Samenvatting Algebra 1

Jonas van der Schaaf

23 mei 2020

Inhoudsopgave

1 Groepen

Groepsaxioma's Een groep is een paar van een verzameling G met een bewerking $\circ\colon G \times G \to G$ met de volgende eigenschappen:

1. Associativiteit: voor elke $a, b, c \in G$ geldt dat
$$(a \circ b) \circ c = a \circ (b \circ c),$$
2. Neutraal element: er is een $e \in G$ zodat voor elke $g \in G$ geldt dat
$$e \circ g = g \circ e = g,$$
3. Voor elke $a \in G$ is er een a^* zodat
$$a \circ a^* = a^* \circ a = e.$$

Abelse Groepen Zij G een groep. Als voor elke $a, b \in G$ geldt dat $a \circ b = b \circ a$, dan heet G abels, en dan zeggen we dat elk element in G commuteert.

Multiplicatieve notatie In de rest van deze samenvatting zal ik (bijna) altijd de multiplicatieve notatie gebruiken, dat komt overeen met $a \circ b = ab$, $\underbrace{a \circ \cdots \circ a}_{n\times} = a^n$ en $a^* = a^{-1}$.

Simpele stellingen over inverses Zij G een groep, dan geldt dat:

1. Er is precies 1 eenheidselement in een groep,
2. Elk element $a \in G$ heeft precies 1 inverse,
3. Voor elke $a, b \in G$ geldt dat
$$\left(a^{-1}\right)^{-1} = a$$
en dat
$$(ab)^{-1} = b^{-1}a^{-1}.$$

Verder geldt voor $n, m \in \mathbb{Z}$ dat $a^{n+m} = a^n \cdot a^m$ en dat $a^{nm} = (a^n)^m$.

Uniciteit van producten Zij G een groep en $a, b \in G$. Dan is er precies één $x \in G$ zodat $ax = b$, namelijk $x = a^{-1}b$.

Ook is er precies één $y \in G$ zodat $ya = b$, namelijk $y = ba^{-1}$.

Producten van meer dan 1 element Zij G een groep met $a_1, \ldots, a_n \in G$ dan is het product $a_1 \cdots a_n$ inductief gedefinieerd als $(a_1 \cdots a_{n-1})a_n$. Ook volgt door inductie toe te passen uit deze definitie dat $(a_1 \cdots a_k)(a_{k+1} \cdots a_n) = a_1 \cdots a_n$.

2 Ondergroepen, homomorfismen en directe producten

2.1 Ondergroepen

Definitie van een ondergroep Zij G een groep en laat $H \subseteq G$ een deelverzameling zijn. Dan geldt dat H een ondergroep is precies als:

1. H niet leeg is ($H \neq \varnothing$),
2. voor elke $a, b \in H$ geldt dat $ab \in H$ (ook wel H is gesloten),
3. voor alle $a \in H$ ook geldt dat $a^{-1} \in H$.

Ondergroepen en groepen Zij G een groep en $H \subseteq G$ een ondergroep. Dan is H ook een groep met dezelfde werking als op G.

Equivalente eigenschappen van ondergroep Zij G een groep en $H \subseteq G$ een deelverzameling, dan is H ook een ondergroep als geldt dat

1. H niet leeg is,
2. voor elke $a, b \in H$ geldt dat $ab^{-1} \in H$.

Doorsnedes van ondergroepen Zij G een groep en $(H_i)_{i \in I}$ een collectie ondergroepen, dan geldt dat

$$\bigcap_{i \in I} H_i$$

ook een ondergroep is van G.

2.2 Groepshomomorfismen

Definitie van een homomorfisme Zij G_1, G_2 groepen. Dan is $f\colon G_1 \to G_2$ een groepshomomorfisme als voor elke $a, b \in G_1$ geldt dat

$$f(ab) = f(a)f(b).$$

De verzameling van homomorfismen van G_1 naar G_2 wordt als $\mathrm{Hom}(G_1, G_2)$ genoteerd.

Isomorfismen Zij G_1, G_2 groepen en $f\colon G_1 \to G_2$ een bijectief homomorfisme, dan wordt het ook wel een isomorfisme genoemd. Als er een isomorfisme tussen twee groepen G_1, G_2 bestaat, dan heten deze isomorf, en dat wordt genoteerd als $G_1 \cong G_2$.

