Samenvatting Algebra 1

Jonas van der Schaaf

10 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: $G_1 \times G_2 \cong G_2 \times G_2$,
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 $\gcd(n_i, n_j) = 1$. 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

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

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

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

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

$$\operatorname{orde}(G) \coloneqq \#G.$$

Stelling van Euler Zij $a \in \mathbb{Z}$ en $m \in \mathbb{N}$ met $\gcd(a, m) = 1$. 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

$$aH \coloneqq \{ah \mid h \in H\}$$

een linkernevenklasse van H en

$$Ha \coloneqq \{ha \mid h \in H\}$$

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

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

Hieruit volgt dat $\text{orde}(H) \mid \text{orde}(G)$ 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 $\text{orde}(x) \mid \text{orde}(G)$.

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

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

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

4 Groepen die misschien handig zijn

Quaternionen

Viergroep van Klein

Quaternionengroep (niet de quaternionen)

Symmetriegroep

Diëdergroep