VRIJE UNIVERSITEIT BRUSSEL

Inleiding tot de Groepentheorie

Eric Jespers

Bachelor Wiskunde
2016–2017
titularis: Jan De Beule

Vrije Universiteit Brussel
Vakgroep Wiskunde

Voorwoord

Het concept "groep" is één van de meest fundamentele in "recente" wiskunde. De oorsprong van dit concept kan men reeds impliciet terug vinden in de studie van congruente meetkundige figuren en afstandbewarende functies (bewegingen) in de ruimte.

Abel (1802-1829)

Het is pas sedert de eerste helft van de negentiende eeuw dat het idee duidelijk werd gedefiniëerd en erkend als een belangrijke wiskundige gedachte. In die tijd was het begrip groep reeds prominent aanwezig in het werk van Abel en Galois, en dit in het kader van hun studie naar de oplosbaarheid van polynoomvergelijkingen over een veld in termen van radicalen.

Later werd het begrip "beweging" veralgemeend en dit verduidelijkte een belangrijk verband tussen de verschillende meetkunden en de transformatiegroepen van hun meetkundige objecten. Het werk van Lie (1842-1899) omtrent continue groepen versterkte het belang van het "groep" concept. Rond het einde van de 19-de eeuw werd het fundamentele belang van groepen bijzonder duidelijk. Rond deze tijd werden transformatiegroepen en permutatiegroepen veralgemeend en kwam de abstracte theorie van groepen tot stand. Ook de meetkundige benadering kende een opleving door het *Erlangen program* van Felix Klein, die meetkundes ging classificeren in functie van hun symmetriegroepen.

Galois (1811-1832)

Een eerste belangrijk boek met een overzicht van de stand van zaken in het begin van de 20-ste eeuw is dat van Burnside "Theory of Groups of Finite Order", gepubliceerd in 1911. Tot in 1955 evolueerde groepentheorie gestadig, maar vanaf 1955 kwam er een explosie in het onderzoek. Dit vanwege de publicatie van enkele fundamentele ontdekkingen.

Lie (1842-1899)

In deze cursus geven wij een inleiding in de groepentheorie. Een ander belangrijk aspect is om de studenten de "kunst" van "abstracte" bewijzen maken te leren appreciëren en aan te leren.

De studiebenadering in deze cursus verschilt misschien van wat je tot nu toe gewoon bent in andere wiskunde cursussen. Tot op heden heb je waarschijnlijk veel oefeningen/problemen kunnen oplossen door naar "gelijkaardige problemen" te zoeken in de tekst en dan wat de oplossingsmethode aan te passen. In deze cursus zal deze methode slechts eventueel doenbaar zijn voor een zeer beperkt aantal opgaven/problemen, maar het zal voor de meeste problemen niet werken. Het is van belang dat je de materie zeer goed begrijpt, en dat je dus problemen pas aanpakt na een eerste grondige studie van de relevante theorie. Anderzijds zal het voorkomen dat je abstracte begrippen zal moeten hanteren in oefeningen, en dat je precies daardoor een dieper inzicht ontwikkelt in deze begrippen.

De cursus staat vol van definities, stellingen, eigenschappen en voorbeelden. De definities zijn van uiterst belang omdat wij moeten overeenkomen wat er precies (en dus eenduidig) bedoeld wordt me de gebruikte terminologie. Dikwijls wordt een definitie gevolgd door voorbeelden die een concept illustreren. Voorbeelden zijn het belangrijkste hulpmiddel in de tekst: geef er dus veel aandacht aan. Een nuttige hint voor de studie van deze cursus is om stellingen eerst grondig te lezen. Sla in eerste instantie het bewijs over, maar tracht te verstaan wat de stelling precies zegt. Dit kan je o.a. doen door na te gaan wat de inhoud van een stelling betekent voor een concreet voorbeeld. Na een goed begrip van de stelling lees je grondig een bewijs en probeer elke stap te verstaan. Bewijzen in algebra zijn dikwijls "moeilijker" dan b.v. in analyse en meetkunde omdat je meestal geen suggestieve tekening kan maken. Een bewijs is meestal echter "gemakkelijk" als je het "juiste vertrekpunt of de juiste benadering" vindt.

Klein (1849-1925)

Inhoudsopgave

Hoofdstuk 1

Groepen

1.1 Definities

Een groep is een niet-ledige verzameling waarop er een *interne* bewerking gedefinieerd is die aan bepaalde eisen voldoet. In een concrete context kan deze bewerking een optelling, vermenigvuldiging, samenstelling van functies, etc. zijn. In een abstracte context zoals deze noemen we de bewerking het "product", of de "groepsbewerking". Het begrip *intern* zit ingebakken in de volgende definitie.

Definitie 1.1.1. Een binaire bewerking op een niet ledige verzameling S is een afbeelding $* : S \times S \to S$.

In deze context zijn de meeste bewerkingen binair, en zullen we meestal spreken over een bewerking op S. Als $*$ een bewerking is op S, dan noteren we beeld $*(s,t)$ bijna altijd door $s * t$.

Soms zullen we ook de functionele notatie handhaven, dan is de bewerking doorgaans voorgesteld foor een letter, bijvoorbeeld f, en noteren we het beeld van twee elementen onder de bewerking gewoon als $f(x,y)$.

Definitie 1.1.2. Beschouw een bewerking $*$ op een niet ledige verzameling S.

(i) De bewerking $*$ is *associatief* als voor alle $s_1, s_2, s_3 \in S$ geldt dat $s_1 * (s_2 * s_3) = (s_1 * s_2) * s_3$

(ii) Een *neutaal element voor* $*$ is een element $e \in S$ waarvoor geldt dat $s*e = e*s = s$ voor alle $s \in S$.

(iii) Als er een neutraal element $e \in S$ bestaat voor $*$, dan noemen we een element $t \in S$ waarvoor geldt $t * s = s * t = e$ een *invers element van* s *voor* $*$ of een *inverse van* s *voor* $*$.

(iv) We noemen $*$ *abels* of *commutatief* als $s * t = t * s$ voor alle elementen $s, t \in S$.

Definitie 1.1.3. Beschouw een niet ledige verzameling S met een bewerking $*$.

(i) We noemen $S, *$ een *semigroep* als $*$ associatief is.

(ii) We noemen een semigroep $S, *$ een *monoïde* is er een neutraal element $e \in S$ bestaat voor $*$.

(iii) We noemen een monoïde $S, *$ een *groep* als er voor elk element s een inverse bestaat voor $*$.

(iv) Een *abelse semigroep* (respectievelijk, *monoïde* of *groep*) is een semigroep $(S, *)$ (respectievelijk, monoïde of groep) waarbij $*$ abels is.

Voorbeelden 1.1.4. (1) Beschouw de verzameling der natuurlijke getallen $\mathbb{N}$. Beschouw de bewerking $+$. Deze bewerking is associatief. Het element $0 \in \mathbb{N}$ heeft de eigenschap dat $0 + n = n + 0 = n$ voor alle $n \in \mathbb{N}$. De structuur $\mathbb{N}, +$ is dus een monoïde. Het is duidelijk dat niet elk element een inverse heeft voor $+$, dus $\mathbb{N}, +$ is **geen** groep. Het is wel duidelijk dat $+$ een abelse bewerking is op $\mathbb{N}$.

De bewerking $\cdot$ heeft dezelfde eigenschappen, maar nu is $1 \in \mathbb{N}$ een neutraal element voor $\cdot$. Ook $\mathbb{N}, \cdot$ is een abelse monoïde maar geen groep.

(2) Beschouw de verzameling der gehele getallen $\mathbb{Z}$. Beschouw de bewerking $+$. Deze bewerking is associatief, abels, en $0 \in \mathbb{Z}$ is een neutraal element. Daarenboven heeft elk element $x \in \mathbb{Z}$ een inverse voor $+$. De structuur $\mathbb{Z}, +$ is dus een abelse groep.

De bewerking $\cdot$ is eveneens associatief en abels, en nu is $1 \in \mathbb{Z}$ een neutraal element voor $\cdot$. Echter hebben enkel de elementen 1 en -1 een inverse voor $\cdot$. Dus $\mathbb{Z}, \cdot$ is geen groep. Merk op dat $\cdot$ ook een bewerking is op de verzameling $\mathbb{Z} \setminus \{0\}$. Immers, het product van twee niet nul elementen is steeds verschillend van nul. In dit geval is $\mathbb{Z} \setminus \{0\}, \cdot$ evenmin een groep.

(3) Beschouw de verzameling der rationale getallen $\mathbb{Q}$. Het eenvoudig na te gaan dat $\mathbb{Q}, +$ een abelse groep is, en dat $\mathbb{Q} \setminus \{0\}, \cdot$ eveneens een abelse groep is.

(4) Beschouw $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ de verzameling van de complexe getallen. De bewerking $+$ is als volgt gedefinieerd op $\mathbb{C}$

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

Men gaat eenvoudig na dat $(\mathbb{C}), +$ een abelse groep is.

(5) De verzameling $\mathbb{C} \setminus \{0\}$ van alle niet-nul complexe getallen, voorzien van de gewone vermenigvuldiging als bewerking is een abelse groep. Herinner dat, voor $a, b, c, d \in \mathbb{R}$,

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

en als $0 \neq a + bi \in \mathbb{C}$ dan is

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

dus in de groep $(\mathbb{C} \setminus \{0\}, \cdot)$,

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

De complex toegevoegde van $z = a + bi$ (met $a, b \in \mathbb{R}$) is

$$\overline{z} = a - bi$$

en de modulus van z is

$$z| = |a + bi| = \sqrt{a^2 + b^2} \,.$$

Dus als $z \neq 0$ (of equivalent $|z| \neq 0$) dan

$$z^{-1} = |z|^{-2} \overline{z} \,.$$

(6) De verzameling $\{1, -1\} \subset \mathbb{Z}$ voorzien van de vermenigvuldiging is een abelse groep. De verzameling $\{1, i, -1, -i\} \subset \mathbb{C}$ voorzien van de vermenigvuldiging is een abelse groep.

Net zoals voor de vermenigvuldiging van getallen zullen wij dikwijls de bewerking $*$ niet schrijven (vooral als de bewerking duidelijk is uit de context). Dus $a * b$ schrijft men dan eenvoudig als ab. In bovenstaande voorbeelden zullen we typisch de bewerking $\cdot$ weglaten uit de notatie, dus ab i.p.v. $a \cdot b$. We zullen de bewerking $+$ wel zo goed als altijd noteren.

Bovenstaande voorbeelden en hun eigenschappen zijn welbekend. We weten bijvoorbeeld dat het neutraal element voor de optelling in $\mathbb{Z}$ uniek is, en dat elk geheel getal een unieke inverse heeft voor de optelling. Dit kunnen we nu bewijzen voor elke groep.

Eigenschap 1.1.5. *Zij G een groep. Dan gelden de volgende eigenschappen:*

(1) G bevat slechts één neutraal element. Wij noteren dit element meestal e of e_G.

(2) Voor een element $g \in G$ bestaat slechts één element $h \in G$ zodat $gh = hg = e$. Men noemt h het inverse element van g en noteert dit element g^{-1}.

Bewijs. (1) Veronderstel dat e en f twee neutrale elementen zijn. Dus voor alle $g \in G$ geldt

$$eg = g = ge \text{ en } fg = g = gf \,.$$

Bijgevolg, als we in de eerste gelijkheid $g = f$ stellen, dan volgt $ef = f$, en met $g = e$ in de tweede gelijkheid volgt $ef = e$. Dus $e = f$.
(2) Zij $g \in G$ en zij $h_1, h_2 \in G$ zodat

$$gh_1 = gh_2 = e \text{ en } h_1 g = h_2 g = e.$$

Dan

$$h_2(gh_1) = h_2 e = h_2$$

en

$$h_2(gh_1) = (h_2 g)h_1 = eh_1 = h_1.$$

Dus $h_1 = h_2$. □

Merk op dat Eigenschap 1.1.5 ook geldt in een monoïde. We noteren een monoïde $S, *$ ook soms als $S, *, e$, om aan te geven welk element het neutraal element is.

Abelse groepen zijn genoemd naar de Noorse wiskundige Niels Hendrik Abel (1802-1829). Hij was o.a. geinteresseerd in de oplosbaarheid van polynoomvergelijkingen. In 1928 bewijs hij het volgende. Als de wortels van zo'n vergelijking kunnen uitgedrukt worden als rationale functies $f, g, \ldots, h$ in een van de wortels, zeg x, en als voor elke twee wortels, $f(x)$ and $g(x)$, geldt dat $f(g(x)) = g(f(x))$, dan is de vergelijking oplosbaar door radikalen. Abel toonde aan dat deze functies een permutatie geven van de wortels van de vergelijking; dus deze functies zijn elementen van de groep van permutaties van de wortels. Het was die commutativiteitseigenschap in deze permutatiegroep die geleid heeft tot de terminologie "abelse groep". Later kan je dit alles in detail bestuderen in de cursus Galoistheorie.

1.2 Voorbeelden en enkele elementaire eigenschappen

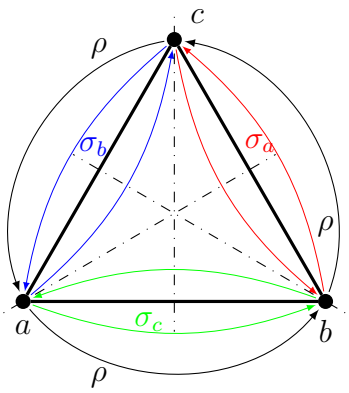
Voorbeelden 1.2.1. (7) De verzameling $\mathbb{R}^2$ is abelse groep voor de optelling van koppels, d.w.z. $(a, b) + (a', b') = (a + a', b + b')$. Meer algemeen is een vectorruimte V een abelse groep voor de optelling van vectoren.

(8) Zij $\mathrm{Afb}(X)$ de verzameling van alle functies met domein en codomein de verzameling X. Dus

$$\mathrm{Afb}(X) = \{f \mid f : X \to X\}.$$

Dan is $\circ$ (de samenstelling van functies) een binaire bewerking op $\mathrm{Afb}(X)$:

$$\mathrm{Afb}(X) \times \mathrm{Afb}(X) \to \mathrm{Afb}(X) \ : \ (f, g) \mapsto f \circ g.$$



Figuur 1.1: Enkele symmetrieën van een gelijkzijdige driehoek

Bovendien is $(\mathrm{Afb}(X), \circ)$ een monoïde met als neutraal element 1_X, de identieke functie op X (dus $1_X(x) = x$ voor alle $x \in X$). Als X meer dan één element bevat dan is $(\mathrm{Afb}(X), \circ)$ geen groep. In dit geval zij $x, y \in X$ met $x \neq y$. Zij dan

$$c_x : X \to X : a \mapsto x,$$

de constante functie op X. Dan is c_x geen bijectie en er bestaat dus geen functie $g \in \mathrm{Afb}(X)$ zodat $c_x \circ g = 1_X = g \circ c_x$.

(9) Zij X een verzameling. De Boolse groep $(\mathcal{P}(X), +)$ bestaat uit de verzameling $\mathcal{P}(X)$ waarvan de elementen alle deelverzamelingen van X zijn dus $\mathcal{P}(X) = \{Y \mid Y \subset X\}$, en de bewerking "het symmetrisch verschil", genoteerd $+$. Voor $A, B \in \mathcal{P}(X)$ is per definitie:

$$A + B = (A \setminus B) \cup (B \setminus A).$$

Het neutraal element is de lege verzameling $\emptyset$. Merk op dat $A + A = \emptyset$. Dus $A^{-1} = A$.

(10) Beschouw een gelijkzijdige driehoek in het Euclidisch vlak, zie Figuur 1.2. Er zijn precies 6 isometrieën[1] van het Euclidisch vlak, dit zijn drie spiegelingen, twee rotaties en de identieke afbeelding. De identieke afbeelding noteren we als e, de spiegelingen als $\sigma_a, \sigma_b, \sigma_c$. De rotatie van 120^0 in tegenwijzerzin noteren we als ρ. De samenstelling van isometrieën in een Euclidisch vlak is opnieuw een isometrie. Merk op dat $\rho \circ \rho$ de rotatie in tegenwijzerzin over 240^0 is, en dat $(\rho \circ \rho) \circ \rho = e$. We zullen verderop formeel de

[1] Een isometrie is een afstandsbewarende bijectie van het Euclidisch vlak die bijgevolg de meetkundige eigenschappen bewaart: o.a. incidentie, afstand en hoek

notatie $\rho^2 := \rho \circ \rho$ definiëren. De verzameling G van isometrieën wordt dan

$$G = \{\sigma_a, \sigma_b, \sigma_c, \rho, \rho^2, e\}\,.$$

Men kan nu eenvoudig controleren dat $G, \circ$ een groep is.

Eigenschap 1.2.2 (Veralgemeende associativiteit)**.** *Zij S een groep. Als $s_1, \ldots, s_n \in S$ dan is het element $s_1 s_2 \cdots s_n$ uniek bepaald in S (d.w.z. dit element is onafhankelijk van de plaatsing van de haakjes).*

Bewijs. Wij bewijzen dit door inductie. De basisstap is $n = 3$, en deze geldt wegens de associativiteit. Veronderstel nu dat het resultaat geldt voor producten van minder dan n factoren. Beschouw nu het product $s_1 s_2 \cdots s_n$ op twee verschillende manieren

$$(s_1 \cdots s_i)(s_{i+1} \cdots s_n) \text{ en } (s_1 \cdots s_j)(s_{j+1} \cdots s_n)\,,$$

we mogen veronderstellen dat $i \leq j$. Elk van de vermelde producten tussen haakjes kan zelf veel haakjes bevatten, maar wegens de inductiehypothese zijn deze haakjes niet nodig. Als $i = j$ dan zijn beide producten dezelfde. Veronderstel dus dat $i < j$. Weer wegens de inductiehypothese mogen wij de eerste uitdrukking herschrijven als

$$(s_1 \cdots s_i)([s_{i+1} \cdots s_j][s_{j+1} \cdots s_n])$$

en de tweede uitdrukking als

$$([s_1 \cdots s_i][s_{i+1} \cdots s_j])(s_{j+1} \cdots s_n).$$

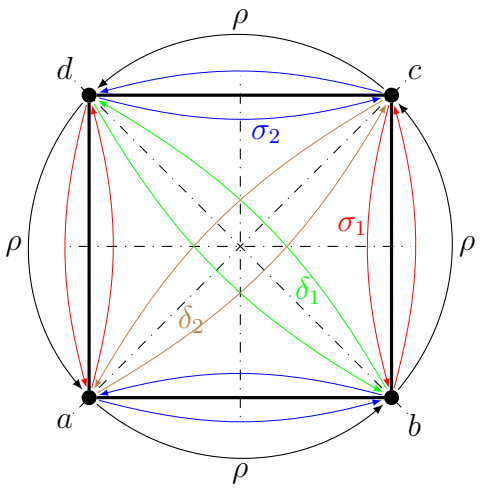
Elk van de uitdrukkingen $x = s_1 \cdots s_i$, $y = s_{i+1} \cdots s_j$ en $z = s_{j+1} \cdots s_n$ is onafhankelijk van haakjes. De eerste uitdrukking is nu van de vorm $x(yz)$ en de tweede $(xy)z$. Wegens de associativiteit zijn deze dezelfde. □

De veralgemeende associativiteit laat toe om machten van elementen te definiëren.

Definitie 1.2.3. Zij S een goep met eenheidselement e. Als $s \in S$ en $0 \neq n \in \mathbb{N}$, dan definiëert men de n-de macht van s inductief als volgt:

$$s^0 = e \text{ en } s^{n+1} = s^n s\,.$$

Weer wegens de veralgemeende associativiteit is de volgende eigenschap duidelijk.



Figuur 1.2: Enkele symmetrieën van een vierkant

Eigenschap 1.2.4. *Zij S een groep. Als $s \in S$ en $m, n \in \mathbb{N}$ dan*

$$s^{n+m} = s^n s^m \text{ en } (s^n)^m = s^{nm}\,.$$

Merk op dat voor semigroepen Eigenschap 1.2.2 ook geldt, net als Eigenschap 1.2.4 voor $n, m \in \mathbb{N} \setminus \{0\}$. Voor semigroepen geldt ook Definitie 1.2.3 voor $n \geq 1$, en voor $n \geq 0$ als de semigroep een monoïde is. We beschouwen nog enkele voorbeelden.

Voorbeelden 1.2.5. (11) Zij X een niet ledige verzameling. We definiëren $\mathrm{Sym}(X)$ als de verzameling van alle **bijecties** van X naar zichzelf. Merk op dat $\mathrm{Sym}(X) \subset \mathrm{Afb}(X)$. Omdat bijecties echter inverteerbaar zijn, is $\mathrm{Sym}(X), \circ$ een groep. Men noemt dit de symmetrische groep op de verzameling X (of de *permutatiegroep* op X).

(12) We beschouwen opnieuw het Euclidisch vlak $\mathbb{R}^2$. Definieer $I(\mathbb{R}^2)$ als de *isometrieën* (dus de aftandsbewarende bijecties) van het Euclidisch vlak. Dus een bijectie f van de punten van $\mathbb{R}^2$ behoort tot $I(\mathbb{R}^2)$ als

$$\|f(a,b) - f(c,d)\| = \|(a,b) - (c,d)\|\,.$$

Het is duidelijk dat $I(\mathbb{R}^2), \circ$ een groep is.

Zij nu een Ω een figuur in het reële vlak (bijvoorbeeld een driehoek of een vierkant). Dan noteert men met $\Sigma(\Omega)$ de symmetriegroep in het reële vlak van de figuur Ω, d.w.z $\Sigma(\Omega)$ is de verzameling van alle $f \in I(\mathbb{R}^2)$ zodat

$$f(\Omega) = \Omega\,.$$

De verzameling $\Sigma(\Omega)$ een deelverzameling van $I(\mathbb{R}^2)$. In Voorbeelden 1.2.1 (10) hebben we de groep van isometrieën van een gelijkzijdige driehoek bestudeerd. In dit voorbeeld kiezen we voor Ω een vierkant, zie Figuur 1.2.5.

Herinner dat $\|(a,b)\| = \sqrt{a^2+b^2}$. Zulke functies behoren uiteraard tot $\mathrm{Sym}(\mathbb{R}^2)$. Dus: $(I(\mathbb{R}^2), \circ)$ is een groep bevat in $\mathrm{Sym}(\mathbb{R}^2)$. Voorbeelden van functies die tot deze groep behoren zijn de rotaties, reflecties en translaties.

Nemen wij nu voor Ω een vierkant (met zijden van lengte 1, en met de oorsprong als doorsnede van de diagonalen), dan permuteert elk element van $\Sigma(\Omega)$ de hoekpunten $\{a,b,c,d\}$ van Ω en bovendien is een element van $\Sigma(\Omega)$ bepaald door de beelden van de hoekpunten. Dus zijn er ten hoogste 24 mogelijkheden voor elementen van $\Sigma(\Omega)$. Doch niet elke permutatie van de hoekpunten is afkomstig van een element in $\Sigma(\Omega)$. Inderdaad als $\|v_i - v_j\| = 1$ dan moeten ook de beeldpunten van v_i en v_j op een afstand 1 van elkaar liggen. Dit levert dan nog 8 mogelijkheden en

$$\Sigma(\Omega) = \{e, \sigma_1, \sigma_2, \delta_1, \delta_2, \rho, \rho^2, \rho^3\}$$

met ρ een rotatie over 90 graden in tegenwijzerzin en σ_1, σ_2 en δ_1, δ_2 reflecties. Enkele gelijkheden kan men eenvoudig nagaan: $\sigma_1^2 = \sigma_2^2 = \delta_1^2 = \delta_2^2 = e$, $\rho^4 = e$, en $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1 = \rho^2$.

We noteren de reflectie ten opzichte van de diagonaal ac als δ_1. Het is eenvoudig na te gaan dat $\rho \circ \delta_1 = \sigma_2$, en $\rho^3 \circ \delta_1 = \sigma_1$, we kunnen dus ook alle elementen van $\Sigma(\Omega)$ schrijven als een samenstelling van ρ's en δ_1's:

$$\Sigma(\Omega) = \{1, \rho, \rho^2, \rho^3, \delta_1, \rho \circ \delta_1, \rho^2 \circ \delta_1, \rho^3 \circ \delta_1\},$$

en deze elementen voldoen aan de volgende relaties:

$$\rho^4 = e,\ \delta_1^2 = 1,\ \delta_1 \circ \rho = \rho^3 \circ \delta_1. \tag{1.1}$$

In plaats van een gelijkzijdige driehoek, of een vierkant, kunnen we algemeen een regelmatige n-hoek beschouwen in het Euclidisch vlak. De groep isometrieën die een regelmatige n-hoek op zichzelf afbeeldt noemt men de diëdergroep van orde $2n$, genoteerd als D_{2n}. Deze groep bevat altijd precies $2n$ elementen. De groep van isometrieën die de gelijkzijdige driekhoek op zichzelf afbeelden, is dus D_6, de groep uit dit voorbeeld is dus D_8.