Endomorfismen Een homomorfisme van een groep naar zichzelf heet een endomorfisme. De verzameling endomorfismen van G wordt genoteerd als $\mathrm{End}(G)$.

Automorfismen Een isomorfisme van een groep naar zichzelf heet een automorfisme. De verzameling automorfismen van G wordt genoteerd als $\mathrm{Aut}(G)$.

Eigenschappen van een homomorfisme Zij G_1, G_2 groepen en $f\colon G_1 \to G_2$ een homomorfisme. Laat $e_1 \in G_1$ het eenheidselement van G_1 zijn en $e_{2 \in G_2}$ het eenheidselement van G_2. Dan geldt dat

1. $f(e_1) = e_2$,
2. voor elke $a \in G_1$ geldt dat $f(a^{-1}) = f(a)^{-1}$.

Kernen van homomorfismen Zij G_1, G_2 groepen, $f\colon G_1 \to G_2$ een homomorfisme en e_2 het eenheidselement van G_2. Dan is de kern van f als volgt gedefinieerd:

$$\ker(f) = \{g \in G \mid f(g) = e_2\}.$$

De kern is een ondergroep van G_1. Ook is het beeld $f[G_1]$ een ondergroep van G_2.

Injectieviteit Zij G_1, G_2 groepen, $f\colon G_1 \to G_2$ een homomorfisme en e_1 het eenheidselement van G_1. Dan geldt dat f een injectieve functie is precies als

$$\ker(f) = \{e_1\}.$$

Samenstellingen van homomorfismen Zij G_1, G_2, G_3 groepen en $f\colon G_1 \to G_2$ en $g\colon G_2 \to G_3$ homomorfismen. Dan is $f \circ g$ ook een homomorfisme.

Inverses van isomorfismen Zij G_1, G_2 groepen en $f\colon G_1 \to G_2$ een isomorfisme, dan is f^{-1} ook een isomorfisme.

Equivalentie en isomorfismen Zij G_1, G_2, G_3 groepen, dan geldt dat

1. $G_1 \cong G_1$,
2. als $G_1 \cong G_2$, dan geldt ook dat $G_2 \cong G_1$,
3. als $G_1 \cong G_2$ en $G_2 \cong G_3$, dan geldt ook dat $G_1 \cong G_3$.

2.3 Directe producten

Definitie van het directe product Zij G_1, G_2 twee groepen, dan geldt dat $G_1 \times G_2$ met de bewerking

$$(G_1 \times G_2) \times (G_1 \times G_2) \to G_1 \times G_2 \colon ((g_1, h_1), (g_2, h_2)) \mapsto (g_1 g_2, h_1 h_2)$$

een groep vormt.

Eigenschappen van het directe product Voor drie groepen G_1, G_2, G_3 geldt in zekere zin dat ze de volgenden eigenschappen hebben

1. Commutativiteit: $G_1 \times G_2 \cong G_2 \times G_1$,
2. associativiteit: $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3) \cong G_1 \times G_2 \times G_3$.

Isomorfisme tussen een groep en ondergroepen Zij G een ondergroep met twee ondergroepen H_1, H_2 met de volgende eigenschappen

1. Voor alle $h_1 \in H_1$ en $h_2 \in H_2$ geldt dat $h_1 h_2 = h_2 h_1$m
2. $H_1 \cap H_2 = \{e\}$,
3. voor elke $g \in G$ geldt dat $g = h_1 h_2$ voor een $h_1 \in H_1$ en $h_2 \in H_2$.

Dan geldt dat $G \cong H_1 \times H_2$.

Chinese reststelling Zij $n, m \in \mathbb{N}$ met $\text{ggd}(n, m) = 1$. Dan geldt dat

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

met het isomorfisme

$$f\colon \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \colon a \mod nm \to (a \mod n, a \mod m).$$

Algemenere versie Zij $n_1, \ldots, n_t$ positieve gehele getallen zijn zodat voor alle $i, j \in \{1, \ldots, t\}$ geldt dat $\operatorname{ggd}(n_i, n_j) = 1$. Definieer $N \coloneqq \prod_{i=1}^t n_i$. Dan geldt dat

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$$

met het isomorfisme

$$f\colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}\colon a \mod N \mapsto (a \mod n_1, \ldots, a \mod n_t).$$

3 Voortbrengers, orde en index

3.1 Voortbrengers

Definitie van een voortbrenger Zij G een groep en $S \subseteq G$ een deelverzameling. Dan geldt dat

$$\langle S \rangle := \{g \in G \mid g = x_1 \cdots x_n, n \in \mathbb{N}_0, x_i \in S \text{ of } x_i^{-1} \in S\}.$$

Voor elke S geldt dat $\langle S \rangle$ een ondergroep is.

