Hoofdstuk 5

Cyclische groepen

5.1 Definitie

Definitie 5.1. Cyclische groepen zijn groepen voortgebracht door 1 element.

Als G wordt voortgebracht door a en $a^n = e$, dan noteren we de groep als $C_n = \langle a \rangle$. Elk element van G is dan van de vorm a^k met $1 \leq k \leq n$.
Voor elke natuurlijk getal n bestaat er juist 1 cyclische groep van orde n.

Stelling 5.2. *Cyclische groepen zijn altijd abels.*

Bewijs. Als $C_n = \langle a \rangle$ en $g, h \in C_n$ dan is $gh = a^k.a^l = a^{k+l} = a^l.a^k = hg$. Bijgevolg is C_n abels. □

Het rekenen met elementen uit C_n komt neer op het optellen van de exponenten, vandaar:

Stelling 5.3. *De eindige cyclische groepen van orde n zijn isomorf met de verzameling restklassen modulo n met de optelling als bewerking:*

$$C_n, \cdot \cong \mathbb{Z}_n, +$$

Bewijs. Definieer $\varphi : \mathbb{Z}_n \to C_n : k \mapsto a^k$. Dit is een homomorfisme want $\varphi(k + l) = a^{k+l} = a^k.a^l = \varphi(k).\varphi(l)$. Bovendien is φ zeker surjectief en ook

injectief want $\varphi(k) = \varphi(l) \Rightarrow a^k = a^l \Rightarrow n|k-l \Rightarrow k-l = 0 \Rightarrow k = l$. Bijgevolg is φ een isomorfisme en volgt het gestelde. □

Een andere mogelijke realisatie voor C_n is de verzameling van alle complexe n-de machtswortels uit 1. Deze vormen is het complexe vlak een regelmatige n-hoek. C_n is ook te realiseren als de groep van alle rotaties van een regelmatige n-hoek.

5.2 De structuur van cyclische groepen

Bestuderen we nu de structuur van C_n: we zoeken informatie over de orde van de elementen , de toevoegingsklassen en de deelgroepen. Omdat elke cyclische groep abels is bestaan de toevoegingsklassen allemaal uit 1 element. Wat betreft de orde van de elementen, kunnen we gebruik maken van een resultaat uit hoofdstuk 1:

$$o(a^k) = \frac{n}{ggd(k,n)}$$

Rest ons nog een onderzoek naar de mogelijke deelgroepen van C_n.

Stelling 5.4. *Elke deelgroep H van een cyclische groep is cyclisch.*

Bewijs. Stel $G = \{a : a^n = e\}$ en noteer met m het kleinste positieve getal waarvoor $a^m \in H$. Omdat H een deelgroep is $\langle a^m \rangle \subseteq H$. Neem nu $a^k \in H$ met $0 \leq k < n$. Dan geldt $k = m.q + r$, en dus is $a^k = (a^m)^q.a^r$. Bijgevolg is $a^r = a^k.(a^m)^{-q} \in H$. Maar $r < m$, wat tegen het gegeven is. Dus moet $r = 0$ en is $a^k \in \langle a^m \rangle$. Bijgevolg is $H \subseteq \langle a^m \rangle$ en daaruit volgt dat $H = \langle a^m \rangle$. Dus is H cyclisch. □

Gevolg 5.5. *Elke deelgroep is normaal. Dus C_n is enkelvoudig als het geen echte deelgroep heeft. Een cyclische groep C_n is dus enkelvoudig als en slechts als n priem is. De eerste reeks basisstenen om groepen te bouwen zijn dus de cyclische groepen van priemorde C_p.*

Gevolg 5.6. *De enige groep met p elementen, met p priem, is de cyclische groep C_p.*

Maar welke deelgroepen kunnen we dan krijgen? Bij cyclische groepen C_n is de orde van een deelgroep natuurlijk een deler van n. Bovendien geldt hier ook het omgekeerde:

Stelling 5.7. *Voor elke deler d van n bestaat er juist 1 deelgroep van orde d van C_n.*

