

Samenvatting Algebra 1

Kyndylan Nienhuis

19 mei 2008

1 Gehele getallen

Ggd's De grootste gemene deler van a en b is gelijk aan het kleinste element van de verzameling $\{ax + by \mid x, y \in \mathbb{Z}\}$.

Het Euclidische algoritme Je kan dit gebruiken om ggd's uit te rekenen, de x, y in $\text{ggd}(a, b) = ax + by$ te vinden, en inverses te bepalen in $(\mathbb{Z}/n\mathbb{Z})^*$.

Priemfactorisatie $n = \prod_{p \in \mathcal{P}} p^{\text{ord}_p(n)}$.

2 Equivalentierelaties

Relaties, equivalentierelaties, partities, volledige representantensystemen.

3 Groepen

Voorwaarden Associativiteit, eenheidselement, en inverse. Voor abelse groepen ook commutativiteit.

Voorbeelden Viergroep van klein V_4 , en de quaterniongroep Q (niet abels). Ook soms handig: $\mathbb{Z}/n\mathbb{Z}$, en $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggd}(a, n) = 1\}$.

Daarnaast is er nog de algemene lineaire groep $\text{GL}_n(\mathbb{R})$ van reële 2×2 matrices, met determinant ongelijk aan nul.

Euler phi-functie De Euler phi-functie: $\varphi(n) = \#\{k \mid \text{ggd}(k, n) = 1\}$, met $k \in \{1, \dots, n\}$. De rekenregels zijn $\varphi(p^k) = p^k - p^{k-1}$ voor p priem, en $\varphi(ab) = \varphi(a)\varphi(b)$ voor $\text{ggd}(a, b) = 1$.

Orde De orde van een element is de kleinste n met $a^n = e$; en als n niet bestaat, dan is de orde oneindig. De orde van een element deelt de orde van de groep.

Als de orde van a oneindig is, dan zijn alle machten van a verschillend, anders zijn er precies orde(a) verschillende machten.

Linksvermenigvuldiging ($x \mapsto gx$) en rechtsvermenigvuldiging zijn bijecties.

4 Symmetriegroepen

Symmetrische groepen De verzameling $S(X)$ van bijecties $X \rightarrow X$ is een groep. Als X eindig is, dan noemen we $S(X)$ een permutatiegroep.

Als $X = \{1, \dots, n\}$ dan noteren we S_n voor $S(X)$. Deze groep heet de symmetrische groep op n symbolen.

Isometriën Een isometrie is een afstandsbehoudende bijectie. De orthogonale groep $O_2(\mathbb{R})$ bestaat uit de isometriën $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ die de oorsprong vastlaten.

Diëdergroep De diëdergroep is gedefinieerd als $D_n = \{t \in O_2(\mathbb{R}) \mid t(\Delta_n) = \Delta_n\}$. Als r een draaiing is over $2\pi/n$, en s een spiegeling, dan geldt $D_n = \{\text{id}, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$. Rekenregels zijn $rs = sr^{-1}$ en $s^2 = \text{id}$.

5 Ondergroepen en homomorfismen

Ondergroepen Een deelverzameling H van een groep G is een ondergroep als H een groep is met dezelfde bewerking, en hetzelfde eenheidselement.

Om aan te tonen dat H een ondergroep is, is het voldoende om aan te tonen dat $H \neq \emptyset$ en als $x, y \in H$ dan $xy^{-1} \in H$.

Voortgebrachte groepen Zij $S \subseteq G$. De verzameling $\langle S \rangle$ bestaat uit alle eindige producten van elementen x met $x \in S$ of $x^{-1} \in S$, en is een ondergroep van G . Het heet de ondergroep voortgebracht door S .

Je gebruikt dit wanneer je een ondergroep nodig hebt waar bepaalde elementen, zeg a, b, c , in zitten. In dit geval kan je dus $\langle \{a, b, c\} \rangle$ gebruiken.

Homomorfismen Een afbeelding $f : G \rightarrow G'$ is een homomorfisme als $f(xy) = f(x)f(y)$ voor alle $x, y \in G$. Er geldt $f(e_G) = e_{G'}$, en $f(x)^{-1} = f(x^{-1})$. De kern is een ondergroep van G , en het beeld een van G' . Om aan te tonen dat een homomorfisme injectief is, kun je aantonen dat $\ker(f) = \{e_G\}$.

Zij $\mathcal{O}(G)$ de verzameling ondergroepen van G . Een homomorfisme $f : G \rightarrow G'$ geeft aanleiding tot een afbeelding $\psi : \mathcal{O}(G) \rightarrow \mathcal{O}(G')$ met $H \mapsto f(H) = \{f(h) \mid h \in H\}$, en een afbeelding $\chi : \mathcal{O}(G') \rightarrow \mathcal{O}(G)$ met $H' \mapsto f^{-1}(H') = \{h \mid f(h) \in H'\}$. Als f bijectief is, dan zijn ψ, χ bijectief.

