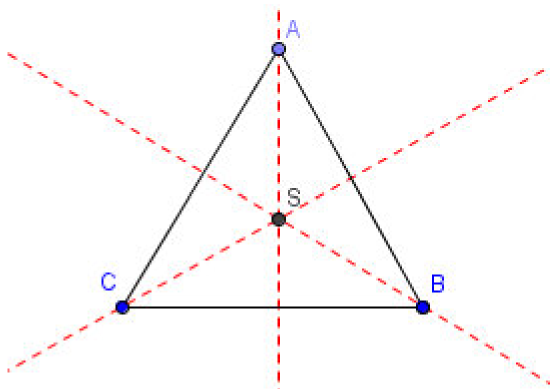
Hoofdstuk 6

Dihedrale groepen

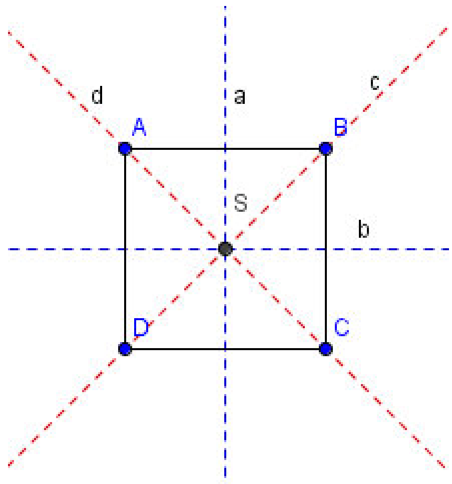
6.1 Definitie

Definitie 6.1. De dihaeder groep is de symmetriegroep van een regelmatige n-hoek. Dit is de verzameling van alle transformaties in het vlak die de regelmatige n-hoek op zichzelf afbeelden, uitgerust met de samenstelling van transformaties.

Als notatie gebruikt men zowel D_n als D_{2n}. Wij kiezen voor de eerste notatie. Een regelmatige n-hoek heeft $2n$ symmetrieën: n rotaties over de hoeken $\frac{2\pi}{n}$ met als centrum het middelpunt van de omgeschreven cirkel en n spiegelingen. Als n oneven is dan gaan de n symmetrieassen door een hoekpunt en door het midden van de overstaande zijde.



Als n even is zijn er $\frac{n}{2}$ symmetrieassen door de middens van overstaande zijden en $\frac{n}{2}$ symmetrieassen door overstaande hoekpunten.



De samenstelling van twee spiegelingen is een rotatie rond het snijpunt van de spiegelassen over een hoek gelijk aan het dubbel van de hoek tussen de spiegelassen.
Als we de rotatie over een hoek $\frac{2\pi}{n}$ voorstellen door r dan zijn alle rotaties van de vorm r^k met $1 \leq k \leq n-1$. De identieke transformatie kan beschouwd worden als een rotatie over 0°.
Als we 1 van de spiegelingen voorstellen door s dan zijn de andere spiegelingen de samenstelling van deze spiegeling en een rotatie, dus van de vorm sr^k met $1 \leq k \leq n-1$. Bovendien geldt er dat

$$sr^k = r^{n-k}s$$

Elke spiegeling is een element van orde twee. Dus:

$$D_n = \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}$$

Een andere mogelijke notatie is dat we voor een rotatie over een hoek $\frac{2\pi.k}{n}$ het symbool r_k gebruiken en voor een spiegeling met een as die een hoek van $\frac{\pi.k}{n}$ maakt met de X-as het symbool s_k gebruiken. De dihaeder groep bestaat dan uit de elementen $r_0, \cdots, r_{n-1}, s_0, \cdots, s_{n-1}$. Voor het samenstellen van de elementen gebruiken we de volgende rekenregels: $r_ir_j = r_{i+j}$, $r_is_j = s_{i+j}$, $s_ir_j = s_{i-j}$ en $s_is_j = r_{i-j}$, waarbij voor de som en het verschil van de indices modulo n wordt gewerkt.

De dihaedergroep D_1 bevat de rotatie over $0°$, de identieke transformatie dus, en de spiegeling s rond de X-as. Dus is $D_1 = \{1, s\} \cong C_2$.
De dihaedergroep D_2 wordt voortgebracht door de rotatie r over $180°$ en de spiegeling s rond de X-as. Dus is $D_2 = \{1, r, s, sr\} \cong C_2 \times C_2$. Hierbij stelt sr de spiegeling rond de Y-as voor.
Dit zijn de enige twee dihaedergroepen die abels zijn. Dus:

$$\forall n \geq 3 : D_n \text{ is niet abels.}$$

Vanaf nu veronderstellen we dat $n \geq 3$.