Cyclische groep Een groep heet cyclisch als geldt dat $\langle x \rangle = G$ voor een $x \in G$. Dan heet x een voortbrenger van G.

Orde van een element Zij G een groep en $x \in G$. Dan is de orde van x gedefinieerd als

$$\operatorname{orde}(x) := \begin{cases} \min\{n \in \mathbb{N} \mid x^n = e\} = \# \langle x \rangle & \{n \in \mathbb{N} \mid x^n = e\} \neq \varnothing \\ \infty & \{n \in \mathbb{N} \mid x^n = e\} = \varnothing \end{cases}.$$

Het enige element met orde 1 is het eenheidselement.

Machten van veelvouden van de orde Zij $x \in G$ een element met orde $n < \infty$. Dan geldt voor $m \in \mathbb{Z}$ dat $x^m = e$ dan en slechts dan als $n \mid m$.

Isomorfismen van gegenereerde ondergroepen Zij G een groep en $x \in G$. Dan geldt dat

1. $\langle x \rangle \cong \mathbb{Z}$ als $\operatorname{orde}(x) = \infty$,
2. $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$ als $\operatorname{orde}(x) = n < \infty$.

Ordes en homomorfismen Zij G_1, G_2 groepen en $x \in G_1$ een element met $\operatorname{orde}(x) = n < \infty$. Dan heeft $f(x)$ ook eindige orde en $\operatorname{orde}(f(x)) \mid \operatorname{orde}(x)$. Als f injectief is geldt dat $\operatorname{orde}(f(x)) = \operatorname{orde}(x)$.

3.2 Ordes van (onder)groepen

Orde van een groep Zij G een groep, dan is de orde van G gedefinieerd als

$$\operatorname{orde}(G) := \#G.$$

Stelling van Euler Zij $a \in \mathbb{Z}$ en $m \in \mathbb{N}$ met $\operatorname{ggd}(a, m) = 1$. Dan geldt dat $a^{\varphi(m)} \equiv 1 \mod m$.

Kleine stelling van Fermat Zij p een priemgetal en $a \in \mathbb{Z}$, dan geldt dat $a^p \equiv a \mod p$.

3.3 Nevenklassen

Definitie van een nevenklasse Zij G een groep en $H \subseteq G$ een ondergroep. Laat $a \in G$. Dan heet

$$aH := \{ah \mid h \in H\}$$

een linkernevenklasse van H en

$$Ha := \{ha \mid h \in H\}$$

een rechternevenklasse van H.

De verzameling rechternevenklassen van H wordt genoteerd als G/H en de verzameling linkernevenklassen als $H \backslash G$.

Elementen van nevenklassen Zij G een groep en $H \subseteq G$ een ondergroep. Dan gelden de volgende drie eigenschappen voor alle $a, b \in G$:

1. $aH = bH$ dan en slechts dan als $a^{-1}b \in H$,
2. óf $aH = bH$ óf $aH \cap bH = \varnothing$,
3. elk element zit in precies 1 nevenklasse.

Aantallen elementen van nevenklassen Zij G een groep en $H \subseteq G$ een ondergroep, dan geldt voor elke $a \in G$ dat
$$\#aH = \#H.$$

Index van een ondergroep Zij G een groep en $H \subseteq G$ een ondergroep, dan is de index van H als volgt gedefinieerd:
$$[G : H] \coloneqq \#(G/H).$$

Representantensysteem Zij G een groep, $H \subseteq G$ een ondergroep en $S \subseteq G$ een verzameling zodat het precies 1 element uit elke nevenklasse bevat, dan heet S een representantensysteem en dan geldt dat $\#S = [G : H]$. Bovendien geldt ook dat

$$G = \coprod_{s \in S} sH.$$

De stelling van Lagrange Zij G een groep en $H \subseteq G$ een ondergroep. Dan geldt dat

$$\mathrm{orde}(G) = [G : H] \cdot \mathrm{orde}(H).$$

Hieruit volgt dat $\mathrm{orde}(H) \mid \mathrm{orde}(G)$ als G eindig is, want $[G : H] \in \mathbb{N}$.

