de α_i. De naam 'symmetrische groep' voor S_n verwijst naar dit feit. De meeste groepen die optraden in de vorige eeuw waren ondergroepen van permutatiegroepen. Het idee van een abstracte groep als in Definitie 3.1 stamt van Cayley, die groepen definieerde met behulp van vermenigvuldigingstabellen (Cayley-diagrammen) ("A group is defined by means of the laws of combinations of its symbols"), maar het heeft geruime tijd geduurd voordat dat idee ingang vond. Bovenstaande stelling van Cayley werd veel gebruikt om abstract gedefinieerde groepen concreet te realizeren. Een definitie als in (3.1) komt in de wiskundige literatuur voor het eerst voor in 1882, in twee bijna gelijktijdige artikelen van Weber* en von Dyck**

Laat nu T een regelmatig viervlak of tetraëder zijn met hoekpunten a, b, c, d. We bepalen de symmetriegroep G_T van T.

(6.12) Propositie. *De symmetriegroep G_T van een tetraëder is isomorf met S_4.*

Bewijs. Iedere symmetrie g van T ligt vast door de beelden van de hoekpunten onder g. We vinden dus een injectieve afbeelding $j : G_T \to S_4$ door aan g de permutatie van de hoekpunten toe te voegen. De spiegeling in het vlak door de ribbe cd loodrecht op de ribbe ab levert de verwisseling $(a\,b)$. We krijgen dus alle voortbrengers van $S_4 \cong S(\{a, b, c, d\})$ en dus is j surjectief.

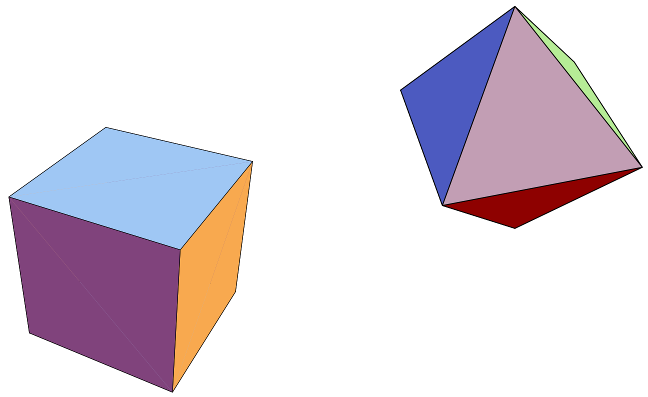
Op soortgelijke manier vinden we voor de kubus K een homomorfisme van de symmetriegroep G_K van de kubus naar S_8. Maar we kunnen een ander homomorfisme maken door te kijken wat een element $g \in G_K$ met de vier lichaamsdiagonalen $d_1, \ldots, d_4$ van de kubus doet. De lichaamsdiagonalen zijn de lijnstukken door de oorsprong die overstaande hoekpunten verbinden.

** Joseph-Louis Lagrange, Italiaans-Frans wiskundige, 1736–1813

*** Paolo Ruffini, Italiaans wiskundige, 1765–1822.

* H. Weber, Duits wiskundige, 1842–1913

** Walter von Dyck, Duits wiskundige, 1856-1934, leerling van Felix Klein

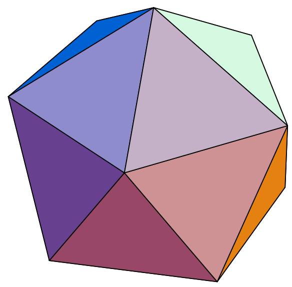


kubus en octaeder

Ieder element $g \in G_K$ levert een permutatie van de d_i, dus een element van S_4 en we vinden zo een homomorfisme $\phi : G_K \to S_4$. Dit homomorfisme is niet injectief. De puntspiegeling $x \mapsto -x$ om de oorsprong brengt de kern van j voort: $\ker(\phi) = \{\pm 1\}$. De symmetrieen met determinant $+1$ vormen een ondergroep G_K^+.

Opgave. Laat zien dat ϕ een isomorfisme $G_K^+ \xrightarrow{\sim} S_4$ levert. Concludeer dat $\#G_K = 48$. Wat betekent dit voor de symmetriegroep van het regelmatig achtvlak?

Tenslotte beschouwen we de icosaeder. De groep G_I^+ van rotaties die de icosaeder in zich voeren bevat 60 elementen. Ieder van de 12 hoekpunten blijft onder 5 rotaties op zijn plaats. Als $P = \{p_1, \ldots, p_{12}\}$ de hoekpunten van I zijn dan is de afbeelding $G_I^+ \to P$ gegeven door $g \mapsto g(p_1)$ surjectief en $5 : 1$.



icosaeder

(6.13) Propositie. *De groep G_I^+ van orthogonale symmetriën (rotaties) van een icosaeder is isomorf met de alternerende groep A_5.*

Bewijs. Er zijn vijf verschillende manieren waarop in een icosaeder I een kubus gelegd kan worden (ingeschreven kubus). Of equivalent: er zijn vijf drietallen orthogonale lijnstukken die middens van overstaande ribben verbinden. Een symmetrie van een icosaeder permuteert deze vijf objecten. Dit levert een injectie $G_I^+ \longrightarrow S_5$. Ga nu na dat de rotaties even permutaties leveren. (De 20 draaiingen die een vlak van I in zich voeren leveren 20 3-cykels die A_5 voortbrengen.)

Opgaven

1) Schrijf de volgende permutaties in S_7 als product van disjuncte cykels.
i) $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 5$, $4 \mapsto 6$, $5 \mapsto 2$, $6 \mapsto 4$.
ii) $1 \mapsto 6$, $2 \mapsto 3$, $3 \mapsto 5$, $4 \mapsto 4$, $5 \mapsto 7$, $6 \mapsto 1$, $7 \mapsto 2$.

2) Laat zien dat de inverse van de k-cykel $(a_1\, a_2\, \ldots\, a_k)$ gelijk is aan $(a_k\, \ldots\, a_2\, a_1)$.

3) Bepaal het teken van alle elementen van S_3. Stel een vermenigvuldigingstabel voor S_3 op.

4) Laat $\sigma, \tau \in S_n$. Bewijs: $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$ en $\epsilon(\sigma^{-1}\tau\sigma) = \epsilon(\tau)$.

5) Laat $\sigma = (a_1\, \ldots a_k)$ een k-cykel zijn. Bewijs $\tau\sigma\tau^{-1} = (\tau(a_1)\, \ldots\, \tau(a_k))$.

6) Laat σ een n-cykel in S_n zijn. Bewijs dat een element τ alleen dan met σ commuteert als τ een macht van σ is.

7) Laat $\sigma, \tau \in S_n$. De elementen $\sigma\tau$ en $\tau\sigma$ hebben hetzelfde cykeltype. Bewijs dit.

8) Bewijs: de orde van een permutatie $\sigma \in S_n$ is het kgv van de lengtes die optreden in het cykeltype.

9) Bepaal welke getallen optreden als orde van een element van S_7.

10) Laat $\sigma \in S_n$. Een inversie van σ is een paar $(i\, j)$ met $i < j$ en $\sigma(i) > \sigma(j)$. Laat zien dat $\epsilon(\sigma)$ gelijk is aan $(-1)^I$, met I het aantal inversies van σ.

11) Laat $H \subset S_n$ een ondergroep zijn. Bewijs: òf de helft van alle elementen van H is even, òf alle elementen van H zijn even.

12) Bepaal het aantal elementen van orde 2, 3 en 5 in A_5.

13) Laat zien dat S_n een groep bevat die isomorf is met D_n.

14) Bewijs dat de groep van rotaties van een dodecaeder isomorf is met A_5.

15) Laat zien dat de rotatiegroep G_I^+ bestaat uit 24 draaiingen van orde 5, 20 draaiingen van orde 3 en 15 draaiingen van orde 2, plus het eenheidselement.

16) Zij G een eindige groep van orde $2k$ met k oneven. Laat $g \in G$ een element van orde 2 zijn. Bewijs dat de permutatie $\lambda_g : G \to G$ een oneven permutatie in $S(G)$ is.

17) Als g, h elementen van een groep G zijn, dan heet het element $[g, h] = ghg^{-1}h^{-1}$ de *commutator* van g en h. De ondergroep voortgebracht door alle commutatoren heet de *commutatorondergroep* en wordt genoteerd $[G, G]$. Bereken de commutator van $(1\,2\,3)(1\,4\,5)$ in A_n voor $n \geq 5$. Bereken de commutatorondergroep van A_n voor $n \geq 5$.

