Hoofdstuk 8

Werking van een groep

8.1 Permutatiegroepen

Een permutatie van een verzameling X is een bijectie van die verzameling op zichzelf. Een verzameling X met n elementen heeft juist $n!$ permutaties. De verzameling van alle permutaties van een verzameling is een groep voor de samenstelling.

Definitie 8.1. De groep van alle permutaties van een gegeven verzameling X is de symmetriegroep op n elementen, genoteerd als $Sym(X)$.

Definitie 8.2. Een permutatiegroep is een deelgroep van een symmetriegroep.

Als $X = \{1, 2, 3, \cdots, n\}$, dan noteren we de symmetriegroep door S_n. Stel dat de elementen van X gegeven zijn door $1, 2, 3, 4$, dan kunnen we een permutatie σ met $\sigma(1) = 1, \sigma(2) = 4, \sigma(3) = 2$ en $\sigma(4) = 3$ weergeven als volgt:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

We kunnen ook de cykelnotatie of Cayley notatie gebruiken : $(2, 4, 3)$. Hiermee geven we aan dat 2 wordt afgebeeld op 4 en 4 wordt dan weer afgebeeld op 3. Het beeld van 3 is 2. Dit noemen we een cykel van lengte 3.

Het element 1 wordt niet vernoemd en dat betekent dat 1 op zichzelf wordt afgebeeld.
De Cayley notatie van een permutatie is niet uniek bepaald. Vorige permutatie kan ook geschrven worden als $(4, 3, 2)$. Twee Cayley notaties bepalen dezelfde permutatie op de volgorde van de verschillende cykels na en op de cyclische volgorde van de termen binnen de cykels na. Zo is $(1, 8, 2)(3, 6, 5)(4, 7) = (7, 4)(3, 6, 5)(2, 1, 8)$.

Definitie 8.3. Een cykel van lengte 2 noemt men een transpositie of omwisseling.

We geven nu een aantal eigenschappen van de elementen van S_n:

Stelling 8.4. *Disjuncte cykels commuteren.*

Bewijs. Gegeven zijn twee cykels: $\sigma = (a_1, a_2, \cdots, a_m)$ en $\tau = (b_1, b_2, \cdots, b_n)$ waarbij $\{a_1, \cdots, a_m\} \cap \{b_1, \cdots, b_n\} = \emptyset$. Dan is $(\sigma.\tau)(a_i) = \sigma(a_i) = (\tau.\sigma)(a_i)$. Ook is $(\tau.\sigma)(b_j) = \tau(b_j) = (\sigma.\tau)(b_j)$. Voor elk ander element x is $(\sigma.\tau)(x) = x = (\tau.\sigma)(x)$. □

Stelling 8.5. *Elke permutatie is een product van disjuncte cykels.*

Bewijs. We bewijzen dit door inductie op n. Als $n = 1$, is de enige permutatie de identieke afbeelding en deze kunnen we schrijven als (1), een cykel van lengte 1. Veronderstel dat de eigenschap klopt voor elke k met $k < n$ en neem $\sigma \in S_n$ met orde m. Construeer $Q = \{1, \sigma(1), \sigma^2(1), \cdots, \sigma^{m-1}(1)\}$. Als $Q = X$, dan is σ een cykel:$(1, \sigma(1), \sigma^2(1), \cdots, \sigma^{m-1}(1))$. Als $Q \neq X$, dan heeft $X \setminus Q$ minder elementen dan n en kunnen we de inductiestap toepassen. σ beperkt tot $X \setminus Q$ is dus te schrijven als een product van disjuncte cykels: $\tau_1.\tau_2.\cdots.\tau_k$. Bijgevolg is $\sigma = (1, \sigma(1), \sigma^2(1), \cdots, \sigma^{m-1}(1)).\tau_1.\tau_2.\cdots.\tau_k$. Hieruit volgt het gestelde. □

De orde van een cykel is gelijk aan het aantal elementen waaruit hij bestaat. Een transpositie heeft dus orde 2. Er zijn echter ook permutaties van orde 2 die geen transposities zijn, bijvoorbeeld $(1, 2).(3, 4)$. De orde van een permutatie is dan het kleinste gemene veelvoud van de ordes van de cykels waaruit die permutatie bestaat.

Stelling 8.6. *Elke permutatie is te schrijven als product van een eindig aantal transposities.*

Bewijs. Het volstaat te bewijzen dat een cykel te schrijven is als een product van transposities. Neem $\sigma = (1, 2, \cdots, k)$. We kunnen dit ook schrijven als $\sigma = (1, k).(1, k-1).\cdots.(1, 3).(1, 2)$. Hieruit volgt het gestelde. □

Stelling 8.7. *Een permutatie kan nooit geschreven worden als het product van zowel een even aantal transposities als het product van een oneven aantal transposities.*

Bewijs. Veronderstel dat $\sigma = \sigma_1.\sigma_2.\cdots.\sigma_m = \tau_1.\tau_2.\cdots.\tau_n$ met m even en n oneven. Omdat $\tau_i^{-1} = \tau_i$ volgt hieruit dat $\tau_n.\cdots.\tau_1.\sigma_1.\cdots.\sigma_m = I$, met I de identieke permutatie. Dan zou de identieke permutatie het product zijn van een oneven aantal permutaties, wat onmogelijk is. Neem bijvoorbeeld de functie $f(x) = \prod_{i<j}(x_i - x_j)$. Elke transpositie verandert het teken van f. Als de identieke permutatie uit een oneven aantal transposities zou bestaan, dan zou het teken veranderen wat natuurlijk niet zo is. □

Als het aantal transposities waaruit een permutatie bestaat even is dan noemen we dit een *even permutatie*. Anders spreken we van een *oneven permutatie*. We noemen dit de pariteit van de permutatie en we noteren die als $sgn(\sigma)$. Vorige stelling verklaart dat deze pariteit goed gedefinieerd is. We kunnen hier ook een getal aan hechten: $+1$ voor een even permutatie en -1 voor een oneven permutatie. Als σ bestaat uit r transposities dan geldt:

$$sgn(\sigma) = (-1)^r$$

Gevolg 8.8. *De pariteit van een k-cykel is $(-1)^{k-1}$. Dus, een cykel is even als zijn lengte (of orde) oneven is.*