Ondergroep van een ondergroep Zij G een eindige groep en $H_2 \subseteq H_1 \subseteq G$ ondergroepen. Dan geldt dat
$$[G : H_1] = [G : H_2] \cdot [H_2 : H_1].$$

Ordes van elementen en groepen Zij G een groep en laat $x \in G$. Dan geldt dat $\mathrm{orde}(x) \mid \mathrm{orde}(G)$.

Groepen met ordes van priemgetallen Zij G een groep met $\mathrm{orde}(G) = p$, dan is G cyclisch en $G \cong \mathbb{Z}/p\mathbb{Z}$.

Kleine groepen en cycliciteit Zij G een groep met $\mathrm{orde}(G) \leq 5$, dan geldt dat G cyclisch is of $G \cong V_4$.

Stelling van Cauchy Zij G een eindige groep en p een priemgetal zodat $p \mid \mathrm{orde}(G)$. Dan is er een $x \in G$ met $\mathrm{orde}(x) = p$.

4 Ondergroepen en factorgroepen

4.1 Normaaldelers

Definitie van een normaaldeler Zij G een groep en $N \subseteq G$ een ondergroep. Dan heet N een normaaldeler als voor alle $g \in G$ en $n \in N$ geldt dat

$$gng^{-1} \in N.$$

Dit wordt ook wel genoteerd als $N \triangleleft G$.

Het centrum van een groep Zij G een groep. Dan is het centrum van G gedefinieerd als $Z(G) \coloneqq \{g \in G \mid \forall h \in G \colon gh = hg\}$. Het centrum is een normaaldeler.

De commutatorondergroep Zij G een groep. Dan is de commutatorondergroep van G gedefinieerd als $[G, G] \coloneqq \langle\{[g, h] \mid g, h \in G\}\rangle$. Dit is ook een normaaldeler. We definiëren ook dat $G_{ab} = G/[G, G]$.

Normaaldelers en linkse/rechtse nevenklassen Zij G een groep en $N \subseteq G$ een ondergroep. Dan is N een normaaldeler dan en slechts dan als $aN = Na$ voor alle $a \in G$.

Ondergroepen van index 2 Zij G een groep en N een ondergroep met $[G : N] = 2$, dan geldt dat $N \triangleleft G$.

Kernen van homomorfismen Zij G_1, G_2 groepen en $f \colon G_1 \to G_2$ een homomorfisme, dan geldt dat $\ker(f) \triangleleft G$.

4.2 Factorgroepen

Constructie van de factorgroep Zij G een groep en $N \triangleleft G$. Dan vormt G/N een groep met de bewerking $G/N \times G/N \colon (\overline{a}, \overline{b}) \mapsto \overline{ab}$.

Bovendien geldt dat $\text{orde}(G/N) = [G : N]$, en als G abels is, dan is G/N dat ook.

Normaaldelers zijn kernen Zij G een groep en $N \triangleleft G$. Dan is N de kern van het homomorfisme

$$\varphi \colon G \to G/N \colon g \mapsto gN.$$

Dit homomorfisme heet het natuurlijke/canonieke homomorfisme. De functie φ is ook surjectief.

Normaaldeler en kern Zij G een groep en $N \subset G$ een ondergroep. Dan geldt dat $N \triangleleft G$ dan en slechts dan als $N = \ker(f)$ voor een homomorfisme f.

Normaaldeler en ondergroepen Zij G een groep $N \triangleleft G$ en $H \subseteq G$ een ondergroep zodat $N \subseteq H$. Dan geldt dat N/H een ondergroep is van G/N.

Normaaldelers en abelse groepen Zij G een groep en $N \triangleleft G$, dan is G/N abels precies als $[G, G] \subseteq N$.