18) Bewijs dat S_n voortgebracht wordt door de verwisselingen $(1\, i)$ met $i = 2, \ldots, n$.

19) Bewijs dat S_n wordt voortgebracht wordt door de permutaties $(1\,2)$ and $(1\,2\,3\, \ldots\, n)$.

7. Nevenklassen en Index

Bei längerer Beschäftigung mit einer solchen Theorie beobachtet man nun,
dass die anfangs recht abstrakten Dinge in unserer Vorstellung
mehr und mehr Leben annehmen
E. Artin*

We hebben in het voorgaande hoofdstuk gezien dat de symmetrische groep S_n voor $n \geq 2$ in twee delen uiteenvalt: de even permutaties en de oneven permutaties. We kunnen iedere oneven permutatie schrijven als een vast oneven element maal een even element:

$$S_n = A_n \sqcup \tau A_n$$

met τ een vast element met $\epsilon(\tau) = -1$. Dit is een voorbeeld van een vast patroon: een ondergroep H van een groep G geeft een verdeling van G in disjuncte deelverzamelingen van de vorm $gH = \{gh : h \in H\}$.

(7.1) Definitie. Laat H een ondergroep van een groep G. Een *linkernevenklasse* van H is een deelverzameling van de vorm

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

Een *rechternevenklasse* van H is een deelverzameling van de vorm

$$Hg = \{hg : h \in H\}.$$

De verzameling linkernevenklassen wordt genoteerd ** met G/H; de verzameling rechternevenklassen met $H\backslash G$.

We laten nu eerst zien dat de verdeling van G die dit levert hoort bij een equivalentierelatie. We definiëren een equivalentierelatie op G via

$$x \sim y \Longleftrightarrow x^{-1}\, y \in H.$$

Dat dit een equivalentierelatie is volgt direct uit het feit dat H een ondergroep is: $x \sim x$ want $e \in H$; $x \sim y \Longrightarrow y \sim x$ want met $x^{-1}y$ ligt ook de inverse $y^{-1}x$ in H; als $x \sim y$ en $y \sim z$ dan $x^{-1}z = x^{-1}y\, y^{-1}z \in H$.

Merk op dat we in plaats van

$$x^{-1}y \in H \qquad \text{ook} \qquad y \in xH$$

kunnen schrijven. Dus de equivalentieklassen zijn de linkernevenklassen. Hieruit volgt direct dat verschillende nevenklassen disjunct zijn:

$$xH = yH \qquad \text{of} \quad xH \cap yH = \emptyset.$$

* Emil Artin, Duits wiskundige, 1898–1962

** Deze gelukkig gekozen notatie stamt van Camille Jordan, een van de pioniers van de groepentheorie, wiens 'Théorie des Substitutions' uit 1870 een belangrijke rol heeft gespeeld.

Schematisch ziet dat er dus zo uit:

Nevenklassenindeling.

g_1H	g_2H	g_3H	$\ldots$
$\ldots$	$\ldots$		
			g_nH

We geven nu eerst wat voorbeelden.

(7.2) Voorbeelden.

i) Laat $G = \mathbb{Z}$ en laat $H = n\mathbb{Z}$. Dan zijn de linkernevenklassen de verzamelingen van de vorm

$$x + n\mathbb{Z} = \{x + k\,n : k \in \mathbb{Z}\}.$$

Dit zijn precies de restklassen modulo n. Wegens de commutativiteit zijn dit ook de rechternevenklassen. De verzameling (linker)nevenklassen wordt genoteerd met $\mathbb{Z}/n\mathbb{Z}$ wat in overeenstemming is met de al eerder ingevoerde notatie voor de verzameling restklassen modulo n.

ii) Laat $G = \mathbb{R}^*$ en H de ondergroep $\mathbb{R}_{>0}$. Als x positief is dan is $x\mathbb{R}_{>0} = \mathbb{R}_{>0}$. Is $x < 0$ dan is $x\mathbb{R}_{>0}$ gelijk aan $\mathbb{R}_{<0}$. We vinden zo twee linkernevenklassen: de positieve getallen en de negatieve getallen. Rechternevenklassen leveren hetzelfde omdat $\mathbb{R}^*$ commutatief is.

iii) Laat $G = \mathbb{R}^2$ en laat L de ondergroep zijn gegeven door een lijn door de oorsprong. Dan zijn de linkernevenklassen precies de verzamelingen van de vorm

$$x + L = \{x + v : v \in L\}.$$

Rechternevenklassen leveren precies hetzelfde. Dit zijn de lijnen evenwijdig aan L.

iv) Laat $G = S_3$ en $H = \{e, (2\,3)\}$. Er zijn dan drie linkernevenklassen

$$\begin{aligned} H &= \{(1), (2\,3)\}, \\ (1\,2\,3)H &= \{(1\,2\,3),\ (1\,2)\}, \\ (1\,3\,2)H &= \{(1\,3\,2),\ (1\,3)\} \end{aligned}$$

De rechternevenklassen zijn:

$$\begin{aligned} H &= \{(1), (2\,3)\}, \\ H(1\,2\,3) &= \{(1\,2\,3),\ (1\,3)\}, \\ H(1\,3\,2) &= \{(1\,3\,2),\ (1\,2)\} \end{aligned}$$

We zien hier dat met $\tau = (1\,2\,3)$ geldt $\tau H \neq H\tau$.

Merk op dat nevenklassen in het algemeen geen ondergroepen zijn: gH zal als $g \notin H$ het eenheidselement niet bevatten. Wel is er altijd een bijectie

$$H \xleftrightarrow{1-1} gH, \qquad x \mapsto gx$$

gegeven door beperking van de afbeelding λ_g (vermenigvuldiging van links met g) tot H. Dus de nevenklassen hebben allemaal dezelfde cardinaliteit.

(7.3) Voorbeeld. Laat $f : G \to G'$ een homomorfisme van groepen zijn. Dan is de kern $H = \ker(f) = f^{-1}(\{e'\})$ van f een ondergroep. We beweren dat alle vezels van f nevenklassen zijn. Stel $g_1, g_2 \in G$ hebben hetzelfde beeld: $f(g_1) = f(g_2)$. Dan vinden we

$$f(g_1^{-1}g_2) = e' = f(g_1g_2^{-1}).$$

Dus $g_1^{-1}g_2 \in H$ en $g_1g_2^{-1} \in H$. Dus er zijn elementen $h, h' \in H$ met $g_2 = g_1h$ en $g_1 = h'g_2$. Omgekeerd ieder element van gH en van Hg wordt afgebeeld op $f(g)$ want $f(gh) = f(g)f(h) = f(g)e' = f(g)$ en ook $f(hg) = f(g)$. We zien dus: de vezels van f zijn linkernevenklassen met de extra eigenschap dat het ook rechternevenklassen zijn: $gH = Hg$.

(7.4) Gevolg. *Laat $f : G \to G'$ een homomorfisme zijn met $\ker(f) = H$. Dan geldt voor alle $g \in G$:*

$$f^{-1}(f(g)) = gH = Hg.$$

Schematisch kan men zich de afbeelding zo voorstellen:

g_1H	g_2H	g_3H	$\dots$
$\dots$	$\dots$		
			g_nH

$$\big\downarrow f$$

$$\begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

Als we een volledig stelsel R van representanten van de linkernevenklassen van H in G kiezen (d.w.z. uit iedere nevenklasse precies één element) kunnen we schrijven

$$G = \bigsqcup_{g \in R} gH \qquad \text{(disjuncte vereniging)} \tag{1}$$

(7.5) Definitie. De *index* van een ondergroep H in een groep G is de cardinaliteit van een volledig stelsel van representanten van de linkernevenklassen van H in G. Notatie: $[G : H]$.

Als H eindig veel linkernevenklassen heeft dan is $[G : H]$ gewoon het aantal linkernevenklassen.

(7.6) Voorbeelden.

i) De ondergroep $H = \langle (2\,3) \rangle$ van S_3 heeft index $[G:H] = 3$.
ii) De ondergroep $H = n\mathbb{Z}$ van $\mathbb{Z}$ heeft index n.
iii) A_n heeft index 2 in S_n voor $n \geq 2$.
iv) De ondergroep $\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$ van $\mathrm{SL}_2(\mathbb{Z})$ heeft index ∞.