Stelling 6.2. $D_n \cong C_n \rtimes C_2 \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$.

Bewijs. De verzameling van de rotaties $H = \{1, r, \cdots, r^{n-1}\}$ is een deelgroep van D_n en heeft index 2 en is dus een normaaldeler van D_n. Verder is $K = \{1, s\}$ ook een deelgroep van D_n, $H \cap K = \{1\}$ en $HK = D_n$. Bijgevolg is D_n het semidirect product van H en K. De structuur van D_n wordt bepaald door het homomorfisme $\varphi : K \to Aut(H)$ met $\varphi_s : H \to H : r \mapsto srs = r^{n-1}$. Dan is $r^i r^j = (r^i, 1)(r^j, 1) = (r^i \varphi_1(r^j), 1) = (r^i r^j, 1) = r^{i+j}$. Verder is $r^i s.r^j = (r^i, s)(r^j, 1) = (r^i \varphi_s(r^j), s) = (r^{i-j}, s) = r^{i-j}s$. Uit het feit dat $H \cong \mathbb{Z}_n$ en dat $K \cong \mathbb{Z}_2$ volgt het gestelde. □

Stelling 6.3. *Als n oneven dan is* $D_{2n} \cong D_n \times C_2 \cong D_n \times \mathbb{Z}_2$.

Bewijs. Construeer $A = \{1, r^2, \cdots, r^{2n-2}, s, sr^2, \cdots, sr^{2n-2}\}$ en $B = \{1, r^n\}$. A heeft index 2 in D_{2n} en is dus een normaaldeler. Omdat $(sr^{2k})r^n(sr^{2k})^{-1} = sr^n s = r^n$ is ook B een normaaldeler van D_{2n} en omdat $A \cong D_n$ en $B \cong C_2 \cong \mathbb{Z}_2$ volgt het gestelde. □

6.2 De structuur van dihedrale groepen

We bestuderen nu de structuur van D_n: de ordes van de elementen, de toevoegingsklassen en de deelgroepen.

Stelling 6.4. *De ordes van de elementen van D_n zijn : $o(r^k) = \frac{n}{ggd(r,n)}$ en $o(r^k s) = 2$.*

Bewijs. Het eerste resultaat volgt uit het feit dat de rotaties een cyclische groep van orde n vormen. Omdat de elementen $r^k s$ spiegelingen zijn, is de orde gelijk aan 2. $\square$

Stelling 6.5. *Als n even is dan heeft D_n $\frac{n+6}{2}$ toevoegingsklassen.*

Bewijs. Omdat $sr^k s = r^{-k}$ zijn r^k en r^{-k} toegevoegd. Verder zijn $r^i r^k r^{-i} = r^k$ en $(r^i s) r^k (r^i s)^{-1} = r^{-k}$, dus zijn de enige toegevoegde elementen van r^k ofwel r^k ofwel r^{-k}. Om de toevoegingsklassen van s te vinden berekenen we $r^i s r^{-i} = r^{2i} s$ en $(r^i s) s (r^i s)^{-1} = r^{2i} s$. De andere spiegelingen zijn toegevoegd aan rs. De toevoegingsklassen zijn dus: $C_1 = \{1\}$, $C_2 = \{r^{\frac{n}{2}}\}$, $C'_k = \{r^k, r^{-k}\}$ met $0 < k < \frac{n}{2}$, $C_3 = \{s, r^2 s, r^4 s, \cdots, r^{n-2} s\}$ en $C_4 = \{rs, r^3 s, \cdots,$
$r^{n-1} s\}$. Het aantal klassen is dan $1 + 1 + (\frac{n}{2} - 1) + 1 + 1 = \frac{n+6}{2}$. $\square$

Gevolg 6.6. *Als n even is dan is $Z(D_n) = \{1, r^{\frac{n}{2}}\}$, want het centrum bestaat uit de toevoegingsklassen met 1 element.*

Stelling 6.7. *Als n oneven is dan heeft D_n $\frac{n+3}{2}$ toevoegingsklassen.*