5 Isomorfie- en homomorfiestellingen

De homomorfiestelling Zij G_1, G_2 groepen en $f\colon G_1 \to G_2$ een homomorfisme en $N \lhd G$ met $N \subseteq \ker(f)$. Dan is er een unieke $g\colon G_1/N \to G_2$ met $g(\overline{a}) \coloneqq f(a)$ zodat geldt dat $g \circ \varphi = f$. Bovendien geldt dat $\ker(g) = \ker(f)/N \subseteq G/N$.

Eerste isomorfiestelling Zij G_1, G_2 groepen met $f\colon G_1, G_2$ een homomorfisme, dan geldt dat

$$G_1/\ker(f) \cong f(G_1).$$

Surjectief homomorfisme Als de eisen hierboven gelden en f surjectief is, dan geldt dat $G_1/\ker(f) \cong f(G_1) = G_2$ met een isomorfie gegeven door $a \cdot \ker(f) \mapsto f(a)$.

Homomorfisme tussen abelse groep Zij G, A groepen en A abels. Dan is er voor elk homomorfisme $f\colon G \to A$ een eenduidig bepaald homomorfisme $g\colon G_{ab} \to A$ waarvoor geldt dat $f = g \circ \varphi$. Hier is $\varphi\colon G \to G_{ab}$ de canonieke afbeelding.

Doorsnedes van normaaldelers Zij G een groep, $N \lhd G$ en $H \subseteq G$ een ondergroep. Dan geldt dat:

1. $N \cap H \lhd H$,
2. $HN = \{hn \mid h \in H, n \in N\}$ is een ondergroep van G,
3. $H/(H \cap N) \cong HN/N$ (dit is de tweede isomorfiestelling).

Derde isomorfiestelling Zij G een groep en $N, N' \lhd$ met $N \subseteq N'$. Dan geldt dat N'/N een normaaldeler is van G/N en elke normaaldeler van G/N is van deze vorm. Ook geldt dat

$$(G/N)(N'/N) \cong G/N'.$$

6 Groepswerkingen

Definitie van een groepswerking Zij G een groep en X een verzameling. Een werking is dan een afbeelding:

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

die voldoet aan de volgende twee eigenschappen:

1. Voor elke $x \in X$ geldt dat $e \circ x = x$,
2. voor alle $g, h \in G$ en $x \in X$ geldt dat $g \circ (h \circ x) = (gh) \circ x$.

Groepswerkingen en bijecties Zij G een groep en X een verzameling zodat G op X werkt met $\circ$. Dan is de afbeelding

$$\varepsilon_g : X \to X : x \mapsto g \circ x$$

een bijectie. Ook geldt dat $f : G \to S(X) : g \mapsto \varepsilon_g$ een homomorfisme is.

Homomorfismes naar symmetrische groep Zij G een groep, X een verzameling en $f : G \to S(X)$ een homomorfisme, dan is $G \times X \to X : x \mapsto f(g)(x)$ een groepswerking.

Isomorfie van een groep met de symmetrische groep Elke groep G is isomorf met een ondergroep van $S(G)$. Als $\#G = n < \infty$, dan is G specifiek isomorf met een ondergroep van S_n.

Normaaldelers en ondergroepen Zij G een groep en $H \subseteq G$ een ondergroep met de eigenschap $[G : H] = n < \infty$, dan is er een normaaldeler N met $N \subseteq H$ en $[G : N] \mid n!$.

Ondergroep met bijzondere orde Zij G een groep en H een ondergroep met $\operatorname{ggd}(\#H, ([G : H] - 1)!) = 1$. Dan is H een normaaldeler.

Ondergroep met priemgetal als orde Zij G een groep en $H \subseteq G$ een ondergroep zodat $\#H$ de kleinste priemdeler is van $\#G$. Dan is H een normaaldeler.

Definitie van de baan Zij G een groep die werkt op X, dan is de baan van $x \in X$ onder G gedefinieerd als

$$Gx := \{g \circ x \mid g \in G\}.$$

Equivalentie Zij G een groep die werkt op X, dan heten twee elementen $x, y \in X$ equivalent onder G als er een $g \in G$ is zodat $g \circ x = y$, dit wordt geschreven als $x \sim_G y$. Dit is een equivalentierelatie. De equivalentieklassen zijn precies de banen van X onder G.

Transitief werken Zij G een groep die werkt op X, dan geldt dat G transitief werkt op X als geldt dat $Gx = X$, dus als er precies 1 baan is.