Isomorfïën Een isomorfisme is een bijectief homomorfisme. Twee groepen zijn isomorf als er een isomorfisme tussen bestaat (notatie: $G \cong G'$). Om aan te tonen dat twee groepen niet isomorf zijn, kan je kijken naar de ordes van elementen. Als in de ene groep er een ander aantal elementen met een bepaalde orde is dan in de andere groep, dan zijn de groepen niet isomorf.

Chinese reststelling Zij $m, n \in \mathbb{Z}$ met $\text{ggd}(m, n) = 1$, er geldt $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Een isomorfisme er tussen is bijvoorbeeld $x \bmod mn \mapsto (x \bmod n, x \bmod m)$.

Zij $a, b, m, n \in \mathbb{Z}$ gegeven, en $\text{ggd}(m, n) = 1$. Het stelsel vergelijkingen $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ heeft modulo mn één oplossing. Je vindt dit door met het Euclidisch algoritme de ζ, η in $1 = \zeta m + \eta n$ te bepalen. We zien dat $x = b\zeta m + a\eta n$ voldoet.

6 Permutatiegroepen

Cykels Iedere permutatie $\sigma \in S_n$ is te schrijven als een product van disjuncte cykels. Voor een cykel geldt $(a_1 a_2 a_3 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$, en we zien dat iedere permutatie het product van verwisselingen is. Anders gezegd: S_n wordt voortgebracht door 2-cykels.

Als een permutatie $\sigma \in S_n$ het product is van r disjuncte cykels van lengte l_1, \dots, l_r (met 1-cykels meegerekend), dan heet $\{l_1, \dots, l_r\}$ het cykeltype van σ . Er geldt $\sum_{i=1}^r l_i = n$, en $\text{kgv}(l_1, \dots, l_r) = \text{ord}(\sigma)$.

En een handige rekenregel: zij $\sigma = (a_1 \dots a_k)$, dan $\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_k))$.

Het teken De precieze definitie gaat als volgt. Zij $\pi \in S_n$, en $i, j \in \{1, \dots, n\}$. We noemen (i, j) een inversie als $i < j$ en $\pi(i) > \pi(j)$; laat $I(\pi)$ het aantal inversies zijn. Het tekenhomomorfisme $\varepsilon : S_n \rightarrow \{\pm 1\}$ is nu gedefinieerd als $\varepsilon(\pi) = (-1)^{I(\pi)}$.

Anders gezegd, een permutatie σ is even ($\varepsilon(\sigma) = 1$) als σ uit een even aantal verwisselingen bestaat, en anders oneven ($\varepsilon(\sigma) = -1$). Bijvoorbeeld $\varepsilon((1\ 2)) = -1$, $\varepsilon((2\ 7\ 3)(9\ 1)(5\ 4)) = \varepsilon((2\ 7)(7\ 3)(9\ 1)(5\ 4)) = 1$.

De alternerende groep De verzameling even permutaties $A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$ heet de alternerende groep. Er geldt $\#A_n = n!/2$. De alternerende groep wordt voortgebracht door 3-cykels.

Stelling van Cayley Iedere eindige groep is isomorf met een ondergroep van S_n .

Ruimtelijke figuren Om een isomorfisme aan te tonen tussen de symmetriegroep G van een of ander figuur, en S_n voor een bepaalde n , is het soms handig om te kijken wat er met een bepaald onderdeel van het figuur gebeurt. Zo worden de hoekpunten, lichaamsdiagonalen, orthogonale lijnstukken en overstaande ribben misschien wel op zo'n manier gepermuteerd dat je een link met S_n kan leggen.

7 Nevenklassen en index

Nevenklassen Zij H een ondergroep van G . Een linkernevenklasse van H is van de vorm $gH = \{gh \mid h \in H\}$, en een rechternevenklasse $Hg = \{hg \mid h \in H\}$. De nevenklassen van H , G/H , partitioneren G , en zijn allemaal even groot.

Voor een homomorfisme f met $\ker f = H$ geldt $f^{-1}(f(g)) = gH = Hg$ (de vezels van f zijn nevenklassen).

Lagrange De index van H in G , genoteerd als $[G : H]$, is gelijk aan het aantal nevenklassen van H . (Als dat oneindig is, dan is het de kardinaliteit.) De stelling van Lagrange zegt dat, zij G een eindige groep en H een ondergroep van G , dan $\#G = [G : H]\#H$.