(7.7) Stelling. *(*Lagrange*) Laat G een eindige groep zijn en H een ondergroep van G. Dan geldt*

$$\#G = [G:H]\,\#H.$$

Bewijs. De groep G wordt opgedeeld in disjuncte linkernevenklassen gH als in (1) waarbij g een volledig stelsel representanten R doorloopt. Iedere nevenklasse bevat $\#H$ elementen, dus $\#G = (\#R)\,(\#H)$ en per definitie $\#R = [G:H]$.

Hieruit volgen direct de volgende nuttige delingseigenschappen:

(7.8) Gevolg. *Laat G een eindige groep zijn.*
i) De orde $\#H$ van een ondergroep deelt de orde $\#G$ van G.
ii) De orde van een element $x \in G$ deelt de orde $\#G$ van G.

(7.9) Gevolg. *Iedere eindige groep met als orde een priemgetal p is isomorf met $\mathbb{Z}/p\mathbb{Z}$.*

Bewijs. Noteer de groep met G en kies een element $g \in G$ verschillend van het eenheidselement. Dan is de orde van g niet gelijk aan 1 en een deler van $\#G = p$, dus gelijk aan p. De ondergroep $\langle g \rangle$ is isomorf met $\mathbb{Z}/p\mathbb{Z}$ en gelijk aan G. Daarmee is de isomorfie bewezen.

(7.10) Gevolg. *(Kleine Stelling van Fermat**) Laat p een priemgetal zijn en $a \in \mathbb{Z}$ een getal dat niet door p deelbaar is. Dan geldt:*

$$a^{p-1} \equiv 1 (\bmod p).$$

Bewijs. Beschouw de groep $(\mathbb{Z}/p\mathbb{Z})^*$. Omdat a niet deelbaar is door p is $\bar{a}$ een element van $(\mathbb{Z}/p\mathbb{Z})^*$. Maar nu deelt volgens (7.8) de orde van $\bar{a}$ de orde $p-1$ van $(\mathbb{Z}/p\mathbb{Z})^*$.

(7.11) Gevolg. *Voor elk priemgetal p en voor elke $a \in \mathbb{Z}$ geldt $a^p \equiv a (\bmod p)$.*

Bewijs. Als p geen deler is van a dan volgt door vermenigvuldigen van $a^{p-1} \equiv 1 (\bmod p)$ met a dat $a^p \equiv a (\bmod p)$. Als p het getal a wel deelt geldt $a^p \equiv 0 \equiv a (\bmod p)$.

Opgave. Laat n een positief geheel getal zijn en a een geheel getal met $\mathrm{ggd}(a,n) = 1$. Bewijs dat geldt

$$a^{\phi(n)} \equiv 1 (\bmod n).$$

met $\phi(n)$ de Euler-phi functie.

Met de nu opgedane kennis kunnen we al een aantal groepen van kleine orde thuisbrengen. Bijvoorbeeld, een groep van orde $n \leq 5$ is isomorf met een groep $\mathbb{Z}/n\mathbb{Z}$ of met V_4, de viergroep van Klein. Immers, voor $n = 2, 3$ en 5 volgt dit direct uit (7.9). Stel nu dat G een groep van orde 4 is. De orde van een element $g \neq e$ is een deler van 4, dus gelijk aan 2 of 4. Maar als de orde van g gelijk is aan 4 dan $\langle g \rangle = G$, dus $G \cong \mathbb{Z}/4\mathbb{Z}$.

** P. de Fermat, Frans wiskundige en jurist, 1601–1665

Als dat niet zo is, dan bezit G drie elementen van orde 2, zeg a, b, c. Het product ab kan niet gelijk zijn e (want anders $a = b$), noch aan a (want anders $b = e$) of b. Dus $ab = c$. Zo ziet men ook in dat $ba = c$, en verder dat $ac = ca = b$ en $bc = cb = a$. Dus de vermenigvuldigingstabel van de groep is die van V_4.

Opgaven

1) Laat G een abelse groep zijn en laat $x, y \in G$ elementen van eindige orde zijn. Laat zien dat de orde van xy een deler is van het $\mathrm{kgv}((\mathrm{orde}(x), \mathrm{orde}(y))$.

2) Laat H een ondergroep van de groep G zijn en laat R een volledig stelsel van representanten voor de linkernevenklassen van H zijn. Laat zien dat $\{r^{-1} : r \in R\}$ een volledig stelsel representanten voor de rechternevenklassen van H is. Concludeer dat het aantal nevenklassen gelijk is aan het aantal rechternevenklassen.

3) Bewijs dat de quaterniongroep niet isomorf is met D_4. Bewijs verder dat $S_4 \ncong D_{12}$ en $A_4 \ncong S_3 \times \mathbb{Z}/2\mathbb{Z}$.

4) Stel H is een ondergroep van index 2 in G. Bewijs dat $gH = Hg$ voor alle $g \in G$.

5) Laat k, n positieve getallen zijn met $k \leq n$. Bereken de index van de ondergroep H van permutaties die de deelverzameling $\{1, 2, \ldots, k\}$ op zichzelf afbeelden.

6) Laat H_1, H_2 twee ondergroepen van een eindige groep G zijn met $H_2 \subseteq H_1$. Bewijs de volgende formule

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

Construeer een stelsel representanten voor de linkernevenklassen van H_2 in G wanneer representanten van de linkernevenklassen van H_1 in G en van H_2 in H_1 gegeven zijn.

7) Laat $f : G \to G'$ een homomorfisme van eindige groepen zijn. Bewijs: $\#G = \#\ker(f) \cdot \#f(G)$.

8) Zij G een groep. Laat zien dat de verzameling $\{f : G \to G : \; f \text{ is een automorfisme}\}$ een ondergroep van $S(G)$ is. Deze groep heet de *automorfismengroep* van G. Notatie: $\mathrm{Aut}(G)$.

9) Bewijs dat $a^{13} \equiv a \pmod{35}$ voor alle $a \in \mathbb{Z}$.

10) Laat $f : G \to G'$ een homomorfisme zijn en laat $K = \ker(f)$. Voor een ondergroep H van G geldt

$$f^{-1}(f(H)) = HK = \{hk : h \in H, k \in K\}.$$

Bewijs dit. **11)** Laat p een priemgetal zijn en q een priemfactor van $2^p - 1$. Bewijs dat p een deler is van $q - 1$. Concludeer dat er oneindig veel priemgetallen zijn.

8. Werkingen van groepen

Die Gruppentheorie wirft somit nach allen Seiten neues Licht
S. Lie*

Een en dezelfde groep kan in heel verschillende situaties optreden als symmetriegroep. We spreken dan van een werking van een groep op een verzameling in de volgende zin.

(8.1) Definitie. Laat G een groep zijn en X een verzameling. We zeggen dat G werkt op X als er een afbeelding

$$G \times X \longrightarrow X, \qquad (g, x) \mapsto g \circ x$$

gegeven is die voldoet aan
(W1) $e \circ x = x$ voor alle $x \in X$.
(W2) $(gh) \circ x = g \circ (h \circ x)$ voor alle $g, h \in G$ en $x \in X$.

In de praktijk schrijven we meestal gx voor $g \circ x$. Uit de axioma's W1 en W2 volgt dat de afbeelding $X \to X$, $x \mapsto gx$ een bijectie is: de inverse afbeelding is $X \to X$, $x \mapsto g^{-1}x$ want $g^{-1}g \circ (x) = e \circ x = x$. We vinden dus een afbeelding

$$G \longrightarrow S(X)$$

door aan g de bijectie toe te voegen die g definieert. Axioma W2 zegt dat dit een homomorfisme is. Een alternatieve definitie van een werking is dus

(8.1a) Definitie. Een werking van een groep G op een verzameling X is een homomorfisme $\mu : G \to S(X)$.

Immers, uit $\mu(e) = 1_X$ volgt W1 en verder geldt $\mu(gh) = \mu(g)\mu(h)$ en dat is precies W2.

In het hoofdstuk over symmetriegroepen vinden we een aantal voorbeelden. Bijvoorbeeld de diëdergroep D_n die werkt op de regelmatige n-hoek. Verdere voorbeelden:

(8.2) Voorbeelden.
1) Laat $X = \{1, 2, \ldots, n\}$. Dan werkt S_n op X via $\sigma \circ x = \sigma(x)$.
2) Iedere groep G werkt op zichzelf (dus $X = G$) via linksvermenigvuldiging: $g \circ x = gx$ voor alle $g, x \in G$.
3) Iedere groep G werkt ook op zichzelf via $g \circ x = gxg^{-1}$. Deze werking heet *conjugatie.*
4) Zij H een ondergroep van de groep G. Dan werkt G op de verzameling G/H van linkernevenklassen via

$$g \circ (aH) = gaH \qquad \text{voor alle } g, a \in G.$$

We moeten nagaan dat dit niet van de keuze van de representant a van de linkernevenklasse afhangt. Als a' een element is met $aH = a'H$ dan geldt $a^{-1}a' \in H$. Dus $(ga)^{-1}(ga') \in H$ en dus $gaH = ga'H$.