Gevolg 8.9. *Een transpositie is een oneven permutatie.*

Gevolg 8.10. *De samenstelling van twee even of twee oneven permutaties is een even permutatie. De samenstelling van een even en een oneven permutatie is een oneven permutatie.*

Gevolg 8.11. *Het inverse van een even permutatie is even en het inverse van een oneven permutatie is oneven.*

Gevolg 8.12. *Een permutatie en een toegevoegde permutatie hebben dezelfde pariteit.*

Stelling 8.13. *De pariteit van een permutatie is een multiplicatieve functie:*

$$sgn(\sigma.\tau) = sgn(\sigma).sgn(\tau)$$

Bewijs. Als σ het product is van k transposities en τ het product van k' transposities, dan is $\sigma.\tau$ het product van $k + k'$ transposities en dus is $sgn(\sigma.\tau) = (-1)^{k+k'} = (-1)^k.(-1)^{k'} = sgn(k).sgn(k')$. □

Gevolg 8.14. *De functie $sgn : S_n \to \{1, -1\} : \sigma \mapsto sgn(\sigma)$ is een groepshomomorfisme en de kern van dit homomorfisme is de verzameling van alle even permutaties. Deze vormt dus een normaaldeler van S_n. Als $n \geq 3$ dan is de index van deze groep in S_n gelijk aan 2.*

Definitie 8.15. De groep van alle even permutaties in S_n noemt men de alternerende groep A_n.

Gevolg 8.16. *Voor $n > 1$ zijn er evenveel even als oneven permutaties, dus de orde van A_n is gelijk aan $\frac{n!}{2}$.*

8.2 De stelling van Cayley

De symmetriegroep S_n is een van de eerste voorbeelden van een groep. Het is een zeer belangrijk voorbeeld, deels door de stelling van Cayley, die elke groep voorstelt als deelgroep van een symmetriegroep. Dit is belangrijk omdat symmetriegroepen vrij concreet zijn en er kan gemakkelijk in worden gerekend.

Stelling 8.17. *Elke groep G is isomorf met een deelgroep van de groep van de permutaties van G.*

Bewijs. Gegeven $g \in G$ en construeer $\lambda_g : G \to G : x \mapsto \lambda_g(x) = gx$. Deze linkervermenigvuldiging met g is een bijectie, dus λ_g is een permutatie van G. Bestudeer nu de afbeelding Λ die elk element g van G afbeeldt op λ_g. Deze afbeelding is goed gedefinieerd, want als $g_1 = g_2$, dan is $g_1x = g_2x$ voor elke x en dus is $\lambda_{g_1} = \lambda_{g_2}$. Ook is Λ een homomorfisme want $\lambda_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \lambda_{g_1}(\lambda_{g_2}(x)) = (\lambda_{g_1} \circ \lambda_{g_2})(x)$. Tenslotte bewijzen we ook nog dat Λ injectief is. Als $\Lambda(g_1) = \Lambda(g_2)$ dan geldt voor elke x dat $g_1x = g_2x$ en dus is $g_1 = g_2$. Bijgevolg is $G \cong \Lambda(G)$, wat moest bewezen worden. □

Elke groep is dus isomorf met een permutatiegroep. Als we de elementen van G schikken als $\{g_1, g_2, \cdots, g_n\}$, dan geeft de linkervermenigvuldiging met g_i de i-de rij weer in de Cayleytabel van G. Het is gewoon een herschikking van de elementen $\{g_1, g_2, \cdots, g_n\}$. Als we dan de elementen g_i vervangen door i, vinden we:

Gevolg 8.18. *Elke groep G is isomorf met een deelgroep van S_n.*

Laten we dit even in een voorbeeld uitwerken.
Bekijk de bewerkingstabel van de Viergroep:

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Dan is

$$\lambda_a = \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix}$$

en daarmee correspondeert

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4)$$

Zo vinden we dat

$$G \cong \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

G is dus isomorf met een deelgroep van S_4. Algemeen is het mogelijk dat G isomorf is met een deelgroep van S_k met $k < n$. De vraag stelt zich dan welk de kleinste r is zodat G isomorf is met een deelgroep van S_r.

8.3 Acties van groepen

We veralgemenen de procedure om met een element van een groep een permutatie te laten overeenkomen.

Definitie 8.19. Zij G een groep en X een verzameling. Een actie of werking van G op X is een groepshomomorfisme $\alpha : G \to S(X) : g \mapsto \alpha_g$. We zeggen dat G werkt op X door middel van α.

Definitie 8.20. Een linkse actie van een groep G op een verzameling X is een afbeelding $\lambda : G \times X \to X$ die voldoet aan:

(a) $\forall g, h \in G, \forall x \in X : \lambda(gh, x) = \lambda(g, \lambda(h, x))$

(b) $\forall x \in X : \lambda(e, x) = x$

Elke actie α bepaalt een linkse actie $\lambda = G \times X \to X : (g, x) \mapsto \alpha_g(x)$. En elke linkse actie λ bepaalt een actie $\alpha : G \to S(X) : g \mapsto (\alpha_g : X \to X : x \mapsto \lambda(g, x))$.

Definitie 8.21. Een actie α van een groep G op een verzameling X heet *getrouw* indien α injectief is.

Bij een getrouwe actie van een groep G op een verzameling X, is G dus isomorf met een permutatiegroep op X.

Definitie 8.22. Een actie α van een groep G op een verzameling X heet *transitief* indien $\forall x, y \in X : (\exists g \in G : \alpha_g(x) = y)$, en heet *strikt transitief* indien $\forall x, y \in X : (\exists! g \in G : \alpha_g(x) = y)$.