We hebben gezien in dit voorbeeld dat elk element te schrijven is als een product dat bestaat uit twee welgekozen elementen, en dat er bepaalde gelijkheden, in dit geval noemen we ze *relaties* bestaan tussen de elementen van de groep. We zullen dit verderop formaliseren, maar men kan nagaan dat de relaties (1.1) de groep D_8 bepalen, dit

betekent, precies omdat deze relaties gelden, kunnen er door het nemen van willekeurige producten van ρ en δ_1 geen andere elementen meer bekomen worden dan diegenen die we al hebben.

(13) Zij $a, b \in \mathbb{R}$ met $a \neq 0$ en zij $f_{a,b} : \mathbb{R} \to \mathbb{R}$ de functie gedefiniëerd als volgt:

$$f(x) = ax + b\,.$$

De affiene groep $\mathrm{GA}(1, \mathbb{R})$ is de verzameling van alle functies $f_{a,b}$, dus

$$\mathrm{GA}(1, \mathbb{R}) = \{f_{a,b} \mid a, b \in \mathbb{R},\ a \neq 0\}\,.$$

De bewerking is de samenstelling van functies. Merk op dat

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b}\,.$$

(14) Beschouw de verzameling

$$\mathcal{A} = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mid a, b \in \mathbb{R},\ a \neq 0 \right\}$$

een groep voor de matrixvermenigvuldiging. Bovendien is de functie

$$\psi : \mathrm{GA}(1, \mathbb{R}) \to \mathcal{A} : f_{a,b} \mapsto \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

een bijectie zodat

$$\psi(f_{a,b} \circ f_{c,d}) = \psi(f_{a,b})\psi(f_{c,d})\,.$$

In dit voorbeeld is het in zekere zin duidelijk dat de groepen $\mathrm{GA}(1, \mathbb{R})$ en $\mathcal{A}$, in abstracte zin, *gelijk* zijn. Dit zullen we ook illustreren in het voorbeeld (16).

(15) Herinner dat elk complex getal $z = a + bi$ (met $a, b \in \mathbb{R}$) kan geschreven worden als

$$z = r\ (\cos\theta\ +\ i\ \sin\theta),$$

met $\theta \in \mathbb{R}$ en $\theta \in [0, 2\pi)$ en $r = |z|$. Men noemt θ het argument van z. De getallen r en θ noemt men de poolcoördinaten van z. Merk op dat

$$\cos\theta = \frac{a}{\sqrt{a^2 + b^2}}$$

en

$$\sin\theta = \frac{b}{\sqrt{a^2 + b^2}}\,.$$

Wij gebruiken ook dikwijls de volgende notatie:

$$e^{i\theta} = \cos\theta + i\ \sin\theta\,.$$

Indien $r > 0$ dan bestaat er een getal $y \in \mathbb{R}$ zodat $r = e^y$. Dus schrijft men ook

$$e^{y+i\theta} = e^y(\cos\theta + i\sin\theta)\,.$$

Met deze notatie la, men de volgende welbekende formules eenvoudig herschrijven ($\alpha, \beta \in \mathbb{R}$):

$$\begin{aligned}\sin(\alpha+\beta) &= \sin\alpha\ \cos\beta + \cos\alpha\ \sin\beta\\ \cos(\alpha+\beta) &= \cos\alpha\ \cos\beta - \sin\alpha\ \sin\beta\end{aligned}$$

als

$$e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}\,.$$

Een bewijs door inductie geeft dan, voor $n \in \mathbb{N}$ en $\alpha \in \mathbb{R}$:

$$e^{in\alpha} = \left(e^{i\alpha}\right)^n\,,$$

of dus

$$\cos n\alpha + i\ \sin n\alpha = (\cos\alpha + i\ \sin\alpha)^n$$

de formule van De Moivre (1667-1754).

Zij n nu een niet-nul natuurlijk getal en zij

$$\xi_n = e^{2\pi i/n} = \cos(2\pi/n) + i\ \sin(2\pi/n)\ .$$

Merk op dat

$$e^{2k\pi i/n}e^{2l\pi i/n} = e^{2(k+l)\pi i/n}\,,$$

voor alle $k, l \in \mathbb{Z}$, en

$$(\xi_n)^n = 1\,,$$

men zegt dat ξ_n een n-de (complexe) éénheidswortel is. Het is ook duidelijk dat $(\xi_n^k)^n = (\xi_n^n)^k = 1$. Dus de verzameling E_n is gesloten onder de vermenigvuldiging. Er geldt ook dat $\xi_n^k\xi_n^{(n-k)} = 1$, dus elk element in E_n heeft een inverse. We weten nu genoeg om te besluiten dat $E_n, \cdot$ een abelse groep is.

(16) We gebruiken de complexe n-de eenheidswortel ξ_n uit het vorige voorbeeld. Definieer

$$a = \begin{bmatrix} \xi_n & 0 \\ 0 & \xi_n^{-1} \end{bmatrix} \quad \text{en} \quad b = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

Door de eigenschappen van matrixvermenigvuldiging kunnen de volgende eigenschappen eenvoudig gecontroleerd worden:

$$a^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

en

$$b^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

en $ba = a^{n-1}b$. We definiëren nu $G = \{a^k | 1 \leq k \leq n\} \cup \{a^k b | 1 \leq k \leq n\}$. Door de eigenschappen van a en b kan men nu eenvoudig nagaan dat G een groep is voor de gewone matrixvermenigvuldiging. Kiezen we nu bijvoorbeeld $n = 4$, dan zien we onmiddellijk, precies door de relaties voor a en b, dat G in zekere zin de zelfde groep is als D_8. Dit blijkt waar te zijn voor alle n. Op deze wijze vindt men dus een algebraïsche beschrijving van de diëdergroepen D_{2n}. Een afbeelding $\psi : G \to D_8$ zoals in voorbeeld (14) wordt volledig bepaald door het beeld van a en b. Gelet op de relaties voor a en b, is het bijna onmiddellijk duidelijk dat

$$\psi(a) = \rho, \psi(b) = \delta_1$$

een afbeelding ψ zal bepalen zodanig dat $\psi(gh) = \psi(g) \circ \psi(h)$. In het hoofdstuk over groephomomorfismen zullen we het nodige materiaal ontwikkelen om wiskundig te beschrijven wat het betekent dat twee groepen in zekere zin dezelfde zijn.

1.3 Vermenigvuldigingstabel

Definitie 1.3.1. Men noemt een groep G eindig als de verzameling G eindig veel elementen bevat. Het aantal elementen in de verzameling G noteert men als $|G|$ (men noemt dit ook de orde van de groep).

Voor eindige groepen kan men de bewerking voorstellen in een tabel, die men de *Cayleytabel* (of vermenigvuldigingstabel) noemt.

Zij $(G, *)$ een eindige groep en zij $g_1, \ldots, g_n$ een lijst (zonder herhalingen) van al de elementen van G. Een vermenigvuldigingstabel van G is een tabel als volgt

$*$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	$\cdots$	$g_1 * g_j$	$\cdots$	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	$\cdots$	$g_2 * g_j$	$\cdots$	$g_2 * g_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\cdots$	$\vdots$
g_i	$g_i * g_1$	$g_i * g_2$	$\cdots$	$g_i * g_j$	$\cdots$	$g_i * g_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\cdots$	$\vdots$
g_n	$g_n * g_1$	$g_n * g_2$	$\cdots$	$g_n * g_j$	$\cdots$	$g_n * g_n$

We herbekijken enkele voorbeelden. De groep E_n, met $n = 4$ uit voorbeeld (15) heeft de volgende Cayleytabel.

$\cdot$	1	ξ_4	ξ_4^2	ξ_4^3
1	1	ξ_4	ξ_4^2	ξ_4^3
ξ_4	ξ_4	ξ_4^2	ξ_4^3	1
ξ_4^2	ξ_4^2	ξ_4^3	1	ξ_4
ξ_4^3	ξ_4^3	1	ξ_4	ξ_4^2

Vervolgens geven wij de Cayleytabel van de diëdergroep D_6 van orde 6, met D_6 beschreven zoals in Voorbeeld (16). Man kan deze tabel volledig narekenen, en dit kan het efficiëntst gebeuren door de relaties $a^3 = b^2 = e$ en $ba = a^2b$ te gebruiken. Merk op dat e hier staat voor de 2×2 eenheidsmatrix over $\mathbb{C}$.

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Groepen kunnen ook gedefinieerd worden door middel van een Cayleytabel. Daarbij vertrekken we van een verzameling elementen, en leggen we de binaire bewerking op deze elementen volledig vast door de Cayleytabel. Aldus definieert men vaak de zogenaamde viergroep van Klein. Dit is de groep $G = \{e, a, b, c\}$ met de bewerking gedefiniëerd via de volgende Cayleytabel. In dit geval moet men aan de hand van de gegeven tabel nagaan dat G een groep is.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

1.4 Elementaire Eigenschappen

In deze sectie bewijzen we enkele belangrijke eigenschappen van groepen.

Eigenschap 1.4.1. *Zij G een groep. Dan gelden de volgende eigenschappen:*

1. *G bevat slechts één neutraal element. Wij noteren dit element meestal e of e_G.*
2. *Voor een element $g \in G$ bestaat slechts één element $h \in G$ zodat $gh = hg = e$. Men noemt h het inverse element van g en noteert dit element g^{-1}.*
3. *als $g, h \in G$ dan $(gh)^{-1} = h^{-1}g^{-1}$.*
4. *als $g \in G$ dan $(g^{-1})^{-1} = g$.*
5. *Voor $g_1, g_2, h \in G$: als $g_1h = g_2h$ of $hg_1 = hg_2$ dan $g_1 = g_2$, de vereenvoudigingswetten.*

Bewijs. (1). Veronderstel dat e en f twee neutrale elementen zijn. Dus voor alle $g \in G$,

$$eg = g = ge \text{ en } fg = g = gf\,.$$

Bijgevolg, als wij de eerste vergelijking toepassen met $g = f$ dan $ef = f$ en uit de tweede vergelijking (met $g = e$) volgt $ef = e$. Dus $e = f$.

(2). Zij $g \in G$ en zij $h_1, h_2 \in G$ zodat

$$gh_1 = gh_2 = e \text{ en } h_1g = h_2g = e\,.$$

Dan

$$h_2(gh_1) = h_2e = h_2$$

en

$$h_2(gh_1) = (h_2g)h_1 = eh_1 = h_1\,.$$

Dus $h_1 = h_2$.

(3).

$$\begin{aligned}(gh)(h^{-1}g^{-1}) &= g\left(h(h^{-1}g^{-1})\right)\\ &= g\left((hh^{-1})g^{-1}\right)\\ &= g(eg^{-1})\\ &= gg^{-1}\\ &= e\end{aligned}$$

Analoog bewijst men $(h^{-1}g^{-1})(gh) = e$. Dus $(gh)^{-1} = h^{-1}g^{-1}$.

(4). Omdat $(g^{-1})\ ((g^{-1}))^{-1} = e = ((g^{-1}))^{-1}\ (g^{-1})$ en $g^{-1}g = e = gg^{-1}$ volgt er wegens (2) dat $(g^{-1})^{-1} = g$.

(5). Veronderstel $g_1h = g_2h$, dan

$$(g_1h)h^{-1} = (g_2h)h^{-1}\,.$$

Wegens de associativiteit volgt er dan

$$g_1 = g_1e_G = g_1(hh^{-1}) = (g_1h)h^{-1} = (g_2h)h^{-1} = g_2(hh^{-1}) = g_2e_G = g_2\,.$$

□

In een groep kunnen wij ook negatieve machten definiëren.

Definitie 1.4.2. Zij G een groep. Als $g \in G$ en $n \in \mathbb{N}$, dan

$$g^{-n} = (g^{-1})^n\,.$$

Eigenschap 1.4.3. *Zij G een groep en $g \in G$. Als $n, m \in \mathbb{Z}$ dan*

$$g^{n+m} = g^ng^m,\ \ (g^n)^m = g^{nm} \text{ en } (g^{-1})^n = (g^n)^{-1}\,.$$

Als g en h twee commuterende elementen zijn van G (d.w.z. $gh = hg$) dan $(gh)^n = g^nh^n$.

Bewijs. Veronderstel eerst dat g en h commuteren. Voor $n \in \mathbb{N}$, bewijs door inductie dat $hg^n = g^nh$ en ook $(gh)^n = g^nh^n$. Merk op dat ook g^{-1} en h^{-1} commuteren. Als n negatief is, dan is $-n \geq 0$ en dus

$$\begin{aligned}(gh)^n &= \left((gh)^{-1}\right)^{-n}\\ &= \left(h^{-1}g^{-1}\right)^{-n}\\ &= \left(g^{-1}h^{-1}\right)^{-n}\\ &= \left(g^{-1}\right)^{-n}\left(h^{-1}\right)^{-n}\\ &= g^nh^n\end{aligned}$$

Dus is het laatste gedeelte van de eigenschap bewezen.

Het eerste gedeelte van de eigenschap is reeds gekend voor $n, m \geq 0$. De andere gevallen laten wij als oefening. □

De notatie s^n, met n positief, ontstaat door de bewerking $s * t$ multiplicatief st te schrijven, inderdaad $s^n = ss \cdots s$ (er zijn n factoren). Wanneer de bewerking de optelling $+$ is dan betekent dit $s + s + \cdots + s$, en dan zou dit beter geschreven worden als sn. Deze notatie gaan we slechts gebruiken wanneer wij met abelse (semi)groepen werken. Eigenschap 1.4.3 wordt dan $(n+m)g = ng+mg$, $m(ng) = (mn)g$ en $n(g+h) = ng+nh$.

1.5 De orde van een element

Definitie 1.5.1. Zij G een groep en $g \in G$. De orde van het element g is het kleinste niet-nul natuurlijk getal n zodat $g^n = e$. Als er zo geen natuurlijk getal bestaat dan zegt men dat g oneindige orde heeft. De orde van g noteert men als $o(g)$.

Merk op dat als $g \in G$ eindige orde n heeft dan $g^{-1} = g^{n-1}$.

Eigenschap 1.5.2. *In een eindige groep heeft elk element eindige orde.*

Bewijs. Zij $g \in G$ en beschouw de deelverzameling

$$\{e, g, g^2, \ldots, g^n, \cdots\} = \{g^n \mid n \in \mathbb{N}\}.$$

Omdat G een eindige verzameling is moet er herhaling in de lijst voorkomen. Dus bestaan $m > n$ zodat $g^m = g^n$. Bijgevolg $g^{m-n} = g^m g^{-n} = e$. Er bestaat dus een niet nul natuurlijk getal k zodat $g^k = e$, bijgevolg heeft g eindige orde. □

Duidelijk heeft het neutraal element van een groep steeds orde 1. In een oneindige groep kunnen er elementen bestaan van eindige orde. Bijvoorbeeld het element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ heeft orde 2 en duidelijk is $\mathrm{GL}_2(\mathbb{R})$ een oneindige groep.

Eigenschap 1.5.3. *Zij G een groep en $g \in G$. Zij $n, m \in \mathbb{Z}$. Veronderstel dat g eindige orde k heeft. Dan*

1. *$g^n = g^m$ als en slechts als $k|(n-m)$.*
2. *$g^n = e$ als en slechts als $k|n$.*

Bewijs. Veronderstel $o(g) = k < \infty$. Zij $n \in \mathbb{Z}$ en schrijf $n = qk + r$ met $q, r \in \mathbb{Z}$ en $0 \leq r < k$. Dan $g^n = e$ als en slechts als $g^n = g^{qk} g^r = (g^k)^q g^r = e$, of equivalent, $g^r = e$.

Omdat $r < k$, verkrijgen wij aldus $g^n = e$ als en slechts als $r = 0$, d.w.z. $k|n$. Dit bewijst (2).

(1) volgt nu eenvoudig omdat $g^n = g^m$ als en slechts als $g^{n-m} = g^n(g^m)^{-1} = e$. □

Definitie 1.5.4. Een groep G is *cyclisch* als er een $g \in G$ bestaat zodat $G = \{g^n \mid n \in \mathbb{Z}\}$. Men noemt g een *voortbrenger* van G.

Merk op dat een cyclische groep abels is. De groep $(\mathbb{Z}, +)$ is cyclisch met voortbrenger 1. Merk op dat ook -1 een voortbrenger is. De groep E_n bestaande uit de complexe n-de éénheidswortels is cyclisch met voortbrenger $e^{2\pi i/n}$. Er zijn echter nog andere mogelijke voortbrengers, namelijk alle elementen van de vorm $e^{2\pi ki/n}$, met $1 < k < n$ en $(k, n) = 1$.

Eigenschap 1.5.5. *Zij G een groep. Dan:*

1. *Zij G een eindige groep van orde n. Dan, G is cyclisch als en slechts als G een element g van orde n bevat. (In dit geval $G = \{1, g, \ldots, g^{n-1}\}$.)*
2. *G is cyclisch van oneindige orde als en slechts G een element g van oneindige orde bevat zodat $G = \{g^n \mid n \in \mathbb{Z}\}$. In dit geval is $g^n \neq g^m$ als $n \neq m$.*

Bewijs. Bewijs van (1). Veronderstel dat G een eindige cyclische groep is van orde n. Dan, bestaat er een $g \in G$ zodat $G = \{g^k \mid k \in \mathbb{Z}\}$. Omdat G eindig is weten wij dat g eindige orde heeft, zeg $o(g) = m$. Dus volgt er $\{g^k \mid k \in \mathbb{Z}\} = \{1, g, \ldots, g^{m-1}\}$, met $g^i \neq g^j$ voor $0 \leq i, j \leq m - 1$ en $i \neq j$. Bijgevolg $G = \{1, g, \ldots, g^{m-1}\}$ en dus $o(g) = m = |G| = n$.

Omgekeerd, als $|G| = n$ en $g \in G$ met $o(g) = n$ dan is

$$\{e, g, g^2, \ldots, g^{n-1}\} \subseteq G\,.$$

Al de machten $e, g, g^2, \cdots, g^{n-1}$ zijn verschillend. Omdat $|G| = n$ volgt er dus dat $\{e, g, g^2, \ldots, g^{n-1}\} = G$.

Bewijs van (2). Dit laten wij als oefening. □

Voorbeelden 1.5.6. We hernemen enkele voorbeelden.

1.6 Algebraïsche structuren

Groepen zijn als het ware de bouwstenen van vele algebraïsche structuren.

Definitie 1.6.1. Zij R een verzameling met twee bewerkingen $+$ en $\cdot$ die voldoen aan de volgende eigenschappen:

1. $(R, +)$ is een abelse groep (het neutraal element noteert men meestal 0 en men noemt dit het nulelement van R),
2. $(R, \cdot)$ is een monoïde,
3. voor alle $a, b, c \in R$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
en
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$
(de distributiviteitswetten).

Dan noemt men $(R, +, \cdot)$ een **ring**. Indien bovendien $(R \setminus \{0\}, \cdot)$ een abelse groep is, dan noemt men R een lichaam (of een veld). Het neutraal element van $(R, \cdot)$ noemt men het éénheidselement van de ring en noteert men meestal als 1.

Voorbeelden 1.6.2. (1) Duidelijk zijn $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ en $(\mathbb{C}, +, \cdot)$ lichamen, en is $(\mathbb{Z}, +, \cdot)$ een commutatieve ring (d.w.z. een ring met $(\mathbb{Z}, \cdot)$ een abelse monoïde) die geen lichaam is.

(2) Als R een ring is dan noteren wij met $M_n(R)$ de verzameling van alle $n \times n$-matrices over R. Een $n \times n$-matrix met op de (i, j)-de plaats het element r_{ij} noteren wij meestal als volgt
$$(r_{ij})$$
De som en product van matrices werd in lineaire algebra als volgt gedefiniëerd:
$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$
en
$$(a_{ij})\ (b_{ij}) = (c_{ij})$$
met
$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$
Er volgt dat $(M_n(R), +, \cdot)$ een ring is met als éénheidselement I_n, de identiteitsmatrix.

Zij F een lichaam. De determinant van een matrix $A \in M_n(F)$ noteren wij met $\det(A)$. De verzameling van alle matrices $A \in M_n(F)$ met $\det(A) \neq 0$ noteert men als

$\mathrm{GL}_n(F)$. Met $\mathrm{SL}_n(F)$ noteert men de verzameling van alle $A \in M_n(F)$ met $\det(A) = 1$. Er volgt dat $(M_n(F), \cdot)$ een monoïde is en dat beide

$$(\mathrm{GL}_n(F), \cdot)$$

en

$$(\mathrm{SL}_n(F), \cdot)$$

groepen zijn (men noemt deze, respectievelijk, de lineaire groep van graad n over F en de speciaal lineaire groep van graad n over F). Beiden hebben als neutraal element I_n.

(3) Als R een ring is dan noteren wij

$$U(R) = \{a \in R \mid \text{er bestaat } b \in R \text{ zodat } ab = ba = 1\}$$

Er volgt dat $(U(R), \cdot)$ een groep is. Men noemt dit de groep van de inverteerbare elementen van R. Zo is bijvoorbeeld

$$U(M_n(F)) = \mathrm{GL}_n(F),$$

voor een lichaam F.

(4) Men noemt een inverteerbare matrix $A \in M_n(\mathbb{R})$ stochastisch als elk van zijn kolomsommen gelijk is aan 1. D.w.z., als $A = (a_{ij})$, dan

$$\sum_{i=1}^{n} a_{ij} = 1, \quad \text{voor elke } j \text{ met } 1 \leq j \leq n.$$

De verzameling van alle zulke stochastische matrices noteren wij als

$$\sum(n, \mathbb{R}).$$

Deze verzameling voorzien van de vermenigvuldiging van matrices is een groep. Men noemt dit de stochastische groep van graad n.

(7) Zij $Q = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Definiëer dan

$$\varphi : \sum(2, \mathbb{R}) \to \mathcal{A} : A \mapsto QAQ^{-1}.$$

Dit is een bijectie die voldoet aan

$$\varphi(AB) = \varphi(A)\varphi(B).$$

1.6.1 Restklassenringen

In deze paragraaf definiëren we een belangrijke klasse van eindige ringen. Daartoe herhalen we het begrip equivalentierelatie.

Definitie 1.6.3. Zij R een *relatie* op een verzameling X (dus R is een deelverzameling van $X \times X$). Voor $x, y \in X$, noteren wij $(x, y) \in R$ ook als xRy. Men noemt R een equivalentierelatie als de volgende voorwaarden voldaan zijn, voor alle $x, y, z \in X$:

1. xRx (reflexiviteit),
2. als xRy dan yRx (symmetrie),
3. als xRy en yRz dan xRz (transitiviteit).

Voor $x \in X$ noteren wij

$$[x]_R = \{y \in X \mid xRy\},$$

de *equivalentieklasse* van x. (In de cursus lineaire algebra noteert men $[x]_R$ als E_x.)

De verzameling van alle equivalentieklassen noteren wij X/R. Dus

$$X/R = \{[x]_R \mid x \in X\}.$$

Merk op dat de equivalentieklassen van R (op een niet-lege verzameling X) een *partitie* vormen van X, d.w.z.,

1. elke $[x]_R \neq \emptyset$,
2. $\cup_{x \in X}[x]_R = X$,
3. als $[x]_R \cap [y]_R \neq \emptyset$ dan $[x]_R = [y]_R$.

Definitie 1.6.4. Stel $n \in \mathbb{N} \setminus \{0, 1\}$. Op de verzameling $\mathbb{Z}$ definiëren we de relatie $\equiv_n$, de *congruentierelatie* modulo n, als volgt:

$$x \equiv_n y \text{ als en slechts als } n|(x - y).$$

De notatie $n|(x - y)$ wil zeggen dat n een deler is (in $\mathbb{Z}$) van $x - y$. D.w.z., er bestaat een $m \in \mathbb{Z}$ zodat $nm = x - y$. De equivalentieklasse van x noteren wij als $[x]_n$, of ook als $[x]$. De verzameling van de equivalentieklassen $\mathbb{Z}/\equiv_n$ noteren wij als $\mathbb{Z}/n\mathbb{Z}$. Wij willen nu op deze verzameling twee bewerkingen $+$ en $\cdot$ definiëren. Maar om na te gaan dat

deze bewerkingen inderdaad functies zijn (men zegt dikwijls "goed gedefinieerd" zijn) moet men eerst het volgende lemma bewijzen.

Lemma 1.6.5. *Zij $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Als*

$$[a_1]_n = [a_2]_n \text{ en } [b_1]_n = [b_2]_n$$

dan

$$[a_1 + b_1]_n = [a_2 + b_2]_n$$

en

$$[a_1 b_1]_n = [a_2 b_2]_n.$$

Bewijs. Omdat $[a_1]_n = [a_2]_n$ en $[b_1]_n = [b_2]_n$ bestaan er $r, s \in \mathbb{Z}$ zodat

$$a_1 - a_2 = rn \text{ en } b_1 - b_2 = sn.$$

Dus

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = (r + s)n.$$

Bijgevolg

$$n \mid ((a_1 + b_1) - (a_2 + b_2))$$

en daarom $[a_1 + b_1]_n = [a_2 + b_2]_n$.

Analoog bewijst men het tweede gedeelte. □

Men definiëert nu als volgt twee bewerkingen op $\mathbb{Z}/n\mathbb{Z}$:

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : ([a]_n, [b]_n) \mapsto [a]_n + [b]_n = [a + b]_n$$

en

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : ([a]_n, [b]_n) \mapsto [a]_n \cdot [b]_n = [ab]_n.$$

Eigenschap 1.6.6. *Zij n een geheel getal groter dan 1. Dan is $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ een commutatieve ring met nulement $[0]_n$ en éénheidselement $[1]_n$.*

1.7 Vergelijkingen in Groepen

Omdat in een groep elk element een invers element heeft, kunnen wij vergelijkingen in één veranderlijke oplossen. Dit gaat als volgt.