Bewijs. Het bewijs verloopt analoog aan het vorige bewijs buiten het feit dat alle spiegelingen nu toegevoegd zijn aan s. De toevoegingsklassen zijn: $C_1 = \{1\}$, $C'_k = \{r^k, r^{-k}\}$ met $0 < k < \frac{n}{2}$, $C_2 = \{s, rs, r^2 s, \cdots, r^{n-1} s\}$. Het aantal klassen is dan $1 + \frac{n-1}{2} + 1 = \frac{n+3}{2}$. $\square$

Gevolg 6.8. *Als n oneven dan is $Z(D_n) = \{1\}$, want het centrum bestaat uit de toevoegingsklassen met 1 element.*

We hebben dus gevonden dat een rotatie enkel toegevoegd is aan zijn inverse (welke een andere rotatie is tenzij voor de identieke en bij even n de rotatie $r^{\frac{n}{2}}$). De verzameling spiegelingen bestaat uit 1 of 2 toevoegingsklassen naargelang n oneven of even is. In het laatste geval horen de symmetrieassen door de middens van overstaande zijden bij elkaar en de symmetrieassen door overstaande hoekpunten vormen de andere klasse.

Bestuderen we nu de deelgroepen van D_n. Een eerste soort deelgroepen vinden we door de deelgroepen te nemen van het cyclische deel $N = \{1, r, r^2, \cdots,$
$r^{n-1}\}$. Het aantal deelgroepen is gelijk aan het aantal delers van n, genoteerd door $\tau(n)$. Deze deelgroepen zijn allemaal cyclisch en hebben als orde $\frac{n}{d}$, waarbij d een deler is van n. Deze deelgroepen zijn ook allemaal normaaldelers in D_n.

Stelling 6.9. *Als H een deelgroep is van D_n, dan is H ofwel een deelgroep van N ofwel is $|H \cap N| = d$ en $|H| = 2d$, met d een deler van n.*

Bewijs. Omdat N een normaaldeler is van D_n, is $HN \leq D_n$
$\Rightarrow |HN|$ deelt $2n \Rightarrow \frac{|H||N|}{|H\cap N|}$ deelt $2n$. Dan is $\frac{|H||N|}{|H\cap N|}$ gelijk aan 1 of 2. In het eerste geval ligt H helemaal in N en is H dus een deelgroep van N. In het andere geval is $|H| = 2|H \cap N| = 2d$ en omdat $H \cap N \leq N$ is d een deler van n. □

Stelling 6.10. *Stel $m.d = n$ en $A(i, d) = \{sr^{i+km} : 0 \leq k < d\}$ en $0 \leq i < m$. Dan is $B(i, d) = A(i, d) \cup \langle r^m \rangle$ een deelgroep van D_n met orde $2d$.*

Bewijs. Het aantal elementen van $A(i, d)$ is gelijk aan d want stel dat twee elementen zouden gelijk zijn dan is $sr^{i+km} = sr^{i+lm} \Rightarrow r^{(k-l)m} = 1$. Dan is $n|(k - l)m \Rightarrow d|k - l \Rightarrow k = l$. Omdat de orde van $\langle r^m \rangle$ gelijk is aan d, is het aantal elementen van $B(i, d)$ gelijk aan $2d$. Bovendien is $B(i, d)$ een deelgroep van D_n, want $sr^{i+km}.(sr^{i+lm})^{-1} = r^{(l-k)m} \in B(i, d)$ en $sr^{i+km}.(r^{pm})^{-1} = sr^{i+(k-p)m} \in B(i, d)$. □

Gevolg 6.11. *Er zijn $m = \frac{n}{d}$ van dergelijke deelgroepen $B(i, d)$, want $B(i, d) = B(j, d) \Leftrightarrow A(i, d) = A(j, d) \Leftrightarrow i \equiv j$ mod m*

Gevolg 6.12. *Als deze deelgroepen $B(i,d)$ zijn dihaedergroepen want ze worden voortgebracht door twee elementen van orde 2: r^d en $r^i s$. Het bewijs hiervan vinden we terug in 5.4*

Stelling 6.13. *Het aantal deelgroepen van D_n is gelijk aan $\tau(n) + \sigma(n)$ met $\sigma(n)$ de som van het aantal delers van n.(Stephan A.Cavior,1975)*