* Sophus Lie, Noors wiskundige, 1842–1899

(8.3) Voorbeeld. Laat $G = SL_2(\mathbb{R})$ en $X = \mathcal{H} = \{z = x + i\,y \in \mathbb{C} : y > 0\}$, het *bovenhalfvlak* van het complexe vlak. De groep $SL_2(\mathbb{R})$ werkt op $\mathcal{H}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ z = \frac{az+b}{cz+d}.$$

Het imaginaire gedeelte van $(az+b)/(cz+d)$ is $y/|cz+d|^2$ en is weer positief. Aan W1 is ten duidelijkste voldaan. De verificatie van axioma W2 is een kleine berekening die we aan de lezer overlaten.

Een werking van groep G op een verzameling X definieert een equivalentierelatie op X met

$$x \sim y \iff \text{er is een } g \in G \text{ met } gx = y.$$

De equivalentieklassen heten banen:

(8.4) Definitie. Laat G een groep zijn die werkt op een verzameling X. Als x een punt is van X dan heet

$$Gx = \{gx : g \in G\}$$

de *baan* van x. De *stabilisator* (of *isotropiegroep*) van x is de ondergroep

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

Het aantal elementen van de baan heet de *lengte* van de baan. Als er precies één baan is dan heet de werking *transitief.*

Een werking is transitief dan en slechts dan als voor elk paar punten $x, x' \in X$ er een $g \in G$ is met $gx = x'$.

Opgave. Ga na dat de genoemde equivalentierelatie een equivalentierelatie is. Concludeer dat verschillende banen disjunct zijn en dat X een vereniging is van disjuncte banen.

(8.5) Voorbeelden.

i) De werking van S_n op $X = \{1, 2, \ldots, n\}$ is transitief want $(1\,x)$ voert 1 in x over, dus de baan van 1 is geheel X. De stabilisator van x is de verzameling

$$\{\sigma \in S_n : \sigma(x) = x\}$$

een ondergroep van orde $(n-1)!$.

2) De werking van G op zichzelf via linkstranslatie is transitief. De stabilisator van een element is $\{e\}$.

3) De werking van G op zichzelf door conjugatie is belangrijk omdat we er veel van kunnen leren over de structuur van G. De banen heten *conjugatieklassen* en zijn van de vorm

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

De stabilisatorgroep van een element $x \in G$ heet hier *centralisator*, genoteerd met C_x, en bestaat uit alle elementen van G die met x commuteren

$$C_x = \{g \in G : gx = xg\}.$$

4) De werking van $SL_2(\mathbb{R})$ op het bovenhalfvlak $\mathcal{H}$ is transitief. (Ga dit na!) De stabilisator K van i is de ondergroep

$$G_i = K = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 = 1\}.$$

De werking van de ondergroep $SL_2(\mathbb{Z})$ op $\mathcal{H}$ is niet transitief. De stabilisator van $i = \sqrt{-1}$ is de ondergroep van orde 4

$$\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\}.$$

(8.6) Propositie. *Als G op X werkt dan levert de afbeelding $g \mapsto gx$ een bijectie*

$$G/G_x \longleftrightarrow Gx.$$

tussen de linkernevenklassen van G_x en de punten van de baan van x en dus $\#Gx = [G : G_x]$.

Bewijs. We weten

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

Hieruit volgt de injectiviteit. De surjectiviteit is duidelijk. Dit bewijst de bewering.

Als we dit toepassen op voorbeeld (8.3) en (8.5) 4) vinden we interpretatie van het bovenhalfvlak

$$SL_2(\mathbb{R})/K \longleftrightarrow \mathcal{H}$$

als verzameling van linkernevenklassen.

De stabilisatoren van punten uit een baan zijn geconjugeerde ondergroepen:

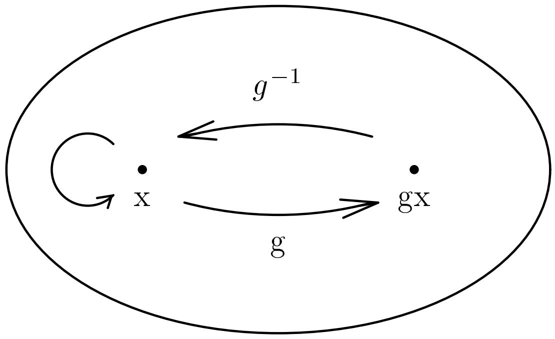
(8.7) Lemma. *Laat G een groep zijn die op een verzameling X werkt. Dan geldt*

$$G_{gx} = gG_xg^{-1}.$$

Bewijs. Er geldt

$$h \in G_{gx} \Longleftrightarrow h \circ gx = gx \Longleftrightarrow g^{-1}hgx = x \Longleftrightarrow g^{-1}hg \in G_x \Longleftrightarrow h \in gG_xg^{-1}$$

waaruit de bewering volgt.



Als $R \subset X$ een deelverzameling is van X die uit iedere baan precies één punt bevat (d.w.z. R is een volledig stelsel representanten) dan kunnen we schrijven

$$X = \bigsqcup_{x \in R} Gx$$

en we zien zo in dat

$$\#X = \sum_{x \in R} [G : G_x].$$

Dit kunnen we in het bijzonder toepassen op de conjugatiewerking van een groep op zichzelf:

$$\#G = \sum_{x \in R} [G : C_x]. \qquad \text{(klassenformule)}$$

(8.8) Definitie. Een punt $x \in X$ met $Gx = \{x\}$ onder een werking van G heet een *vast punt* of *dekpunt*. De verzameling vaste punten wordt genoteerd met X^G.

(8.9) Propositie. *Laat p een priemgetal zijn en G een groep waarvan de orde een macht van p is. Als G op een verzameling X werkt dan geldt de congruentie*

$$\#X^G \equiv \#X \pmod{p}.$$

Bewijs. De verzameling X is disjuncte vereniging van banen. De lengte van een baan Gx is gelijk aan $[G : G_x]$ en vanwege de Stelling van Lagrange een deler van $\#G$. Dus de lengte van een baan is 1 of is deelbaar door p. De lengte van een baan is 1 dan en slechts dan als $Gx = \{x\}$, d.w.z. $x \in X^G$. Dit bewijst de bewering.

Met behulp van deze propositie kunnen we een belangrijk resultaat van Cauchy* bewijzen.

* Augustin-Louis Cauchy, Frans wiskundige, 1789–1857

(8.10) Stelling. *(Cauchy) Laat G een eindige groep zijn en p een priemgetal dat de orde van G deelt. Dan bevat G een element van orde p.*

Bewijs. Laat X de verzameling zijn gegeven door

$$\{(g_1, g_2, \ldots, g_p) \in G \times \ldots \times G : g_1 g_2 \cdots g_p = e\}.$$

Deze verzameling heeft cardinaliteit $(\#G)^{p-1}$; we kunnen de eerste $p-1$ coordinaten vrij kiezen, waarna de laatste dan eenduidig vast ligt.

De groep $\Gamma = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ werkt op X door cyclisch verwisselen:

$$a \circ (g_1, g_2, \ldots, g_p) = (g_{1+a}, g_{2+a}, \ldots, g_{p+a}).$$

Hierbij worden de indices modulo p genomen. Merk op dat het product van de g_{i+a} weer gelijk is aan e. (Laat $x = g_1 g_2 \cdots g_a$ en $y = g_{a+1} \cdots g_p$ dan weten we dat $xy = e$ zodat ook $g_{1+a} g_{2+a} \cdots g_{p+a} = yx = e$.) Uit (8.9) weten we nu dat $\#X \equiv \#X^\Gamma (\operatorname{mod} p)$ en omdat $p | \#X$ volgt dat p een deler is van $\#X^\Gamma$. Maar X^Γ is niet leeg, want het element $(e, e, \ldots, e)$ zit erin. Dus moeten er nog meer elementen in X^Γ zitten. Voor een element van X^Γ zijn alle coordinaten gelijk: $g_1 = g_2 = \ldots = g_p$. Als $(g, \ldots, g) \in X$ dan volgt uit de conditie dat het product van de coordinaten gelijk is aan e dat $g^p = e$. Als $g \neq e$ dan impliceert dit dat g orde p heeft. Daarmee is de stelling bewezen.