Definitie van de stabilisator Zij G een groep die werkt op X. Dan is de stabilisator van een $x \in X$ gedefinieerd als

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

Stabilisatoren en ondergroepen Zij G een groep die werkt op X. Dan is G_x een ondergroep van G en voor elke $g \in X$ geldt dat $gG_xg^{-1} = G_{g \circ x}$.

Nevenklassen van de stabilisator en banen Zij G een groep die werkt op X en $x \in X$. Dan geldt dat de afbeelding

$$f\colon G/G_x \to Gx\colon aG_x \mapsto a \circ x,$$

een welgedefinieerde bijectie. Daardoor geldt dat $\#Gx = [G : G_x]$.

Verzamelingen en indices van ondergroepen Zij G een groep de werkt op X. LZij Y een verzameling met precies één element uit elke baan. Dan geldt dat

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

Conjugatie en groepswerking Zij G een groep die op zichzelf werkt met

$${}^{g}x \coloneqq gxg^{-1},$$

dan heten de banen Gx de conjugatieklassen van x. Twee elementen $x, y \in G$ heten geconjugeerd als geldt dat er een $g \in G$ zodat geldt dat $gxg^{-1} = y$.

Groepen met orde van de macht van een priemgetal Zij G een groep met$\#G = p^k$ met p priem, dan geldt dat $Z(G) \neq \{e\}$.

Formule van Burnside Zij G een groep die werkt op een eindige verzameling X. Definiëer dan de fixpunten van g als

$$X^g \coloneqq \{x \in X \mid g \circ x = x\}.$$

Dan geldt voor het aantal banen $\#X/G$ dat het gelijk is aan

$$\#X/G = \frac{1}{\#G} \cdot \sum_{g \in G} \#X^g.$$

7 Automorfismen

7.1 De automofismegroep

Definitie van de automorfismegroep Zij G een groep. Dan geldt dat

$$\mathrm{Aut}(G) = \{f\colon G \to G \mid G \text{ is een isomorfisme}\} \subseteq S(G)$$

een ondergroep is.

Inwendige automorfismen Zij G een groep. Definiëer $\varphi_a\colon G \to G\colon g \mapsto aga^{-1}$ voor $a \in G$. Dan is de verzameling

$$\mathrm{Inn}(G) \coloneqq \{\varphi_a \mid a \in G\}$$

een normaaldeler van $\mathrm{Aut}(G)$ en $\mathrm{Inn}(G) \cong G/Z(G)$.

Automorfismen van normaaldelers Zij G een groep en $N \lhd G$. Dan is er een groepshomomorfisme $f\colon G \to N$ met $f(a) \coloneqq \varphi_a \mid N$. Als N abels is geldt bovendien dat de functie $g\colon G/N \to \mathrm{Aut}(N)$ met $g(aN) = f(a)$ een goed gedefiniëerd homomorfisme is.

Groepen en priemgetallen Deze stelling bestaat uit twee delen:

1. Zij p een priemgetal en G een groep met $\#G = p^2$. Dan geldt dat $G \cong \mathbb{Z}/p^2\mathbb{Z}$ of $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
2. Zij p, q priemgetallen met $p > q$ en $\mathrm{ggd}(p-1, q) = 1$. Dan is elke groep van de orde pq cyclisch, dus $G \cong \mathbb{Z}/pq\mathbb{Z}$.

7.2 Semidirecte producten

Definitie van het semidirecte product Zij H, N twee groepen en $\tau\colon H \to \mathrm{Aut}(N)$ een homomorfisme, dan vormt de verzameling $N \times H$ de bewerking

$$(n_1, h_1) \cdot (n_2, h_2) \coloneqq (n_1\tau(h_1)(n_2), h_1h_2))$$

deze groep wordt genoteerd als $N \rtimes_\tau H$. Als duidelijk is welk homomorfisme bedoeld wordt wordt dat vaak genoteerd als $N \rtimes H$.

Semidirecte en directe producten Zij N, H groepen en $\tau\colon H \to \mathrm{Aut}(N)$ het triviale homomorfisme. Dan is het directe product $N \times H$ dezelfde groep als $N \rtimes_\tau H$.