Eigenschap 1.7.1. *Zij G een groep. Als $g, h \in G$ dan bestaat er een unieke $x \in G$ zodat $gx = h$, en er bestaat een unieke $y \in G$ zodat $yg = h$.*

Bewijs. Zij $x = g^{-1}h$ dan is $gx = h$ en dus bestaat er minstens één oplossing voor de vergelijking. Dat er precies één oplossing bestaat volgt uit het volgende: als $gx_1 = gx_2$ dan $x_1 = x_2$.

Analoog bewijst men de uniciteit van de oplossingen voor de vergelijking $yg = h$. □

Als dus G een eindige groep is dan is elke rij en elke kolom van de Cayleytabel een permutatie van de elementen van G. Een tabel die aan deze laatste voorwaarde voldoet noemt men een Latijns vierkant. Dus de Cayleytabel van een eindige groep is een Latijns vierkant. Doch het omgekeerde is niet waar.

Door gebruik te maken van deze eigenschap kan men groepen van orde twee, drie en vier eenvoudig bepalen. Bijvoorbeeld zij G een groep van orde drie. Wij noteren het neutraal element e en de twee andere elementen a en b. Dan zien wij dat er slechts één mogelijkheid voor de Cayley tabel is, namelijk

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Er bestaat dus ten hoogste één groep met drie elementen (op benaming van de elementen na). Doch $(\mathbb{Z}_3, +)$ is een groep met drie elementen. Bijgevolg is er precies één groep met drie elementen.

Zij nu $G = \{e, a, b, c\}$ een groep met vier elementen. Dan bevat G een element van orde twee. Inderdaad, veronderstel dat dit niet zo is. Dan heeft a ofwel orde drie ofwel orde vier (ga dit na). Dit laatste geval is echter onmogelijk want dan is a^2 van orde twee. In het andere geval is het element van G dat niet behoort tot $\{e, a, a^2\}$ een element dat gelijk is aan zijn inverse (ga dit na) en dus een element van orde twee. Dus steeds verkrijgen wij een contradictie.

Veronderstel dan dat b een element van orde twee is. Dan zijn er fundamenteel twee overblijvende mogelijkheden: ofwel is elk element verschillend van e van orde twee, ofwel is er een element van orde niet twee. Op benaming na zijn er dan slechts twee mogelijke Cayleytabellen:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

en

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

De laatste groep is cyclisch $\{e, a, a^2, a^3\}$ en de eerste is de Viergroep van Klein.

1.8 Directe producten

Wij geven nu een methode om uit twee (of meerdere groepen) een nieuwe groep te construeren.

Zij $(G, *)$ en $(H, \diamond)$ groepen. Dan is

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

een groep voor de volgende bewerking

$$(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \diamond h_2).$$

Men noemt dit het *direct product* van G en H. De groepen G en H noemt men de factoren van het direct product. Het neutraal element van deze groep is (e_G, e_H), met e_G het neutraal element van G en e_H het neutraal element van H.

Algemener, zij I een indexverzameling en, voor elke $i \in I$, zij G_i een groep. Dan is het direct product van deze groepen de verzameling

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I} \mid g_i \in G_i \text{ voor } i \in I\}$$

voorzien van de bewerking

$$(g_i)(g_i') = (g_i g_i').$$

Merk op dat dit direct product commutatief is als en slechts elke groep G_i commutatief is.

Als $(G, *)$ en $(H, \diamond)$ telkens de abelse groep $(\mathbb{R}, +)$ is, dan is $G \times H$ de groep $(\mathbb{R}^2, +)$.

Beschouw de abelse groepen $(\mathbb{Z}_2, +)$ en $(\mathbb{Z}_3, +)$. Dan is $\mathbb{Z}_2 \times \mathbb{Z}_3$ ook een abelse groep en het element $([1]_2, [1]_3)$ heeft orde 6. Dus is dit direct product een cyclische groep van orde 6.

De groep $\mathbb{Z}_2 \times \mathbb{Z}_2$ heeft geen element van orde 4. Elk element verschillend van het neutraal element heeft orde 2. Deze groep is de Viergroep van Klein.

Eigenschap 1.8.1. *Zij $G = G_1 \times G_2 \times \cdots \times G_n$ een direct product van groepen. Als $g_i \in G_i$ eindige orde m_i heeft dan is*

$$o(g_1, g_2, \ldots, g_n) = \text{kgv}(m_1, m_2, \ldots, m_n).$$

Bewijs. Wij merken op dat

$$(g_1, \ldots, g_n)^k = e \text{ als en slechts als } g_i^k = e_{G_i} \text{ (voor elke) } 1 \leq i \leq n.$$

Dit laatste is equivalent met $m_i | k$. Dus het kleinste niet nul natuurlijk getal k dat deze voorwaarden vervult is $\text{kgv}(m_1, m_2, \ldots, m_n)$. □

Hoofdstuk

2 Deelgroepen

2.1 Definitie

Definitie 2.1.1. Zij $(G, *)$ een groep. Een deelverzameling H van G die een groep is voor de bewerking $*$ (beperkt tot H) noemt men een *deelgroep* van G.

Indien H een deelgroep is van G, dan noteren we dikwijls $H \leqslant G$.

Eigenschap 2.1.2. *Zij $(G, *)$ een groep. De volgende voorwaarden zijn equivalent voor een deelverzameling H van G:*

1. *H is een deelgroep van G;*
2. *de volgende voorwaarden zijn voldaan:*
   (a) *$H \neq \emptyset$,*
   (b) *als $h_1, h_2 \in H$ dan $h_1 * h_2 \in H$,*
   (c) *als $h \in H$ dan $h^{-1} \in H$;*
3. *de volgende voorwaarden zijn voldaan:*
   (a) *$H \neq \emptyset$,*
   (b) *als $h_1, h_2 \in H$ dan $h_1 * h_2^{-1} \in H$.*

Bewijs. (1) $\Rightarrow$ (2). Omdat $e_H \in H$ is $H \neq \emptyset$. Ook als $h_1, h_2 \in H$ dan is $h_1 * h_2 \in H$.

Omdat $e_H e_G = e_H$ en $e_H e_H = e_H$ volgt er dat $e_H e_G = e_H e_H$. Dus $e_H = e_G$.

Zij nu $h \in H$. Zij h^{-1} de inverse van h in G en zij h' de inverse van h in H. Dan

$$hh^{-1} = e_G = e_H = hh'$$

en dus (door vereenvoudiging) $h^{-1} = h' \in H$.

(2) $\Rightarrow$ (1). Wegens voorwaarde (2.b) definiëert $*$ een bewerking op de niet-lege verzameling H. Omdat $(G, *)$ associatief is is ook $(H, *)$ associatief. Wegens voorwaarden (2.a) en (2.c) bestaat er een $h \in H$ en en dus ook $h^{-1} \in H$. Bijgevolg is $hh^{-1} = e_G \in H$. Dus is e_G ook het neutraal element van $(H, *)$. Wegens voorwaarde (2.c) heeft elk element van H een inverse in H. Dus is $(H, *)$ een groep.

De equivalentie van (2) en (3) laten wij als oefening. □

Gevolg 2.1.3. *Zij G een eindige groep. De volgende voorwaarden zijn equivalent voor een niet lege deelverzameling H van G:*

1. $H \leqslant G$
2. *als $h_1, h_2 \in H$ dan $h_1 * h_2 \in H$.*

Bewijs. Wegens de vorige eigenschap is het voldoende dat uit (2) volgt dat $h^{-1} \in H$ als $h \in H$. Welnu, omdat G eindig is heeft elk element $h \in H$ eindige orde. Zij k de orde van $h \in H$. Dan $h^{-1} = h^{k-1} \in H$. □

De volgende eigenschap zal ons in staat stellen om het concept *voortbrengers van een groep* te definiëren.

Eigenschap 2.1.4. *Zij G een groep en $\{H_i \mid i \in I\}$ een verzameling deelgroepen van G. Dan is*

$$\bigcap_{i \in I} H_i = \{g \in G \mid g \in H_i, \text{ voor alle } i \in I\}$$

een deelgroep van G.

Bewijs. Zij $D = \bigcap_{i \in I} H_i$. Omdat $e \in H_i$ voor elke i volgt er dat $e \in D$. Dus $D \neq \emptyset$. Verder, als $g_1, g_2 \in D$ dan $g_1 g_2^{-1} \in D$. Dus is D een deelgroep. □

2.2 Voorbeelden

(1) Beschouw de groep $\mathbb{Z}, +$. Kies $n \in \mathbb{Z} \setminus \{0\}$ en definieer $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$. Kies twee elementen $a, b \in n\mathbb{Z}$. Het is duidelijk dat $a - b \in n\mathbb{Z}$, dus $n\mathbb{Z}$ is een deelgroep van $\mathbb{Z}, +$.

(2) Beschouw de groep $\mathbb{C}, \cdot$. Definieer $N := \{z \in \mathbb{C} \mid |z| = 1\}$. Omdat $|z^{-1}| = \frac{1}{|z|}$, volgt dus dat voor twee elementen $a, b \in N$, $|a \cdot b^{-1}| = 1$, dus $a \cdot b^{-1} \in N$ en dus N is een deelgroep van $\mathbb{C}, \cdot$.

(3) Beschouw de groep $\mathrm{GL}_n(F), \cdot$, F een lichaam, $\cdot$ de gewone matrixvermenigvuldiging. De verzameling van matrices uit $\mathrm{GL}_n(F)$ met determinant 1, genoteerd als $\mathrm{SL}_n(F)$ vormt samen met $\cdot$ een deelgroep van $\mathrm{GL}_n(F), \cdot$.

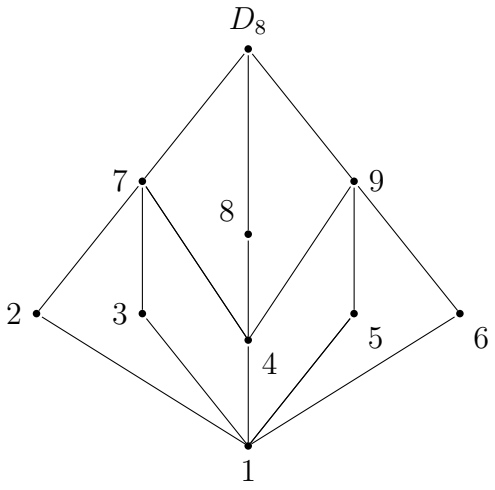
(4) Beschouw de groep $\mathbb{Z}_n, +$. Stel $n = 4$. Het is duidelijk dat $A = \{[0]_4, [2]_4\}$ een deelgroep is van $\mathbb{Z}_4$. Ga na als oefening dat $\mathbb{Z}_7$ als deelgroepen enkel $\{[0]_7\}$ en zichzelf heeft.

(5) Beschouw de D_{2n}, de diëdergroep van orde $2n$, we hebben gezien dat $D_{2n} = \{a^k, a^k b | k = 1 \dots n\}$. Noteer het eenheidselement als e. Veronderstel dat $n = 4$. Het is vrijwel onmiddellijk duidelijk dat de volgende deelverzamelingen deelgroepen zijn van D_8: $\{e, a, a^2, a^3\}$, $\{e, a^2, ab, a^3 b\}$, $\{e, a^2, b, a^2 b\}$, $\{e, a^2\}$, $\{e, b\}$, $\{e, ab\}$, $\{e, a^2 b\}$ en $\{e, a^3 b\}$. Samen met de triviale deelgroep, i.e. $\{e\}$ en de volledige groep D_8 zelf, is dit de volledige lijst van deelgroepen van D_8 (al vergt het een beetje werk om dit aan te tonen).

(6) Beschouw twee groepen G en H en hun direct product $G \times H$. Opnieuw is onmiddellijk duidelijk dat $\{(g, h) \mid g = e_G, h \in H\}$ en $\{(g, h) \mid g \in G, h = e_H\}$ twee deelgroepen zijn van $G \times H$.

Beschouw een niet-ledige verzameling V en een *partiële orderelatie* R of V, dit is een relatie die reflexief, anti-symmetrisch en transitief is. Dat de relatie R anti-symmetrisch is betekent per definitie dat xRy en yRx impliceert dat $x = y$. Een partiële orderelatie is een *orderelatie* als per definitie voor elke koppel (x, y) geldt dat xRy of yRx. Een verzameling V samen met een partiële orderelatie noemt men een partieel geordende verzameling (of ook poset). Beschouw een poset $V, \preccurlyeq$ en een niet-ledige deelverzameling $R \subset V$. Een *infimum* van R is een element $z \in V$ zodat $\forall x \in V, z \preccurlyeq x$ en $\forall x \in R, y \preccurlyeq x \Rightarrow y \preccurlyeq z$. Een infimum is dus de *grootste ondergrens*, waarbij "grootste" hier refereert naar de partiële ordening $\preccurlyeq$. Analoog wordt een *supremum* van R als kleinste bovengrens gedefinieerd. Een poset $V, \preccurlyeq$ is een tralie als elke twee elementen een uniek infimum en een uniek supremum hebben.

Beschouw nu de verzameling van alle deelgroepen van een groep G. Deze verzameling is niet ledig. Immers, de triviale deelgroep $\{e_G\}$ en de groep G zelf zijn deelgroepen van G. Noteer deze verzameling als $\mathcal{S}$. De relatie $\subset$ is duidelijk een partiële orderelatie. Aangezien de doorsnede van twee deelgroepen opnieuw een deelgroep is, is het eenvoudig om een infimum van twee elementen te construeren: dit is de doorsnede van de twee groepen. De constructie van een supremum is vergelijkbaar. Beschouw twee deelgroepen A, B van G. Noem H de verzamelingen van alle deelgroepen van G die A en B als groep omvatten. Deze verzameling is niet-ledig, ze bevat de groep G zelf. Volgens



Figuur 2.1: Hassediagram van de tralie van deelgroepen van D_8

Eigenschap 2.1.4 is de doorsnede van alle deelgroepen in deze verzameling opnieuw een deelgroep. Dit is het supremum van A en B.

We geven alle deelgroepen van D_8 een label: (1) $\{e\}$; $\{e, b\}$, $\{e, a^2b\}$, $\{e, a^2\}$, $\{e, ab\}$, en $\{e, a^3b\}$ respectievelijk (2) tot en met (6); $\{e, a^2, b, a^2b\}$, $\{e, a, a^2, a^3\}$, $\{e, a^2, ab, a^3b\}$ respectievelijk (7), (8) en (9). Figuur 2.1 is het zogenaamde Hassediagram van de deelgroepentralie van D_8.

2.3 Voortbrengers

Definitie 2.3.1. Zij X een deelverzameling van een groep G dan is de doorsnede van alle deelgroepen die X omvatten een deelgroep van G, namelijk de kleinste (voor de inclusierelatie) die X omvat. Men noteert deze groep als $\langle X \rangle$ en noemt dit de deelgroep voortgebracht door X. Indien $X = \{x_1, x_2, \cdots, x_n\}$ dan noteert men $\langle X \rangle$ ook als $\langle x_1, x_2, \cdots, x_n \rangle$.

Als $X = \{x\}$ dan noemt men $\langle x \rangle$ de cyclische deelgroep van G voortgebracht door x.

Merk op dat een groep G cyclisch is als en slechts als er een $g \in G$ bestaat zodat $G = \langle g \rangle$.

Ook $\langle \emptyset \rangle = \{e\}$.

Eigenschap 2.3.2. *Zij $(G, *)$ een groep en X een niet lege deelverzameling van G. Dan*

$$\langle X\rangle = \{x_1 * x_2 * \cdots x_n \mid n \in \mathbb{N}_0,\ x_i \in X \text{ of } x_i^{-1} \in X,\ 1 \leq i \leq n\}.$$

Indien G een eindige groep is dan

$$\langle X\rangle = \{x_1 * x_2 * \cdots x_n \mid n \in \mathbb{N}_0,\ x_i \in X,\ 1 \leq i \leq n\}.$$

Bewijs. Omdat, per definitie, $\langle X\rangle$ de kleinste deelgroep van G is die alle elementen van X bevat, behoren alle elementen $x_1 * x_2 * \cdots x_n$ tot $\langle X\rangle$ (met $n \in \mathbb{N}_0$ en x_i of $x_i^{-1} \in X$). Stel

$$D = \{x_1 * x_2 * \cdots x_n \mid n \in \mathbb{N}_0,\ x_i \in X \text{ of } x_i^{-1} \in X,\ 1 \leq i \leq n\}$$

dan is D omvat in alle deelgroepen die X omvatten. Verder, als $d_1, d_2 \in D$ dan verifiëert men eenvoudig dat $d_1 d_2^{-1} \in D$. Omdat D niet leeg is volgt er dus dat D reeds een deelgroep is die X omvat. Het eerste gedeelte van het resultaat volgt dan.

Het tweede gedeelte bewijst men analoog en men maakt gebruik van het feit dat in eindige groep G een niet lege deelverzameling D een deelgroep is als $d_1 d_2 \in D$ voor $d_1, d_2 \in D$. □

Voorbeelden

(1) De groep van de complexe n-de éénheidswortels is cyclisch:

$$E_n = \langle e^{2\pi i/n}\rangle.$$

(2) Een andere cyclische groep is

$$\mathbb{Z}_n = \langle [1]_n\rangle.$$

(3) Stellen we zoals gebruikelijk, met $\xi_n = e^{\frac{2\pi i}{n}}$,

$$a = \begin{bmatrix} \xi_n & 0 \\ 0 & \xi_n^{-1} \end{bmatrix} \quad \text{en} \quad b = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

Dan is de diëdergroep $D_{2n} = \langle a, b\rangle$.

De volgende relaties gelden voor de voortbrengers van D_{2n}:

$$a^n = 1,\ b^2 = 1 \text{ en } ba = a^{-1}b.$$

Met behulp van deze relaties (en de associativiteit) kan men alle mogelijke producten in D_{2n} berekenen. Met andere woorden, de volledige groep D_{2n} is in feite bepaald door deze drie relaties, of nog, een groep voortgebracht door de "abstracte" elementen a en b die aan deze drie relaties voldoen, is noodzakelijk de groep D_{2n}. Men schrijft dit als

$$D_{2n} = \langle a, b \mid a^n = 1,\ b^2 = 1,\ ba = a^{-1}b \rangle.$$

Dit is een voorbeeld van een groep G die gegeven is via voortbrengers (a en b in dit geval) en relaties ($ba = a^{-1}b$, $a^n = 1$ en $b^2 = 1$ in dit geval); men noemt dit een presentatie van G. Dus de elementen van de groep G bestaan uit producten van machten van de generatoren en men maakt identificaties via de gegeven lijst relaties. Bijvoorbeeld in D_{2n} zijn de elementen $a^i b$ en ba^{-i} gelijk.

Men moet echter wel voorzichtig zijn dat men alle mogelijke identificaties maakt die volgen uit de gegeven relaties. Bijvoorbeeld

$$\langle a \mid a^2 = 1,\ a^3 = 1 \rangle = \{1\}.$$

Inderdaad $1 = a^3 = a^2 a = 1a = a$.

De studie van groepen aan de hand van presentaties is een bloeiend onderzoeksdomein uit de *computationele* groepentheorie. Zo is het probleem of een groep met een gegeven presentatie een eindig aantal element heeft, een niet-triviaal probleem uit dit gebied.

(4) Beschouw de groep

$$V = \langle a, b \mid ab = ba,\ a^2 = 1,\ b^2 = 1 \rangle.$$

Uit de relatie $ab = ba$ volgt dat elk element van V kan geschreven worden als $a^i b^j$ met $i, j \in \mathbb{Z}$. Omdat $a^2 = 1$ en $b^2 = 1$ is het voldoende dat $i, j \in \{0, 1\}$. Dus

$$V = \{1, a, b, ab\}.$$

Nu moet men nog aantonen dat deze vier elementen verschillend zijn. Men kan dit bijvoorbeeld aantonen door een "model" van deze groep te geven. De Viergroep van Klein is zo een model (het is voortgebracht door twee elementen die voldoen aan de vermelde relaties).

(5) Wij definiëren nu een groep van orde acht, de quaternionengroep van orde 8. In $\mathrm{GL}_2(\mathbb{C})$ nemen wij de matrices

$$J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ en } L = JK = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Zij

$$Q_8 = \{I, -I, J, -J, K, -K, L, -L\}.$$

Dit is een deelgroep van $\mathrm{GL}_2(\mathbb{C})$. Om dit aan te tonen, en aangezien Q_8 eindig is, is het voldoende te bewijzen dat Q_8 multiplicatief gesloten is. Dit volgt uit de volgende relaties:

$$J^2 = K^2 = L^2 = -I$$

en

$$JK = L,\ KJ = -L,\ KL = J,\ LK = -J,\ LJ = K \text{ en } JL = -K.$$

Dus

$$Q_8 = \langle J, K \rangle.$$

In een latere cursus geven wij de theoretische fundering voor presentaties. Wij vermelden nog dat de groep voortgebracht door een verzameling X die aan geen verdere relaties voldoet de *vrije groep* op X genoemd wordt. Dus deze groep bestaat uit alle producten van machten van elementen in X. Als $X \neq \emptyset$ dan bevat deze groep oneindig veel elementen en als $|X| \geq 2$ dan is deze groep ook niet commutatief.

2.4 Speciale Deelgroepen

Er zijn heel wat belangrijke deelgroepen in een groep. Wij behandelen hier slechts enkele.

Definitie 2.4.1. Zij G een groep en zij $g \in G$. De **centralisator** van $g \in G$ is de verzameling

$$C_G(g) = \{x \in G \mid xg = gx\}.$$

Het **centrum** van G is de verzameling

$$Z(G) = \{x \in G \mid xg = gx \text{ voor alle } g \in G\} = \bigcap_{g \in G} C_G(g).$$

Eigenschap 2.4.2. *Zij G een groep en $g \in G$. Dan zijn $C_G(g)$ en $Z(G)$ deelgroepen van G.*

Bewijs. Omdat, $eg = g = ge$ verkrijgen wij $e \in C_G(g)$; i.h.b., $C_G(g) \neq \emptyset$. Als $h_1, h_2 \in$

$C_G(g)$ dan

$$\begin{aligned}(h_1h_2)g &= h_1(h_2g)\\ &= h_1(gh_2)\\ &= (h_1g)h_2\\ &= (gh_1)h_2\\ &= g(h_1h_2)\end{aligned}$$

Dus $h_1h_2 \in C_G(g)$.

Ook volgt uit $h_1g = gh_1$ dat $h_1^{-1}h_1gh_1^{-1} = h_1^{-1}gh_1h_1^{-1}$. Dus $gh_1^{-1} = h_1^{-1}g$, m.a.w., $h_1^{-1} \in C_G(g)$.

Er volgt dat $C_G(g)$ een deelgroep is van G. Analoog bewijst men dat het centrum een deelgroep is. □

Een groep G is commutatief als en slechts als $G = Z(G)$.

Het centrum van $GL_n(F)$ (F een lichaam) is de groep $\{fI_n \mid 0 \neq f \in F\}$.

Het centrum van D_8 is de deelgroep $\langle a^2\rangle = \{1, a^2\}$. In het algemeen, voor $n \geq 3$,

$$Z(D_{2n}) = \begin{cases} \{1\} & \text{als } n \text{ oneven} \\ \langle a^{n/2}\rangle & \text{als } n \text{ even}\end{cases}$$

2.5 Cyclische groepen

Eigenschap 2.5.1. *Een deelgroep van een cyclische groep is cyclisch.*

Bewijs. Zij $G = \langle g\rangle$ een cyclsiche groep. Dus $G = \{g^k \mid k \in \mathbb{Z}\}$. Zij H een deelgroep. Als $H = \{1\}$ dan is $H = \langle 1\rangle$, en dus is H cyclisch. Veronderstel dat $H \neq \{1\}$ en zij $g^k \in H$ met k minimaal in $\mathbb{N}_0$. Wij tonen nu aan dat $H = \langle g^k\rangle$. Inderdaad, zij $g^n \in H$. Schrijf $n = qk + r$ met $q, r \in \mathbb{Z}$ en $0 \leq r < k$. Dan

$$g^r = g^n g^{-qk} = g^n(g^{-k})^q \in H.$$

Wegens de keuze van k volgt er dat $r = 0$. Bijgevolg $g^n \in \langle g^k\rangle$ en dus $H = \langle g^k\rangle$. □

Eigenschap 2.5.2. *Zij $G = \langle g \rangle$ een cyclische groep van eindige orde n en zij k een geheel getal. Dan is de orde van de cyclische deelgroep $\langle g^k \rangle$ gelijk aan $\frac{n}{\text{ggd}(n,k)}$. I.h.b. is de orde van elke deelgroep van een eindige cyclische groep G een deler van de orde van G.*

Bewijs. Omdat $G = \langle g \rangle$ eindige orde n heeft weten wij reeds dat $o(g) = n$. Zij nu $k \in \mathbb{Z}$. Dan is g^k van orde l als en slechts als l is het kleinste niet nul natuurlijk getal zodat $(g^k)^l = 1$, of equivalent, l is het kleinste niet nul natuurlijk getal zodat $n|(kl)$. Duidelijk $l = \frac{n}{\text{ggd}(n,k)}$. Bijgevolg is de orde van $\langle g^k \rangle$ gelijk aan $o(g^k) = \frac{n}{\text{ggd}(n,k)}$. □

Eigenschap 2.5.3. *Zij $G = \langle g \rangle$ een eindige cyclische groep van orde n en $d \in \mathbb{N}$ een deler van n. Dan heeft G precies één deelgroep van orde d, namelijk $\langle g^{n/d} \rangle$.*

Bovendien zijn er precies d oplossingen voor $x^d = 1$ in G, en dit zijn precies de elementen van $\langle g^{n/d} \rangle$.