(8.11) Opmerking. De definitie van werking die we hebben gegeven heet eigenlijk een *linkswerking*. Een *rechtwerking* van een groep G op een verzameling X wordt gegeven door een afbeelding $G \times X \to X$, $(g, x) \mapsto g \circ x$ die voldoet aan

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

Merk op dat de volgorde in ii) hier anders is dan in Definitie (8.1). Omdat de omkering van de volgorde notationeel onhandig is, schrijven we vaak $(g, x) \mapsto x \circ g$ voor de werking. Het tweede axioma wordt dan

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

Zie Opgave 11 voor het verband.

Opgaven

1) Laat G een eindige groep zijn en p een priemgetal dat $\#G$ deelt. Zij h het aantal ondergroepen van G van orde p. Bewijs: er zijn $h(p-1)$ elementen van orde p in G. Bewijs verder $h \equiv 1 (\operatorname{mod} p)$.

2) Laat G een groep van orde 6 zijn. Bewijs: G bezit 1 of 3 elementen van orde 2. Bewijs verder: $G \cong \mathbb{Z}/6\mathbb{Z}$ of $G \cong S_3$.

3) Laat H een ondergroep zijn van een groep G. Bewijs: $[G : H] = [G : gHg^{-1}]$ voor alle $g \in G$.

4) Laat zien dat de banen van S_n onder de conjugatiewerking op zichzelf $1-1$ corresponderen met de cykeltypen.

5) Bewijs de volgende bewering. Onder de conjugatiewerking van de diëdergroep D_n op zichzelf is het aantal conjugatieklassen van de spiegelingen

$$\begin{cases} 1 & \text{als } n \text{ oneven,} \\ 2 & \text{als } n \text{ even.} \end{cases}$$

6) Bewijs de volgende bewering. Een groep G heeft precies twee ondergroepen $\Longleftrightarrow$ G is eindig en de orde van G is een priemgetal.

7) Laat X een eindige verzameling zijn met een werking van een eindige groep G. Noteer voor $g \in G$ het aantal vaste punten met $x(g) = \#\{x \in X : g(x) = x\}$. Bewijs de volgende *formule van Burnside:**

$$\text{het aantal banen} = \frac{1}{\#G} \sum_{g \in G} x(g).$$

8) Op hoeveel manieren kan men de zijvlakken van een kubus kleuren met zes verschillende kleuren, waarbij verschillende zijvlakken verschillende kleuren hebben en waarbij twee kleuringen als dezelfde worden beschouwd als zij door een rotatie van de kubus in elkaar overgaan?

9) Laat G een groep zijn van orde p^m met p een priemgetal en $m \in \mathbb{Z}_{\geq 1}$. Bewijs dat het centrum van G groter is dan $\{e\}$.

10) De kubus van Rubik. Zij R een kubus van Rubik. Hier hoort een groep bij, de groep G_R van alle zetten die je kunt uitvoeren met deze kubus. Overtuig jezelf daarvan. Bewijs dat de orde van deze groep een deler is van $12! \cdot 2^{12} \cdot 8! \cdot 3^8$. De orde van deze groep is 43252003274489856000.

11) Laat G een groep zijn met een linkswerking op een verzameling X geschreven als $(g, x) \mapsto g \circ x$. Laat zien dat $(g, x) \mapsto g^{-1} \circ x$ een rechtswerking van G op X definieert.

---

* W. Burnside, Engels wiskundige, 1852–1927. Publiceerde een belangrijk boek over groepentheorie *The theory of groups of finite order* (1897)

9. Normaaldelers en quotientgroepen

Die grössten und fruchtbarsten Fortschritte in der Mathematik sind vorzugsweise durch die Schöpfung neuer Begriffe gemacht, nachdem die häufige Wiederkehr zusammengesetzer Erscheinungen dazu gedrängt hat.
R. Dedekind*.

Zoals we in het vorige hoofdstuk zagen hoeven linker- en rechternevenklassen van een ondergroep H in een groep G niet samen te vallen. Wanneer dat wel het geval is spreken we van een normaaldeler.

(9.1) Definitie-Stelling. *Een ondergroep H van een groep G heet een* normaaldeler *als aan één van de volgende drie equivalente eigenschappen voldaan is:*
i) $ghg^{-1} \in H$ *voor alle* $g \in G$ *en* $h \in H$.
ii) $gHg^{-1} = H$ *voor alle* $g \in G$.
iii) $gH = Hg$ *voor alle* $g \in G$.

Bewijs. We moeten laten zien dat de drie condities equivalent zijn. Als een ondergroep voldoet aan een van de drie, dan ook aan alle drie.

i) $\Longrightarrow$ ii). Uit $ghg^{-1} \in H$ volgt

$$gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H.$$

Nogmaals toepassen van i) met g^{-1} in plaats van g levert $g^{-1}Hg \subseteq H$, dus $H = gg^{-1}Hgg^{-1} \subset gHg^{-1}$. Dit bewijst ii). Uit ii), d.w.z. uit

$$\{ghg^{-1} : h \in H\} = \{h : h \in H\}$$

volgt door vermenigvuldiging van rechts met g dat

$$\{gh : h \in H\} = \{hg : h \in H\},$$

d.w.z. $gH = Hg$, dus iii). Uit iii) tenslotte volgt dat iedere uitdrukking gh te schrijven is als $h'g$ voor een zekere $h' \in H$ (die van h afhangt). Vermenigvuldiging van rechts met g^{-1} levert $ghg^{-1} = h' \in H$, dus is aan i) voldaan zoals gewenst. Dit beeindigt het bewijs.

We schrijven soms $N \triangleleft G$ om aan te geven dat N een normaaldeler van G is.

(9.2) Voorbeeld. Laat $f : G \to G'$ een homomorfisme zijn. Dan is de kern van $H = \ker(f)$ een normaaldeler van G. Immers, als $h \in \ker(f)$ dan geldt

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)\, e\, f(g)^{-1} = e'$$

en dus $ghg^{-1} \in H$ voor alle $g \in G$. Dit is het belangrijkste voorbeeld. We zullen later zien dat alle normaaldelers kernen van homomorfismen zijn.

(9.3) Voorbeeld. In iedere groep zijn de triviale ondergroep $H = \{e\}$ en de hele groep $H = G$ normaaldelers. In een commutatieve groep zijn alle ondergroepen normaaldelers.

---

* R. Dedekind, Duits wiskundige, 1831–1916

(9.4) Voorbeeld. Laat G een groep zijn. Het *centrum* van G is de ondergroep

$$Z(G) = \{h \in G : gh = hg \text{ voor alle } g \in G\}.$$

Het centrum is een normaaldeler want voor $h \in Z(G)$ geldt $ghg^{-1} = h \in H$.

(9.5) Voorbeeld.

i) Laat G een groep zijn. De *commutatorondergroep* $[G, G]$ van G is de ondergroep van G voortgebracht door de zgn. *commutatoren*

$$[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$$

met $g_1, g_2 \in G$. Als nu $h \in [G, G]$ dan kunnen we schrijven

$$ghg^{-1} = ghg^{-1}h^{-1}\, h = [g, h]\, h \in H,$$

waaruit volgt dat $gsg^{-1} \in [G, G]$ voor alle voortbrengers s van $[G, G]$. Maar dan geldt ook $g[G, G]g^{-1} \subset [G, G]$, dus de commutatorondergroep is een normaaldeler van G.

ii) Een ondergroep H van G van index 2 is een normaaldeler. De twee linkernevenklassen zijn H en het complement $G - H$. Evenzo: de rechternevenklassen zijn H en $G - H$, dus vallen linker- en rechternevenklassen samen.

(9.6) Constructie van de Quotiënt- of Factorgroep. Een eenvoudig voorbeeld van een normaaldeler N is de ondergroep $n\,\mathbb{Z}$ van $\mathbb{Z}$. De verzameling nevenklassen $\mathbb{Z}/n\mathbb{Z}$ is dan zelf weer een groep en onze ondergroep N is de kern van het homomorfisme $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \bar{x}$. Dit is een speciaal geval van een algemeen patroon: als N een normaaldeler is van een groep G dan kunnen we van de verzameling nevenklassen G/N een groep maken zodat de afbeelding $g \mapsto gN$ een homomorfisme is met kern N. Deze uiterst belangrijke constructie gaan we nu uitvoeren.