Een paar voorbeelden:

- Een groep werkt op zichzelf door linkervermenigvuldiging: $\alpha_g(x) = gx$. Deze actie is getrouw en strikt transitief.
- Een groep werkt op zichzelf door rechtervermenigvuldiging: $\alpha_g(x) = xg^{-1}$. Deze actie is getrouw en strikt transitief.
- Een groep werkt op zichtzelf door toevoeging: $\alpha_g(x) = gxg^{-1}$. Deze actie is niet noodzakelijk getrouw, want $Ker(\alpha) = Z(G)$. Als G meer dan 1 element bevat is deze actie ook niet transitief, want neem $x \neq e$, dan geldt $\forall g \in G : \alpha_g(e) : geg^{-1} = e \neq x$.
- De groep S_3 werkt op $X = \{1, 2, 3\}$ via $\alpha_r = (1, 2, 3)$ en $\alpha_s = (1, 2)$. Deze actie is getrouw, transitief maar niet strikt transitief omdat $\alpha_r(1) = 2 = \alpha_s(1)$.
- Zij H een deelgroep van G dan werkt G als groep op de verzameling van de linkernevenklassen $X = \{xH : x \in G\}$ van H in G via $\alpha_g(xH) = gxH$.

In bepaalde gevallen impliceert transitief vanzelf ook strikt transitief:

Stelling 8.23. *Zij α een getrouwe transitieve actie van een abelse groep G op een verzameling X. Dan is α strikt transitief.*

Bewijs. Zij $x, y \in X$ en $g, h \in G$ zodanig dat $\alpha_g(x) = \alpha_h(x) = y$. Dan geldt voor elke $z \in X$:

$$\begin{aligned}
\alpha_g(z) &= \alpha_g(\alpha_k(x)) \text{ omdat de actie transitief is} \\
&= \alpha_{gk}(x) = \alpha_{kg}(x) \\
&= \alpha_k(\alpha_g(x)) = \alpha_k(\alpha_h(x)) \\
&= \alpha_{kh}(x) = \alpha_{hk}(x) \\
&= \alpha_h(\alpha_k(x)) = \alpha_h(z)
\end{aligned}$$

Dus is $\alpha_g = \alpha_h$ en omdat de actie getrouw is volgt hieruit dat $g = h$. Bijgevolg is α strikt transitief. □

Met een actie van G op X en een element x van X kan men een bijzondere deelgroep van G en een bijzondere deelverzameling van X associëren.

Definitie 8.24. Zij α een actie van een groep G op een verzameling X en $x \in X$. De *stabilisator* of isotropiegroep van x is $G_x = \{g \in G : \alpha_g(x) = x\}$

De stabilisator van x is dus de verzameling van alle groepselementen g waarvoor α_g het element x vasthoudt.

Definitie 8.25. Zij α een actie van een groep G op een verzameling X en $x \in X$. De *baan* of orbit van x is de deelverzameling $G(x) = \{\alpha_g(x) : g \in G\}$ van X.

Stelling 8.26. *De stabilisator van x is een deelgroep van G.*

Bewijs. Zij $g, h \in G_x$, dan is $\alpha_h(x) = x \Rightarrow \alpha_{h^{-1}}(x) = x$. Maar dan is ook $\alpha_{gh^{-1}}(x) = x$ en is G_x dus een deelgroep van G. □

Stelling 8.27. *Als α een transitieve actie is van G op X, dan is $\forall x \in X : G(x) = X$.*

Bewijs. Neem x een willekeurig element van X. Voor elke $y \in X$ bestaat er een $g \in G$ zodat $\alpha_g(x) = y$, maar dan is $y \in G(x)$. Bijgevolg is $G(x) = X$. □

Stelling 8.28. *Als α een strikt transitieve actie is van G op X, dan is $\forall x \in X : G_x = \{e\}$.*

Bewijs. Stel $g \in G_x$, dan is $\alpha_g(x) = x$. Omdat $\alpha_e(x) = x$ en omdat α strikt transitief is moet g dus gelijk zijn aan e. Hieruit volgt het gestelde. □

Stelling 8.29. *Elementen in dezelfde baan hebben toegevoegde stabilisatoren.*

Bewijs. Stel $y \in G(x)$, dus $y = \alpha_g(x)$. Neem $h \in G_y$, dan is $\alpha_h(\alpha_g(x)) = \alpha_g(x) \Rightarrow \alpha_{g^{-1}}(\alpha_h(\alpha_g(x))) = x$. Bijgevolg is $g^{-1}hg \in G_x$. Hieruit volgt dat $G_y = g^{-1}G_x g$, wat moest bewezen worden. □

Men zegt ook wel eens dat elementen met toegevoegde stabilisatoren hetzelfde orbit-type hebben.

Stelling 8.30. *De banen van een actie van G op X zijn de equivalentieklassen van de relatie op X gedefinieerd door*

$$v \sim w \Longleftrightarrow \exists g \in G : \alpha_g(w) = v$$

Bewijs. De relatie $\sim$ is reflexief want $\alpha_e(x) = x$, dus $x \sim x$. De relatie is ook symmetrisch want als $v \sim w \Rightarrow \exists g \in G : \alpha_g(w) = v$. Dan is $w = \alpha_g^{-1}(v) = \alpha_{g^{-1}}(v) \Rightarrow w \sim v$. Bovendien is de relatie ook transitief want als $v \sim w$ en $w \sim z$, dan zijn er $g, h \in G$ met $\alpha_g(w) = v$ en $\alpha_h(z) = w$. Maar dan is $\alpha_{gh}(z) = \alpha_g(\alpha_h(z)) = v$. Bijgevolg is $v \sim z$. Neem nu $w \in G(v)$, dan bestaat er dus een $g \in G$ zodat $w = \alpha_g(v) \Rightarrow v \sim w$. Hieruit volgt het gestelde. □

Gevolg 8.31. *De banen van een actie van een groep G op een verzameling X vormen een partitie van X.*

Gevolg 8.32. *Als een groep door toevoeging op zichtzelf werkt, dan zijn de banen niets anders dan de toevoegingsklassen. De stabilisatoren zijn de centralisatoren.*

Als G een eindige groep is, dan zijn het aantal elementen in G, G_x en $G(x)$ door een elegante formule verbonden: de orbit-stabilisator stelling.