Bewijs. Duidelijk is $\langle g^{n/d} \rangle = \{1, g^{n/d}, g^{2(n/d)}, \cdots, g^{(d-1)(n/d)}\}$. Dus er bestaat minstens één deelgroep van orde d. Wij bewijzen nu dat er ten hoogste één is. Zij daarom H ook een deelgroep van orde d. Wegens een vorige eigenschap is H ook cyclisch, en dus $H = \langle g^k \rangle$ voor een $0 \leq k < n$. Dus $g^{kd} = 1$. Omdat g orde n heeft volgt er $n|(kd)$. Er bestaat dus een $v \in \mathbb{Z}$ zodat $vn = kd$, m.a.w., $k = v(n/d)$. Er volgt $H = \langle g^k \rangle \subseteq \langle g^{n/d} \rangle$. Omdat beide groepen van orde d zijn volgt er $H = \langle g^{n/d} \rangle$.

De vorige redenering toont aan dat $(g^k)^d = 1$ als en slechts als $g^k \in \langle g^{n/d} \rangle$. Omdat $|\langle g^{n/d} \rangle| = d$ zijn er precies d oplossingen van de vergelijking $x^d = 1$ in G. □

Voor een geheel getal a noteren wij met $a\mathbb{Z}$ de verzameling $\{az \mid z \in \mathbb{Z}\}$. Dit is de cyclische deelgroep van $(\mathbb{Z}, +)$ voortgebracht door het element a. Voor een ring R schrijf $R^* := R \setminus \{0\}$.

Eigenschap 2.5.4. *Zij a en b niet nul gehele getallen. Dan*

$$\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z} = \text{ggd}(a, b)\mathbb{Z}.$$

Bewijs. In de cyclische groep $(\mathbb{Z}, +)$ is $\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z}$ een deelgroep. Bijgevolg is $\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z}$ een cyclische groep en dus bestaat er een $d \in \mathbb{Z}$ zodat

$$\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Omdat $a \in d\mathbb{Z}$ volgt er $d|a$. Analoog $d|b$ en dus $d|\text{ggd}(a,b)$. Als nu $c \in \mathbb{Z}$ en $c|a$ en $c|b$, dan bestaan $v, w \in \mathbb{Z}$ zodat $cv = a$ en $cw = b$. Schrijf $d = xa + yb$. Dan $d = xcv + ycw$ en dus $c|d$. Dit toont aan dat $d = \text{ggd}(a,b)$. □

Eigenschap 2.5.5. *Indien p een priemgetal is dan is $\mathbb{Z}_p$ een lichaam, i.h.b. is de verzameling van niet nul elementen $\mathbb{Z}_p^*$ een abelse groep voor de vermenigvuldiging.*

Bewijs. Zij nu p een priemgetal en $[0]_p \neq [a]_p \in \mathbb{Z}_p$. Dan $\text{ggd}(a,p) = 1$. Dus, bestaan er (wegens het eerste gedeelte van de eigenschap) $v, w \in \mathbb{Z}$ zodat

$$va + wp = 1.$$

Bijgevolg

$$[v]_p[a]_p = [v]_p[a]_p + [w]_p[p]_p = [1]_p,$$

en is $[v]_p$ de inverse van $[a]_p$. Er volgt dat $\mathbb{Z}_p^*$ een abelse groep voor de vermenigvuldiging is en dus is $\mathbb{Z}_p$ een lichaam. □

Hoofdstuk

3 Nevenklassen

Zij G een eindige groep, d.w.z., G is een groep met eindig veel elementen. Zij H een deelgroep. In dit hoofdstuk bewijzen wij dat de orde van H een deler is van de orde van G (Stelling van Lagrange). Om dit te bewijzen voeren wij het begrip nevenklasse in.

3.1 Definitie

Definitie 3.1.1. Zij G een groep en H een deelgroep. Als $g \in G$ dan is de linkernevenklasse van g de verzameling

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

De rechternevenklasse van g is de verzameling

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

Duidelijk is $eH = H = He$ en $g \in gH$. Dus is $gH \neq H$ als $g \notin H$. Ook $gH \cap H = \emptyset$ als $g \notin H$.

Eigenschap 3.1.2. *Zij H een deelgroep van een groep G. Zij R de relatie op G gedefiniëerd door*

$$aRb \text{ als en slechts als } a^{-1}b \in H.$$

Dan is R een equivalentierelatie op G en de equivalentieklasse die $g \in G$ bevat is de linkernevenklasse gH.

Bewijs. Wij moeten drie eigenschappen bewijzen om aan te tonen dat R een equivalentierelatie is.

Omdat H een deelgroep is geldt voor $g \in G$ dat $g^{-1}g = 1 \in H$. Dus gRg. Dit toont aan dat R reflexief is.

Veronderstel dat aRb, d.w.z. $a^{-1}b \in H$. Omdat H een deelgroep is volgt er $b^{-1}a = (a^{-1}b)^{-1} \in H$. Bijgevolg bRa. Dus is R symmetrisch.

Veronderstel aRb en bRc, dan $a^{-1}b, b^{-1}c \in H$ en dus

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H.$$

Bijgevolg aRc en dus is R transitief.

Wij bepalen nu de equivalentieklasse van $g \in G$. Zij daarom $x \in G$. Dan, $x \in G$ is in de equivalentieklasse van g als en slechts als $g^{-1}x \in H$, of equivalent $x \in gH$. Dus is de equivalentieklasse van g de linkernevenklasse gH. □

Uit de vorige eigenschap volgt onmiddellijk het volgende resultaat.

Eigenschap 3.1.3. *Zij H een deelgroep van een groep G, en zij $a, b \in G$. Dan*

1. *$aH = bH$ als en slechts als $a^{-1}b \in H$ (dus $aH = H$ als en slechts als $a \in H$).*
2. *als $aH \neq bH$ dan $aH \cap bH = \emptyset$.*
3. *$\bigcup_{g \in G} gH = G$.*

Bovendien, $|aH| = |H|$.

3.2 Stelling van Lagrange

Stelling 3.2.1. *(Stelling van Lagrange)*
Zij H een deelgroep van een eindige groep G. Dan is $|H|$ een deler van $|G|$ en het aantal linker (respectievelijk rechter) nevenklassen van H in G is gelijk aan $\frac{|G|}{|H|}$.

Bewijs. Wij weten reeds dat de linkernevenklassen gH ($g \in G$) de equivalentieklassen zijn voor de relatie R en $|gH| = |H|$. Omdat de equivalentieklassen een partitie vormen van de eindige verzameling G volgt het resultaat. □

Uit de vorige eigenschap weten wij dat het aantal linker nevenklassen gelijk is aan het aantal rechter nevenklassen. Wij noemen dit aantal de index.

Definitie 3.2.2. Het aantal linker (of rechter) nevenklassen van een deelgroep H van een groep G noemt men de *index* van H in G. Dit wordt gewoonlijk genoteerd als $[G : H]$.

Eigenschap 3.2.3. *Zij G een eindige groep.*

1. *Als $g \in G$ dan is $o(g)$ een deler van $|G|$.*
2. *Als H en K deelgroepen zijn van G met $H \subseteq K$, dan $[G : H] = [G : K]\,[K : H]$.*

Bewijs. Wij weten dat $|\langle g \rangle| = o(g)$. Dus wegens de Stelling van Lagrange, $o(g)$ deelt $|G|$.

Wegens de Stelling van Lagrange,

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

□

3.3 Toepassingen

Eigenschap 3.3.1. *Elke groep van priem orde is een cyclische groep.*

Bewijs. Zij G een groep van orde p, een priemgetal. Zij $e \neq g \in G$, dan is $H = \langle g \rangle$ een deelgroep van G. Wegens de Stelling van Lagrange is $|H|$ een deler van p. Dus $|H| = 1$ of $|H| = p$. Omdat $H \neq \{1\}$ volgt er $|H| = p$ en dus $H = G$. Bijgevolg is G cyclisch. □

Eigenschap 3.3.2. (Fermat)
Zij p een priem getal. Als $a \in \mathbb{Z}$ dan

$$a^p \equiv_p a.$$

Bewijs. Als $[a]_p = [0]_p$ dan $[a]_p^p = [a]_p = [0]_p$, dus $a^p \equiv_p a$. Veronderstel nu dat $[a]_p \neq [0]_p$. Dan is $[a]_p \in \mathbb{Z}_p^*$. Omdat $\mathbb{Z}_p^*$ een groep is met $p-1$ elementen verkrijgen wij uit de Stelling van Lagrange dat $o([a]_p)|(p-1)$. Dus $[a]_p^{p-1} = [1]_p$. Vermenigvuldig dan met $[a]_p$ en wij verkrijgen $[a]_p^p = [a]_p$. □

Een andere welbekende stelling van Fermat (Fermat's Last Theorem) : voor alle gehele getallen $n \geq 3$, bestaan er geen strikt positieve gehele getallen a, b, c zodat $a^n + b^n = c^n$. Fermat beweerde dat hij een "mooi" bewijs had van dit resultaat maar dat de

marge te klein was om het bewijs op te schrijven. Hij bewees het elders voor $n = 4$ en, later, bewezen anderen het voor kleine waarden van n. Het is een bijzondere uitdaging geworden om het algemene resultaat te bewijzen. Vele wiskundigen hebben zich hierover gebogen en heel wat nieuwe technieken zijn ontwikkeld. Pas in 1995 bewees Andrew Wiles Fermat's Last Theorem.

Eigenschap 3.3.3. (Wilson)
Zij p een priem getal. Dan

$$(p-1)! \equiv_p -1.$$

Bewijs. Als $p = 2$ dan is dit resultaat duidelijk. Veronderstel dus dat $p \neq 2$. Als $a_1, a_2, \cdots, a_n$ alle elementen zijn in een eindige abelse groep G, dan is $a_1 a_2 \cdots a_n$ gelijk aan het product van alle elementen van orde 2 (elk ander element wordt "geschrapt" met zijn inverse). Nu heeft $\mathbb{Z}_p^*$ slechts $[-1]_p$ als element van orde 2. Er volgt dus dat het product van alle elementen van $\mathbb{Z}_p^*$, namelijk $[(p-1)!]_p$, gelijk is aan $[-1]_p$. Dus $(p-1)! \equiv_p -1$. □

De Euler φ-functie wordt als volgt gedefiniëerd:

$$\varphi(1) = 1$$

en voor $m \in \mathbb{N}$, $m > 1$,

$$\varphi(m) = |\{r \in \mathbb{N} \mid (r, m) = 1 \text{ en } 1 \leq r < m\}|.$$

Eigenschap 3.3.4. *(Euler)*
Zij $m \in \mathbb{N}_0$. Dan

$$|U(\mathbb{Z}_m)| = \varphi(m).$$

Zij $r \in \mathbb{N}_0$. Als $(r, m) = 1$ dan

$$r^{\varphi(m)} \equiv_m 1.$$

Bewijs. Beschouw de multiplicatieve groep $U(\mathbb{Z}_m)$ van de inverteerbare elementen in de ring $\mathbb{Z}_m$. Als a een niet nul geheel getal is dan $a\mathbb{Z} + m\mathbb{Z} = \text{ggd}(a, m)\mathbb{Z}$. Er volgt dat $[a]_m \in U(\mathbb{Z}_m)$ als en slechts als $(a, m) = 1$. Dus $|U(\mathbb{Z}_m)| = \varphi(m)$.

Als nu $[r]_m \in U(\mathbb{Z}_m)$ volgt er $[r]_m^{\varphi(m)} = [1]_m$. Dus volgt ook het laatste gedeelte van de eigenschap. □

Hoofdstuk 4

Normaaldelers

In dit hoofdstuk bestuderen wij speciale deelgroepen, namelijk deze waarvoor een linkerenevenklasse steeds een rechternevenklasse is. In het volgende hoofdstuk kunnen wij uit zulke groepen nieuwe groepen construeren.

4.1 Definitie

Voor twee deelverzamelingen X en Y van een groep G noteert men

$$XY = \{xy \mid x \in X,\ y \in Y\}.$$

Als $X = \{x\}$ dan noteren wij XY ook als xY.

In het algemeen is XY verschillend van YX. Maar merk op dat gelijkheid wel kan optreden, ook als de elementen van X en Y niet noodzakelijk commuteren. Inderdaad, in D_{2n} geldt $\{a\}\ \{1, b\} = \{a, ab\}$ maar $\{1, b\}\ \{a\} = \{a, a^{n-1}b\}$. Ook $\langle a\rangle\{b\} = \{b\}\langle a\rangle$.

Definitie 4.1.1. Zij N een deelgroep van een groep G. Men noemt N een normale deelgroep van G als en slechts als $gN = Ng$ voor alle $g \in G$. Met $N \lhd G$ noteert men dat N een normale deelgroep is van G.

Als N een normale deelgroep is van een groep G, dan noteert men de verzameling van de nevenklassen van N in G (dus equivalentieklassen) als G/N.

Eigenschap 4.1.2. *Zij $N \leqslant G$. Dan zijn de volgende voorwaarden equivalent:*

1. $N \lhd G$,
2. $gNg^{-1} = N$ *voor alle* $g \in G$,
3. $gNg^{-1} \subseteq N$ *voor alle* $g \in G$,
4. *elke rechter nevenklasse van* N *is een linker nevenklasse.*

Bewijs. Als $gN = Ng$ dan $gNg^{-1} = Ngg^{-1}$ en dus $gNg^{-1} = N$. Dus volgt (2) uit (1). Dat (3) uit (2) volgt is evident.

Veronderstel nu (3). Dan $gNg^{-1} \subseteq N$ voor elke $g \in G$. Nu is ook $g^{-1} \in G$ en dus $g^{-1}N(g^{-1})^{-1} \subseteq N$, voor elke $g \in G$. Dit laatste is equivalent met $N \subseteq gNg^{-1}$. Bijgevolg $N = gNg^{-1}$ en dus $Ng = gN$, dit bewijst (1).

Uiteraard volgt (4) uit (1). Er blijft dus te bewijzen dat (1) volgt uit (4). Gegeven is dus dat voor elke $g \in G$ een $h \in G$ bestaat zodat $Ng = hN$. Dus $g \in hN$. Omdat hN een equivalentieklasse is volgt er $hN = gN$. Dus $Ng = gN$ (voor elke $g \in G$). Dit toont aan dat $N \lhd G$. □

Gevolg 4.1.3. *Voor een willekeurige groep G geldt steeds $Z(G) \lhd G$. In een abelse groep zijn alle deelgroepen normale deelgroepen.*

Bewijs. Onmiddellijk uit Eigenschap 4.1.2. □

Normale deelgroepen werden in 1831 geintroduceerd door Evariste Galois, dit in het kader van het probleem wanneer een polynoomvergelijking oplosbaar is door radikalen. Galois merkte op dat een deelgroep H van een groep G van permutaties twee ontbindingen van G gaf (wij noemen dit linkse en rechtse nevenklassen). Als de twee ontbindingen samenvallen, dus als de linkse nevenklassen dezelfde zijn als de rechtse, dan noemde Galois de ontbinding "echt". Dus een deelgroep met een echte ontbinding noemen wij een normale deelgroep. Camille Jordan ging verder met deze ideeen, in 1865 en 1869. Hij definieerde ook normale deelgroepen (zonder de term te gebruiken) en was de eerste die een definitie gaf van een simpele groep.

4.2 Elementaire eigenschappen

Eigenschap 4.2.1. *Zij $N \leqslant G$. Als $[G : N] = 2$ dan is $N \lhd G$.*

Bewijs. Gegeven is $[G : N] = 2$, d.w.z. er bestaan slechts twee linkernevenklassen. Omdat deze een partitie vormen van G en omdat $N = eN$ één van de linkernevenklassen is, volgt er dat $G \setminus N$ de andere linkernevenklasse is. Dus, als $g \notin N$, dan $gN \neq N$ en bijgevolg $gN = (G \setminus N)$.

Er zijn ook slechts twee rechternevenklassen. Men bewijst dan analoog dat $Ng = (G \setminus N)$ voor $g \notin N$. Dus voor zo een element g, $gN = (G \setminus N) = Ng$. Indien $g \in N$ dan $gN = N = Ng$. Bijgevolg $N \lhd G$. □

Omdat $\langle a \rangle$ een deelgroep is van index twee in D_{2n} volgt er dat $\langle a \rangle \lhd D_{2n}$. Doch $\{1, b\}$ is niet normaal in D_{2n}.

Eigenschap 4.2.2. *Zij $N \lhd G$. Als $H \leqslant G$, dan is*

$$\langle H \cup N \rangle = HN = NH.$$

Bewijs. Omdat $\langle H \cup N \rangle$ de kleinste deelgroep is van G die H en N omvat is het duidelijk dat $HN \subseteq \langle H \cup N \rangle$. Wij bewijzen nu dat HN een deelgroep is. Omdat deze H en N omvat volgt er dan $\langle H \cup N \rangle = HN$.

Inderdaad, $e = ee \in HN$. Als $h_1, h_2 \in H$ en $n_1, n_2 \in N$, dan

$$(h_1 n_1)(h_2 n_2) = h_1 h_2 (h_2^{-1} n_1 h_2) n_2.$$

Omdat N een normale deelgroep is, $n_3 = h_2^{-1} n_1 h_2 \in N$. Bijgevolg

$$(h_1 n_1)(h_2 n_2) = h_1 h_2 (n_3 n_2) \in HN.$$

Ook

$$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} (h_1 n_1^{-1} h_1^{-1}) \in HN.$$

Dus is inderdaad HN een deelgroep.

Analoog bewijst men dat $\langle H \cup N \rangle = NH$. (Of men bewijst rechtstreeks, met methoden zoals in de voorgaande redenering, dat $NH = HN$.) □

In het algemeen is een willekeurige deelgroep H van een groep G geen normale deelgroep. Daarom definiëert men de **normalisator** van H in G als de verzameling

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Eigenschap 4.2.3. *Zij $H \leqslant G$. Dan is $N_G(H) \leqslant G$ en het is de grootste deelgroep (voor de inclusie relatie) waarin H een normale deelgroep is.*

Bewijs. Duidelijk is $e \in N_G(H)$. Als $g_1, g_2 \in N_G(H)$ dan

$$\begin{aligned} (g_1 g_2) H (g_1 g_2)^{-1} &= (g_1 g_2) H (g_2^{-1} g_1^{-1}) \\ &= g_1 (g_2 H g_2^{-1}) g_1^{-1} \\ &= g_1 H g_1^{-1} \\ &= H \end{aligned}$$

Ook, omdat $g_1 H g_1^{-1} = H$ volgt er

$$H = g_1^{-1} g_1 H g_1^{-1} g_1 = g_1^{-1} H g_1$$

Dus $g_1 g_2, g_1^{-1} \in N_G(H)$. Bijgevolg is $N_G(H)$ een deelgroep die H bevat, en uiteraard is $H \lhd N_G(H)$.

Als D een deelgroep is van G die H omvat en $H \lhd D$ dan is, voor elke $d \in D$, $dHd^{-1} = H$. Dus $D \subseteq N_G(H)$. Er volgt dat $N_G(H)$ de grootste deelgroep is die H omvat en waarin H normaal is. $\square$

Hoofdstuk

5 Quotiëntgroepen

In dit hoofdstuk gebruiken wij normale deelgroepen om nieuwe (kleinere) groepen te vormen.

5.1 Definitie

Definitie 5.1.1. Zij G een groep en $N \lhd G$. Dan is

$$G/N = \{gN \mid g \in G\}$$

de verzameling van alle nevenklassen van N in G. Op deze verzameling definiëren we de bewerking $*$:

$$(gN) * (hN) = (gh)N\,,$$

voor alle $g, h \in G$.

Stelling 5.1.2. *Zij G een groep en $N \lhd G$. Dan is $G/N, *$ een groep. Men noemt dit de* quotiëntgroep *van G door N. Het neutraal element van deze groep is eN en $(gN)^{-1} = g^{-1}N$.*

Bewijs. Wij moeten eerst en vooral aantonen dat de bewerking goed gedefiniëerd is. D.w.z., als $g_1N = g_2N$ en $h_1N = h_2N$ dan moeten wij aantonen dat $g_1h_1N = g_2h_2N$. Dat dit inderdaad zo is volgt uit de volgende redenering, waarbij Eigenschap 4.1.2 nodig is.

$$\begin{aligned} g_1h_1N = g_1h_1NN = g_1(h_1N)N = (g_1N)(h_1N) = (g_2N)(h_2N) = \\ g_2(Nh_2)N \ = g_2(Nh_2)N = g_2(h_2N)N = g_2h_2NN = g_2h_2N \end{aligned}$$

Men toont nu eenvoudig aan dat al de groepvoorwaarden voldaan zijn. Bovendien, $e_{G/N} = e_GN$, $(gN)^{-1} = (g^{-1})N$. □

In het vervolg zullen we de bewerking $*$ niet meer noteren.

Het is onmiddellijk duidelijk dat G/N abels is als G abels is. Maar er zijn voorbeelden van niet abelse groepen zodat G/N abels is voor sommige normale deelgroepen N of G.

Voorbeelden 5.1.3. 1. Zij $\mathbb{Z}$ de additieve groep van de gehele getallen en zij $n > 1$ een natuurlijk getal. Dan is $n\mathbb{Z} \lhd \mathbb{Z}$. De elementen van de quotiëntgroep $\mathbb{Z}/n\mathbb{Z}$ zijn de nevenklassen

$$a + n\mathbb{Z},$$

met $a \in \mathbb{Z}$. Dit zijn precies de equivalentieklassen $[a]_n$ van de equivalentierelatie $\equiv_n$ gedefinieerd in Paragraaf 1.6.1, dus dit rechtvaardigt ook de notatie die we daar gebruikt hebben.

Uiteraard geldt voor $a, b \in \mathbb{Z}$:

$$[a]_n + [b]_n = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = [a + b]_n.$$

De additieve structuur $\mathbb{Z}/n\mathbb{Z}, +$ uit Paragraaf 1.6.1 kan men dus ook bekomen als een quotiëntgroep van de additieve groep $\mathbb{Z}, +$.

2. Zij F een lichaam. Het is eenvoudig na te gaan dat $\mathrm{SL}_n(F) \lhd \mathrm{GL}_n(F)$. De elementen van de quotiëntgroep zijn de nevenklassen

$$A \cdot \mathrm{SL}_n(F),$$

met $A \in \mathrm{GL}_n(F)$. Zij $\det(A) = a$, dan bestaat een $B \in \mathrm{GL}_n(F)$ zodat

$$A = D(a)\ B,$$

met

$$D(a) = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Er volgt dat $\det(B) = 1$ en dus $B \in \mathrm{SL}_n(F)$. Bijgevolg

$$A \cdot \mathrm{SL}_n(F) = D(a)B \cdot \mathrm{SL}_n(F) = D(a) \cdot \mathrm{SL}_n(F).$$

Duidelijk is $D(a) \cdot \mathrm{SL}_n(F) \neq D(b) \cdot \mathrm{SL}_n(F)$ als $a \neq b$, $a, b \in F^*$. Er volgt dat

$$\mathrm{GL}_n(F)/\mathrm{SL}_n(F) = \{D(a) \cdot \mathrm{SL}_n(F) \mid 0 \neq a \in F\}.$$

3. Beschouw de diëdergroep $D_6 = \langle a, b \rangle$ van orde 6. Herinner dat $a^3 = 1$, $b^2 = 1$ en $ba = a^2b$.

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Zij $N = \langle a \rangle = \{1, a, a^2\}$. Dan is $[D_6 : N] = 2$ en dus is $N \lhd D_6$. De quotiëntgroep D_6/N heeft twee elementen: N en bN. De Cayleytabel van deze quotiëntgroep is:

	N	bN
N	N	bN
bN	bN	N

Dus $D_6/N = \langle bN \rangle$, een cyclische groep van orde 2.

Merk op dat we de Cayleytabel van D_6 kunnen opdelen in blokken zodat de elementen in één blok precies deze zijn van een nevenklasse van N. Dit is mogelijk omdat $N \lhd D_6$.