Een leuk gevolg: laat $f : G \rightarrow G'$ een homomorfisme van eindige groepen zijn. Er geldt $\#G = \#\ker f \cdot \#f(G)$. Hieruit volg nu $\#f(G) \mid \#G$, en we wisten al $\#f(G) \mid \#G'$.

8 Werkingen van groepen

Werkingen Laat G een groep zijn, en X een verzameling. We zeggen dat G werkt op X als er een afbeelding $G \times X \rightarrow X$, $(g, x) \mapsto g \circ x$ gegeven is, die voldoet aan $e \circ x = x$, en $(gh) \circ x = g \circ (h \circ x)$.

Een alternatieve definitie is: een werking van een groep G op een verzameling X is een homomorfisme $\mu : G \rightarrow S(X)$.

Banen en stabilisators Zij $x \in X$. de baan van x is $Gx = \{g \circ x \mid g \in G\}$. De banen partitioneren X . Als er precies één baan is, dan noemen we de werking transitief. De stabilisator van x is de ondergroep $G_x = \{g \in G \mid g \circ x = x\}$. Er geldt $G_{gx} = gG_xg^{-1}$.

Er is een bijectie $G/G_x \leftrightarrow Gx$, en er geldt $\#G = \#Gx \cdot \#G_x$.

Dekpunten Een punt $x \in X$ heet een dekpunt als $Gx = \{x\}$. De verzameling dekpunten wordt genoteerd met X^G . Voor een groep G waarvan de orde een macht van p is, met p priem, geldt $\#X^G \equiv \#X \pmod{p}$.

Je kunt dit soms gebruiken als je op zoek bent naar een element met een bepaalde eigenschap. Je hebt dan een groep G nodig, waarvan de orde een macht van een priemgetal is. Het meest voor de hand liggende is dan $\mathbb{Z}/p\mathbb{Z}$ met p priem. Dan kies je je X , en een werking van G op X . Dit doe je zodanig dat als je een dekpunt hebt, je een element kan vinden met de eigenschap die je zoekt. Nu kun je de stelling gebruiken ($\#X^G \equiv \#X$ dus) om aan te tonen dat er dekpunten zijn, en dat er dus elementen zijn met de gevraagde eigenschap. Zie ook het bewijs van de stelling van Cauchy (blz. 58).

Stelling van Cauchy Zij G een eindige groep, en p een priemgetal dat de orde van G deelt. Er geldt $\#\{g \in G \mid \text{ord}(g) = p\} \equiv -1 \pmod{p}$.

Iets vergelijkbaars geldt voor ondergroepen: $\#\{H \text{ een ondergroep} \mid \#H = p\} \equiv 1 \pmod{p}$.

Burnside Laat X een eindige verzameling zijn, met een werking van een eindige groep G . Er geldt:

$$\text{het aantal banen} = \frac{1}{\#G} \sum_{g \in G} \#\{x \in X \mid g \circ x = x\}.$$

Dit kan je heel goed gebruiken bij sommen in de trant van op hoeveel manieren kan je een voetbal met \mathfrak{k} verschillende kleuren verven. Het probleem hierbij is dat wanneer je denkt twee voetballen verschillend gekleurd te hebben, en iemand ze draait, er opeens kan blijken dat ze hetzelfde zijn.

De aanpak is als volgt. Je neemt een verzameling X van voetballen, die, zolang je ze niet draait, anders gekleurd zijn (dat zijn er waarschijnlijk zo'n \mathfrak{k}^{32}). Vervolgens laat je de symmetriegroep G van een voetbal daar op werken. Met de formule van Burnside kan je berekenen hoeveel banen er zijn. En dan ben je klaar, want een baan bestaat uit voetballen die na een draaiing toch hetzelfde gekleurd blijken te zijn. Zie ook aanvullende opgave 11.

9 Normaaldivisors en quotiëntgroepen

Normaaldivisors Om van een verzameling N aan te tonen dat het een normaaldivisor is van G (notatie $N \triangleleft G$) kan je de volgende dingen doen.

- Je toont aan dat N een ondergroep is, en dat voor iedere $g \in G$ en $n \in N$ geldt dat $gng^{-1} \in N$. (Of, wat er erg op lijkt: $gN = Ng$.)
- Een andere manier is dat je laat zien dat N de kern is van een homomorfisme.
- Als G eindig is, kan je ook laten zien dat N een ondergroep van index p is, met p het kleinste priemgetal dat de orde van G deelt.
- Of je toont aan dat N een ondergroep van index 2 is. (Dit lijkt op de vorige, maar G hoeft nu niet eindig te zijn.)