Bewijs. Zij d een deler van n. Neem het element $a = g^{n/d}$, waarbij g een generator is van C_n. De orde van a is d, want $a^d = g^n = e$. Dus is de orde van de deelgroep voortgebracht door a gelijk aan d. Er is dus minstens 1 deelgroep van orde d. Bewijzen we nu nog dat er niet meer dan 1 kan zijn. Stel H een andere deelgroep van orde d, dan is deze zeker cyclisch en wordt dus voortgebracht door een element g^k, waarvoor geldt dat $g^{kd} = e$. Dus moet n een deler zijn van kd en bestaat er een v zodat $nv = kd \Rightarrow k = v.\frac{n}{d}$. Dan is H een deel van de groep voortgebracht door $g^{n/d}$ en omdat deze twee groepen allebei orde d hebben zijn ze gelijk. Er is dus juist 1 deelgroep van orde d. □

Gevolg 5.8. *In een eindige cyclische groep genereren 2 elementen dezelfde deelgroep als en slechts als ze dezelfde orde hebben.*

Stelling 5.9. *Als H en H' twee deelgroepen zijn van C_n dan is H een deelgroep van H' als en slechts als de orde van H een deler van de orde van H'.*

Bewijs. Als $H < H'$, dan is de orde van H een deler van de orde van H'. Omgekeerd als de orde van H een deler is van de orde van H', dan is er in H' een deelgroep waarvan de orde gelijk is aan de orde van H. Maar er is maar 1 deelgroep van deze orde in C_n. Dus dat moet H zijn en dus is H een deelgroep van H'. □

Stelling 5.10. *Voor elke deler d van n zijn er $\varphi(d)$ elementen van orde d in C_n.*

Bewijs. Er is slechts 1 deelgroep van orde d in C_n. Stel dat die wordt voortgebracht door a. Elk element van orde d genereert dezelfde deelgroep. Nu weten we dat a^k een generator is als k en d onderling ondeelbaar zijn. Bijgevolg zijn er $\varphi(d)$ elementen van orde d in C_n. □

Alle deelgroepen van C_n worden dus gevonden door alle delers te berekenen van n. De tralie van deze deelgroepen komt overeen met de tralie van alle delers van n met de relatie: is een deler van.

5.3 De automorfismegroep van C_n

Stelling 5.11. *$Aut(C_n) \cong \mathbb{Z}_n^\times, .$*

Bewijs. In de groep $\mathbb{Z}_n, +$ kan je elk element dat onderling ondeelbaar is met n als generator gebruiken. Een automorfisme van $\mathbb{Z}_n$ beeldt een generator af op een generator, dus

$$Aut(C_n) = Aut(\mathbb{Z}_n, +) \cong \mathbb{Z}_n^\times, .$$

□

Gevolg 5.12. *Als p priem is, dan heeft C_p juist $p-1$ automorfismen. Als p en q verschillende priemen zijn dan zijn er in C_{pq} juist $(p-1)(q-1)$ automorfismen. In C_{p^2} zijn er $p(p-1)$ automorfismen.*

Om de automorfisme groepen van de cyclische groepen te bestuderen moeten we dus de groepen $\mathbb{Z}_n^\times, .$ bestuderen. De orde van deze groepen is het aantal getallen dat onderling ondeelbaar is met n. Dit aantal wordt gegeven door de functie van Euler : $\varphi(n)$. Als p priem is dan is $\varphi(p) = p-1$ en $\varphi(p^k) = p^k - p^{k-1}$. Verder geldt dat de Euler functie multiplicatief is: $\varphi(r.s) = \varphi(r).\varphi(s)$

De groepen $\mathbb{Z}_n^\times, .$ zijn niet altijd cyclisch en als ze cyclisch zijn is het niet altijd eenvoudig om een generator te vinden. Er bestaat daar zelfs geen methode voor. Proberen maar! $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is niet cyclisch want er zijn meerdere deelgroepen van orde 2: $\{1, 4\}$, $\{1, 14\}$, $\{1, 11\}$. Daarom kan $\mathbb{Z}_{15}^\times$ nooit isomorf zijn met C_8 omdat er dan voor elke deler d van 8 slechts juist 1 deelgroep van orde d mag zijn.

Stelling 5.13. *$\mathbb{Z}_n^\times, .$ is cyclisch als en slechts als $n = 1, 2, 4$ of $n = p^k$ of $n = 2p^k$ met p een oneven priem en $k \geq 1$.*

Bewijs. We zullen aantonen dat er voor n verschillend van de waarden in de stelling, er twee deelgroepen kunnen worden gevonden van orde 2. Bijgevolg kan de groep niet cyclisch zijn. Een eerste deelgroep van $\mathbb{Z}_n^\times, .$ is $\{1, -1\}$.