Stelling 8.33. *Zij α een actie van een eindige groep op een verzameling X en zij $x \in X$. Dan is*

$$\#G = (\#G_x).(\#G(x))$$

Bewijs. De stelling van Lagrange zegt ons dat

$$\#G = (\#G_x).[G : G_x]$$

Het volstaat dus een bijectie te vinden tussen de verzameling linkernevenklassen van G_x en $G(x)$. Definieer $\mu(gG_x) = \alpha_g(x)$. Deze afbeelding is goed gedefinieerd want als $gG_x = hG_x \Rightarrow h^{-1}g \in G_x \Rightarrow \alpha_{h^{-1}g}(x) = x \Rightarrow \alpha_g(x) = \alpha_h(x)$. De afbeelding μ is injectief want als $\mu(gG_x) = \mu(hG_x) \Rightarrow \alpha_g(x) = \alpha_h(x) \Rightarrow h^{-1}g \in G_x \Rightarrow gG_x = hG_x$. Bovendien is μ surjectief want als $y \in G(x)$dan bestaat er een $g \in G : \alpha_g(x) = y \Rightarrow y = \mu(gG_x)$. □

Gevolg 8.34. *Als α een transitieve actie is van een eindige groep op een verzameling X, dan geldt: $\#G = (\#G_x).(\#X)$.*

Gevolg 8.35. *Het aantal elementen in de baan van x is de index van G_x in G.*

Gevolg 8.36. *Het aantal elementen in de baan van x is steeds een deler van de orde van G.*

Gevolg 8.37. *Als een groep G op zichzelf werkt door toevoeging zegt de orbit-stabilisator stelling dat de orde van G gelijk is aan het aantal elementen in een toevoegingsklasse vermenigvuldigd met het aantal elementen van de centralisator van een element van die toevoegingsklasse.*

Definitie 8.38. De *fixpunt* verzameling van een groepselement g voor een actie α op een verzameling X is de deelverzameling van X bestaande uit die elementen die door de actie van g ter plaatse blijven.

We noteren de fixpunt verzameling door X^g, dus $X^g = \{x \in X = \alpha_g(x) = x\}$. We formuleren nu de orbit-tel stelling:

Stelling 8.39. *Voor een actie van een eindige groep G op een eindige verzameling X is het aantal banen gelijk aan het gemiddelde van het aantal elementen in de verschillende fixpunt verzamelingen:*

$$\#\ banen\ = \frac{1}{\#G}\sum_{g\in G} X^g$$

Bewijs. Bestuderen we de deelverzameling van $G \times X$ bestaande uit de elementen (g, x) waarvoor $\alpha_g(x) = x$. We gaan het aantal elementen hiervan op twee manieren berekenen. Als we onze aandacht vestigen op de eerste component g dan is het aantal koppels (g, x) met $\alpha_g(x) = x$ juist de fixpunt verzameling X^g. Bijgevolg is het aantal elementen in de besproken verzameling gelijk aan $\sum_{g \in G} X^g$. Als we onze aandacht vestigen op de tweede component x dan is het aantal koppels (g, x) met $\alpha_g(x) = x$ juist gelijk aan de stabilisator deelgroep G_x en daarom is het aantal elementen van de bewuste verzameling gelijk aan $\sum_{x \in X} \#G_x$. Alle elementen w van de orbit $G(v)$ hebben een toegevoegde stabilisator deelgroep en bijgevolg geldt voor deze elementen dat $\#G_v = \#G_w$. Maar dan kunnen we vorige som ook uitschrijven over alle verschillende orbits $G(x_1), \cdots, G(x_t)$:

$$\sum_{x \in X} \#G_x = \sum_{i=1}^{t} \#G(x_i).\#G_{x_i} = \sum_{i=1}^{t} \#G$$

Maar dan hebben we:

$$t\#G = \sum_{g \in G} X^g$$

en hieruit volgt het gestelde. □

We gaan deze stellingen toepassen om eigenschappen van eindige groepen te vinden.

Stelling 8.40. *Zij G een eindige p-groep met p priem. Dan is $Z(G)$ niet triviaal.*

Bewijs. We laten G werken op zichzelf door toevoeging. De aantal elementen van een toevoegingsklasse is steeds een deler van p^n en is dus van de vorm p^{k_i} met $0 \leq k_i < n$. De klassevergelijking leert ons dat $|G| = p^n = |Z(G)| + \sum_i p^{k_i}$. Hieruit volgt dat p een deler is van de orde van $Z(G)$ en dus is het centrum van G niet-triviaal. □

Stelling 8.41. *Als p priem is en $|G| = p^2$ dan is G cyclisch ofwel is G isomorf met $C_p \times C_p$.*

Bewijs. Als G een element van orde p^2 heeft is de groep cyclisch. Stel dat er zo geen element is, dan hebben alle elementen orde p. Vorige stelling leert ons dat $Z(g)$ niet triviaal is, dus de index van $Z(G)$ in G is gelijk aan p. Neem $tZ(G)$ een voortbrengend element van $G/Z(G)$. Dan is elk element van G van de vorm $t^i z$ met $0 \leq i < p$ en $z \in Z(G)$. Maar dan is $g.g' = t^i z_1.t^j.z_2 = t^{i+j}.z_1 z_2 = t^j z_2.t^i z_1 = g'g$. Bijgevolg is G abels. Neem a een element van orde p en $H = \langle a \rangle$. Neem ook b een element van orde p buiten H en noteer $K = \langle b \rangle$. H en K zijn isomorf met C_p. Omdat G abels is volstaat het nu te bewijzen dat e het enige element is in $H \cap K$ en dat elk element van G te schrijven is als het product van een element uit H en een element uit K. Omdat p priem is, is elk element van H ook voortbrengend element van K en omgekeerd. Als er dus een gemeenschappelijk element, verschillend van e zou zijn , dan zou $H = K$. Het is duidelijk dat bH een voortbrengend element is van G/H, dus is elk element van G te schrijven onder de vorm $b^i h$ met $h \in H$ en $b^i \in K$. Hieruit volgt het gestelde. □