Quotiëntgroepen Zij $N \triangleleft G$. De verzameling G/N is een groep met de bewerking $g_1N \circ g_2N = g_1g_2N$. Deze groep heet de quotiëntgroep, en ook G modulo N . De orde is $[G : N]$.

Kanonieke afbeelding De afbeelding $\varphi : G \rightarrow G/N$, $g \mapsto gN$ heet de kanonieke afbeelding en is een surjectief homomorfisme met als kern N .

Voor H een ondergroep van G geldt er dat $\varphi(H)$ een ondergroep is van G/N , en voor H' een ondergroep van G/N is $\varphi^{-1}(H')$ een ondergroep van G . Er geldt $\varphi(\varphi^{-1}(H')) = H'$ en $\varphi^{-1}(\varphi(H)) = HN = \{hn \mid h \in H, n \in N\}$.

We zie nu dat er een bijjectie is tussen de ondergroepen van G/N en de ondergroepen van G die N omvatten (voor die H geldt namelijk $HN = H$).

Centrum Het centrum van G is de normaaldivisor $Z(G) = \{h \in G \mid gh = hg \text{ voor alle } g \in G\}$. Als $G/Z(G)$ cyclisch is, dan is G abels.

Commutatorondergroep De commutatorondergroep $[G, G]$ van G is de ondergroep van G voortgebracht door de commutatoren $[g_1, g_2] = g_1g_2g_1^{-1}g_2^{-1}$ met $g_1, g_2 \in G$. De commutatorondergroep is een normaaldivisor.

Zij $N \triangleleft G$, dan is G/N abels dan en slechts dan als $[G, G] \subseteq N$. De 'minimale' manier om een abels quotiënt te krijgen is door G uit te delen naar zijn commutatorondergroep. We noemen $G/[G, G]$ de abels gemaakte G , en noteren G_{ab} .

Conjugatie Een groep G werkt op zichzelf door via $g \circ x = gxg^{-1}$. Deze werking heet conjugatie. De stabilisatorgroep heet hier centralisator, genoteerd C_x , en bestaat uit alle elementen van G die met x commuteren: $C_x = \{g \in G \mid gx = xg\}$.

Een conjugatie is ook te zien als een automorfisme: $\lambda_g : G \rightarrow G$ met $x \mapsto gxg^{-1}$. Zij $Aut(G)$ de groep van automorfismen van G . We hebben nu een homomorfisme $\mu : G \rightarrow Aut(G)$ met $g \mapsto \lambda_g$.

Als we dit toepassen op een normaaldivisor N van G krijgen we iets interessants. We kunnen namelijk de g waarmee we conjugeren buiten de normaaldivisor kiezen, omdat $gxg^{-1} \in N$ voor $x \in N$. Er geldt dus dat λ_g ook een automorfisme van N is, en we hebben nu een homomorfisme $\mu : G \rightarrow Aut(N)$ met $g \mapsto \lambda_g$.

10 Isomorfiestellingen

Homomorfiestelling Zij $f : G \rightarrow G'$ een homomorfisme, en N een normaaldeler van G met $N \subseteq \ker f$. Er is een eenduidig bepaald homomorfisme $h : G/N \rightarrow G'$ zodat $h(gN) = f(g)$ voor alle $g \in G$ (anders gezegd: $h \circ \varphi = f$ met $\varphi : G \rightarrow G/N$ het kanonieke homomorfisme).

Als G' abels is, dan weten we dat $[G, G] \subseteq \ker f$ (want $G/\ker f$ is abels). We passen het vorige toe, en we zien dat er een eenduidig bepaald homomorfisme $h : G_{ab} = G/[G, G] \rightarrow G'$ is, met $h \circ \varphi = f$.

Vind de homomorfismen Als je alle homomorfismen van G naar G' moet vinden, kan je het vorige goed gebruiken. Als G' abels is, dan hoef je alleen te zoeken naar homomorfismen van G_{ab} naar G' . En als van een normaaldeler N hebt aangetoond dat het bevat is in de kern van elk homomorfisme $G \rightarrow G'$, dan hoef je alleen te zoeken naar de homomorfismen $G/N \rightarrow G'$.

Tweede isomorfiestelling Zij N een normaaldeler van G , en H een ondergroep van G . Dan geldt er $H/(H \cap N) \cong HN/N$, waarbij $HN = \{hn \mid h \in H, n \in N\}$.

Dit is te bewijzen door de kanonieke afbeelding φ te beperken tot H , en de eerste isomorfiestelling toe te passen.

Eerste isomorfiestelling Zij $f : G \rightarrow G'$ een homomorfisme van groepen. Er geldt $G/\ker f \cong f(G)$.