

11. AUTOMORFISMEN EN SEMI-DIRECTE PRODUCTEN

*these images are almost tangible for the trained mind,
but are far removed from those that are given directly
by life and physical experience.*

Y.I. Manin*

De automorfismen $f : G \xrightarrow{\sim} G$ van groep G vormen een groep $\text{Aut}(G)$, de automorfismengroep van G . Hierbij is de bewerking de samenstelling van afbeeldingen. Ieder element g van G bepaalt een automorfisme van G :

$$\phi_g : G \longrightarrow G, \quad x \mapsto gxg^{-1}. \quad (1)$$

Deze automorfismen heten *inwendige* automorfismen en vormen een ondergroep $\text{Inn}(G)$ van $\text{Aut}(G)$. We bepalen nu eerst deze ondergroep.

(11.1) Stelling. *De groep $\text{Inn}(G)$ is een normaaldeeler van $\text{Aut}(G)$ en is isomorf met de quotiëntgroep $G/Z(G)$ met $Z(G)$ het centrum van G .*

Bewijs. De ondergroep $\text{Inn}(G)$ is een normaaldeeler wegens

$$\psi\phi_g\psi^{-1} = \phi_{\psi(g)} : x \mapsto \psi^{-1}(x) \mapsto g\psi^{-1}(x)g^{-1} \mapsto \psi(g)x\psi(g^{-1})$$

voor $\psi \in \text{Aut}(G)$. Dus $\psi\phi_g\psi^{-1} = \phi_{\psi(g)}$. Het homomorfisme $i : G \rightarrow \text{Aut}(G)$ gegeven door $g \mapsto \phi_g$, met ϕ_g als in (1), heeft als beeld $\text{Inn}(G)$. De kern bestaat uit die g waarvoor geldt $gxg^{-1} = x$ voor alle $x \in G$, d.w.z. $g \in Z(G)$. Dus $\ker(i) = Z(G)$ is een normaaldeeler en wegens de eerste isomorfstelling volgt $G/Z(G) \cong \text{Inn}(G)$.

(11.2) Voorbeelden.

i) $\text{Aut}(\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. Een automorfisme ϕ van \mathbb{Z} ligt vast door het beeld van 1 vanwege

$$\phi(n) = \underbrace{\phi(1 + 1 + \dots + 1)}_{n \times} = \underbrace{\phi(1) + \dots + \phi(1)}_{n \times} = n\phi(1)$$

en $\phi(-n) = -\phi(n)$. Het beeld van 1 moet een voortbrenger zijn. Er zijn in \mathbb{Z} precies twee voortbrengers: 1 en -1 . De identieke afbeelding e en de afbeelding α met $\alpha(n) = -n$ zijn automorfismen en $\alpha^2 = e$.

ii) $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Ook hier geldt dat een automorfisme ϕ van $\mathbb{Z}/n\mathbb{Z}$ vastligt door $\phi(\bar{1})$. Verder is er ook een element \bar{x} dat onder ϕ op $\bar{1}$ wordt afgebeeld, dus

$$\phi(\bar{x}) = x\phi(\bar{1}) = \bar{1}.$$

Dit betekent dat $\phi(1)$ in $(\mathbb{Z}/n\mathbb{Z})^*$ ligt. Dit levert een injectief homomorfisme

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^* \quad \text{met } \phi \mapsto \phi(1). \quad (2)$$

Omgekeerd is voor vaste $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$ de afbeelding $\psi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ met $\psi(\bar{m}) = m\bar{x}$ een automorfisme. Dit bewijst dat (2) surjectief is.

* Russisch wiskundige, werkzaam aan het Max-Planck-Institut für Mathematik in Bonn

De quotiëntgroep $\text{Aut}(G)/\text{Inn}(G)$ heet de groep van *uitwendige* automorfismen.

Laat G een groep zijn en $N \triangleleft G$ een normaaldeler. Ieder element $g \in G$ bepaalt een automorfisme van N :

$$\phi_g : N \rightarrow N, \quad n \mapsto gng^{-1}.$$

Dit automorfisme van N hoeft geen inwendig automorfisme van N te zijn als $g \notin N$. Het automorfisme ϕ_g geeft ons informatie hoe elementen van N commuteren met g . Het bewijs van de volgende stelling laat zien hoe die informatie gebruikt kan worden.

(11.3) Stelling. *Laat p en q twee verschillende priemgetallen zijn.*

- i) *Als G een groep is van orde p^2 dan $G \cong \mathbb{Z}/p^2\mathbb{Z}$ of $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*
- ii) *Als G een groep is van orde pq met $p < q$ en p deelt niet $q - 1$ dan is G cyclisch van orde pq .*

Bewijs. i) Kies een element $x \in G$ van orde p . Dat kan wegens de Stelling van Cauchy. Volgens (9.12) is $N = \langle x \rangle$ een normaaldeler van G . Laat nu $y \in G - N$. Als de orde van y gelijk is aan p^2 dan is $G = \langle y \rangle$ cyclisch van orde p^2 . Zoniet, dan is de orde van y gelijk aan p .