Stelling 8.42. *Als p priem is en G is een niet-abelse groep met $|G| = p^3$ dan is $Z(G) \cong C_p$ en $G/Z(G) \cong C_p \times C_p$.*

Bewijs. We weten dat het centrum niet triviaal is dus, dus is het aantal elementen in het centrum gelijk aan p, p^2 of p^3. Omdat G niet abels is kan de laatste situatie niet. Als $|Z(G)| = p^2$, dan is $G/Z(G)$ cyclisch en dus is G abels, wat tegen het gegeven is. Bijgevolg is $Z(G) \cong C_p$.
Dan is $|G/Z(G)| = p^2$. Volgens vorige stelling is $G/Z(G)$ dan cyclisch of isomorf met $C_p \times C_p$. Cyclisch kan het niet zijn, want dan zou G weer abels zijn. Hieruit volgt dan het gestelde. □

Gevolg 8.43. *Er zijn 5 groepen van orde p^3 met p priem: drie abelse groepen: $C_{p^3}, C_p \times C_{p^2}$ en $C_p \times C_p \times C_p$ en de twee groepen vermeld in bovenstaande stelling.*

Stelling 8.44. *Stel H een deelgroep van G met eindige index n. Dan bestaat er een normaaldeler N van G met $N \subset H$ en zodat de index van N in G een deler is van $n!$.*

Bewijs. We laten G werken op de verzameling X van alle linkernevenklassen van H in G. Deze werking wordt gegeven door een homomorfisme $\alpha : G \rightarrow$

$S(X)$. Zij N de kern van dit homomorfisme. De stabilisator van eH is gelijk aan H zodat inderdaad $N \subset H$. De eerste isomorfismestelling geeft een isomorfisme van G/N met het beeld van α, wat een deelgroep is van $S(X)$. Omdat $S(x)$ orde $n!$ heeft, volgt uit de stelling van Lagrange dat de index van N in G een deler is van $n!$. □

Stelling 8.45. *Zij G een eindige groep en p het kleinste priemgetal dat de orde van G deelt. Als H een deelgroep is van G met index p dan is H een normaaldeler van G.*

Bewijs. Volgens vorige stelling bestaat er een normaaldeler n van G die bevat is in H en zodat de index van N in G een deler is van $p!$. Anderzijds weten we uit de stelling van Lagrange dat de index van N in G een deler is van de orde van G. De veronderstelling dat p het kleinste priemgetal is dat de orde van G deelt impliceert dat $ggd(p!, |G|) = p$. Dus de index van N in G is een deler van p en omdat $[g : N] = [G : H] \,.\, [H : N] = p \,.\, [H : N]$. Dus is $[H : N] = 1$ waaruit volgt dat $H = N$. Bijgevolg is H een normaaldeler van G. □

8.4 De stellingen van Sylow

Stel dat G een eindige groep is waarbij $|G| = p^n q$. Hierbij is p een priemgetal en is p geen deler van q. De stelling van Lagrange zegt dat de orde van een deelgroep steds een deler is van de orde van de groep zelf. Het omgekeerde is niet steeds waar. Als m een deler is van de orde van de groep G, dan bestaat er niet noodzakelijk een deelgroep van orde m. Volgens de stelling van Lagrange is de orde van de grootst mogelijke echte deelgroep van G gelijk aan p^n. Een deelgroep van orde p^n noemt men een *p-Sylow deelgroep* van G. Maar bestaat er wel zo een Sylow deelgroep ? De Sylow stellingen geven het bewijs van het bestaan van dergelijke Sylow deelgroepen en geven ook eigenschappen ervan.

Stelling 8.46. *Zij G een eindige groep en p een priemdeler van $|G|$. Dan bestaat er een p-Sylowdeelgroep van G.*

Bewijs. Zij $|G| = p^n q$ met p een priemgetal dat q niet deelt. Zij S de verzameling van alle deelverzamelingen van grootte p^n. We definieren een actie van G op S via $\alpha_g(A) = gA$. Het aantal elementen van S is het aantal p^n-combinaties uit een verzameling van $p^n q$ elementen. Dit getal is niet deelbaar door p, want

$$\binom{p^n q}{p^n} = \frac{p^n q}{p^n} . \frac{p^n q - 1}{p^n - 1} \cdots \frac{p^n q - i}{p^n - i} \cdots \frac{p^n q - pn + 1}{1}$$

In elke breuk is de macht van p in teller en noemer dezelfde en worden alle $p's$ dus weggedeeld zodat p geen deler is van $\binom{p^n q}{p^n}$.

Omdat S de disjuncte unie is van banen, is er minstens 1 baan waarvan het aantal elementen niet deelbaar is door p. Veronderstel dat $A \in S$ met $\#G(A)$ niet deelbaar door p. We proberen nu te bewijzen dat de stabilisator G_A de gezochte p-Sylow deelgroep is. We weten dat $|G(A)| = [G : G_A] = \frac{|G|}{|G_A|}$. Omdat p geen deler mag zijn van $|G(A)|$ moet $|G_A|$ een veelvoud zijn van p^n. Nu is $G_A = \{g \in G : gA = A\}$. Als x een element is van G_A en $a \in A$ dan is $xa \in A$. De rechternevenklasse $G_A a$ besaat dus uit elementen van A. Omdat G_A en zijn rechternevenklasse evenveel elementen hebben moet het aantal elementen van G_A kleiner of gelijk zijn aan p^n. Bijgevolg is het aantal elementen in G_A juist gelijk aan p^n en hiermee is het gestelde bewezen. □

Gevolg 8.47. *Elke p-deelgroep van G is bevat in een p-Sylow deelgroep van G.*

Gevolg 8.48. *Als $|G| = p^n.q$, dan bevat G deelgroepen van orde p^i met $1 \leq i \leq n$. Elke deelgroep van orde p^i is normaaldeler van een deelgroep van orde p^{i+1}.*

De volgende stellingen gaan over de struktuur van de p-Sylow deelgroepen en hun aantal. merk op dat als P een p-Sylow deelgroep is van G en $x \in G$, dan is xPx^{-1} een deelgroep met hetzelfde aantal elementen als P. Dus is xPx^{-1} ook een p-Sylow deelgroep van G. Om de volgende stellingen te bewijzen hebben we ook nog het begrip G-stabiel nodig.