Semidirecte producten en surjectieve homorfismen Zij N, H groepen en $\tau\colon H \to \mathrm{Aut}(N)$ een homomorfisme. Dan is de deelverzameling $\{e_N\} \times H \subseteq N \rtimes_\tau H$ een ondergroep en $\{e_N\} \times H \cong H$. Ook geldt dat de functie $\pi\colon N \rtimes_\tau H \to H\colon (n, h) \mapsto h$ een surjectief homomorfisme is met de kern $N \rtimes_\tau \{e\} \cong N$.

Semidirecte producten van ondergroepen Zij G een groep met $N, H \subseteq G$ een ondergroepen zodat de volgende eigenschappen gelden:

1. $N \cap H = \{e\}$,
2. $G = NH$,
3. $N \lhd G$.

Dan geldt dat $G \cong N \rtimes_\tau H$ met $\tau\colon H \to \mathrm{Aut}(N)\colon h \mapsto \varphi_h$.

Karakteristieke ondergroepen Zij G een groep en $H \subseteq G$ een ondergroep. Dan geldt dat H karakteristiek is als voor alle $\psi \in \mathrm{Aut}(G)$ geldt dat $\psi(H) = H$.

Voorbeelden van karakteristieke ondergroepen Zij G een groep, dan geldt dat $Z(G)$ en $[G, G]$ karakteristieke ondergroepen zijn.

8 Groepen die misschien handig zijn

8.1 De groepen $\mathbb{Z}/n\mathbb{Z}$ en $(\mathbb{Z}/n\mathbb{Z})^*$

De groep $\mathbb{Z}^+ = \mathbb{Z}$ is abels, dus elke ondergroep is een normaaldeler. Elke ondergroep van $\mathbb{Z}$ is van de vorm $n\mathbb{Z}$. Dan kun je de factorgroep $\mathbb{Z}/n\mathbb{Z}$ construeren. De groep $\mathbb{Z}/n\mathbb{Z}$ heeft orde n.

Je vermenigvuldiging uitvoeren in de restklassen, dan geldt dat

$$(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n) \coloneqq \#\{m \mid \mathrm{ggd}(n, m) = 1\}.$$

Voor $\mathbb{Z}/n\mathbb{Z}$ geldt dat $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Alle conjugatieklassen hebben precies 1 element, en $Z(G) = G$ want G is abels.

8.2 Quaternionen

Optelling De verzameling van quaternionen $\mathbb{H}^+$ is als volgt gedefinieerd:

$$\mathbb{H}^+ \coloneqq \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

met de bewerking

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

Dit vormt een groep.

Vermenigvuldiging De quaternionen kunnen ook vermenigvuldigd worden. De groep $\mathbb{H}^*$ is de groep quaternionen met vermenigvuldiging en is als volgt gedefinieerd:

$$\mathbb{H}^* \coloneqq \mathbb{H}^+ \setminus \{0\},$$

de vermenigvuldiging gaat volgens de volgende regels:

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

Deze vermenigvuldiging vormt ook een groep. Deze vermenigvuldiging is niet commutatief.

8.3 Viergroep van Klein

De viergroep van Klein is een groep van orde 4 met $V_4 \coloneqq \{e, a, b, c\}$ die de volgende vermenigvuldiginstabel heeft:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	d	e	a
c	c	c	a	e.

Elk element van V_4, behalve de eenheid, heeft orde 2, want $x \cdot x = e$ voor alle $x \in V_4$.

Deze groep kan ook geschreven worden als ondergroep van S_4, namelijk als volgt:

$$V_4 = \{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Voor de automorfismegroep van V_4 geldt dat $\mathrm{Aut}(V_4) \cong S_3$, want de elementen a, b, c kunnen gepermuteerd worden.

8.4 Quaternionengroep

De ondergroep $Q \coloneqq \{1, -1, i, -i, j, -j, k, -k\} \subseteq \mathbb{H}^*$ is een niet abelse ondergroep van $\mathbb{H}^*$ van acht elementen.

8.5 Symmetriegroep

Zij X een verzameling. Dan is de groep $S(X) \coloneqq \{f\colon X \to X \mid f \text{ is een bijectie}\}$ een groep met als bewerking functiesamenstelling. De elementen van een $S(X)$ heten permutaties. We noteren $S_n \coloneqq S(\{1, \ldots, n\})$. Deze verzameling heeft $n!$ elementen.