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

In $D_8 = \langle a, b \rangle$ met $a^4 = b^2 = 1$ en $ba = a^3b$ is $N = \langle a^2 \rangle = \{1, a^2\}$ een normale deelgroep en de elementen van D_8/N zijn de nevenklassen $N = \{1, a^2\}$, $Na = \{a, a^3\}$, $Nb = \{b, ba^2\}$ en $Nab = \{ab, a^3b\}$. De Caleytabel van deze groep is

	N	Na	Nb	Nab
N	N	Na	Nb	Nab
Na	Na	N	Nab	Nb
Nb	Nb	Nab	N	Na
Nab	Nab	Nb	Na	N

In blokvorm komt dit overeen met

$\cdot$	e	a^2	a	a^3	b	a^2b	ab	a^3b
e	e	a^2	a	a^3	b	a^2b	ab	a^3b
a^2	a^2	e	a^3	a	a^2b	b	a^3b	ab
a	a	a^3	a^2	e	ab	a^3b	a^2b	b
a^3	a^3	a	e	a^2	a^3b	ab	b	a^2b
b	b	a^2b	a^3b	ab	e	a^2	a^3	a
a^2b	a^2b	b	ab	a^3b	a^2	e	a	a^3
ab	ab	a^3b	b	a^2b	a	a^3	e	a^2
a^3b	a^3b	ab	a^2b	b	a^3	a	a^2	e

5.2 Deelgroepen van quotiëntgroepen

Stelling 5.2.1. *Stel G een groep en $N \lhd G$. Dan gelden de volgende eigenschappen.*

1. *Als $D \leqslant G$ een deelgroep is die N omvat dan is $D/N = \{dN \mid d \in D\}$ een deelgroep van G/N.*
2. *Elke deelgroep $\overline{D}$ van G/N is van de vorm D/N met D een deelgroep van G die N omvat. Een voorbeeld van zo een deelgroep D is $\{g \in G \mid gN \in \overline{D}\}$.*

Dus definiëert de correspondentie

$$D \mapsto D/N$$

een bijectie tussen de verzameling van de deelgroepen van G/N en de verzameling van deelgroepen van G die N omvatten.

Onder deze bijectie worden normale deelgroepen van G die N omvatten afgebeeld op normale deelgroepen van G/N.

Bewijs. (1) is eenvoudig te bewijzen.

(2) Zij $\overline{D}$ een deelgroep van G/N. Zij $D = \{g \in G \mid gN \in \overline{D}\}$. Men bewijst dan dat D een deelgroep is van G. Omdat, voor $n \in N$, $nN = N \in \overline{D}$ hebben wij dat $N \subseteq D$. Ook is $D/N = \overline{D}$.

(2) toont aan dat de afbeelding $D \mapsto D/N$ surjectief is. Deze afbeelding is ook injectief. Inderdaad, zij D_1, D_2 deelgroepen van G die N bevatten. Als $D_1/N = D_2/N$, dan bestaat voor elke $d_2 \in D_2$ een $d_1 \in D_1$ zodat $d_2N = d_1N$. Dus, $d_2 \in d_1N \subseteq D_1$. Bijgevolg $D_2 \subseteq D_1$. Analoog volgt de omgekeerde inclusie. Dus $D_1 = D_2$. $\square$

Hoofdstuk

6 Homomorfismen

In dit hoofdstuk bestuderen wij afbeeldingen tussen groepen die de algebraïsche structuur bewaren.

6.1 Definitie

Definitie 6.1.1. Zij $(G, *)$ en $(H, \diamond)$ groepen. Een afbeelding

$$f : G \to H$$

is een (groep-)homomorfisme als, voor alle $a, b \in G$,

$$f(a * b) = f(a) \diamond f(b)\,.$$

Voorbeelden 6.1.2. (1) Zij F een lichaam. Dan is $F^* = F \setminus \{0\}$ een abelse groep voor de vermenigvuldiging in F. De afbeelding

$$\det : \mathrm{GL}_n(F) \to F^* : A \mapsto \det(A).$$

is een homomorfisme.

(2) De afbeelding

$$E_n \to \mathbb{Z}/n\mathbb{Z} : e^{2k\pi i/n} \mapsto [k]_n$$

is een homomorfisme.

(3) Zij $\mathrm{GA}(1, \mathbb{R})$ de verzameling van alle functies

$$f : \mathbb{R} \to \mathbb{R}$$

van de vorm

$$f(x) = ax + b,$$

met $a, b \in \mathbb{R}$ en $a \neq 0$. Wij noteren deze functie als $f_{a,b}$. Dan is $\mathrm{GA}(1, \mathbb{R})$ een groep voor de samenstelling van functies. Zij $\mathcal{A}$ de verzameling van alle reële matrices van de vorm

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}.$$

Dit is een deelgroep van $\mathrm{GL}_2(\mathbb{R})$. Bovendien is

$$\varphi : \mathrm{GA}(1,\mathbb{R}) \to \mathcal{A} : f_{a,b} \mapsto \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

een bijectief homomorfisme.

(4) De afbeelding

$$(\mathbb{R}, +) \to (\mathbb{R}_0^+, \cdot) : x \mapsto e^x$$

is een bijectief homomorfisme. De inverse afbeelding

$$(\mathbb{R}_0^+, \cdot) \to (\mathbb{R}, +) : x \mapsto \ln x$$

is ook een bijectief homomorfisme.

(5) Zij $N \lhd G$. De afbeelding

$$\mathrm{nat} : G \to G/N : g \mapsto gN = \overline{g}$$

is een surjectief groephomomorfisme. Men noemt dit het *natuurlijke groephomomorfisme* van G naar G/N.

Eigenschap 6.1.3. *Zij $f : G \to H$ een groephomomorfisme. Dan gelden de volgende eigenschappen, voor alle $g \in G$:*

1. $f(e_G) = e_H$,
2. $f(g^{-1}) = f(g)^{-1}$,
3. $f(g^n) = (f(g))^n$, *voor alle* $n \in \mathbb{Z}$.

Bewijs. (1) Omdat $e_G e_G = e_G$ volgt er $f(e_G)f(e_G) = f(e_G) = e_H f(e_G)$. Dus $f(e_G) = e_H$.

(2) Uit $gg^{-1} = e_G = g^{-1}g$ volgt $f(g)f(g^{-1}) = f(e_G) = e_H = f(g^{-1})f(g)$. Dus $f(g)$ heeft als inverse $f(g^{-1})$ in H.

(3) Ga dit zelf na. □

6.2 Isomorfismen

Definitie 6.2.1. Een groephomomorfisme $f : G \to H$ dat injectief (respectievelijk surjectief) is noemt men een monomorfisme (respectievelijk epimorfisme).

Een groephomomorfisme $f : G \to H$ dat een epimorfisme en monomorfisme is noemt men een isomorfisme. Men zegt dan dat de groepen G en H isomorf zijn; men noteert dit als $G \cong H$.

Een isomorfisme $f : G \to G$ noemt men een automorfisme.

Twee cyclische groepen van dezelfde orde zijn isomorfe groepen.

Zij G een groep en $g \in G$, dan noemt men de afbeelding

$$\varphi_g : G \to G : x \mapsto gxg^{-1}$$

de conjugatie door g (of het inwendige automorfisme bepaald door g). Deze afbeelding is een automorfisme. De verzameling

$$\mathcal{C}(x) = \{gxg^{-1} \mid g \in G\}$$

noemt men de *conjugatieklasse* van x in G. Deze verzameling is ook een equivalentieklasse voor de equivalentierelatie $\sim$ op G gedefiniëerd als volgt:

$$x \sim y \text{ als en slechts als } y = gxg^{-1} \text{ voor een } g \in G\,.$$

Definitie 6.2.2. Zij G een groep. Dan noteert men met $\mathrm{Aut}(G)$ de verzameling van alle automorfismen van G. Voorzien van de bewerking "de samenstelling van functies" is dit een groep en men noemt dit de *automorfismegroep* van G. Met $\mathrm{Inn}(G)$ noteren wij de verzameling van alle inwendige automorfismen van G.

Eigenschap 6.2.3. *Zij G een groep, dan is* $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

Bewijs. Duidelijk is $\varphi_e \in \mathrm{Inn}(G)$. Ook

$$\varphi_g \circ \varphi_h^{-1} = \varphi_{gh^{-1}}\,.$$

Dus is $\mathrm{Inn}(G)$ een deelgroep van $\mathrm{Aut}(G)$.

Zij nu $f \in \mathrm{Aut}(G)$ dan

$$f \circ \varphi_g \circ f^{-1} = \varphi_{f(g)}\,.$$

Dus is $\mathrm{Inn}(G)$ een normale deelgroep van $\mathrm{Aut}(G)$. □

Eigenschap 6.2.4. *Zij $f : G \to H$ een groephomomorfisme. Voor elk element $g \in G$ geldt $o(f(g)) \mid o(g)$.*

Bewijs. Omdat f een groephomomorfisme is, geldt, met $n = o(g)$, $f(g)^n = f(g^n) = f(e_G) = e_H$. Dus $o(f(g)) \mid n$. □

Eigenschap 6.2.5. *Zij $f : G \to H$ een groepisomorfisme. Als $g \in G$, dan hebben g en $f(g)$ dezelfde orde.*

Bewijs. Bewijs dit zelf. □

Deze laatste eigenschap is dikwijls nuttig om aan te tonen dat twee groepen niet isomorf zijn. Beschouw bijvoorbeeld de groepen D_8 en Q_8. Beiden zijn van orde 8. De groep D_8 heeft twee elementen van orde vier (al de anderen zijn van orde twee of één). De groep Q_8 heeft zes elementen van orde vier. Dus wegens de vorige eigenschap zijn beide groepen niet isomorf. Man kan aantonen dat dit de enige (op isomorfisme na) niet abelse groepen van orde acht zijn.

6.3 Homomorfismestellingen

Definitie 6.3.1. Zij $f : G \to H$ een groephomomorfisme. De kern van f is de verzameling

$$\ker(f) = \{g \in G \mid f(g) = e_H\}.$$

Eigenschap 6.3.2. *Zij $f : G \to H$ een groephomomorfisme.*

1. $\ker(f) \lhd G$,
2. *f is een monomorfisme als en slechts als* $\ker(f) = \{e_G\}$.
3. $\mathrm{Im}(f) = f(G) \leqslant H$.

Bewijs. (1) Omdat $f(e_G) = e_H$ hebben wij dat $e_G \in \ker(f)$. Als $g_1, g_2 \in \ker(f)$ dan

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = f(g_1) f(g_2)^{-1} = e_H e_H = e_H$$

en dus $g_1 g_2^{-1} \in \ker(f)$. Dit toont aan dat $\ker(f)$ een deelgroep is van G. Ook, voor $g_1 \in \ker(f)$ en $g \in G$,

$$f(g g_1 g^{-1}) = f(g) f(g_1) f(g)^{-1} = f(g) e_H f(g)^{-1} = e_H \,,$$

d.w.z. $g g_1 g^{-1} \in \ker(f)$. Bijgevolg is $\ker(f) \lhd G$.

Bewijs zelf dat $\mathrm{Im}(f) = \{f(g) \mid g \in G\}$ een deelgroep is van H.

Wij bewijzen nu (2). Veronderstel dat f een monomorfisme is en $g \in \ker(f)$. Dan $f(g) = e_H = f(e_G)$. Wegens de injectiviteit van f verkrijgen wij aldus dat $g = e_G$. Dus $\ker(f) = \{e_G\}$.

Omgekeerd, veronderstel dat $\ker(f) = \{e_G\}$. Zij $g_1, g_2 \in G$ zodat $f(g_1) = f(g_2)$. Dan

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2)^{-1} = f(g_1) f(g_1)^{-1} = e_H \,.$$

Dus $g_1 g_2^{-1} \in \ker(f) = \{e_G\}$. Bijgevolg $g_1 g_2^{-1} = e_G$ en dus $g_1 = g_2$. □

Wij zien dus dat elke kern van een groephomomorfisme een normale deelgroep is. Omgekeerd is een normale deelgroep N van een groep G de kern van het natuurlijke epimorfisme $\mathrm{nat} : G \to G/N$. Dus is er een één-één correspondentie tussen normale deelgroepen en kernen van groephomomorfismen.

Stelling 6.3.3 (Eerste Isomorfismestelling)**.** *Zij $f : G \to H$ een groephomomorfisme. Dan*

$$G/\ker f \cong f(G).$$

Bewijs. Definiëer

$$\psi : G/\ker(f) \to f(G)$$

als volgt

$$\psi(g \ker(f)) = f(g).$$

Eerst en vooral moeten wij aantonen dat ψ goed gedefiniëerd is. Zij daarom $g_1, g_2 \in G$ zodat $g_1 \ker(f) = g_2 \ker(f)$, d.w.z., $g_2^{-1} g_1 \in \ker(f)$. Dus

$$f(g_1) = f(g_2 g_2^{-1} g_1) = f(g_2) f(g_2^{-1} g_1) = f(g_2) e_H = f(g_2).$$

Bijgevolg is ψ inderdaad goed gedefiniëerd.

Dat ψ een homomorfisme is volgt uit het volgende:

$$\begin{aligned} \psi\left((g_1 \ker(f))\,(g_2 \ker(f))\right) &= \psi(g_1 g_2 \ker(f)) \\ &= f(g_1 g_2) \\ &= f(g_1) f(g_2) \\ &= \psi(g_1 \ker(f))\ \psi(g_2 \ker(f)) \end{aligned}$$

Als $g \in G$, dan $f(g) = \psi(g \ker(f))$. Dus is ψ surjectief. Om aan te tonen dat ψ injectief is is het voldoende om aan te tonen dat $\ker(\psi) = \{e_{G/\ker(f)}\}$. Zij daarom $g\ker(f) \in \ker(\psi)$. Dus $f(g) = e_H$ en bijgevolg $g \in \ker(f)$. Er volgt $g\ker(f) = \ker(f) = e_{G/\ker(f)}$. □

Wij geven enkele toepassingen van de homomorfismestelling.

(1) Beschouw het epimorfisme

$$\det : \mathrm{GL}_n(F) \to F^* .$$

Dan is $\ker(\det) = \mathrm{SL}_n(F)$ en

$$\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^*.$$

(2) Beschouw het epimorfisme (van additieve groepen)

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : z \mapsto [z]_n = z + n\mathbb{Z}.$$

Dan is $\ker(f) = n\mathbb{Z}$. en dus

(3) Zij $E = \{c \in \mathbb{C} \mid |c| = 1\}$. Dan is E een abelse groep voor de vermenigvuldiging van complexe getallen en

$$E = \{e^{x2\pi i} \mid x \in \mathbb{R}\}.$$

Beschouw

$$\varphi : \mathbb{R} \to E$$

gedefiniëerd als volgt

$$\varphi(x) = e^{2\pi i x}.$$

Dan is φ een groepepimorfisme van de groep $(\mathbb{R}, +)$ naar de groep $(E, \cdot)$. Omdat $\ker(\varphi) = \mathbb{Z}$ verkrijgen wij

$$E \cong \mathbb{R}/\mathbb{Z}.$$

(4) Beschouw $G_1 \times G_2$, het direct product van de groepen G_1 end G_2. Definiëer

$$p_1 : G_1 \times G_2 \to G_1 : (g_1, g_2) \mapsto g_1.$$

Dan is p_1 een groepepimorfisme met $\ker(p_1) = \{e_{G_1}\} \times G_2$. Dus

$$(G_1 \times G_2)/(\{e_{G_1}\} \times G_2) \cong G_1.$$

Analoog is

$$p_2 : G_1 \times G_2 \to G_2 : (g_1, g_2) \mapsto g_2$$

een groepepimorfisme en $\ker(p_2) = G_1 \times \{e_{G_2}\}$. Dus

$$(G_1 \times G_2)/(G_1 \times \{e_{G_2}\}) \cong G_2.$$

Eigenschap 6.3.4. *Zij G een groep. Dan is $(\mathrm{Aut}(G), \circ)$ een groep met als normale deelgroep $\mathrm{Inn}(G)$. Bovendien,*

$$G/Z(G) \cong \mathrm{Inn}(G).$$

Bewijs. Beschouw de afbeelding

$$\varphi : G \to \mathrm{Inn}(G) : g \mapsto \varphi_g.$$

Verifiëer dat φ een groepepimorfisme is. Zij nu $g \in G$, dan is $g \in \ker(\varphi)$ als en slechts als $\varphi_g = 1_G$, d.w.z., voor alle $x \in G$,

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

Dit laatste is equivalent met $gx = xg$ voor alle $x \in G$. M.a.w. $g \in Z(G)$. Dus $\ker(\varphi) = Z(G)$ en het resultaat volgt uit de eerste homomorfismestelling. □

Enkele toepassingen van de homomorfismestellingen zijn gegeven in de volgende stelling.

Gevolg 6.3.5. *Zij H en N deelgroepen van een groep G.*

1. *(Tweede Isomorfismestelling)*
   Als $N \lhd G$, dan is
   - *(a) $N \lhd HN$,*
   - *(b) $H \cap N \lhd H$, en*
   - *(c) $H/(N \cap H) \cong HN/N$.*
   - *(d) Als G ook eindig is dan $|HN| = \frac{|H|\,|N|}{|H \cap N|}$.*
2. *(Derde Isomorfismestelling)*
   Als $N \lhd G$ en $H \lhd G$ met $N \subseteq H$, dan
   - *(a) $H/N \lhd G/N$, en*
   - *(b) $(G/N)/(H/N) \cong G/H$.*

Bewijs. (1) Uit Eigenschap 4.2.2 weten wij reeds dat $\langle H \cup N \rangle = HN = NH$. Omdat N een normale deelgroep is van G is uiteraard N een normale deelgroep van HN. Definiëer

$$f : H \to HN/N : h \mapsto hN.$$

Dan, voor $h_1, h_2 \in H$,

$$f(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = f(h_1)f(h_2).$$

Dus is f een groephomomorfisme. Omdat voor $h \in H$ en $n \in N$,

$$hnN = hN$$

volgt er dat f surjectief is. Verder is $h \in \ker(f)$ als en slechts als $hN = N$, d.w.z. $h \in N$. Dus is $\ker(f) = H \cap N$ en i.h.b. is $H \cap N$ een normale deelgroep van H. Wegens de eerste isomorfismestelling verkrijgen wij ook $H/(N \cap H) \cong HN/N$.

Als G bovendien eindig is, dan volgt uit $H/(N \cap H) \cong HN/N$ dat

$$[H : (N \cap H)] = [HN : N]$$

en dus

$$\frac{|H|}{|N \cap H|} = \frac{|HN|}{|N|}.$$

Bijgevolg

$$|HN| = \frac{|H|\,|N|}{|H \cap N|}.$$

(2) Omdat H en N normale deelgroepen zijn met $N \subseteq H$ bestaan de quotiëntgroepen G/N en G/H. Definiëer de afbeelding

$$\psi : G/N \to G/H : gN \mapsto gH.$$

Ga na dat dit goed gedefiniëerd is en dat ψ een epimorfisme is. Nu is $gN \in \ker(\psi)$ als en slechts als $\psi(gN) = gH = H$, d.w.z. $g \in H$. Bijgevolg $\ker(\psi) = \{gN \mid g \in H\} = H/N$. I.h.b. is $H/N \lhd G/N$. Wegens de eerste isomorfismestelling verkrijgen wij aldus $(G/N)/(H/N) \cong G/H$. □

Beschouw de additieve groep $\mathbb{Z}, +$. Zij $n, m \in \mathbb{Z}$ dan

$$n\mathbb{Z}/(n\mathbb{Z} \cap m\mathbb{Z}) \cong (n\mathbb{Z} + m\mathbb{Z})/m\mathbb{Z}.$$

Dus

$$n\mathbb{Z}/\mathrm{kgv}(n, m)\mathbb{Z} \cong \mathrm{ggd}(n, m)\mathbb{Z}/m\mathbb{Z}.$$

Merk op dat beide groepen cyclisch zijn van orde $\mathrm{kgv}(n, m)/n$.

Wij vermelden nog een nuttige eigenschap (wij hebben deze al verschillende keren impliciet gebruikt).

Eigenschap 6.3.6. *Zij $f : G \to H$ een groephomomorfisme. Zij D een normale deelgroep van G. Als $D \subseteq \ker(f)$ dan bestaat er een uniek groephomomorfisme*

$$\overline{f} : G/D \to H$$

zodat

$$\overline{f} \circ nat = f$$

met

$$nat : G \to G/D : g \mapsto \overline{g} = gD.$$

Hoofdstuk

7 Permutatiegroepen

In dit hoofdstuk bestuderen wij permutatiegroepen en tonen aan dat elke groep als een deelgroep kan beschouwd worden van een permutatiegroep.

Het idee van het tellen van het aantal herschikkingen van de letters van een alfabet gaat ver terug in de geschiedenis. In de 13de eeuw werden "herschikkingen" reeds als een "abstract object" aanvaard. De wiskundige Abu-l-Abbas ibn al-Banna (1256-1321, uit Marrakech) gaf al een volledig bewijs dat het aantal herschikkingen van een verzameling met n elementen gelijk is aan n!. Het was pas in de 18de eeuw, o.a. door Lagrange, dat er aan herschikkingen werd gedacht als functies van een verzameling naar zichzelf. Het was Augustin-Louis Cauchy (1789-1857) die de fundering van de theorie van permutatiegroepen legde en notatie invoerde.

7.1 Stelling van Cayley

Stelling 7.1.1 (Stelling van Cayley)**.** *Een groep G is isomorf met een deelgroep van de symmetrische groep $Sym(G)$.*

Bewijs. Beschouw de afbeelding

$$\psi : G \to \mathrm{Sym}(G) : g \mapsto \psi_g$$

met

$$\psi_g : G \to G : x \mapsto gx\,.$$

Wegens de vereenvoudigingseigenschappen in een groep is ψ_g injectief. Voor $y \in G$ geldt dat $\psi(g^{-1}y) = y$. Dus is elke ψ_g ook surjectief, en bijgevolg $\psi_g \in \mathrm{Sym}(G)$. Bijgevolg is ψ inderdaad een functie van G naar $\mathrm{Sym}(G)$. Omdat $\psi_g \circ \psi_h = \psi_{gh}$ is ψ een groephomomorfisme. Als $g \in \ker(\psi)$ dan $\psi_g = 1_G$. Dus $gx = x$ voor alle $x \in G$. Bijgevolg $g = e_G$ en dus is ψ een monomorfisme. Wegens de eerste isomorfismestelling volgt er dat $G \cong \psi(G)$ en deze laatste is een deelgroep van de symmetrische groep $\mathrm{Sym}(G)$. □

In een artikel van 1854 gaf Arthur Cayley (1821-1895) een abstract klinkende definitie van het begrip groep: "een verzameling symbolen, $1, \alpha, \beta, \ldots,$" allen verschillend en zodanig dat het product van elke twee van hen (in gelijk welke volgorde) of het product van elk een van hen met zichzelf, tot de verzameling behoort, noemt men een groep." De symbolen die Cayley gebruikte waren, echter, steeds operatoren op een verzameling. Waarschijnlijk was hij zich niet bewust van een ander soort groep. Cayley schreef dat artikel, en vele andere, toen hij aan een advocaat was. In 1863 werd hij professor aan de Universiteit van Cambridge en hij schreef toen verschillende belangrijke artikels die geleid hebben tot een axiomatische definitie (1882) van een abstracte groep, door Walter Van Dyck. Zijn vroegere opemerking/definite is dus voor een kwart eeuw niet opgemerkt.

7.2 Eindige Permutatiegroepen

Zij X een verzameling met n elementen. Meestal beschouwen wij X als de verzameling $\{1, 2, \ldots, n\}$ en wij noteren dan $\mathrm{Sym}(X)$ als S_n. Dikwijls schrijft men dan een permutatie $f : X \to X$ in de vorm

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

Het is dan ook eenvoudig na te gaan dat

$$|S_n| = n!$$

Inderdaad, elk element van de verzameling $\{1, 2, \ldots, n\}$ komt precies éénmaal voor in de tweede rij. Er zijn n keuzes voor het eerste element in de rij. Bijgevolg zijn er $n - 1$ keuzes voor het tweede element in de rij, enz. Dus zijn er in totaal $n(n-1)\cdots 2\ 1$ mogelijkheden.

Definitie 7.2.1. Een permutatie f is een k-cyclus als er er k verschillende elementen $i_1, i_2, \ldots, i_k$ in $\{1, 2, \ldots, n\}$ bestaan zodat $f(i) = i$ voor $i \notin \{i_1, \cdots, i_k\}$ en

$$f(i_1) = i_2,\ f(i_2) = i_3, \cdots, f(i_{k-1}) = i_k,\ f(i_k) = i_1.$$

Men schrijft deze k-cyclus als

$$(i_1\ i_2\ \cdots\ i_k).$$

Men noemt k de lengte van de cyclus.

Een 2-cyclus noemt men een transpositie.

Definitie 7.2.2. Twee permutaties π en φ noemt men disjunct als $\varphi(i) = i$ voor elke $i \in X$ met $\pi(i) \neq i$.

Wij merken op dat disjunctie permutaties commuteren, d.w.z., $\pi \circ \varphi = \varphi \circ \pi$.

Lemma 7.2.3. *Zij $f \in S_n$ en $i \in \{1, \ldots, n\}$. Als k het kleinste getal is in $\mathbb{N}_0$ zodat $f^k(i) \in \{i, f(i), \ldots, f^{k-1}(i)\}$ dan $f^k(i) = i$.*

Bewijs. Veronderstel dat $f^k(i) = f^l(i)$ voor een $0 < l < k$ dan $f^{k-l}(i) = f^{-l}(f^k(i)) = i$. Dit is echter in contradictie met de keuze van k. □

Er volgt dus dat $f \in S_n$ een k cyclus is als $k \in \mathbb{N}_0$ en een $i \in \{1, \ldots, n\}$ bestaan zodat

1. k is het kleinste getal in $\mathbb{N}_0$ zodat $f^k(i) = i$, en
2. $f(j) = j$ voor alle $j \notin \{i, f(i), \ldots, f^{k-1}(i)\}$.