Definitie 8.49. Als G werkt op een verzameling X en $x \in X$ dan noemt men x G-stabiel als $\forall g \in G : \alpha_g(x) = x$.

merk op dat als x een G-stabiel element is van X, dat de baan van x enkel uit x betsaat, dus $G(x) = \{x\}$.

Stelling 8.50. *Als G een groep is met $|G| = p^r$ met p priem en G werkt op een verzameling X waarbij S de verzameling is van alle G-stabiele elementen, dan is $|S| \equiv |X| \mod p$.*

Bewijs. Stel $x_1, x_2, \cdots, x_m$ representanten van de disjuncte banen, die meer dan 1 element bevatten, onder de werking van G op X. Dan is $X = S \cup G(x_1) \cup G(x_2) \cup \cdots \cup G(x_m)$. Bijgevolg is $|X| = |S| + \sum_i |G(x_i)|$. Omdat het aantal elementen in een baan een deler is van de orde van G, is $|G(x_i)|$ deelbaar door p en daaruit volgt het gestelde. □

Stelling 8.51. *Zij G een groep van orde $p^n q$ met p priem en geen deler van q. Als P een p-Sylow deelgroep is van G en H een willekeurige deelgroep is van G met orde een macht van p, dan is $H \subseteq xPx^{-1}$ voor een $x \in G$. Meer speciaal : twee p-Sylow deelgroepen zijn steeds toegevoegd.*

Bewijs. Neem X de verzameling van de linkernevenklassen van P in G en laat H werken op X. Neem S de verzameling van alle H-stabiele elementen van X. We weten uit vorige stelling dat $|X| \equiv |S| \mod p$ en omdat $|X| = \frac{|G|}{|P|} = q$ en q niet deelbaar is door p is $|S| \not\equiv 0 \mod p$. Bijgevolg is S niet leeg. Veronderstel dat $aP \in S$. De baan van aP is $\{haP : h \in H\}$ en omdat die baan maar 1 element bevat moet voor elke $h \in H$ gelden dat $haP = aP$. Dit betekent dat $h \in aPa^{-1}$ en bijgevolg is $H \subseteq aPa^{-1}$. Hiermee is het eerste deel van de stelling bewezen. Veronderstel nu dat P' een tweede p-Sylow deelgroep is van G, dan volgt uit het eerste deel van de stelling dat $P' \subseteq aPa^{-1}$ voor een $a \in G$. Omdat de ordes van P' en aPa^{-1} gelijk zijn aan elkaar, volgt het gestelde. □

Stelling 8.52. *Als P een p-Sylow deelgroep is van G en als $N_G(P) \leq H \leq G$, dan is $N_G(H) = H$.*

Bewijs. Neem $x \in N_G(H)$. Omdat $P \leq H \lhd N_G(H)$ geldt dat $xPx^{-1} \leq H$. Omdat P en xPx^{-1} p-Sylow deelgroepen zijn van G bestaat er een element h van H zodat $xPx^{-1} = hPh^{-1}$ en dus is $x^{-1}h \in N_G(H) \leq H$. Bijgevolg behoort x tot H en is de stelling bewezen. □

Stelling 8.53. *Als P een p-Sylow deelgroep is van G en $N \triangleleft G$, dan is $P \cap N$ een p-Sylowdeelgroep van N en $(PN)/N$ is een p-Sylowdeelgroep van G/N.*

Bewijs. $[N : P \cap N] = [PN : P]$ en dit is onderling ondeelbaar met p. Bijgevolg is $P \cap N$ een p-groep en dus ook een p-Sylow deelgroep van N. Verder is ook $[G/N : (PN)/N] = [G : PN]$ ook onderling ondeelbaar met p en dus is $|(PN)/N| = |P/(P \cap N)|$ een macht van p en hieruit volgt het gestelde. □

Gevolg 8.54. *Een p-Sylow deelgroep P van G is een normaaldeler van G als en slechts als het de enige p-Sylow deelgroep is van G.*

Stelling 8.55. *Het aantal p-Sylow deelgroepen van G is een deler van de orde van G en is van de vorm $1 + kp$ voor een $k \geq 0$.*

Bewijs. Zij P een p-Sylow deelgroep van G. Volgens de tweede stelling van Sylow is de verzameling X van alle p-Sylow deelgroepen van G gegeven door $X = \{gPg^{-1} \text{ met } g \in G\}$. We laten G werken op X door toevoeging, met andere woorden $\alpha_g(Q) = gQg^{-1}$ waarbij $Q = aPa^{-1}$. Dan geldt er dat $G(P) = X$ en $G_P = \{g \in G : gPg^{-1} = P\}$ en dat is de normalisator van P in G. Het aantal elementen van X is dus de index van de normalisator van P in G en is dus een deler van de orde van G. Bovendien is het aantal elementen van X niet deelbaar door p want $\frac{|G|}{|N_G(P)|}$ is een deler van $q = \frac{|G|}{|P|}$ omdat $P \subseteq N_G(P)$.
Laten we nu P als groep werken op X door toevoeging. Als S de verzameling is van alle P-stabiele elementen van X , dan is $|X| \equiv |S| \bmod p$. Omdat nu $|X|$ niet deelbaar is door p is S niet leeg. Er bestaat dus een p-Sylow deelgroep Q zodat, onder de werking van P, de baan van Q enkel uit Q bestaat. Dit betekent dat $xQx^{-1} = Q$ voor elke $x \in P$. Dan is $P \subseteq N_G(Q)$. Bijgevolg zijn zowel P als Q deelgroepen van de normalisator $N_G(Q)$. Omdat $|N_G(Q)| = p^n q'$, met q' een deler van q, zijn P en Q zelfs p-Sylowdeelgroepen van $N_G(Q)$. Maar Q is normaal in $N_Q(Q)$, dus is er maar 1 p-Sylow deelgroep en dus is $P = Q$. Maar dan telt S maar 1 element. We weten dat $|X| \equiv |S| \bmod p$, dus $|X| \equiv 1 \bmod p$. Hieruit volgt het gestelde. □