De tekenfunctie Zij $\sigma \in S_n$, dan is de volgende functie een homomorfisme:

$$P\colon S_n \to \mathrm{GL}_n(n, \mathbb{R})$$

met $P(\sigma)_{ij} = \delta_{i,\sigma(j)}$.

Aangezien de determinant det ook een homomorfisme is met $\mathrm{GL}_n(n, \mathbb{R}) \to \mathbb{R}$, geldt dat $\varepsilon \coloneqq \det \circ P$ ook een homomorfisme is met als beeld $\{1, -1\}$. We noemen $\varepsilon(\sigma)$ het teken van $\sigma \in S_n$. De kern $A_n \coloneqq \ker(\varepsilon)$ is een normaaldeler van grootte $\frac{n!}{2}$.

Commutatorondergroepen Zij $n \in \mathbb{N}$, dan geldt voor S_n dat

$$[S_n, S_n] = A_n,$$

en dat

$$[A_n, A_n] = \begin{cases} \{(1)\} & n \in \{1, 2, 3\} \\ V_4 & n = 4 \\ A_n & n \geq 5 \end{cases}$$

8.6 Diëdergroep

Beschouw een regelmatige n-hoek. Dan is D_n gedefinieerd als de congruenties die de n-hoek in zichzelf overvoeren met de bewerking van samenstelling. De groep D_n heeft orde $2n$.

De groep D_n bestaat uit rotaties en spiegelingen:

$$D_n \coloneqq \left\{\rho_0, \rho_{\frac{\pi}{n}}, \ldots, \rho_{\frac{2n-2}{n}\pi}\right\} \cup \left\{\sigma_0, \ldots, \sigma_{\frac{n-1}{n}\pi}\right\}.$$

Voor het gemak wordt geschreven $\rho \coloneqq \rho_0$ en $\sigma \coloneqq \sigma_0$. Dan is $\rho_{\frac{k}{n}\pi} = \rho^k$ en $\sigma_{\frac{k}{n}\pi} = \rho^k\sigma$.

Dus $D_n = \{\rho^k \mid k \in \mathbb{N}\} \cup \{\rho^k\sigma \mid k \in \mathbb{N}\}$. Ook gelden de volgende rekenregels:

$$\begin{aligned} \rho^n &= \rho, \\ \sigma^2 &= \mathrm{Id}_X, \\ \sigma\rho^k &= \rho^{n-k}\sigma. \end{aligned}$$

Diëdergroep D_n met even n Het centrum $Z(D_n)$ heeft twee elementen $Z(D_n) = \left\{e, \rho^{\frac{n}{2}}\right\}$ en de commutatorgroep is $\left\langle \rho^2 \right\rangle$. De conjugatieklassen zijn als volgt:

- $\{e\}$,
- $\left\{\rho^{\frac{n}{2}}\right\}$,
- $\frac{n}{2} - 1$ klassen van de vorm $\left\{\rho^i, \rho^{-i}\right\}$,
- $\left\{\rho^1\sigma, \rho^3\sigma, \ldots, \rho^{n-1}\sigma\right\}$,
- $\left\{\sigma, \rho^2\sigma, \ldots, \rho^{n-2}\sigma\right\}$.

Diëdergroep D_n met oneven n Deze groep heeft als centrum $Z(D_n) = \{e\}$, en de commutatorgroep is $[G, G] = \langle \rho \rangle$. Het heeft de volgende conjugatieklassen:

- $\{e\}$,
- $\frac{n-1}{2}$ klassen van de vorm $\left\{\rho^i, \rho^{-i}\right\}$,
- $\left\{\sigma, \rho^1\sigma, \ldots, \rho^{n-1}\sigma\right\}$.

8.7 Een tabel van alle groepen met orde < 16

De groepen die hier staan zijn alle groepen op isomorfisme met $\#G < 16$.

Orde	Abels	Niet abels
1	C_1	-
2	C_2	-
3	C_3	-
4	C_4, V_4	-
5	C_5	-
6	C_6	S_3
7	C_7	-
8	$C_8, C_4 \times C_2, (C_2)^3$	Q, D_4
9	$C_9, C_3 \times C_3$	
10	C_{10}	D_5
11	C_{11}	-
12	$C_{12}, C_2 \times C_6$	D_6, A_4, B
13	C_{13}	-
14	C_{14},	D_7
15	C_{15}	