Eigenschap 7.2.4. *Elke permutatie is een product van disjuncte cyclussen. Dit product is uniek op de volgorde van de cyclussen na. We noemen dit de (disjuncte) cyclus ontbinding van de permutatie (meestal schrijft men niet de cyclussen van lengte één).*

Bewijs. Zij $X = \{1, \ldots, n\}$ en $F = \{i \in X \mid f(i) = i\}$. Voor elke $i \in F$ vormen wij de 1-cyclus (i). Zij nu i het kleinste getal in $X \setminus F$ en zij k het kleinste getal in $\mathbb{N}_0$ zodat $f^k(i) \in \{i, f(i), \ldots, f^{k-1}(i)\}$. Wegens de vorige eigenschap, $f^k(i) = i$ en wij vormen de k-cyclus

$$(i\ f(i)\ \cdots\ f^{k-1}(i)).$$

Als er nog een getal j bestaat in X dat niet behoort tot

$$F \cup \{i, f(i), \cdots, f^{k-1}(i)\},$$

zij dan l het kleinste getal in $\mathbb{N}_0$ zodat $f^l(j) \in \{j, f(j), \ldots, f^{l-1}(j)\}$ en vorm de l-cyclus $(j\ f(j)\ \cdots\ f^{l-1}(j))$. Er volgt dat f het product is van alle aldus gevormde cyclussen.

Ga zelf na dat deze ontbinding uniek is. □

De ontbinding van

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 3 & 5 & 6 & 2 & 4 & 8 & 9 & 1 & 10 \end{pmatrix}$$

in S_{10} is

$$(1\ 7\ 8\ 9)(2\ 3\ 5)(4\ 6)(10).$$

Aangezien wij een cyclus van lengte één meestal niet schrijven, noteren wij deze permutatie dus meestal eenvoudiger als $(1\ 7\ 8\ 9)(2\ 3\ 5)(4\ 6)$

Wij weten dat S_3 zes elementen heeft en het is gemakkelijk na te gaan dat

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

Merk op dat de inverse van een k-cyclus terug een k-cyclus is

$$(i_1\ i_2\ \cdots\ i_k)^{-1} = (i_k\ i_{k-1}\ \cdots i_2\ i_1)$$

De orde van een k-cyclus in de groep S_n is precies de lengte van de cyclus.

Eigenschap 7.2.5. *Zij $f \in S_n$ en $f = c_1c_2\cdots c_l$, een product van disjuncte cyclussen c_i van respectievelijke lengte k_i. Dan is*

$$o(f) = kgv(k_1, k_2, \ldots, k_l)$$

Bewijs. Wij moeten dus het kleinste getal $k \in \mathbb{N}_0$ bepalen zodat

$$f^k = 1$$

Welnu, omdat disjuncte cyclussen commuteren verkrijgen wij

$$\begin{aligned} f^k &= (c_1c_2\cdots c_l)^k \\ &= c_1^k c_2^k \cdots c_l^k \end{aligned}$$

Dus, weer omdat de betrokken cyclussen disjunct zijn, volgt er dat $f^k = 1$ als en slechts als elke $c_i^k = 1$ (voor $1 \leq i \leq l$). Maar omdat $o(c_i) = k_i$ verkrijgen wij dus dat elke $k_i|k$. Bijgevolg $\text{kgv}(k_1, k_2, \ldots, k_l)|k$. Omdat

$$f^{\text{kgv}(k_1,k_2,\ldots,k_l)} = 1$$

volgt het resultaat. □

Dus

$$o((1\ 7\ 8\ 9)(2\ 3\ 5)(4\ 6)(10)) = \text{kgv}(4, 3, 2) = 12.$$

Beschouw nu $\pi = (1\ 7\ 8\ 9)(2\ 3\ 5)(4\ 8)$. Dan

$$o(\pi) = o((1\ 7\ 8\ 4\ 9)(2\ 3\ 5)) = 15.$$

Eigenschap 7.2.6. *Elke k-cyclus (met $k \geq 2$) in S_n is een product van $k-1$ transposities. Bijgevolg is de groep S_n voortgebracht door alle transposities $(i\ j)$, met $i \neq j$ en $i, j \in \{1, 2, \cdots, n\}$.*

Bewijs. Ga na dat

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)\cdots(i_1\ i_3)(i_1\ i_2).$$

□

De ontbinding van een permutatie in transposities is niet uniek. Bijvoorbeeld, $(1\ 2) = (3\ 4)(1\ 2)(3\ 4)$. Doch wij zullen aantonen dat de pariteit van het aantal transposities in de ontbinding eenduidig bepaald is.

Om dit aan te tonen benodigen wij het volgende. Zij $f(X_1, X_2, \ldots, X_n)$ een polynoom in n veranderlijken $X_1, X_2, \ldots, X_n$ over $\mathbb{R}$. Als $\varphi \in S_n$ dan is φf per definitie de polynoom

$$f(X_{\varphi(1)}, X_{\varphi(2)}, \ldots, X_{\varphi(n)}).$$

Bijvoorbeeld, als

$$f(X_1, X_2, X_3, X_4) = X_1X_2 + 3X_4 - 7X_2X_3X_4$$

en

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

dan

$$\varphi f = X_3X_4 + 3X_2 - 7X_4X_1X_2.$$

Eigenschap 7.2.7. *Zij f een polynoom in de veranderlijken $X_1, X_2, \ldots, X_n$ en $\varphi, \pi \in S_n$. Zij e de identiteit van S_n. Dan*

1. *$ef = f$,*
2. *$(\varphi\pi)f = \varphi(\pi f)$*
3. *voor elke $r \in \mathbb{R}$, $\varphi(rf) = r(\varphi f)$.*

Bewijs. Ga dit zelf na. □

Wij beschouwen nu de volgende polynoom in de veranderlijken $X_1, X_2, \cdots, X_n$:

$$\Delta_n = \prod_{1 \leq i < j \leq n} (X_i - X_j).$$

Definitie 7.2.8. Voor elke $\varphi \in S_n$ is ofwel $\varphi\Delta_n = \Delta_n$, ofwel is $\varphi\Delta_n = -\Delta_n$. In het eerste geval noemt men φ een even permutatie en in het tweede geval noemt men φ een oneven permutatie.

Beschouw nu de afbeelding

$$\operatorname{sgn} : S_n \to \{1, -1\}$$

gedefiniëerd als volgt

$$\operatorname{sgn}(\varphi) = \begin{cases} 1 & \text{als } \varphi \text{ even is,} \\ -1 & \text{als } \varphi \text{ oneven is.} \end{cases}$$

Eigenschap 7.2.9. *1. De afbeelding sgn is een groephomomorfisme. De kern van dit homomorfisme noemt men de alternerende groep van graad n, en deze wordt genoteerd A_n.*

2. Elke transpositie is oneven.

3. Een k-cyclus is even als en slechts als k oneven is.

4. A_n is een normale deelgroep van S_n, en van index 2 indien $n \geq 2$.

5. $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ als $n \geq 2$.

Bewijs. (1) Wij moeten bewijzen dat $\operatorname{sgn}(fg) = \operatorname{sgn}(f)\operatorname{sgn}(g)$ voor $f, g \in S_n$. Dit volgt uit de volgende redenering

$$\begin{aligned} \operatorname{sgn}(fg)\Delta_n &= fg\Delta_n \\ &= f(g\Delta_n) \\ &= f(\operatorname{sgn}(g)\Delta_n) \\ &= \operatorname{sgn}(g)(f\Delta_n) \\ &= \operatorname{sgn}(g)\operatorname{sgn}(f)\Delta_n \end{aligned}$$

(2) Uit de definitie merken we eerst op dat $\operatorname{sgn}(1\ 2) = -1$. Dus $(1\ 2)$ is oneven. Neem nu $k \in \{3, \ldots, n\}$. Dan

$$(1\ k) = (2\ k)(1\ 2)(2\ k)^{-1}.$$

Omdat $(1\ 2)$ oneven is en sgn een groephomomorfisme is volgt er dat $(1\ k)$ ook oneven is. Neem nu een willekeurige transpositie $(l\ k)$ dan

$$(l\ k) = (1\ l)(1\ k)(1\ l)^{-1}.$$

Omdat $(1\ k)$ oneven is en sgn een groephomomorfisme is volgt er dat $(l\ k)$ oneven is.

(3) Wij weten dat een k-cyclus het product is van $k-1$ transposities. Weer omdat sgn een homomorfisme is volgt er dus dat een k-cyclus even is als en slechts als k oneven is.

(4) en (5) A_n is de kern van sgn en sgn is surjectief (als $n \geq 2$). Dus volgt het resultaat uit de eerste isomorfismestelling. □

Wij weten reeds dat S_n voortgebracht is door transposities. Wij hebben aangetoond dat elke transpositie een product is van transposities van de vorm $(1\ k)$. Dus verkrijgen wij onmiddellijk het eerste gedeelte van de volgende eigenschap. Het tweede gedeelte bewijst men analoog.

Eigenschap 7.2.10. *1.* $S_n = \langle (1\ 2), (1\ 3), \cdots, (1\ n) \rangle$,

2. $S_n = \langle a_1 = (1\ 2),\ a_2 = (2\ 3), \cdots,\ a_{n-1} = (n-1\ n) \rangle$ *en de volgende relaties zijn voldaan*

$$\begin{aligned} a_k^2 &= 1,\ (1 \leq k \leq n-1); \\ (a_k\ a_{k+1})^3 &= 1,\ (1 \leq k \leq n-1); \\ (a_i\ a_j)^2 &= 1,\ (1 \leq i, j \leq n-1 \text{ en } |i-j| > 1). \end{aligned}$$

Eigenschap 7.2.11. *Zij* $f, g \in S_n$. *Zij* $g = c_1 \cdots c_k$, *de ontbinding in disjuncte cyclussen. Dan wordt de ontbinding in disjuncte cyclussen van*

$$fgf^{-1}$$

bekomen door in elke cyclus c_j *een getal* i *te vervangen door* $f(i)$.

Twee permutaties zijn geconjugeerd als en slechts als het type van hun cyclus ontbinding hetzelfde is.

Hoofdstuk 8

Eindige Abelse Groepen

In dit hoofdstuk classificeren wij de eindige abelse groepen.

8.1 Directe Producten

Eigenschap 8.1.1. *Zij G een groep. Als G_1 en G_2 deelgroepen zijn zodat:*

1. *G_1 en G_2 zijn normale deelgroepen van G,*
2. *$G_1 G_2 = G$,*
3. *$G_1 \cap G_2 = \{e\}$,*

dan is G isomorf met het direct product $G_1 \times G_2$.

Bewijs. Voorwaarde (2) zegt dat elk element g van G kan geschreven worden in de vorm $g = g_1 g_2$ met $g_1 \in G_1$ en $g_2 \in G_2$. Wij tonen nu aan dat deze uitdrukking uniek is. Veronderstel dus dat

$$g_1 g_2 = g_1' g_2'$$

met $g_i' \in G_i$. Dan $(g_1')^{-1} g_1 = g_2' g_2^{-1} \in G_1 \cap G_2$. Wegens voorwaarde (3) verkrijgen wij $(g_1')^{-1} g_1 = g_2' g_2^{-1} = e$ en dus $g_1 = g_1'$ en $g_2 = g_2'$.

Wij tonen nu aan dat de elementen van G_1 commuteren met de elementen van G_2. Zij dus $g_i \in G_i$. Dan, omdat $G_i \lhd G$,

$$g_1 g_2 g_1^{-1} \in G_2$$

en

$$g_2 g_1^{-1} g_2^{-1} \in G_1.$$

Dus

$$g_1 g_2 g_1^{-1} g_2^{-1} \in G_2 \cap G_1$$

en bijgevolg

$$g_1 g_2 g_1^{-1} g_2^{-1} = e.$$

Dus $g_1 g_2 = g_2 g_1$.

Er volgt dat de afbeelding

$$f : G = G_1 G_2 \to G_1 \times G_2 : g_1 g_2 \mapsto (g_1, g_2)$$

goed gedefiniëerd is. Ook is dit een isomorfisme van groepen. □

Het omgekeerde van de vorige stelling is uiteraard ook waar. Inderdaad als $G = G_1 \times G_2$ dan $G = H_1 H_2$ met $H_1 = G_1 \times \{e_{G_2}\}$ en $H_2 = \{e_{G_1}\} \times G_2$. De groepen H_i zijn normaal in G en $H_1 \cap H_2 = \{e\}$.

De Viergroep van Klein $\{e, a, b, c\}$ is isomorf met $\{e, a\} \times \{e, b\}$, en dus isomorf met $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

De cyclische groep $\mathbb{Z}/6\mathbb{Z}$ is isomorf met $\{[0]_6, [2]_6, [4]_6\} \times \{[0]_6, [3]_6\}$; en dus met $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

8.2 Fundamentele Stelling

Lemma 8.2.1. *Zij G een abelse groep.*

1. *Als $m \in \mathbb{N}$ dan is $G(m) = \{g \in G \mid g^m = e\}$ een deelgroep van G.*
2. *Als $|G| = mn$ en $(m, n) = 1$, dan $G \cong G(m) \times G(n)$.*

Bewijs. (1) Duidelijk is $e \in G(m)$. Als $g_1, g_2 \in G(m)$, dan (omdat G abels is),

$$(g_1 g_2^{-1})^m = g_1^m (g_2^m)^{-1} = ee = e.$$

Dus $g_1 g_2^{-1} \in G(m)$.

(2) Omdat $(m, n) = 1$ bestaan er $v, w \in \mathbb{Z}$ zodat $vm + wn = 1$. Als $g \in G$, dan

$$g = g^1 = g^{vm+wn} = g^{vm} g^{wn}.$$

Verder is $g^{|G|} = g^{mn} = e$. Dus $g^{vm} \in G(n)$ en $g^{wn} \in G(m)$. Bijgevolg $G = G(m)G(n)$. Omdat G abels is zijn beide groepen $G(n)$ en $G(m)$ normale deelgroepen van G. Ook is $G(n) \cap G(m) = \{e\}$. Inderdaad, zij g in de doorsnede. Dan $g^n = g^m = e$. Dus ook

$$g^1 = g^{vm} g^{wn} = (g^m)^v (g^n)^w = ee = e.$$

Er volgt dat

$$G = G(m)G(n) \cong G(m) \times G(n).$$

□

Definitie 8.2.2. Zij G een groep en p een priemgetal. Als de orde van elk element van G een macht van p is dan noemt men G een p-groep.

Een voorbeeld van een p-groep is de cyclische groep $\mathbb{Z}/p^n\mathbb{Z}, +$. Ook eindige directe producten van p-groepen zijn p-groepen. De groep $\mathbb{Z}/p^n\mathbb{Z}, +$ is geen p-groep.

Eigenschap 8.2.3. *Zij G een eindige p-groep. Dan:*

1. *het homomorf beeld van G is ook een p-groep,*
2. *voor elke normale deelgroep $N \lhd G$ is G/N een p-groep,*
3. *Als G abels is, dan is de orde van G is een macht van p.*

Bewijs. (1) Veronderstel dat $\varphi : G \to H$ een groephomomorfisme is. Uit Eigenschap 6.2.4 weten we dat de $o(\varphi(g)) \mid o(g)$ voor alle $g \in G$. Omdat $o(g)$ een macht van een priemgetal p is, geldt dit dus ook voor $o(\varphi(g))$. Dus $\operatorname{Im}\varphi$ is een p-groep.

(2) Voor een gegeven normale deelgroep $N \lhd G$, geldt dus, door (1) toe te passen op het natuurlijk epimorfisme $\text{nat} : G \to G/N$ (zie pagina 51), dat G/N een p-groep is, dus $o(gN)$ is een macht van het priemgetal p voor elk element $gN \in G/N$.

(3) Als $G = \{e\}$ dan is dit resultaat triviaal. Veronderstel dus dat $e \neq g \in G$. Dan is $N = \langle g \rangle$ een normale deelgroep van G en $|N| = o(g) = p^n$ voor een $n \in \mathbb{N}_0$. Nu $|G/N| = \frac{|G|}{|N|} < |G|$ en door (2) is G/N een p-groep. Dus door inductie mag men veronderstellen dat $|G/N| = p^m$ voor een $m \in \mathbb{N}$. Dus $|G| = p^m|N| = p^{n+m}$.

□

Lemma 8.2.4. *Veronderstel dat G een eindige abelse groep is. Dan is G het direct product van eindige abelse p-groepen*

Bewijs. Veronderstel dat $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$, met $p_1, \cdots, p_k$ verschillende priemgetallen. Stel $m = p_1^{n_1}$, en $n = \frac{|G|}{m}$. Dan voldoen G, samen met de getallen m en n, aan de voorwaarden van Eigenschap 8.2.1. Dus $G \cong G(m) \times G(n)$, en $G(m)$ is een p_1-groep. Dit argument kan nu recursief toegepast worden op de groep $G(n)$, met $n = p_2^{n_2}\cdots p_k^{n_k}$, waaruit het lemma volgt. □

Lemma 8.2.5. *Veronderstel dat G een eindige, abelse p-groep is. Dan is G isomorf met het direct product van cyclische p-groepen. Bovendien is deze ontbinding uniek.*

Bewijs. We bewijzen de stelling door middel van inductie op de orde van G. Voor de triviale group is de stelling triviaal. Dus veronderstel dat $|G| > 1$. Kies een element $x \in G$ van maximale orde, dus met de eigenschap dat $o(x) \geq o(y)$ voor alle elementen $y \in G$. Stel $A = \langle x \rangle$. Wegens de inductiehypothese geldt

$$G/A \cong \langle g_i A \rangle \times \cdots \times \langle g_m A \rangle \,,$$

en $o(g_i A) = p^{t_i}$, omdat elk van de componenten van het direct product cyclische p-groepen zijn.

Nu tonen we aan dat er voor elke g_i een element $y_i \in G$ bestaat, met $g_i A = y_i A$ en $o(y_i) = p^{t_i}$. Dus beschouw een element $gA \in G/A$ met $o(gA) = p^t$. Aangezien $o(gA) \leq o(g)$ (door b.v. Eigenschap 8.2.3 (2)), geldt $p^t \mid o(g)$. Omdat $o(gA) = p^t$, geldt $g^{p^t} \in A$, dus $g^{p^t} = x^n$, met $n < o(x)$. Noteer $o(x) = p^i$ en $o(g) = p^j$.

Omdat $p^t \mid o(g)$, geldt $j \geq t$. Noem w het grootste natuurlijk gelal met $p^w \mid n$. Aangezien $o(x) > n$, volgt $w < i$. We tonen nu aan dat $w \geq t$. Er geldt:

$$o(g^{p^t}) = \frac{p^j}{\gcd(p^j, p^t)} = \frac{p^j}{p^t} = p^{j-t}$$

en

$$o(x^n) = \frac{p^i}{\gcd(p^i, n)} = \frac{p^i}{(p^i, p^w)} = p^{i-w} \,.$$

Dus $p^{j-t} = p^{i-w}$, of nog, $w = t + i - j$. Omdat, $o(x) = p^i \geq o(y) = p^j$ volgt er $i \geq j$ en dus $w \geq t$, zoals gewenst.

Dus $n = cp^t$ voor een $c \in \mathbb{N}$ en dus $g^{p^t} = (x^c)^{p^t}$ zodat $(gx^{-c})^{p^t} = e$ en $gA = (gx^{-c})A$ (en gx^{-c} heeft orde p^t).

Er bestaan dus $y_i \in G$ zodat $o(y_i) = p^{t_i}$ en $g_i A = y_i A$. Stel $B = \langle y_1, \cdots, y_m \rangle = \{y_1^{r_1} \cdots y_m^{r_m} \mid 0 \leq r_i < p^{t_i}\}$. Nu is $AB = G$. Wij tonen nu aan dat $A \cap B = \{e\}$. Zij daarom $a \in A \cap B$. Dan $a = y_1^{r_1} \cdots y_m^{r_m}$ met $0 \leq r_i < p^{t_i}$. Dan, in G/A,

$$e_{G/A} = aA = (y_1 A)^{r_1} \cdots (y_m A)^{r_m}.$$

Omdat G/A het direct product is van de $\langle y_i A \rangle$ en $o(y_i A) = p^{t_i}$ volgt er dat elke $r_i = 0$. Dus is $a = e$.

Er volgt dat $G \cong A \times B$ (uit Eigenschap 8.1.1). Passen we nu de inductiehypothese toe op B, dan volgt het lemma. Tenslotte volgt eveneens dat

$$G \cong C_{p^{t_1}} \times C_{p^{t_2}} \times \ldots \times C_{p^{t_r}} \,,$$

met $t_1 \geq t_2 \geq \ldots \geq t_r \geq 1$, en $C_{p^{t_i}}$ een cyclische groep van orde p^{t_i}.

Er blijft te bewijzen dat de ontbinding uniek is. Zij daarom

$$\langle x_1 \rangle \times \cdots \times \langle x_r \rangle \cong \langle y_1 \rangle \times \cdots \times \langle y_s \rangle$$

met $o(x_i) = p^{t_i}$, $t_1 \geq t_2 \geq \cdots \geq t_r \geq 1$, en $o(y_j) = p^{u_j}$, $u_1 \geq u_2 \geq \cdots \geq u_s \geq 1$. Er volgt dat de p-machten isomorf zijn en dus

$$\langle x_1^p \rangle \times \cdots \times \langle x_r^p \rangle \cong \langle y_1^p \rangle \times \cdots \times \langle y_s^p \rangle.$$

Omdat deze groepen van kleinere orde zijn mag men per inductie veronderstellen dat de ontbinding uniek is. Gebruik deze informatie en toon vervolgens aan dat het aantal i met $t_i = 1$ hetzelfde is als het aantal j met $u_j = 1$. Dit alles bewijst het gewenste resultaat. □

Stelling 8.2.6 (Fundamentele Stelling van Eindige Abelse Groepen)**.** *Zij G een niet triviale eindige abelse groep. Dan is G isomorf met een direct product van cyclische groepen, elk van orde een macht van een priemgetal. De priemen die voorkomen zijn delers van de orde van G, en elke priemdeler van $|G|$ komt voor in de ontbinding. Bovendien als p zo een priemgetal is, en als $p^{t_1} \geq p^{t_2} \geq \cdots \geq p^{t_r}$ de orden van de cyclische p-groepen zijn die voorkomen in deze ontbinding, dan zijn deze getallen uniek bepaald (men noemt deze de invarianten van G).*

Bewijs. De combinatie van Lemma 8.2.4 end Lemma 8.2.5 bewijzen de stelling. □

Hoofdstuk

9 Acties

Door het abstraheren van de fundamentele eigenschappen van permutaties is men tot het begrip groep gekomen. Een belangrijk kenmerk dat deze groepeigenschappen niet vermelden is dat groepen ingebed zijn in permutatiegroepen. Wij zullen deze eigenschap nu terug herstellen.

9.1 Definitie

Definitie 9.1.1. Zij X een verzameling en $(G, *)$ een groep. Dan voert G een (linker) actie uit op X als er een groephomomorfisme

$$\pi : G \to \mathrm{Sym}(X) : g \mapsto \pi_g$$

bestaat.

Uiteraard is π een groephomomorfisme als

$$\pi_{g*h} = \pi_g \circ \pi_h,$$

voor alle $g, h \in G$. Dus in het bijzonder, $\pi_e = 1_X$, de identiteit op X. Voor $x \in X$, noteren wij $\pi_g(x)$ als $g \cdot x$. Wij verkrijgen aldus een afbeelding

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

die voldoet aan de volgende eigenschappen:

1. voor $g, h \in G$, $x \in X$, $(g * h) \cdot x = g \cdot (h \cdot x)$,
2. voor $x \in X$, $e \cdot x = x$.

Net zoals in het bewijs van de stelling van Cayley bewijst men dat het bestaan van zulke afbeelding een actie definiëert van G op X.

Voorbeelden 9.1.2. (1) De identieke afbeelding $\mathrm{Sym}(X) \to \mathrm{Sym}(X)$ definiëert een actie van $\mathrm{Sym}(X)$ op X.

(2) De stelling van Cayley zegt dat een groep $(G, *)$ een actie voert op G. In dit geval, voor elke $g, x \in G$:

$$\pi_g(x) = g * x$$

en dus

$$g \cdot x = g * x.$$

Dit is de *linkse translatie* actie.

(3) Een ander voorbeeld is de *conjugatie* op een groep G:

$$G \times G \to G : (g, x) \mapsto g * x * g^{-1}.$$

(4) Zij G een groep en $\mathcal{P}(G)$ de verzameling van alle deelverzamelingen van G. Dan is

$$G \times \mathcal{P}(G) \to \mathcal{P}(G) : (g, D) \mapsto gD$$

een actie van G op $\mathcal{P}(G)$ (de linkse translatie op deelverzamelingen). Ook voert G een actie uit op de verzameling van alle deelgroepen van G, dit door middel van de conjugatie.

(5) Zij V een vectorruimte over een lichaam F, dan voert $F^\times$ een actie uit op V.