1. Stel dat $n = 2^s$ met $s > 2$, dan is $1 + 2^{s-1} \neq \pm 2^s$. Dus is $(1 + 2^{s-1})^2 = 1$ mod 2^n en is $\{1, 1 + 2^{s-1}\}$ een deelgroep van orde 2.
   Voor groepen C_n met n een macht van 2 met exponent groter dan 2, is de automorfismegroep dus niet cyclisch.

2. Stel dat n geen priemmacht is en ook niet tweemaal een priemmacht. Dan is $n = a.b$ met a en b onderling ondeelbaar zodat er een x en een y bestaat waarvoor $ax + by = 1$. Construeer dan $t = ax - by = ax - (1 - ax) = 2ax - 1$. Dit element t heeft bij deling door a als rest -1 en bij deling door b als rest $+1$, zodat a en b delers zijn van $t^2 - 1$. Omdat a en b onderling ondeelbaar zijn is ook n een deler van $t^2 - 1$. Nu kan t nooit gelijk zijn aan 1 mod n anders zou ook a gelijk zijn aan 1 mod n. Maar t kan ook niet gelijk zijn aan -1 mod n, dus is $\{1, t\}$ een deelgroep van orde 2.
Voor groepen C_n met n geen macht van een oneven priemgetal of tweemaal de macht van een oneven priemgetal, is de automorfismegroep dus niet cyclisch.

□

5.4 Enkele stellingen

Stelling 5.14. *Het direct product van 2 cyclische groepen van orde n en m is cyclisch als n en m onderling ondeelbaar zijn.*

$$ggd(n, m) = 1 \Rightarrow C_n \times C_m = C_{nm}$$

Bewijs. Stel $G = \langle x \rangle$ met $x^n = e_G$ en $H = \langle y \rangle$ met $x^m = e_H$ en $ggd(n, m) = 1$. Neem nu het element $(x, y) \in G \times H$ en veronderstel dat de orde van dit element gelijk is aan k. Dan is $(x, y)^k = (x^k, y^k) = (e_G, e_H) \Rightarrow n|k$ en $m|k$. Omdat nu n en m onderling ondeelbaar zijn zal ook nm een deler zijn van k. Maar $(x, y)^{nm} = (e_G, e_H) \Rightarrow k|nm$ Bijgevolg is $k = nm$ en is $G \times H = \langle (x, y) \rangle$. □

Gevolg 5.15. *Als $n_1, n_2, \cdots, n_s$ natuurlijke getallen zijn groter dan 1 en paarsgewijs onderling ondeelbaar en als C_i een cyclische groep is van orde n_i, dan is $C_1 \times C_2 \times \cdots \times C_s$ cyclisch van orde $n_1.n_2.\cdots.n_s$.*

Stelling 5.16. *G is een groep van orde pq met p en q priem. Veronderstel dat $p < q$ en p geen deler is van $q - 1$. Dan is G cyclisch.*

Bewijs. Volgens de stelling van Cauchy bestaan er in G elementen g en h van orde p en q. Deze 2 elementen brengen G voort. Als nu G abels is dan heeft gh orde pq en is G cyclisch. Veronderstel dat G niet abels is , dan gaan we bewijzen dat g en h toch commuteren. Nu is $N = \langle h \rangle \cong \mathbb{Z}_q$, zodat $Aut(N) \cong \mathbb{Z}_q^\times$ en volgens stelling 4.11 is deze groep cyclisch van orde $q - 1$. Beschouw dan het homomorfisme $\varphi : G \to Aut(N) : g \mapsto \varphi_g : N \to N : h \mapsto ghg^{-1}$. De orde van φ_g is een deler van de orde van g en die is gelijk aan p. De orde van φ_g is ook een deler van $q - 1$. Omdat p geen deler is van $q - 1$ moet $\varphi_g = e$ en bijgevolg zullen g en h commuteren. Maar dan is de orde van gh gelijk aan pq en is G cyclisch van orde pq. □

Gevolg 5.17. *G is een groep van orde pq met p en q priem. Veronderstel dat $p < q$ en p geen deler is van $q - 1$. Dan is $G = C_{pq} = C_p \times C_q$.*

Gevolg 5.18. *Er is maar 1 groep van orde pq met p en q priem , $p < q$ en p geen deler van $q - 1$.*