Gevolg 8.56. *Als $|G| = p^n.q$ dan is het aantal p-Sylow deelgroepen n_p gegeven door: $n_p|q$ en $n_p \equiv 1 \bmod p$.*

Gevolg 8.57. *Het aantal p-Sylow deelgroepen n_p is gegeven door $n_p = [G : N_G(P)]$ waarbij P een willekeurige p-Sylowdeelgroep is.*

Gevolg 8.58. *Elke eindige abelse groep is het product van zijn p-Sylow deelgroepen. Om deze groepen te klassificeren volstaat het dus de structuur te bestuderen in het geval de orde een priemmacht is. Stel $|A| = p^n$, dan is $A \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ met $n_1 \geq n_2 \geq \cdots \geq n_k$ en $n_1 + n_2 + \cdots + n_k = n$.*

Bestuderen we even een voorbeeld: stel dat $|G| = 6 = 2.3$. Dan weten we dat n_2 een deler is van 3 en dat $n_2 = 1 + 2k$, dus $n_2 = 1$ of $n_2 = 3$. Verder is n_3 een deler van 2 en $n_3 = 1 + 3k$, dus moet $n_3 = 1$. Dit geeft volgende tabel:

n_2	n_3	G
1	1	$C_2 \times C_3$
3	1	D_3

We kunnen de stellingen van Sylow gebruiken om een klassificatie te geven van bepaalde types van groepen. We veronderstellen dat p, q, r verschillende priemgetallen zijn en dat $p < q < r$.

(a) Als $|G| = pq$ en p is geen deler van $q - 1$, dan bestaan er een unieke p-Sylow deelgroep en een unieke q-Sylow deelgroep. Deze groepen zijn dus nooit enkelvoudig. want $n_p = 1 + kp$ en $n_p | q$, dus is $n_p = 1$ of q. Dit laatste is onmogelijk want anders zou p een deler zijn van $q - 1$. Bijgevolg is de p- Sylowdeelgroep normaal. Omdat $n_q | p$ is de enige mogelijkheid $n_q = 1$ en dus is ook de q-Sylow deelgroep normaal.

(b) Als $|G| = pq$ en p is wel een deler van $q - 1$, dan is er een unieke q-Sylow deelgroep.

(c) Als $|G| = pqr$, dan is er een unieke r-Sylow deelgroep. Als bovendien q geen deler is van $r - 1$, dan is er ook een unieke -q-Sylow deelgroep. Deze groepen zijn dus nooit enkelvoudig. Omdat $n_r | pq$ kan $n_r = 1, p, q,$ of pq. het is duidelijk dat n_r niet gelijk kan zijn aan p of q. Stel dat het gelijk is aan pq, dan zijn er $pq(r - 1)$ verschillende elementen van orde r. Het is ook duidelijk dat $n_q > p$, dus zijn er meer dan $p(q - 1)$ elementen van orde q. Er zijn minstens $p-1$ elementen over van orde p en er is het eenheidselement. Dus dit kan niet en bijgevolg is $n_r = 1$ en is er een unieke r-Sylow deelgroep.

(d) Als $|G| = p^2q$, dan is er unieke p-Sylow deelgroep ofwel een unieke q-Sylow deelgroep. Deze groepen zijn dus nooit enkelvoudig. Want het aantal q-Sylow deelgroepen is $1, p$ of p^2. Het kunnen er nooit p zijn. Stel dat er p^2 zouden zijn, dan zijn er $p^2(q-1)$ elementen van orde q. De rest, en dat p^2 elementen, zijn dan elementen van orde p. Deze vormen dus een unieke p-Sylow deelgroep en die is normaal. In het andere geval is er een unieke en dus normale q-Sylow deelgroep.

(e) Als $|G| = pq^a$, dan is er een unieke q-Sylow deelgroep. Deze groepen zijn dus nooit enkelvoudig.

8.5 De structuur van S_n

Stelling 8.59. *De $n-1$ transposities $\{(1,2),(1,3),\cdots,(1,n)\}$ zijn een voortbrengend stel van S_n.*

Bewijs. We kunnen elke cykel schrijven als een product van transposities. Zo is $(a_1, a_2, \cdots, a_k) = (a_1, a_k)(a_1, a_{k-1})\cdots(a_1, a-3)(a_1, a_2)$. Rest te bewijzen dat elke transpositie te schrijven is als een product van de voortbrengende elementen. Maar $(a, b) = (1, a)(1, b)(1, a)$. Hieruit volgt het gestelde. □

Gevolg 8.60. $\{(1,n),(1,2,3,\cdots,n)\}$ *is een voortbrengend deel van S_n.*

Stelling 8.61. *De alternerende groep A_n wordt voortgebracht door de 3-cykels $\{(1,2,3),(1,2,4),\cdots,(1,2,n)\}$.*

Bewijs. Een element van A_n is te schrijven als de samenstelling van een even aantal transposities. We kunnen de transposities dus twee per twee samennemen en we zien zo dat A_n voortgebracht wordt door de permutaties $(1,j)(1,i) = (1,i,j)$. Als $i \neq 2 \neq j$, dan hebben we dat
$(1,2,j)^{-1}(1,2,i)(1,2,j) = (j,2,1)(1,2,i)(1,2,i) = (1,i,j)$. Als $i = 2$ dan hebben we al de gewenste vorm. Als $j = 2$ dan is $(1,i,j) = (1,j,2) = (1,2,i)(1,2,i)$ en bijgevolg wordt A_n voortgebracht door alle 3-cykels van de vorm $(1,2,i)$. □

We bestuderen nu de toevoegingsklassen van S_n.
De toevoegingsklassen van S_n corresponderen met de cykelstruktuur van de permutaties. Twee elementen van S_n zijn toegevoegd als en slechts als ze bestaan uit hetzelfde aantal cykels van dezelfde lengte. In S_5 zijn $(1,2,3)(4,5)$ en $(1,4,3)(2,5)$ toegevoegd, maar zijn $(1,2,3)(4,5)$ en $(1,2)(4,5)$ niet toegevoegd.