Definitie 9.1.3. Veronderstel dat de groep G een actie voert op de verzameling X. De *baan van $x \in X$ onder de actie van G* is de verzameling

$$\mathcal{O}(x) = \{g \cdot x \mid g \in G\},$$

de stabilisator van x is de verzameling

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

De stabilisatoren zijn deelgroepen van G.

Zij $X_G = \{x \in X \mid g \cdot x = x \text{ voor alle } g \in G\}$.

Beschouw de actie van S_n op $X = \{1, 2, \cdots, n\}$. Dus,

$$S_n \times X \to X : (f, i) \mapsto f(i).$$

Dan, voor elke $i \in X$, $\mathcal{O}(i) = X$ en de stabilisator van i zijn al de permutaties $f \in S_n$ met $f(i) = i$. Dus de stabilisator is een deelgroep isomorf met S_{n-1}.

Voor de conjugatie actie in een groep G zijn de banen de conjugatieklassen en de stabilistor van $g \in G$ is de centralisator $C_G(g)$.

Voor de conjugatie actie op de deelgroepen van een groep G is de stabilisator van een deelgroep D de normalisator $N_G(D) = \{g \in G \mid gDg^{-1} = D\}$.

Voor de linkse translatie op de deelverzamelingen van een groep G is de baan van een deelgroep H de verzameling van alle linkse nevenklassen van H. De stabilisator van H is H zelf.

In het geval van de linkse translatie actie op een groep G is er slechts één baan, de groep G zelf.

Definitie 9.1.4. Veronderstel dat de groep G een actie voert op de verzameling X. Als X de enige baan is dan noemt men de actie transitief.

Wij beschouwen nog een voorbeeld. De groep $\mathrm{GL}_n(\mathbb{R})$ voert een actie uit op $\mathbb{R}^n$ (wij schrijven de elementen van $\mathbb{R}^n$ in kolomvorm).

$$\mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n : (A, X) \mapsto AX.$$

De stabilisator van $X \neq 0$ is de verzameling van alle matrices $A \in \mathrm{GL}_n(\mathbb{R})$ die X als eigenvector hebben met eigenwaarde 1 en de stabilisator van $X = 0$ is $\mathrm{GL}_n(\mathbb{R})$.

Schrijven wij de elementen van $\mathbb{R}^n$ in rijvorm dan verkrijgen wij een afbeelding

$$\mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n : (A, X) \mapsto A \cdot X = XA.$$

Deze voldoet aan, voor alle $A, B \in \mathrm{GL}_n \mathbb{R}$ en $X \in \mathbb{R}^n$,

1. $(AB) \cdot X = B \cdot (A \cdot X)$,
2. $1 \cdot X = X$

Definieert men echter $X \cdot A$ als $X * A$ dan worden de vorige twee eigenschappen als volgt herschreven,

1. $X * (AB) = (X * A) * B$,
2. $X * 1 = X$

Men noemt een afbeelding

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

die voldoet aan (voor alle $x \in X$, $g, h \in G$)

1. $x * (gh) = (x * g) * h$,
2. $x * e = x$

een rechteractie. Dit is equivalent met

$$\psi : G \to \mathrm{Sym}(X) : g \mapsto \psi_g,$$

waarbij

$$\psi_g : X \to X : x \mapsto x * g,$$

is een antihomomorfisme, d.w.z. voor alle $g, h \in G$,

$$\psi(gh) = \psi(h) \circ \psi(g).$$

9.2 Baan-Stabilisator Stelling

Eigenschap 9.2.1. *Veronderstel dat de groep G een (linker) actie voert op de verzameling X. Zij $\sim$ de relatie op X gedefinieerd als volgt:*

$$x_1 \sim x_2 \text{ als er een } g \in G \text{ bestaat zodat } g \cdot x_1 = x_2.$$

Dan is $\sim$ een equivalentierelatie met de banen als equivalentieklassen. Dus de banen vormen een partitie van de verzameling X.

Bewijs. Ga dit zelf na. □

Stelling 9.2.2 (Baan-Stabilisator Stelling)**.** *Veronderstel dat de groep G een (linker) actie voert op de verzameling X. Voor $x \in X$,*

$$|\mathcal{O}(x)| = [G : G_x].$$

Bewijs. Het is voldoende om aan te tonen dat de volgende afbeelding

$$f : \mathcal{O}(x) \to \{gG_x \mid g \in G\} : g \cdot x \mapsto gG_x$$

een bijectie is.

Eerst tonen wij aan dat de afbeelding goed gedefiniëerd is. Veronderstel daarom dat $g \cdot x = h \cdot x$, met $g, h \in G$. Dan $(h^{-1}g) \cdot x = x$ en dus $h^{-1}g \in G_x$. Bijgevolg $hG_x = gG_x$ en dus is de afbeelding inderdaad goed gedefiniëerd.

De afbeelding is duidelijk surjectief. Om aan te tonen dat f injectief is veronderstellen wij dat $f(g \cdot x) = f(h \cdot x)$. Dan $gG_x = hG_x$ en dus $h^{-1}g \in G_x$. Bijgevolg $(h^{-1}g) \cdot x = x$ en dus $h \cdot x = g \cdot x$, zoals gewenst. □

Gevolg 9.2.3. *Veronderstel dat de groep G een (linker) actie voert op de verzameling X. Als G eindig is dan is het aantal elementen in een baan een deler van de orde van de groep G.*

Gevolg 9.2.4. *Voor een groep G en $a \in G$,*

$$|\mathcal{C}(a)| = [G : C_G(a)].$$

Bewijs. Beschouw de conjugatieactie op G. Voor $a \in G$ is de stabilisator precies de centralisator $C_G(a)$ en de baan van a is de conjugatiekklasse $\mathcal{C}(a)$. Dus volgt het resultaat. □

Wij analyseren nu de conjugatieklassen van S_5 en A_5. Herinner dat in S_5 twee permutaties geconjugeerd zijn als en slechts als zij van hetzelfde cyclus type zijn.

S_5	Cyclus type	Aantal	Orde	Teken
	1	1	1	even
	(1 2)	10	2	oneven
	(1 2 3)	20	3	even
	(1 2 3 4)	30	4	oneven
	(1 2 3 4 5)	24	5	even
	(1 2)(3 4 5)	20	6	oneven
	(1 2)(3 4)	15	2	even

A_5	Conjugatieklasse	Aantal	Orde	Teken
	$\mathcal{C}(1)$	1	1	even
	$\mathcal{C}(1\ 2\ 3)$	20	3	even
	$\mathcal{C}(1\ 2\ 3\ 4\ 5)$	12	5	even
	$\mathcal{C}(1\ 2\ 3\ 5\ 4)$	12	5	even
	$(1\ 2)(3\ 4)$	15	2	even

Wij merken dus op dat in S_5 de conjugatieklasse van (1 2 3 4 5) precies 24 elementen bevat, maar dat deze verzameling splitst in twee verzamelingen (twee verschillende conjugatieklassen) in A_5.

De volgende stelling geeft een middel om het aantal banen van een actie van een eindige groep G op een eindige verzameling te bepalen. Voor $g \in G$ noteren wij $X_g = \{x \in X \mid g \cdot x = x\}$ en $X_G = \cap_{g \in G} X_g = \{x \in X \mid g \cdot x = x \text{ voor alle } g \in G\}$.

Stelling 9.2.5. *Zij G een eindige groep die een linker actie voert op de eindige verzameling X. Zij r het aantal banen in X. Dan*

$$r\ |G| = \sum_{g \in G} |X_g|.$$

Bewijs. Zij $n = |\{(g, x) \mid g \in G,\ x \in X,\ g \cdot x = x\}|$. Voor elke $g \in G$ zijn er $|X_g|$ paren met g als eerste component. Dus

$$n = \sum_{g \in G} |X_g|.$$

Voor elke $x \in X$ zijn er $|G_x|$ paren met x als tweede component. Dus

$$n = \sum_{x \in X} |G_x|.$$

Wegens de baan-stabilisator stelling weten wij $|\mathcal{O}(x)| = [G : G_x]$. Dus

$$n = \sum_{x \in X} \frac{|G|}{|\mathcal{O}(x)|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|}.$$

Nu, $\sum_{y \in \mathcal{O}(x)} \frac{1}{\mathcal{O}(y)} = \sum_{y \in \mathcal{O}(x)} \frac{1}{|\mathcal{O}(x)|} = 1$ en dus

$$\sum_{g \in G} |X_g| = n = |G|(\text{aantal banen in } X) = |G|\ r.$$

□

Veronderstel dat de eindige groep G een linker actie voert op de eindige verzameling X. Merk op dat als Y een deelverzameling is van X die precies 1 element bevat uit elke baan die meer dan 1 element bevat, dan

$$|X| = |X_G| + \sum_{y \in Y} |\mathcal{O}(y)|.$$

Stelling 9.2.6. *Zij G een groep van orde p^n (p een priemgetal) en veronderstel dat G een linker actie voert op X. Dan*

$$|X| \equiv |X_G| \pmod{p}.$$

Bewijs. Met notaties zoals in de opmerking voor de stelling. We weten dat $|\mathcal{O}(y)|$ een deler is van $|G| = p^n$. Dus is p een deler van elke $|\mathcal{O}(y)|$. Uit de vergelijking voor de stelling volgt dan $|X| - |X_G|$ deelbaar is door p. □

Wij zullen nu bewijzen dat elke eindige p-groep als orde een macht van p heeft (dus een resultaat zoals in het commutatieve geval). De volgende stelling bevat hiervoor de essentie.

Stelling 9.2.7. *(Stelling van Cauchy) Zij p een priemgetal en G een eindige groep. Als p een deler is van $|G|$ dan heeft G een element van orde p.*

Bewijs. Zij $X = \{(g_1, g_2, \ldots, g_p) \mid g_1 g_2 \cdots g_p = e,\ g_i \in G,\ 1 \leq i \leq p\}$. Merk op dat $X = \{(g_1, g_2, \ldots, g_p) \mid g_p = (g_1 g_2 \cdots g_{p-1})^{-1},\ g_i \in G,\ 1 \leq i \leq p-1\}$. Dus $|X| = |G|^{p-1}$. Omdat $|G|$ deelbaar is door p, volgt dat $|X|$ deelbaar is door p.

Zij $\sigma = (1, 2, 3, \cdots, p) \in S_p$. Wij hebben duidelijk een actie

$$\langle \sigma \rangle \times X \to X$$

gedefinieerd door

$$\sigma(g_1, \cdots, g_p) = (g_2, g_3, \cdots, g_p, g_1)$$

en definieer dan $\sigma^i(g_1, \cdots, g_p)$ iteratief.

Wegens Stelling 9.2.6, $|X| \equiv |X_{\langle \sigma \rangle}| \mod p$. Omdat $p \mid |X|$ volgt er dus dat $p \mid |X_{\langle \sigma \rangle}|$. Omdat $(e, e, \cdots, e) \in X$ volgt er dat $|X_{\langle \sigma \rangle}| \geq p$. Zij dan $(e, e, \cdots, e) \neq (g_1, \cdots, g_p) \in X_{\langle \sigma \rangle}$. Dus, $\sigma(g_1, g_2, \cdots, g_p) = (g_1, g_2, \cdots, g_p)$ en bijgevolg $g_1 = g_2 = \cdots = g_p$. Er volgt dat $g_1^p = g_1 g_2 \cdots g_p = e$. □

Gevolg 9.2.8. *Zij G een eindige groep. Dan is G een p-groep als en slechts als $|G|$ een macht van p is.*

Bewijs. Bewijs dit als een oefening. □

9.3 Sylowstellingen

Lemma 9.3.1. *Zij H een deelgroep van een eindige groep G. Als H een p-groep is (p priem) dan*

$$[N_G(H) : H] \equiv [G : H] \text{ mod } p.$$

I.h.b., als p een deler is van $[G : H]$ dan $N_G(H) \neq H$.

Bewijs. Zij $L = \{gH \mid g \in G\}$ en beschouw de volgende actie

$$H \times L \to L : (h, gH) \mapsto hgH.$$

Merk op dat $L_H = \{gH \mid hgH = gH \text{ voor alle } h \in H\} = \{gH \mid g^{-1}hg \in H \mid \text{ voor alle } h \in H\} = \{gH \mid g \in N_G(H)\} = \{gH \mid gH \subseteq N_G(H)\}$. Dus $|L_H| = [N_G(H) : H]$.

Omdat H een p-groep is, weten wij wegens Gevolg 9.2.8 dat $|H|$ een macht is van p. Ook weten wij uit Stelling 9.2.6 dat $|L| \equiv |L_H| \mod p$. Dus, $[G : H] \equiv [N_G(H) : H] \mod p$. □

Stelling 9.3.2. *(Eerste Sylow stelling) Zij G een eindige groep en $|G| = p^n m$ met $n \geq 1$ en $(p, m) = 1$ (p een priemgetal). De volgende eigenschappen gelden.*

1. *G heeft een deelgroep van orde p^i met i zodat $1 \leq i \leq n$.*
2. *elke deelgroep H van orde p^i is een normale deelgroep van een deelgroep van orde p^{i+1} voor $1 \leq i < n$.*

Bewijs. Wegens Stelling 9.2.7 weten wij dat G een deelgroep heeft van orde p. Wij bewijzen nu door inductie dat als G een deegroep H heeft van orde p^i, met $1 \leq i < n$, dan heeft G een deelgroep van orde p^{i+1} (met H als normale deelgroep). Inderdaad, omdat $i < n$ weten wij dat $p \mid [G : H]$. Wegens Lemma 9.3.1 weten wij ook dat $p \mid [N_G(H) : H]$. Omdat H een normale deelgroep is in $N_G(H)$ kunnen wij de quotientgroep $N_G(H)/H$ vormen. Weer wegens Stelling 9.2.7 verkrijgen wij een deelgroep $\overline{K}$ van $N_G(H)/H$ van orde p. Uit de Isomorfismestellingen weten wij dat $\overline{K} = K/H$ met K een deelgroep van $N_G(H)$ (en dus van G) die H omvat. Duidelijk is $|K| = p^{i+1}$, zoals gewenst. Omdat H een normale deelgroep is van $N_G(H)$ en $H \subseteq K \subseteq N_G(H)$ is duidelijk ook H een normale deelgroep van K. Dus volgt het resultaat. □

Definitie 9.3.3. Een Sylow p-deelgroep P van een groep G is een maximale p-deelgroep van G, d.w.z. dit is een p-deelgroep die niet omvat is in een echt grotere p-deelgroep.

Stelling 9.3.4. *(Tweede Sylow stelling) Zij P_1 en P_2 Sylow p-deelgroepen van een eindige groep G. Dan zijn P_1 en P_2 geconjugeerd, d.w.z., er bestaat een $g \in G$ zodat $P_1 = gP_2g^{-1}$.*

Bewijs. Zij $L = \{gP_1 \mid g \in G\}$ en beschouw de volgende actie

$$P_2 \times L \to L : (y, gP_1) \mapsto (yg)P_1.$$

Wegens Stelling 9.2.6, $|L_{P_2}| \equiv |L| \mod p$. Omdat $p \not| |L| = [G : P_1]$ volgt er dat $|L_{P_2}| \neq 0$. Zij $gP_1 \in L_{P_2}$. Dan $ygP_1 = gP_1$ voor alle $y \in P_2$. Dus $g^{-1}P_2g \subseteq P_1$. Omdat $|P_1| = |P_2|$ en $|g^{-1}P_2g| = |P_2|$ moet $P_1 = g^{-1}P_2g$. Dus zijn P_1 en P_2 geconjugeerd. □

Stelling 9.3.5. *(Derde Sylow Stelling) Als G een eindige groep is en p deelt $|G|$ (met p een priemgetal) dan is het aantal Sylow p-deelgroepen congruent met 1 modulo p en deelt $|G|$.*

Bewijs. Zij P een Sylow p-deelgroep van G. Zij L de verzameling van alle Sylow p-deelgroepen van G. Beschouw de volgende actie

$$P \times L \to L : (g, H) \mapsto gHg^{-1}.$$

Wegens Stelling 9.2.6, $|L| \equiv |L_P| \mod p$.

Nu als $H \in L_P$ dan $gHg^{-1} = H$ voor alle $g \in P$. Dus $P \subseteq N_G(H)$. Duidelijk, $H \subseteq N_G(H)$. Omdat P en H Sylow p-deelgroepen zijn van G, zijn dit dus ook Sylow p-deelgroepen van $N_G(H)$. Maar, wegens Stelling 9.3.4, bestaat $g \in N_G(H)$ zodat $P = gHg^{-1}$. Omdat H normaal is $N_G(H)$ volgt er $P = H$. Dus, $L_P = \{P\}$ en dus $|L| \equiv 1 \mod p$, zoals gewenst.

Beschouw vervolgens de actie

$$G \times L \to L : (g, H) \mapsto gHg^{-1}.$$

Omdat alle Sylow p-deelgroepen geconjugeerd zijn is er slechts één baan (de actie is transitief). Als $P \in L$ dan $|L| = |\text{baan van } P| = [G : G_P]$, wegens de baan-stabilisatorstelling (merk op dat $G_P = N_G(P)$). Omdat $[G : G_P]$ een deler is van G, volgt er dat $|L|$ een deler is van $|G|$. □

De Sylow stellingen zijn te danken aan de Noorse wiskundige Peter Ludvig Mejdell Sylow (1832-1918). Hij publiceerde die stellingen in 1872. Sylow formuleerde zijn stellingen voor permutatiegroepen (omdat de abstracte definitie van groep nog niet bekend

was). In 1887 herbewees Georg Frobenius de stellingen voor abstracte groepen; alhoewel hij opmerkte dat elke groep kan beschouwd worden als een permutatiegroep (Stelling van Cayley). Sylow gaf toepassingen van zijn stellingen voor oplossingen van algebraische vergelijkingen. Hij bewees o.a. dat elke vergelijking wiens Galois-groep een p-groep is oplosbaar is door radikalen. Pas in 1898 werd Sylow Professor aan de Christiana Universiteit. Voordien was hij een leraar.

9.4 Semidirecte producten van groepen

Eigenschap 9.4.1. *Zij N en G groepen en*

$$\pi : G \to Aut(N) : g \mapsto \pi_g$$

een groephomomorfisme. Dan is

$$S = N \times G$$

een groep voor de volgende bewerking

$$(n_1, g_1)(n_2, g_2) = (n_1 \pi_{g_1}(n_2), g_1 g_2).$$

Bovendien zijn $N_0 = N \times \{e_G\}$ en $G_0 = \{e_N\} \times G$ deelgroepen van S. Verder, $N_0 \cong N$ en $G_0 \cong G$ en

1. *$S = N_0 G_0$,*
2. *$N_0 \lhd S$,*
3. *$N_0 \cap G_0 = \{e_S\}$.*

Men noteert deze groep meestal als $N \rtimes_\pi G$.

Bewijs. Wij verifiëren eerst dat S een groep is. Het product definiëert duidelijk een

bewerking. De associativiteit volgt uit het volgende:

$$\begin{aligned}((n_1,g_1)(n_2,g_2))\,(n_3,g_3) &= (n_1\pi_{g_1}(n_2),g_1g_2)(n_3,g_3)\\ &= (n_1\pi_{g_1}(n_2)\pi_{g_1g_2}(n_3),(g_1g_2)g_3)\\ &= (n_1\pi_{g_1}(n_2\pi_{g_2}(n_3)),g_1(g_2g_3))\\ &= (n_1,g_1)(n_2\pi_{g_2}(n_3),g_2g_3)\\ &= (n_1,g_1)\,((n_2,g_2)(n_3,g_3))\end{aligned}$$

Verifiëer zelf dat (e_N,e_G) het neutraal element is.

Verder,

$$(n,g)(\pi_g^{-1}(n^{-1}),g^{-1})=(e_N,e_G)=(\pi_g^{-1}(n^{-1}),g^{-1})(n,g).$$

Dus heeft elk element een invers en is S een groep. De andere voorwaarden zijn eenvoudig te verifiëren. □

Definitie 9.4.2. Een groep S is een semidirect product van een deelgroep N bij een deelgroep G als aan de volgende voorwaarden voldaan is:

1. $S=NG$,
2. $N\lhd S$,
3. $N\cap G=\{e_S\}$.

Eigenschap 9.4.3. *Zij S het semidirect product van N bij G. Dan is de afbeelding*

$$\pi : G\to Aut(N) : g\mapsto \pi_g$$

met

$$\pi_g : N\to N : n\mapsto gng^{-1}$$

een groephomomorfisme.

Bewijs. Omdat $N\lhd S$ is elke π_g een automorfisme van N (het is de beperking van een conjugatie tot N). Duidelijk is π een groephomomorfisme. □

Een voorbeeld van een semidirect product is $D_6=\langle a,b\mid a^3=1,\ b^2=1,\ ba=a^2b\rangle$. Inderdaad

$$D_6\cong C_3\rtimes C_2,$$

met $C_3 = \langle a \rangle$ en $C_2 = \langle b \rangle$. Dus men "ontbindt" de groep D_6 in "eenvoudigere groepen", bovendien hebben deze eenvoudigere groepen geen echte normale deelgroepen.

Definitie 9.4.4. Een groep G noemt men enkelvoudig (simpel) als G en $\{e\}$ de enige normale deelgroepen zijn van G.

Voorbeelden van enkelvoudige groepen zijn de cyclische groepen van orde een priemgetal en ook de alternerende groepen A_n met $n \geq 5$. Al de eindige eenvoudige groepen zijn geklassificeerd. Dit was enorm project en het uiteindelijke bewijs omvat meer dan 10000 blz in vele internationaal gepubliceerde artikels (meestal verschenen in de periode 1955-1985). Momenteel schrijft men een reeks boeken die een een volledig overzichtelijk bewijs en strategie zouden moeten geven. Belangrijke medewerkers aan dit project zijn o.a. Chevalley, Tits, Steinberg, Suzuki, Ree, Mathieu, Burnside, Conway, Janko, Fischer, Brauer, Gorenstein Feit, Aschbacher, Thompson.

Oefeningen

1. Zij $p(x) =$"x is deelbaar door 10" en $q(x) =$"x is even".

   - schrijf $p(x)$ en $q(x)$ met symbolen
   - Geef de negatie van $p(x)$
   - Geef de conjunctie van $p(x)$ en $q(x)$
   - Schrijf "$q(x)$ impliceert $p(x)$", en de contrapositie ervan
   - Schrijf de equivalentie van $p(x)$ en $q(x)$ op

   Zeg van deze uitspraken of ze waar zijn of niet.

2. Stel de waarheidstafel op van de exclusieve of (Xor). Ken je een uitdrukking die equivalent is?

3. Geef de waarheidstafels van

   - $(p \to q) \Rightarrow (q \Rightarrow p)$
   - $q \Leftrightarrow (\neg p \vee \neg q)$
   - $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

4. Toon aan dat $\neg(p \vee q)$ en $\neg p \wedge \neg q$ logisch equivalent zijn. Wat kan je zeggen over $\neg(p \wedge q)$ en $\neg p \vee \neg q$?

5. Toon aan dat $p \Leftrightarrow q$ en $(p \Rightarrow q) \wedge (q \Rightarrow p)$ logisch equivalent zijn.

6. Het aantal rijen van een waarheidstabel hangt af van het aantal samenstellende uitspraken. Wat is het verband?

7. Schrijf de waarheidstafels op voor volgende logische uitspraken en leid er een equivalente vorm voor de uitspraak uit af:

   (a) $\neg(\neg p)$

   (b) $\neg(p \wedge q)$

   (c) $\neg(p \vee q)$

(d) $\neg(p \Leftarrow q)$

(e) $\neg(p \Leftrightarrow q)$

8. Een tautologie (of logische wet) is een uitspraak die steeds waar is. Toon aan dat volgende beweringen tautologieën zijn en interpreteer:

   (a) $\neg(p \wedge (\neg p))$

   (b) $p \vee (\neg p)$

   (c) $(p \wedge p) \Leftrightarrow p$

   (d) $(p \wedge q) \Leftrightarrow (q \wedge p)$

   (e) $(p \vee (q \vee r)) \Leftrightarrow ((p \vee q) \vee r)$

   (f) $\neg(\neg p) \Leftrightarrow p$

   (g) $p \Rightarrow (q \Rightarrow p)$

   (h) $\neg p \Rightarrow (p \Rightarrow q)$

   (i) $(p \Rightarrow q) \vee (q \Rightarrow p)$

9. Is $p \Rightarrow (q \Rightarrow p)$ logisch equivalent met $(p \Rightarrow q) \Rightarrow p$?

10. Noteer volgende oefeningen met behulp van kwantoren. Bepaal eventueel of de bewering waar of vals is. Schrijf de negatie van de bewering op met kwantoren en met woorden.

    (a) "Alle mensen zijn slim."

    (b) "Er zijn mensen die groot zijn."

    (c) "Er zijn mensen die groot zijn en lang haar hebben."

    (d) "Niet alle mensen hebben kort haar."

    (e) "Alle wegen leiden naar Rome."

    (f) "Voor elke mens geldt: als hij groot is, dan is hij niet klein."

    (g) "Een geheel getal is positief."

    (h) "Elk natuurlijk getal is even."

    (i) "Sommige reële getallen zijn positief."