Laat G een groep zijn met normaaldeler N We definiëren nu een bewerking op de verzameling G/N van nevenklassen via:

$$g_1 N \circ g_2 N = g_1 g_2 N.$$

Als we in plaats van gN de uitdrukking $\bar{g}$ schrijven dan wordt de analogie met $\mathbb{Z}/n\mathbb{Z}$ nog duidelijker. De bewerking is dan gewoon $\overline{g}_1 \circ \overline{g}_2 = \overline{g_1 g_2}$.

We moeten nagaan dat dit goed gedefinieerd is, d.w.z. dat dit niet afhangt van de gekozen representanten g_1 en g_2. Een andere representant van $g_1 N$ is van de vorm $g_1 n_1$ met $n_1 \in N$; laat $g_2 n_2$ ook een andere representant zijn van $g_2 N$ met $n_2 \in N$. Dan vinden we

$$g_1 n_1\, g_2 n_2 N = g_1 g_2\, \underbrace{g_2^{-1} n_1 g_2}_{=m}\, n_2 N = g_1 g_2 m n_2 N = g_1 g_2 N$$

waarbij we gebruiken dat ${g_2}^{-1} n_1 g_2 \in {g_2}^{-1} N g_2 = N$, dus zeg ${g_2}^{-1} n g_2 = m \in N$. Verder gebruiken we dat

$$m n_2 N = \{m n_2 n : n \in N\} = N.$$

want vermenigvuldiging met $m n_2$ levert alleen een permutatie van de elementen van N. Daarmee is de bewerking goed gedefinieerd.

Een andere, maar gelijkwaardige, manier om de bewerking te definiëren is door het product $g_1N \circ g_2N$ gelijk te stellen aan de verzameling

$$g_1Ng_2N = \{g_1n_1g_2n_2 : n_1, n_2 \in N\}.$$

Omdat N normaaldeler is geldt $Ng_2 = g_2N$ dus

$$g_1Ng_2N = g_1g_2NN = g_1g_2N$$

waarmee we zien dat dit hetzelfde oplevert en het is direct duidelijk dat de bewerking goed gedefinieerd is.

Deze constructie levert een groep zoals O. Hölder* in 1889 expliciet liet zien; impliciet kwam deze constructie al voor in het werk van Jordan (1875).

(9.7) Stelling. *Met de bewerking $g_1N \circ g_2N = g_1g_2N$ wordt G/N een groep. De afbeelding*

$$\phi : G \longrightarrow G/N, \qquad g \mapsto gN$$

is een surjectief homomorfisme met kern N.

Bewijs. De associativiteit volgt uit die van G:

$$(g_1N \circ g_2N) \circ g_3N = g_1g_2N \circ g_3N = (g_1g_2)g_3N = g_1(g_2g_3)N = g_1N \circ (g_2N \circ g_3N).$$

Het eenheidselement van G/N is $eN = N$. De inverse van gN is $g^{-1}N$. Uit de definitie van de bewerking volgt direct dat ϕ een surjectief homomorfisme is.

De kern van ϕ bestaat uit die nevenklassen met $gN = eN = N$. Maar $gN = N \iff g \in N$, dus $\ker(\phi) = N$. Dit bewijst (9.7).

Deze groep G/N heet de *quotiëntgroep* of *factorgroep* en ook wel G modulo N. De orde van deze groep is $[G : N]$. De afbeelding

$$\phi : G \longrightarrow G/N, \qquad g \mapsto gN$$

heet de *kanonieke afbeelding* en is een homomorfisme vanwege de definitie van de bewerking. De vorming van G/N wordt ook wel 'uitdelen naar N' genoemd.

(9.8) Voorbeelden.

i) Met $G = \mathbb{Z}$ en $N = n\mathbb{Z}$ vinden we $\mathbb{Z}/n\mathbb{Z}$ zoals al aangegeven.

ii) Zij $G = S_n$ en $N = A_n$. Er zijn twee nevenklassen. De groep S_n/A_n is isomorf met de groep $\{\pm 1\}$ waarbij A_n correspondeert met $+1$ en $S_n - A_n$ met -1.

iii) Laat Q de quaterniongroep van orde 8 zijn. Het centrum van Q is de ondergroep $N = \{\pm 1\}$. Dit is een normaaldeler. De vier nevenklassen zijn

$$e = \{\pm 1\},\ a = \{\pm i\},\ b = \{\pm j\},\ c = \{\pm k\}.$$

Om het product van, zeg, $\{\pm i\}$ en $\{\pm j\}$ uit te rekenen moeten we representanten nemen en met elkaar vermenigvuldigen. Representanten zijn i en j en dus

$$\{\pm i\} \circ \{\pm j\} = \{\pm k\}, \qquad \text{dus } ab = c.$$

* O. Hölder, Duits wiskundige, 1859–1937

Zo ook $bc = a$ etc. We zien dat Q/N isomorf is met de Viergroep van Klein. In het bijzonder is deze groep abels, terwijl Q dat niet was.

iv) Laat $G = \mathbb{R}^*$ en $N = \mathbb{R}^*_{>0}$. Er zijn twee nevenklassen $\mathbb{R}^*_{>0}$ en $\mathbb{R}^*_{<0}$. Er geldt

$$\mathbb{R}^*_{<0} \circ \mathbb{R}^*_{<0} = \mathbb{R}^*_{>0}$$

omdat het product van twee negatieve reële getallen positief is.

v) Laat $N = \mathbb{Z}$ en $G = \mathbb{R}$. Representanten van de nevenklassen van $\mathbb{Z}$ in $\mathbb{R}$ worden gegeven door de getallen van het half-open interval $[0, 1)]$. De optelling is de optelling modulo 1 (dus 1 aftrekken als $x + y \geq 1$).

Het nut van deze constructie is dat de quotiëntgroep G/N vaak eenvoudiger is dan de oorspronkelijke groep G. Daarmee kunnen we dan informatie inwinnen over G. We geven een voorbeeld.

(9.9) Stelling. *Laat G een groep zijn met centrum $Z(G)$ zodat $G/Z(G)$ cyklisch is. Dan is G abels.*

Bewijs. We schrijven $Z = Z(G)$. Laat de nevenklasse gZ de voortbrenger van G/Z zijn. Dan is iedere nevenklasse van de vorm $g^i Z$ en dus is ieder element van G te schrijven als $g^i z$ met $z \in Z$. Laat nu $a = g^i z$ en $b = g^j z'$. Dan geldt

$$ab = g^i z g^j z' = g^i g^j z z' = g^{i+j} z z' = g^j z' g^i z = ba,$$

waarbij we gebruiken dat z, z' in het centrum liggen en dus met ieder element commuteren. Dus is G abels.

De volgende stelling beschrijft de ondergroepen van een quotiëntgroep G/N in termen van die van G.

(9.10) Stelling. *Laat G een groep zijn en N een normaaldeler van G. De ondergroepen van G/N zijn precies de ondergroepen*

$$H/N = \{hN : \quad h \in H\},$$

waar H een ondergroep is van G. Er is een bijectie tussen de ondergroepen van G/N en de ondergroepen van G die N omvatten.

Bewijs. Als H een ondergroep van G is $H/N = \{hN : h \in H\}$ een ondergroep van G/N. Dit is eenvoudig te controleren. Omgekeerd, als H' een ondergroep van G/N is dan bekijken we

$$\phi^{-1}(H') = \{h \in G : \phi(h) \in H'\} = \{h \in G : hN \in H'\}$$

waarbij $\phi : G \to G/N$ de kanonieke afbeelding is. Dit is een ondergroep van G die N bevat. Maar dan geldt $H' = \{gN : g \in \phi^{-1}(H')\}$ zoals verlangd.

De afbeelding $H \mapsto \phi(N)$ met inverse $H' \mapsto \phi^{-1}(H')$ geeft de gevraagde bijectie. Daarmee is het bewijs klaar.

We gaan nu na wanneer de quotiëntgroep G/N een abelse groep is.

(9.11) Stelling. *Laat G een groep zijn en N een normaaldeler van G. Dan is G/N abels dan en slechts dan als N de commutatorondergroep $[G,G]$ bevat.*

Bewijs. Met de schrijfwijze $\bar{g} = gN$ moeten we nagaan wanneer $\overline{gh} = \overline{hg}$, d.w.z. wanneer $\overline{ghg^{-1}h^{-1}} = \bar{e}$. Maar dit is het geval voor alle $g, h \in G$ dan en slechts dan als $ghg^{-1}h^{-1} \in N$ voor alle $g, h \in G$. Dus G/N is commutatief dan en slechts en dan als N de voortbrengers van $[G,G]$ bevat, d.w.z. N bevat $[G,G]$. Dit bewijst de stelling.