Stelling 8.62. *Twee permutaties in S_n zijn toegevoegd als en slechts als ze dezelfde cykel lengte hebben.*

Bewijs. Neem een cykel $h = (a_1, a_2, \cdots, a_r)$ en een willekeurige permutatie

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

Dan is $ghg^{-1} = (g(a_1), g(a_2), \cdots, g(a_r))$ en deze permutatie heeft dus dezelfde cykel lengte. Voor meerdere cykels herhalen we dit argument voor elk van de cykels afzonderlijk omdat we tussen alle cykels termen $g^{-1}g$ kunnen plaatsen.
Omgekeerd, neem twee permutaties met dezelfde cykel lengte:
$\sigma = (a_1, \cdots, a_{i_1})(b_1, \cdots, b_{i_2}) \cdots (z_1, \cdots, z_{i_k})$ en
$\tau = (\alpha_1, \cdots, \alpha_{i_1})(\beta_1, \cdots, \beta_{i_2}) \cdots (\zeta_1, \cdots, \zeta_{i_k})$. Construeer dan

$$g = \begin{pmatrix} a_1 & \cdots & b_1 & \cdots & z_{i_k} \\ \alpha_1 & \cdots & \beta_1 & \cdots & \zeta_{i_k} \end{pmatrix}$$

Dan is $\tau = g\sigma g^{-1}$ en dus zijn τ en σ toegevoegd. □

Als we de 1-cykles terug in de cykelontbinding stoppen, zien we dat het aantal toevoegingsklassen in S_n gelijk is aan het aantal partities van n. Een partitie van een natuurlijk getal n is een dalende rij van natuurlijke getallen $p_1 \geq p_2 \geq \cdots \geq p_k$ zodat $n = p_1 + p_2 + \cdots + p_k$. Nemen we als voorbeeld S_3:

cykel lengte	permutaties	aantal elementen
111	e	1
21	$(1,2), (1,3), (2,3)$	3
3	$(1,2,3), (1,3,2)$	2

Stelling 8.63. *Het aantal elementen in de toevoegingsklasse van* $\sigma = 1^{e_1}2^{e_2}\cdots n^{e_n}$ *in* S_n *wordt gegeven door de formule*

$$\frac{n!}{1^{e_1}1!.2^{e_2}2!.\cdots .n^{e_n}n!}$$

Bewijs. De cykel ontbinding van σ is $(.)\cdots(.)(..)\cdots(..)\cdots$. Om de n puntjes in de vullen zijn er $n!$ mogelijkheden. Maar die corresponderen niet noodzakelijk met verschillende permutaties. Neem bijvoorbeeld de e_j verschillende cykles van lengte j. Die kunnen op $e_j!$ manieren gepermuteerd worden en geven toch hetzelfde element van S_n. Bovendien kan elke cykel van lengte j op j manieren geschreven worden: $(a_1, a_2, \cdots, a_j) = (a_2, a_3, \cdots, a_j, a_1)$. Dit kunnen we voor elke cykel van lengte j doen. Dus die j^{e_j} mogelijkheden geven dezelfde permutatie. Hieruit volgt de stelling. □

Gevolg 8.64. *Als* $n \geq 2$*, dan is* $Z(S_n)$ *triviaal.*

We besluiten met een resultaat voor de alternerende groepen.

Stelling 8.65. *Voor* $n \geq 5$ *is* A_n *enkelvoudig.*

Bewijs. Veronderstel dat $N \neq \{e\}$ een normale deelgroep zou zijn van A_n. We gaan bewijzen dat N een 3-cykel bevat. Als dat zo is , dan bevat het alle 3-cykels en dan is $N = A_n$ omdat de 3-cykels de alternerende groep voortbrengen. Bijgevolg zou A_n enkelvoudig zijn.

- Als er een element σ is van N met een cykel met lengte groter dan 3: bvb $\sigma = (1, 2\cdots, r)\tau$ met $r \geq 4$. Neem dan $\delta = (1, 2, 3)$ en construeer $x = \sigma^{-1}\delta^{-1}\sigma\delta \in N$. Dan is $x = (2, 3, r)$ en dus bevat N een 3-cykel.
- Rest het geval dat elk element van N enkel bestaat uit 2-cykles en 3-cykels. Veronderstel dat $\sigma = (1, 2, 3)(4, 5, 6)\tau \in N$. Neem dan $\delta = (1, 2, 4)$ en construeer $x = \sigma^{-1}\delta^{-1}\sigma\delta \in N$. Dan is $x = (1, 2, 4, 3, 6)$ en is er toch een cykel met lengte groter dan 3.
- Dus we mogen veronderstellen dat erhoogstens eéń 3-cykel is en voor de rest 2-cykels: bvb $\sigma = (1, 2, 3)\tau$ met τ een product van

transposities. Maar dan is $\sigma^2 = (1,3,2)$ en bezit N dus een 3-cykel.

- Tenslotte blijft het geval over dat elk element het product is van transposities, en omdat het een even permutatie moet zijn, zijn er minstens 2: bvb $\sigma = (1,2)(3,4)\tau$. Neem dan $\delta = (1,2,3)$ en construeer $x = \sigma^{-1}\delta^{-1}\sigma\delta \in N$. Dan is $x = (1,4)(2,3)$. Construeer dan $y = (1,2,5)^{-1}x(1,2,5) \in N$. Uitrekenen geeft $y = (1,3)(4,5)$. Bijgevolg is $xy = (1,2,3,4,5) \in N$ en bevat N dus wel een cykel van lengte groter dan 3.

□