11. Schrijf alle deelverzamelingen van $\{1, 2, 3\}$.

12. Hoeveel deelverzamelingen heeft een verzameling met 2 elementen? Met 3 elementen? Met n elementen?

13. Wanneer behoort een element niet tot $A \cap B$? Vul aan: $x \notin A \cap B \Leftrightarrow \ldots$

14. analoog: $x \notin A \cup B \Leftrightarrow \ldots$

15. analoog: $x \notin A \backslash B \Leftrightarrow \ldots$

16. Toon aan dat

    - $B \supseteq A \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A$
    - $A \cup (A \cap B) = A$
    - $A \cap (A \cup B) = A$

17. Wanneer is $x \notin \bigcup_{i \in I} A_i$?

18. Geef de betekenis in woorden van de volgende uitspraken. Zeg of ze waar of onwaar zijn. Geef de negatie in symbolen en woorden.

    - $\forall\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Z} : x < y$
    - $\exists\, x \in \mathbb{Z}, \exists\, y \in \mathbb{N} : x > y$
    - $\exists\, x \in \mathbb{Z}, \forall\, y \in \mathbb{Z} : x < y$
    - $\forall\, \varepsilon > 0, \exists\, \delta > 0, \forall\, x \in \mathbb{R}\ |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon$

19. Zij $A = \{2, 3\}$, $B = \{4, 5, 6\}$ en $\mathbb{C} = \{a, b, c, d\}$. Geef $A \times B$, $B \times A$, $A \times \mathbb{C}$, $\mathbb{C} \times B$, A^2, $\mathbb{C} \times \{a\}$.

20. Zij $A = \{1, 2, 3, 4\}$ en beschouw de relatie $\leq$: "is kleiner dan of gelijk aan" op A. Geef de elementen van $\leq$. Geef de inverse relatie van $\leq$.

21. Zij $f : A \longrightarrow B$ een functie en $S_1, S_2 \subseteq A$. Bewijs dat

    (a) $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$
    (b) $f(S_1 \cap S_2) \subset f(S_1) \cap f(S_2)$

    Zoek voorbeelden die dit illustreren.

22. Zij $f : A \longrightarrow B$ een functie die niet noodzakelijk inverseerbaar is, en $S \subset A$ en $T, T_1, T_2 \subset B$. Bewijs dat

    (a) $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$
    (b) $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$
    (c) $f(f^{-1}(T)) \subseteq T$
    (d) $f^{-1}(f(S)) \supseteq S$

    Zoek voorbeelden die dit illustreren.

23. Toon aan: $f : A \longrightarrow B$ is injectief $\iff \forall b \in B : f^{-1}(b)$ bevat hoogstens één element.

24. (a) Zij $f : A \longrightarrow B$. Toon aan dat $f \circ 1_A = f = 1_B \circ f$.
    (b) Toon aan dat de samenstelling van 2 injecties opnieuw een injectie is.
    (c) Toon aan dat de samenstelling van 2 surjecties opnieuw een surjectie is.

25. Zij $f(x) = \sqrt{x}$, $g(x) = x/4$ en $h(x) = 4x - 8$. Zoek het functievoorschrift voor:
    (a) $h \circ g \circ f$
    (b) $h \circ f \circ g$
    (c) $g \circ h \circ f$
    (d) $g \circ f \circ h$
    (e) $f \circ g \circ h$
    (f) $f \circ h \circ g$

26. Zij $f(x) = x - 3$, $g(x) = \sqrt{x}$, $h(x) = x^3$ en $j(x) = 2x$. Schrijf de volgende functies als een samenstelling van de bovenstaande:
    (a) $\sqrt{x-3}$
    (b) $2\sqrt{x}$
    (c) $x^{1/4}$
    (d) $4x$
    (e) $\sqrt{(x-3)^3}$
    (f) $(2x-6)^3$
    (g) $2x - 3$
    (h) $x^{3/2}$
    (i) x^9
    (j) $x - 6$
    (k) $2\sqrt{x-3}$
    (l) $\sqrt{x^3-3}$

27. Toon aan voor inverteerbare functies f en g:
    (a) $(f^{-1})^{-1} = f$
    (b) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

28. Onderzoek of volgende functies inverteerbaar zijn. Zo ja, bepaal de inverse functies. Zo nee, definieer een bijectie $\tilde{f}$ met hetzelfde voorschrift als f en bepaal $(\tilde{f})^{-1}$.

    (a) $f : \mathbb{R} \to \mathbb{R} : x \mapsto |x|$

    (b) $f : \mathbb{R} \to \mathbb{R} : x \mapsto x + 1$

    (c) $f : \mathbb{R} \to \mathbb{R} : x \mapsto 2x + 3$

    (d) $f : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto \sqrt{x}$

    (e) $f : \mathbb{R} \to \mathbb{R} : x \mapsto \sqrt[3]{2x} + 2$

    (f) $f : \mathbb{R} \to \mathbb{R} : x \mapsto 1$

    (g) $f : \mathbb{R}_0 \to \mathbb{R} : x \mapsto \frac{2x-3}{x}$

    (h) $f : \mathbb{R} \to \mathbb{R} : x \mapsto \sin x$

29. Zij $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : h(x, y) = 2x + 3y$. Bepaal het beeld van h. Is h injectief? Surjectief?

30. Bewijs: $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$ als f injectief is (zie oef. 21). Geef een voorbeeld van een functie waarbij $f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$.

31. Bepaal of volgende functies injectief zijn. Geef hun beeld.

    (a) $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto 2x + 1$

    (b) $f : \mathbb{Q} \to \mathbb{Q} : x \mapsto 2x + 1$

    (c) $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto x^3 - x$

    (d) $f : \mathbb{R} \to \mathbb{R} : x \mapsto e^x$

    (e) $f : [-\pi/2, \pi/2] \to \mathbb{R} : x \mapsto \sin x$

    (f) $f : [0, \pi] \to \mathbb{R} : x \mapsto \sin x$

32. Stel $f : A \to B$, met $A = X \cup Y$ en $X \cap Y = \emptyset$. Als $f_{|X}$ en $f_{|Y}$ injectief zijn, wat kan je dan zeggen van f?

33. Bepaal voor elk van de volgende functies $f : \mathbb{Z} \to \mathbb{Z}$ of ze injectief of surjectief zijn. Indien niet surjectief, bepaal $f(\mathbb{Z})$:

    (a) $f(x) = x + 7$

    (b) $f(x) = 2x - 3$

    (c) $f(x) = -x + 5$

    (d) $f(x) = x^2$

(e) $f(x) = -x^2 + x$

(f) $f(x) = x^3$

34. Zelfde vraag als oefening 33, waarbij f als een functie van $\mathbb{R}$ naar $\mathbb{R}$ beschouwd wordt.

35. Toon aan: als A en B verzamelingen zijn, dan geldt: $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$. [examen augustus 2005]

36. Vul aan (gebruik $\subseteq$, $\supseteq$ of $=$) en bewijs: als A en B verzamelingen zijn, dan geldt:

$$(A \times B) \cup (B \times A) \quad \ldots \quad (A \cup B) \times (A \cup B).$$

37. Voor welke bewerkingen wordt $\mathbb{Z}$ een semigroep? Een monoïde? Een groep? Welke bewerkingen zijn commutatief?

(a) $a * b = ab$

(b) $a * b = a + b$

(c) $a * b = a - b$

(d) $a * b = |a - b|$

(e) $a * b = \max(a, b)$

(f) $a * b = a$

38. Zij X een verzameling en stel $c(X)$ de verzameling van alle constante functies $X \to X$. Is $c(X)$ uitgerust met de samenstelling van functies een semigroep? Een monoïde? Een groep? Commutatief?

39. Beschouw de verzameling van alle functies $\mathbb{N} \to \mathbb{N}$ uitgerust met de samenstelling van functies. Is dit een semigroep? Een monoïde? Een groep? Commutatief? Beschouw $f : \mathbb{N} \to \mathbb{N} : x \longmapsto 2x$ en $g : \mathbb{N} \to \mathbb{N} : x \longmapsto [\frac{x}{2}]$. Bepaal $f \circ g$ en $g \circ f$.

40. Zij $(S, *)$ een monoïde met neutraal element e.

(a) Veronderstel dat $a * b = b * c = e$. Toon aan dat $a = c$.

(b) Veronderstel dat f voldoet aan $a * f = a$ voor alle a. Kun je iets besluiten over f? Geldt hetzelfde besluit als $(S, *)$ slechts een semigroep is?

(c) Veronderstel dat f voldoet aan $f * f = f$ (we noemen f een *idempotent*). Kun je iets besluiten over f? Geldt hetzelfde besluit als $(S, *)$ een groep is?

41. Vind een struktuur van monoïde op $\mathbb{N}$ die zo is dat voor elke $n \in \mathbb{N}$ getallen a en b in $\mathbb{N}$ bestaan waarvoor de vergelijking $a * x = b$ precies n oplossingen $x \in \mathbb{N}$ heeft.

42. Zij G een groep en c een element van G. Toon dat de bewerking $x * y = xcy$ een groepsstruktuur op G definieert.

43. Zij G een groep.

    (a) Als $x^2 = e$ voor elke $x \in G$, dan is G abels.

    (b) Als $(xy)^2 = x^2y^2$ voor alle $x, y \in G$, dan is G abels.

    (c) Geef een voorbeeld van een niet abelse G met $(xy)^6 = x^6y^6$ voor alle $x, y \in G$.

44. Zijn de volgende structuren ringen, commutatieve ringen, scheef lichamen, lichamen:
$(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_5, +, \cdot)$, $(\mathbb{Z}_6, +, \cdot)$, $(\mathcal{P}(E), \triangle, \cap)$, $(\mathbb{H}, +, \cdot)$?
Wat kan je over $(\mathcal{M}_2(\mathbb{Z}), +, \cdot)$ zeggen?

45. Bereken de groep van de inverteerbare elementen van de volgende ringen:
$(\mathbb{Z}, +, \cdot), (\mathbb{Z}_5, +, \cdot), (\mathbb{Z}_6, +, \cdot), (\mathbb{Z}_8, +, \cdot), (\mathcal{M}_2(\mathbb{Z}), +, \cdot), (\mathcal{M}_2(\mathbb{R}), +, \cdot)$?

46. De diëdergroep D_{2n} is de symmetriegroep van een regelmatige n-hoek in het vlak.

    (a) Bepaal de symmetriegroep van een niet vierkantige rechthoek.

    (b) Bepaal de symmetriegroep van de verzameling $\mathbb{Z}$ in de 1-dimensionale ruimte. Deze groep wordt de *oneindige diëdergroep* D_∞ genoemd.

47. Bespreek het verband tussen volgende eigenschappen van een groep G.

    (a) G is een eindige groep;

    (b) Elk element van G heeft eindige orde.

48. Toon dat in een groep G geldt dat $o(h) = o(g^{-1}hg)$.

49. In de groep $GL_2(\mathbb{R})$, bepaal de orde van $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, van $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ en van ab.

50. De groepen $\mathbb{Z}_2 \times \mathbb{Z}_6$ en $\mathbb{Z}_3 \times \mathbb{Z}_4$ bestaan allebei uit 12 elementen. Zijn ze cyclisch? Vind een criterium voor de situatie dat $\mathbb{Z}_n \times \mathbb{Z}_m$ cyclisch is.

51. (a) Zij G cyclisch van orde n met een voortbrenger a. Wanneer is a^k ook een voortbrenger van G?

    (b) Vind een groeptheoretisch bewijs dat $\text{ggd}(n-1, n) = 1$.

52. Is de unie van twee deelgroepen opnieuw een deelgroep?

53. Als G een groep is, stel

$$T = \{g \in G \mid o(g) < \infty\} = \{g \in G \mid g^n = e \text{ voor een } n \in \mathbb{N}_0\}$$

(a) Als G abels is, ga na dat dit een deelgroep van G is (men noemt dit de *torsiedeelgroep* van G). Wat als G niet abels is?

(b) Indien $G = (\mathbb{C}^*, \cdot)$, welke $g = \rho e^{i\theta}$ behoren tot T?

54. Bepaal het centrum van de Diëdergroep D_{2n} $(n \geq 1)$.

55. Bepaal:

(a) de linker- en rechternevenklassen van de deelgroep $\mathbb{R} \times \{0\}$ in de groep $(\mathbb{R}^2, +)$.

(b) de linker- en rechternevenklassen van de deelgroep $\mathbb{R}_0^+ \times \mathbb{R}_0^+$ in de groep $(\mathbb{R}_0^2, \cdot)$.

(c) de partitie van de groep $(\mathbb{Z}, +)$ in nevenklassen van de deelgroep $6\mathbb{Z}$ en de partitie van de groep $(\mathbb{Z}_{12}, +)$ in nevenklassen van de deelgroep voorgebracht door het element $3 \in \mathbb{Z}_{12}$.

56. Kan je een groep van 21 elementen construeren zodat er een element in deze groep van orde 6 bestaat?
Kan je een niet cyclische groep van orde 59 vinden?

57. Toon dat een deelgroep bevat in het centrum van een groep steeds normaal is.

58. Vind in S_3 een deelgroep van orde 2 en een van orde 3. Bepaal hun linker en rechter nevenklassen. Zijn de deelgroepen normaal?

59. De quaternionengroep Q_8 bestaat uit de acht elementen

$$\{1, -1, i, -i, j, -j, k, -k\}.$$

(a) Vul de volgende tabel aan:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
-1	$\cdot$	1	$-i$	i	$-j$	j	$-k$	k
i	$\cdot$	$-i$	-1	1	k	$-k$	$-j$	$\cdot$
$-i$	$\cdot$	i	$\cdot$	-1	$-k$	k	$\cdot$	$\cdot$
j	$\cdot$	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$\cdot$	j	k	$-k$	1	$\cdot$	$-i$	$\cdot$
k	$\cdot$	$-k$	j	$-j$	$-i$	i	-1	$\cdot$
$-k$	$\cdot$	k	$-j$	j	i	$-i$	1	-1

(b) Geldt $(-i \cdot j)i = -i(j \cdot i)$? $jk = kj$?

(c) Vind alle deelgroepen van Q_8. Welke zijn normaal?

60. Beschouw de deelgroep

$$G = \{1, (ab)(cd), (da)(bc), (ac)(bd), (abcd), (adcb), (bd), (ac)\}$$

van S_4. Zij $H = \{1, (ab)(cd), (da)(bc), (ac)(bd)\}$, $K_1 = \{1, (ab)(cd)\}$ en $K_2 = \{1, (ac)(bd)\}$. Is H normaal in G? K_i normaal in H? K_i normaal in G?

61. Beschrijf het quotient $(\mathbb{R}_0, \cdot)/(\mathbb{R}_0^+, \cdot)$.

62. Bepaal de torsiedeelgroep van de abelse groep $(\mathbb{R}, +)$, van de deelgroep $(\mathbb{Z}, +)$ en van het quotient $(\mathbb{R}/\mathbb{Z}, +)$.

63. Bestaat er een groep G met centrum Z

    (a) zodat het quotient G/Z cyclisch van orde 13 is?

    (b) zodat G/Z abels is maar G niet?

64. Bewijs eigenschap 8.3.6.

65. Zijn de volgende functies groep homomorfismen? Als zo, bepaal hun kern en beeld.

    (a) $(\mathbb{R}, +) \to (\mathbb{R}, +) : x \mapsto x^2$

    (b) $(\mathbb{R}, +) \to (\mathbb{R}_0^+, \cdot) : x \mapsto e^x$

    (c) $(\mathbb{R}^2, +) \to (\mathbb{R}_0, \cdot) : (x, y) \mapsto e^{x+y}$

    (d) $(\mathbb{R}, +) \to (\mathbb{C}_0, \cdot) : x \mapsto e^{2\pi x}$

    (e) $(\mathbb{Z}, +) \to (\mathbb{Z}, +) : z \mapsto z + 1$

    (f) $(\mathbb{R}_0, \cdot) \to (\mathbb{R}_0, \cdot) : x \mapsto x^3$

    (g) $(\mathbb{C}_0, \cdot) \to (\mathbb{C}_0, \cdot) : x \mapsto x^2$

    (h) $(\mathbb{Z}^2, +) \to (\mathbb{R}, +) : (a, b) \mapsto a + b\pi$

66. (a) Vind een isomorfisme tussen $(\mathbb{R}_0, \cdot)$ en $(\mathbb{Z}_2, +) \times (\mathbb{R}_0^+, \cdot)$.

    (b) Construeer een isomorfisme tussen $(\mathbb{C}_0, \cdot)$ en $(S, \cdot) \times (\mathbb{R}_0^+, \cdot)$, waar $S = \{z \in \mathbb{C} \mid |z| = 1\}$.

67. Beschouw het endomorfisme f van S_3 dat 1,(123) en (132) afbeeldt op 1 en de overige elementen op (12).

    (a) Is f injectief? Surjectief?

    (b) Zijn $\ker f$ en Beeld$f$ (normale?) deelgroepen van S_3?

(c) Ga de eerste isomorfismestelling na op dit voorbeeld.

68. Beschouw een homomorfisme $f : G \to H$. Toon dat als $g \in G$ eindige orde heeft, dan deelt de orde van $f(g)$ de orde van g. Kunnen we meer zeggen als f een monomorfisme is?

69. Zij $f : (\mathbb{R}, +) \to (\mathbb{R}_0, \cdot)$ een homomorfisme dat afleidbaar is als functie $\mathbb{R} \to \mathbb{R}$. Toon aan:

    (a) $f(x) > 0 \ \forall x \in \mathbb{R}$;

    (b) $\exists a \in \mathbb{R} : \ f(x) = e^{ax} \ \forall x \in \mathbb{R}$.

70. Stel $p_1 = 2$, $p_2 = 3$, $p_3 = 5$,...,$p_n =$ het n-de priemgetal. Dan kan elk strikt positief rationaal getal q geschreven worden als een produkt $q = \prod_{n=1}^{\infty} p_n^{m_n}$ waar $m_n \in \mathbb{Z}$ nul wordt voor n voldoende groot. Is

$$f : (\mathbb{Q}_0^+, \cdot) \to \prod_{n \in \mathbb{N}_0} (\mathbb{Z}, +) : q \longmapsto (m_n)_n$$

    een homomorfisme? Een monomorfisme? Een epimorfisme?

71. Volgens de stelling van Cayley (8.1.1) bestaat er een monomorfisme $\mathbb{Z}_6 \to S_6$. Bestaat er ook een monomorfisme $\mathbb{Z}_6 \to S_5$?

72. (a) Zoek een isomorfisme tussen A_4 en de groep van de rotaties van de ruimte die een tetraëder invariant laten.

    (b) Toon aan dat A_4 geen deelgroep van index 2 heeft.

    (c) Ga na dat $K = \{1, (12)(34), (13)(24), (14)(23)\}$ een deelgroep is van A_4.

    (d) Is A_4 enkelvoudig?

73. Zij $GL(2, \mathbb{R})$ de groep van matrices van determinant veschillend van 0 en $SL(2, \mathbb{R})$ de groep van matrices van determinant 1. Gebruik de feit dat de determinant een groepshomomorfisme is en de eerste isomorfisme stelling om de quotient $(GL(2, \mathbb{R})/SL(2, \mathbb{R}), \cdot)$ te bepalen.

74. Zij $S = \{z \in \mathbb{C} \mid |z| = 1\}$ en $\mu_n^{\mathbb{C}} = \{z \in S \mid z^n = 1\}$.

    (a) Bewijs dat $\varphi : (\mathbb{R}, +) \to (S, \cdot) : x \mapsto e^{2\pi i x}$ een groepshomomorfisme is.

    (b) Bepaal $(\mathbb{R}/\mathbb{Z}, +)$.

    (c) Bewijs dat $(S, \cdot) \to (S, \cdot) : z \mapsto z^n$ een homomorfisme is. Wat is de kern? Wat is het beeld?

    (d) Bepaal $(S/\mu_n^{\mathbb{C}}, \cdot)$!

75. Bepaal volgende quotienten:

    (a) $(\mathbb{Z}/5\mathbb{Z}, +)$,

    (b) $(\mathbb{Z}/n\mathbb{Z}, +)$ voor een $n \in \mathbb{N}_0$,

    (c) $(\mathbb{Z}^2/(2\mathbb{Z} \times 5\mathbb{Z}), +)$,

    (d) $(\mathbb{Z}^2/(m\mathbb{Z} \times n\mathbb{Z}), +)$ voor $n, m \in \mathbb{N}_0$.

76. Bepaal de quotient $(\mathbb{R}_0^2/\{(x, y) \in \mathbb{R}_0^2 \mid y = x^2\}, \cdot)$.

77. Bepaal in $(S_{100}, \circ)$

    (a) $|\{q \in S_{100} \mid q \circ (123) \circ q^{-1} = (456)\}|$

    (b) $|\{q \in S_{100} \mid q \circ (123) \circ q^{-1} = (123)\}|$

    (c) $|\{q \in S_{100} \mid q \circ (123)(45) \circ q^{-1} = (345)(67)\}|$

    (d) $|\{q \in S_{100} \mid q \circ (12)(34) \circ q^{-1} = (12)(34)\}|$

    (e) $|\{q \in S_{100} \mid q \circ (123) \circ q^{-1} = (12)\}|$

78. Geef een voorbeeld (als mogelijk) van

    (a) een even permutatie van even orde,

    (b) een even permutatie van oneven orde,

    (c) een oneven permutatie van even orde,

    (d) een oneven permutatie van oneven orde.

79. Bewijs dat een permutatie even is als en slechts als de aantal van cyclussen van even lengte even is. Bewijs dan dat een oneven permutatie altijd van even orde is.

80. Toon aan dat de 3-cyclussen in $(A_4, \circ)$ twee conjugatieklassen vormen, maar dat de 3-cyclussen in $(A_5, \circ)$ alle in een conjugatieklass zijn.

81. (a) Welke groepen zijn isomorf onder $\mathbb{Z}_{18}$, $\mathbb{Z}_2 \times \mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$?

    (b) Ga na dat elk van deze groepen een (juist één?) deelgroep van orde 1, 2, 3, 6, 9 en 18 omvat.

82. (a) Hoeveel rotaties van de ruimte laten een kubus invariant?

    (b) Ken je de groep van deze rotaties?

83. Zij G een groep en p een priemgetal.

    (a) Toon, door gebruik te maken van de Orbiet-stabilisator stelling, dat als $|G| = p^n$, dan heeft G een niet-triviaal centrum.

(b) Als $|G| = p$, dan is G abels;

(c) Als $|G| = p^2$, dan is G abels;

(d) Is dit ook het geval als $|G| = p^3$?

84. Veronderstel dat een groep G een actie uitvoert op een verzameling X. Toon dat voor $x \in X$ en $g \in G$ de stabilisatoren van x en $g \cdot x$ geconjugeerde deelgroepen van G zijn.

85. Zij G een eindige groep met precies twee conjugatieklassen. Toon dat G precies twee elementen telt.

86. Zij G een eindige groep met $|G| = p^n m$ met $n \geq 1$ en $(p, m) = 1$. Zij $N \trianglelefteq G$ met $|N| = p^k$ met $k \leq n$. Bewijs dat N een normale deelgroep is van elke Sylow p-deelgroep van G.

87. Zij G een niet cyclische groep van orde 21.

(a) Hoeveel Sylow 3-deelgroepen heeft G?

(b) Bewijs dat G exakt 14 elementen van orde 3 heeft.

88. Zij G een groep van order 56. We willen bewijzen dat G niet enkelvoudig is.

(a) Bewijs dat G ofwel 1, ofwel 8 Sylow 7-deelgroepen heeft.

(b) Bewijs dat G niet enkelvoudig is, als er exakt een Sylow 7-deelgroep is.

Veronderstel nu dat het aantal Sylow 7-deelgroepen gelijk aan 8 is.

(a) Bewijs dat elke Sylow 7-deelgroep cyclisch is.

(b) Bewijs dat de doorsnede van twee Sylow 7-deelgroepen triviaal is.

(c) Bewijs dat er dus 48 elementen van orde 7 in G zijn.

(d) Bewijs dat in deze geval enkel een Sylow 2-groep kan bestaan.

(e) Bewijs dat dus G niet enkelvoudig is.

89. Beschouw $C_2 =< b \,|\, b^2 = 1 >$ en $C_3 =< a \,|\, a^3 = 1 >$.

(a) Vind al de automorfismen van C_3;

(b) Vind al de homomorfismen van C_2 naar $\mathrm{Aut}(C_3)$;

(c) Als $\pi : C_2 \to \mathrm{Aut}(C_3)$ triviaal is, dan geldt $C_3 \rtimes_\pi C_2 \cong C_3 \times C_2$;

(d) Als $\pi : C_2 \to \mathrm{Aut}(C_3)$ niet triviaal is, dan geldt $C_3 \rtimes_\pi C_2 \cong D_6$.

90. Als G een groep is, H een normale deelgroep, $H \cong \mathbb{Z}_6$, en $G/H \cong \mathbb{Z}_2$, uit hoeveel elementen bestaat G dan? Is G noodzakelijk commutatief? Is G noodzakelijk cyclisch?

91. Schrijf de oneindige diëdergroep als een semidirect produkt.

Index

Bibliografie

[1] M. Artin, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[2] J. B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[3] M. Hall, Jr., *The theory of groups*, The Macmillan Co., New York, N.Y., 1959.

[4] I. N. Herstein, *Abstract algebra*, Prentice Hall, Inc., Upper Saddle River, NJ, third ed., 1996. With a preface by Barbara Cortzen and David J. Winter.

[5] J. F. Humphreys, *A course in group theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1996.