Bewijs. Als H een deelgroep is van D_n, dan is H ofwel een deelgroep van N en zo zijn er $\tau(n)$, ofwel is $|H \cap N| = d$ en $|H| = 2d$, met d een deler van n. Stel $n = m.d$. Omdat $H \cap N < N$ wordt $H \cap N$ voortgebracht door r^m. Nu bestaat er een i met $0 \leq i < n$ waarvoor $sr^i \in H$ en omdat $r^{km} \in H$ is $sr^{i+km} \in H$. Bijgevolg ligt $A(i,d)$ en ook $B(i,d)$ in H. Omdat ze evenveel elementen bevatten is $H = B(i,d)$. Voor elke deler d van n zijn er $\frac{n}{d}$ van dergelijke deelgroepen. Het totaal aantal is dan $\sum_{d|n} \frac{n}{d} = \sum_{d|n} d = \sigma(n)$. □

Gevolg 6.14. *De deelgroepen van een dihedrale groep zijn ofwel cyclisch ofwel dihedraal.*

Gevolg 6.15. *Als $n = d.m$, dan heeft D_n juist m deelgroepen isomorf met D_d en 1 deelgroep isomorf met C_d.*

Gevolg 6.16. *De maximale deelgroepen van D_n zijn: $N = C_n$ de deelgroepen isomorf met D_p, waarbij p een priemdeler is van n.*

Stelling 6.17. *Een echte deelgroep H is een normaaldeler van D_n als en slechts als $H \leq N$ of als n even is en H is 1 van de volgende 2 maximale deelgroepen met index 2: $\langle r^2, s\rangle$ of $\langle r^2, rs\rangle$*

Bewijs. Als H een normaaldeler is van D_n en H bevat een element $r^i s$, dan bevat het de hele toevoegingsklassen van dit element. Als n oneven is, dan is er maar 1 toevoegingsklasse met spiegelingen en dus is $H = D_n$. Als n even is en i is even dan zitten s en $r^2 s$ in H en dus zit ook r^2 in H. Bijgevolg is $H = \langle r^2, s\rangle$. Als i oneven is dan zitten rs en $r^3 s$ in H en bijgevolg zit ook $r^2 = rsr^3 s$ in H. Dan is $H = \langle r^2, rs\rangle$. □

Stelling 6.18. *De afgeleide groep* $D'_n = \langle r^2 \rangle$.

Bewijs. $[r, s] = rsr^{-1}s^{-1} = r^2$. Dus is r^2 een commutator en is $\langle r^2 \rangle \leq D'_n$. Rest te bewijzen dat elke andere commutator een macht van r^2 is. Nu is $\langle r^2 \rangle$ een normaaldeler van D_n en als n even is is $\frac{D_n}{\langle r^2 \rangle} \cong \{1, r, s, rs\}$ abels. Bijgevolg is $D'_n \leq \langle r^2 \rangle$. Hieruit volgt het gestelde. Als n oneven is dan is $\frac{D_n}{\langle r^2 \rangle} \cong \{1, s\}$ en volgt dezelfde redenering. □

Gevolg 6.19. *Als* n *oneven is , geldt* $\langle r^2 \rangle = \langle r \rangle$ *en is dus* $D'_n = \langle r \rangle$.

6.3 De automorfismegroep van D_n

Bestuderen we tenslotte de automorfismegroep van de dihedergroepen. We hebben al informatie over de inwendige automorfismen:

(a) Als n oneven is dan is $Inn(D_n) \cong \frac{D_n}{Z(G)} \cong D_n$.

(b) Als $n = 2k$ even is dan is $Inn(G) \cong \frac{D_n}{\langle r^k \rangle} \cong D_k$.

Stelling 6.20. $Aut(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$.