We zien uit bovenstaande stelling dat de 'minimale' manier om een abels quotiënt van G te krijgen is uitdelen naar de commutatorondergroep $[G,G]$. De quotiëntgroep $G/[G,G]$ heet de "abelse gemaakte" G en wordt genoteerd met G_{ab}.

We geven tenslotte een criterium waarmee je kunt inzien dat sommige ondergroepen een normaaldeler zijn.

(9.12) Propositie. *Laat G een eindige groep zijn en laat p de kleinste priem zijn die de orde van G deelt. Een ondergroep H van G met index $[G : H] = p$ is een normaaldeler.*

Bewijs. De groep G werkt op de verzameling $X = G/H$ van linkernevenklassen van H in G via

$$G/H \xrightarrow{\lambda_a} G/H, \qquad gH \mapsto agH.$$

Dit geeft een afbeelding $j : G \to S(X)$ via $a \mapsto \lambda_a$. Het beeld $j(G)$ van j is een ondergroep van $S(X)$, dus de orde $\#j(G)$ deelt $\#S(X) = p!$. Anderzijds deelt $j(G)$ ook de orde van G wegens $\#G = (\#j(G))\cdot(\#\ker(j))$, vergelijk (7.4). Maar $\mathrm{ggd}(p!, \#G) = p$, dus $\#j(G) = p$. Merk op dat $\#j(G) \neq 1$ want $G \neq H$. Omdat de kern van j de ondergroep H bevat is $\#j(G) \leq p$, dus $\ker(j) = H$. Daarmee is bewezen dat H een normaaldeler is.

Opgaven

1) Laat zien dat een groep G abels is dan en slechts dan als $Z(G) = G$ dan en slechts dan als $[G,G] = \{e\}$. Bereken het centrum van de quaterniongroep en van de diëdergroep D_n.

2) Bewijs dat de commutatorondergroep van de diëdergroep D_n wordt voortgebracht door r^2 met $r \in D_n$ een rotatie van orde n. Wat is $(D_n)_{\mathrm{ab}}$?

3) Laat $H = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subset S_4$. Laat zien dat dit een normaaldeler is van S_4. Bewijs dat H isomorf is met de Viergroep V_4 van Klein. Wat is S_4/H?

4) Laat G een groep zijn met normaaldelers M en N met $M \cap N = \{e\}$. Laat zien dat voor elke $m \in M$ en $n \in N$ geldt $mn = nm$. Als G voortgebracht wordt door $M \cup N$ dan geldt $G \cong M \times N$. Bewijs dit.

5) Bewijs dat iedere ondergroep van de quaterniongroep een normaaldeler is.

6) Geef een voorbeeld van een groep G met normaaldelers M en N zodat $M \cong N$ maar $G/M \not\cong G/N$.

7) Laat G een abelse groep zijn. Laat zien dat

$$T(G) = \{g \in G : \text{de orde van } g \text{ is eindig } \}$$

een ondergroep van G is. Deze ondergroep heet de *torsiegroep* van G. Laat verder zien dat in $G/T(G)$ alleen het eenheidselement eindige orde heeft.

8) Bepaal de torsiegroep van de volgende groepen: $\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}^*$.

9) Laat zien dat S_n en $A_n \times \mathbb{Z}/2\mathbb{Z}$ niet isomorf zijn voor $n \geq 3$.

10) Geef een voorbeeld van een groep G en ondergroepen H, N van G met $H \subset N \subset G$, waarbij N een normaaldeler is van G, H een normaaldeler is van N maar H geen normaaldeler is van G.

11) We noemen een ondergroep H van een groep G *karakteristiek* als $\alpha(H) = H$ voor elk automorfisme α van G . Bewijs dat een karakteristieke ondergroep een normaaldeler is. Geef een voorbeeld van een normaaldeler die niet karakteristiek is.

12) Zij $f : G \to A$ een homomorfisme van een groep G naar een abelse groep. Bewijs dat $\ker(f)$ de commutatorondergroep van G bevat.

13) Laat zien dat $[A_3, A_3] = \{(1)\}$ en $[A_4, A_4] = V_4$. Bewijs verder $[S_n, S_n] = A_n$. (zie Opgave (6.17)).

14) Bewijs: als $H \subseteq Z(G)$ een ondergroep is van een groep G zodat G/H cyklisch is, dan is G abels.

15) Laat zien dat S_4 precies een ondergroep van index 2 heeft.

16) Zij G een eindige groep van orde $2k$ met k oneven. Laat zien dat G een normaaldeler van orde k bevat.

17) Zij G een eindige groep van oneven orde. Laat N een normaaldeler zijn van orde 17. Bewijs dat N bevat is in het centrum van G.

18) Bewijs dat een groep van orde p^2 met p een priemgetal abels is. (Gebruik Opgave 9 van Hoofdstuk 8.)

10. Isomorfiestellingen

Si l'homme s'érait borné à recueiller des faits, la science
ne serait qu'une nomenclature stérile et jamais
il n'eut connu les grandes lois de la nature
Laplace*

De factorgroep G/N die we in het vorige hoofdstuk geconstrueerd hebben heeft een zogenaamde 'universele' eigenschap die wordt uitgedrukt in de volgende stelling.

(10.1) Homomorfiestelling.** . *Laat $f : G \to G'$ een homomorfisme van een groep G naar een groep G' zijn. Laat N een normaaldeler van G zijn met $N \subseteq \ker(f)$. Dan is er een eenduidig bepaald homomorfisme $h : G/N \longrightarrow G'$ zodat $h(gN) = f(g)$ voor alle $g \in G$.*

Een equivalente manier om de bewering van (9.1) uit te drukken is te zeggen dat er een eenduidig bepaald homomorfisme h is zodat het diagram

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\phi"'] & & G' \\ & G/N \arrow[ur, "h"'] & \end{tikzcd}$$

commuteert, d.w.z. $f = h \circ \phi$. Hierbij is $\phi : G \to G/N$ de kanonieke afbeelding.

Bewijs van (10.1). We definiëren de afbeelding $h : G/N \to G'$ eenvoudig door $h(gN) = f(g)$. We moeten nagaan dat h wel gedefinieerd is, dus dat de waarde niet afhangt van de gekozen representant g. Omdat $f(gn) = f(g)f(n) = f(g)$ voor alle $n \in N$ want $N \subseteq \ker(f)$ volgt dit inderdaad. Dan is h een homomorfisme:

$$h(gNg'N) = h(gg'N) = f(gg') = f(g)f(g') = h(gN)h(g'N).$$

Deze afbeelding voldoet aan $h(gN) = f(g)$ zoals gevraagd. Om in te zien dat h uniek is, merken we op dat h vastligt door de eis dat $h(gN) = f(g)$ voor alle g. Einde bewijs.

We zeggen wel dat het homomorfisme $f : G \to G'$ via G/N factoriseert. De volgende stelling geeft een interpretatie van een homomorfisme.

(10.2) Eerste Isomorfiestelling. *Laat $f : G \to G'$ een homomorfisme van groepen zijn. Dan geldt*

$$G/\ker(f) \cong f(G).$$

Bewijs. We passen Stelling (10.1) toe met $N = \ker(f)$ en vinden een homomorfisme $h : G/\ker(f) \to G'$. Vanwege $h(gN) = f(g)$ voor alle $g \in G$ is het beeld van f gelijk aan dat van h. Laat nu $gN \in \ker(h)$. Dan geldt $h(gN) = f(g) = e'$, dus $g \in \ker(f)$. Dus $gN = N$ en we zien dat $\ker(h) = N$, het eenheidselement van G/N. Daarom is h

---

* Pierre-Simon Laplace, Frans wis- en natuurkundige, 1749–1827

** De formulering van deze en de volgende stelling stamt van Emmy Noether, Duits wiskundige, 1882–1935. Zij speelde een buitengewoon belangrijke rol in de ontwikkeling van de abstracte algebra in de eerste decennia van de twintigste eeuw.

injectief. We concluderen dat h een bijectief homomorfisme levert van $G/\ker(f)$ naar $f(G)$. Dit bewijst (10.2).