Bewijs. De elementen van orde n in D_n zijn de elementen r^i waarbij de ggd(i,n)=1. De elementen van orde 2 zijn de elementen $r^j s$ en als n even is het element $r^{\frac{n}{2}}$. De automorfismen van D_n moeten die elementen onderling op elkaar afbeelden. Definieer dus de volgende automorfismen: φ_{ij} met $i \in \mathbb{Z}_n^\times$ en $j \in \mathbb{Z}_n$, waarbij $\varphi_{ij}(s) = sr^j$ en $\varphi_{ij}(r) = r^i$. Dan is $Aut(D_n) = \{\varphi_{ij}\}$. De samenstelling voldoet aan de volgende regel: $\varphi_{i_1 j_1} \circ \varphi_{i_2 j_2} = \varphi_{i_1 i_2, j_1 + i_1 j_2}$. Definieer de deelgroepen $N = \{\varphi_{1j} : j \in \mathbb{Z}_n\}$ en $U = \{\varphi_{i0} : i \in \mathbb{Z}_n^\times\}$. Het is duidelijk dat $N \cong \mathbb{Z}_n$ en $U \cong \mathbb{Z}_n^\times$. Wetende dat $\varphi_{ij}^{-1} = \varphi_{i^{-1}, -ji^{-1}}$, kunnen we aantonen dat N een normaaldeler is van $Aut(D_n)$, want $\varphi_{ij} \circ \varphi_{1k} \circ \varphi_{ij}^{-1} = \varphi_{ij} \circ \varphi_{i^{-1}, k - ji^{-1}} = \varphi_{1,ik} \in N$. Dan is $Aut(D_n) \cong N \rtimes_\Phi U$ voor een zekere $\Phi : U \to Aut(N)$. Hierbij is $\Phi_{\varphi_{i0}}(\varphi_{1j}) = \varphi_{i0} \circ \varphi_{1j} \circ \varphi_{i0}^{-1} = \varphi_{1,ij}$. □

6.4 Enkele stellingen

Een groep die eigenschappen heeft zoals D_n is het homomorfe beeld van D_n of is isomorf met D_n :

Stelling 6.21. *Als $G = \langle a, b : a^n = b^2 = 1$ en $bab^{-1} = a^{-1}\rangle$ dan bestaat er een surjectief homomorfisme $f : D_n \to G$ en als $|G| = 2n$, dan is $G \cong D_n$.*

Bewijs. Uit $bab^{-1} = a^{-1}$ volgt dat $ba^jb^{-1} = a^{-j}$. Toevoeging met b geeft $b^ka^jb^{-k} = a^{(-1)^kj}$ zodat $b^ka^j == a^{(-1)^kjb^k}$. Definieer nu $f : D_n \to G : r^js^k \mapsto a^jb^k$. Het is duidelijk dat f een homomorfisme is, want $f(r^j.r^i) = f(r^{j+i}) = a^{j+i} = a^ja^i = f(r^j).f(r^i)$. Ook is $f(r^js.r^is) = f(r^{j-i}) = a^{j-i} = a^jb.a^ib = f(r^js).f(r^is)$. Het homomorfisme f is bovendien surjectief. Hieruit volgt het gestelde. □

Uit deze stelling kunnen we volgend resultaat afleiden:

Stelling 6.22. *Een eindige, niet-abelse groep voortgebracht door twee elementen van orde 2 is isomorf met D_n.*

Bewijs. Stel $G = \langle x, y\rangle$ met $x^2 = y^2 = 1$. Omdat G niet-abels is weten we dat $xy \neq yx$. Omdat G eindig is bestaat er een n waarvoor geldt dat $(xy)^n = 1$. Noteer nu $a = xy$ en $b = y$. We kunnen dan stellen dat $G = \langle a, b : a^n = b^2 = 1\rangle$. Omdat de orde van a gelijk is aan n en omdat $b \notin \langle a\rangle$ zal de orde van G minstens $2n$ zijn. De waarde van n is minstens 3 want als $n = 2$ zou $a^2 = 1 \Rightarrow xyxy = 1 \Rightarrow xy = y^{-1}x^{-1} = yx$ en dit is onmogelijk omdat G niet-abels is. Bovendien geldt er dat $bab^{-1} = yxyy = yx = y^{-1}x^{-1} = a^{-1}$. Volgens de vorige stelling bestaat er dan een surjectief homomorfisme tussen D_n en G. Dan is de orde van G dus hoogstens $2n$. Bijgevolg is die orde juist gelijk aan $2n$ en is G isomorf met D_n. □

Gevolg 6.23. *Het homomorfe beeld van een dihaedergroep is altijd een dihaeder groep, want dit homomorfe beeld wordt voortgebracht door twee elementen met maximale orde 2. Als beide elementen orde twee hebben dan geldt volgens vorig resultaat dat het beeld een dihaedergroep* *is. Heeft 1 van de voortbrengende elementen echter orde 1 dan krijgen we een cyclische groep van orde 2 en deze is isomorf met* D_1.