Als we dit toepassen op een *surjectief* homomorfisme $f : G \to G'$ vinden we

$$G/\ker(f) \cong G'.$$

(10.3) Voorbeelden.

i) Laat $G = S_n$ en $f = \epsilon : S_n \to \{\pm 1\}$ de tekenafbeelding zijn. Dan krijgen we een isomorfisme
$$S_n/A_n \cong \{\pm 1\}.$$

ii) Laat $G = \mathbb{R}$ en $f : \mathbb{R} \to \mathbb{C}^*$ het homomorfisme zijn gegeven door
$$x \mapsto e^{2\pi i x} = \cos(2\pi x) + i \sin(2\pi x).$$
Het beeld is de cirkel $S^1 = \{z \in \mathbb{C}^* : |z| = 1\}$. De kern van f is de ondergroep $\mathbb{Z}$ van $\mathbb{R}$ en de stelling zegt
$$\mathbb{R}/\mathbb{Z} \cong S^1.$$
We hadden al gezien dat de getallen van het half-open interval $[0, 1)$ een volledig stelsel representanten zijn die we " modulo 1" optellen. Het bovenstaand isomorfisme maakt hiervan nu een cirkel.

We kunnen nu ook (9.11) precizeren als in de volgende propositie.

(10.4) Propositie. *Laat $f : G \to A$ een homomorfisme zijn van een groep G naar een abelse groep A. Dan is er een eenduidig bepaald homomorfisme $h : G_{\mathrm{ab}} = G/[G,G] \to A$ zodat $f = h\phi$, m.a.w. het volgende diagram commuteert.*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\phi"'] & & A \\ & G_{\mathrm{ab}} \arrow[ur, "h"'] & \end{tikzcd}$$

Bewijs. Allereerst is de kern van f een normaaldeler. We verkrijgen een injectief homomorfisme $G/\ker(f) \to f(G) \subseteq A$ en dus is $G/\ker(f)$ een abelse groep. Vanwege stelling (9.11) bevat de kern van f dan $[G, G]$. Stelling (10.1) impliceert nu het resultaat.

We bestuderen nu voor een gegeven normaaldeler N van een groep G het kanonieke homomorfisme
$$\phi : G \longrightarrow G/N.$$
Als $H \subset G$ een ondergroep is dan is het beeld $\phi(H)$ een ondergroep van G/N. Het inverse beeld van $\phi(H)$ is een ondergroep van G die N omvat, zie Stelling (9.10) en dit is
$$HN = \{hn : h \in H, n \in N\}.$$

(10.5) Tweede Isomorfiestelling. *Laat N een normaaldeler van G zijn en $H \subset G$ een ondergroep. Dan is er een isomorfisme*

$$H/(H \cap N) \cong HN/N.$$

Bewijs. We beperken het kanonieke homomorfisme ϕ to H. Dit geeft een homomorfisme $H \to G/N$ met kern $H \cap N$ en beeld HN/N. De eerste isomorfiestelling levert ons nu het gevraagde isomorfisme.

(10.6) Voorbeeld. Laat $G = S_4$ en

$$N = V_4 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Laat $H = \{\sigma : \sigma(1) = 1\} = S_3$ de ondergroep zijn van de elementen die 1 op zijn plaats laten. We vinden dan

$$S_3/(S_3 \cap V_4) \cong S_3V_4/V_4. \qquad (*)$$

Verder is gemakkelijk te zien dat $S_3 \cap V_4 = \{(1)\}$. Dus $(*)$ zegt $S_3 \cong S_3V_4/V_4$. Dit isomorfisme laat zien dat S_3V_4 precies 24 elementen heeft want $\#S_3 = 6$ en $\#V_4 = 4$. Dus geldt

$$S_3V_4 = S_4,$$

omdat allebei cardinaliteit 24 hebben. Dus we kunnen $(*)$ dan lezen als

$$S_3 \xrightarrow{\sim} S_4/V_4.$$

Een meetkundige interpretatie van dit isomorfisme wordt gegeven in opgave 4.

De volgende stelling wijst op een analogie tussen “quotiëntgroep” en quotiënt (in de zin van breuk).

(10.7) Stelling. *Laat N en N' normaaldelers van een groep G zijn met $N \subset N' \subset G$. Iedere normaaldeler van G/N is van de vorm M/N met M een normaaldeler van G met $N \subset M \subset G$. In het bijzonder is N'/N een normaaldeler van G/N en er geldt*

$$(G/N)/(N'/N) \cong G/N'.$$

Bewijs. We hebben al laten zien dat ondergroepen van G/N in 1-1-correspondentie staan met ondergroepen van G die N omvatten. De analoge bewering voor normaaldelers wordt aan de lezer overgelaten.

Om de tweede bewering in te zien bekijken we het kanonieke homomorfisme $\phi' : G \to G/N'$. Omdat N' de normaaldeler N bevat, is er volgens de homomorfiestelling een homomorfisme

$$h : G/N \to G/N' \quad \text{met} \quad h(gN) = \phi'(g) = gN'.$$

Omdat ϕ' surjectief is, is h dat ook. Dus vinden we volgens de isomorfiestelling

$$(G/N)/\ker(h) \cong G/N'.$$

Wat is de kern van h? Wel, het is niet moeilijk in te zien dat geldt

$$\ker(h) = \{gN : g \in N'\} = N'/N.$$

Dit bewijst de stelling.

Een simpel voorbeeld wordt gegeven door de ondergroepen $b\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$ met $a|b$. Dan geldt

$$(\mathbb{Z}/b\mathbb{Z})/\langle \bar{a} \rangle \cong \mathbb{Z}/a\mathbb{Z},$$

waarbij we $\bar{a}$ voor $\bar{a}(\operatorname{mod} b)$ schrijven. Dus bijvoorbeeld $(\mathbb{Z}/6\mathbb{Z})/\langle \bar{3} \rangle \cong \mathbb{Z}/3\mathbb{Z}$.

We sluiten dit hoofdstuk af met een toepassing.

(10.8) Stelling. *Laat H een ondergroep zijn van G met index $[G : H] = n$. Dan is er een normaaldeler $N \subseteq H$ waarvan de index $[G : N]$ een deler is van $n!$.*

Bewijs. Beschouw de werking van G op de verzameling $X = G/H$ van linkernevenklassen via $g \circ (xH) = (gx)H$. Dit geeft een homomorfisme $j : G \to S(X)$. We stellen nu $N = \ker(j)$. We beweren dat $N \subseteq H$ want uit $gxH = xH$ voor alle x volgt met $x = e$ dat $g \in H$. Maar dan is volgens de eerste isomorfiestelling G/N isomorf met een ondergroep van $S(X) \cong S_n$. Dus de index $[G : N] = \#G/N$ is een deler van $\#S_n = n!$. Dit bewijst het resultaat.

Opgaven

1) Bepaal de homomorfismen $S_n \to \mathbb{C}^*$ voor $n \geq 2$.

2) Laat $A = \{f_{a,b} : a \in \mathbb{R}^*, b \in \mathbb{R}\}$ de groep van afbeeldingen

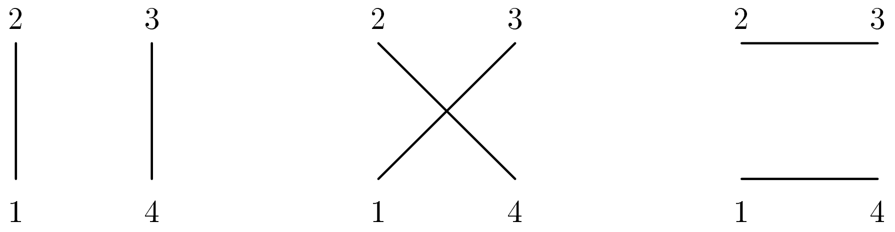
$$f_{a,b} : \mathbb{R} \to \mathbb{R}, \qquad x \mapsto a\,x + b,$$

zijn. Deze groep heet de groep van affiene transformaties. Bewijs dat A isomorf is met de matrixgroep

$$\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^*, b \in \mathbb{R}\}.$$

3) Laat $E_n \subset \mathbb{C}^*$ de ondergroep zijn van n-de machts eenheidswortels: $E_n = \{z \in \mathbb{C}^* : z^n = 1\}$. Bewijs: $\mathbb{C}^*/E_n \cong \mathbb{C}^*$.

4) Gegeven is een vierkant V met hoekpunten $1, 2, 3, 4$. Een permutatie van de hoekpunten geeft aanleiding tot een permutatie van de verzameling L van drie paren lijnstukken:



Welke groep werkt triviaal op L? Bewijs het isomorfisme $S_4/V_4 \cong S_3$.

5) Bewijs dat de torsiegroep $T(\mathbb{C}^*)$ isomorf is met $\mathbb{Q}/\mathbb{Z}$.

6) Bewijs: de symmetriegroep G_I van een icosaeder is niet isomorf met S_5.