Beschouw dan de werking van y op N door conjugatie met y :

$$\psi = \phi_y|_N : N \rightarrow N, \quad \beta \mapsto y\beta y^{-1}.$$

Dit geeft een automorfisme van $N \cong \mathbb{Z}/p\mathbb{Z}$. Omdat $\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ is de orde van ψ een deler van $p - 1$. Anderzijds geldt

$$\psi^p(x) = y^p x y^{-p} = x$$

dus de orde van ψ deelt ook p . Dus de orde van ψ is 1. Maar dat betekent precies dat x en y commuteren. Dan is

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \rightarrow G, \quad (i, j) \mapsto x^i y^j$$

een isomorfisme (Ga na).

ii) Kies een element x van orde q en een element y van orde p . Dan is vanwege (9.12) de ondergroep $N = \langle x \rangle$ een normaaldeler van index p . Net als in deel i) beschouwen we conjugatie met y op N . De orde van ϕ_y is dan een deler van p en van $q - 1$, en dus gelijk aan 1. Dat betekent dat x en y commuteren. Dan is

$$\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \rightarrow G, \quad (i, j) \mapsto x^i y^j$$

een isomorfisme. (Ga na!) Dit bewijst de stelling.

De structuur van een groep laat zich veel beter begrijpen als we G kunnen schrijven als een direct product $G_1 \times G_2$ van twee andere groepen. Ter herinnering: het directe product van twee groepen G_1 en G_2 is het Cartesisch product

$$\{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

met de bewerking gegeven door

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 h_1, g_2 h_2).$$

In het geval van additief geschreven groepen noemt men het directe product vaak *directe som*. De notatie is dan $G_1 \oplus G_2$. Merk op dat G_1 en G_2 via de inclusies

$$\begin{aligned} j_1 : G_1 &\rightarrow G_1 \times G_2, & g_1 &\mapsto (g_1, e_2) \\ j_2 : G_2 &\rightarrow G_1 \times G_2, & g_2 &\mapsto (e_1, g_2) \end{aligned}$$

zijn op te vatten als ondergroepen van $G_1 \times G_2$. Het zijn zelfs normaaldelers en de doorsnede van deze normaaldelers is het eenheidselement (e_1, e_2) . Verder commuteren de elementen van G_1 en G_2 wanneer we ze opvatten als elementen van $G_1 \times G_2$.

Omgekeerd is het vinden van twee ondergroepen met zulke eigenschappen voldoende om een groep G te kunnen schrijven als direct product, zoals de volgende stelling laat zien.

(11.4) Stelling. *Laat G een groep zijn met ondergroepen H_1 en H_2 met de volgende eigenschappen:*

- i) $G = H_1 H_2 = \{h_1 h_2 : h_1 \in H_1, h_2 \in H_2\}$.
- ii) $H_1 \cap H_2 = \{e\}$.
- iii) $h_1 h_2 = h_2 h_1$ voor alle $h_1 \in H_1, h_2 \in H_2$.

Dan definieert $\pi : H_1 \times H_2 \rightarrow G$ met $\pi((h_1, h_2)) = h_1 h_2$ een isomorfisme.

Bewijs. Uit iii) volgt dat π een homomorfisme is:

$$\begin{aligned} \pi((h_1, h_2)(k_1, k_2)) &= \pi(h_1 k_1, h_2 k_2) = h_1 k_1 h_2 k_2 \stackrel{\text{iii)}}{=} h_1 h_2 k_1 k_2 \\ &= \pi((h_1, h_2)\pi(k_1, k_2)). \end{aligned}$$

Eigenschap i) impliceert dat π surjectief is en als $(h_1, h_2) \in \ker(\pi)$ dan volgt uit $h_1 h_2 = e$ dat $h_1^{-1} = h_2 \in H_1 \cap H_2 = \{e\}$ en dus dat $\ker(\pi) = \{e\}$. Dit bewijst de stelling.

(11.5) Voorbeelden.

- i) De groep \mathbb{C}^* is isomorf met het direct product van de ondergroepen $\mathbb{R}_{>0}^*$ en $S^1 = \{z \in \mathbb{C}^* : |z| = 1\}$.
- ii) De symmetriegroep van de kubus G_K heeft een ondergroep G_K^+ van rotaties en een ondergroep van orde 2 voortgebracht door de puntspiegeling rond de oorsprong. Deze spiegeling is de lineaire afbeelding $x \mapsto -x$ en die commuteert met alle andere lineaire afbeeldingen van \mathbb{R}^3 . Dit bewijst dat G_K een direct product is: $G_K \cong G_K^+ \times \{\pm\}$.

Bekijken we nu het voorbeeld van de groep $A = \{f_{a,b} : a \in \mathbb{R}^*, b \in \mathbb{R}\}$ van affine transformaties

$$f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto a x + b.$$

Het ligt voor de hand te kijken of A een direct product is van de ondergroepen $H_1 = \mathbb{R}$ en $H_2 = \mathbb{R}^*$. Maar de vermenigvuldiging is anders want het effect van $f_{a,b} \circ f_{c,d}$ is

$$\begin{aligned} x \mapsto cx + d &\mapsto a(cx + d) + b \\ &\mapsto acx + (b + ad). \end{aligned}$$

dus

$$(b, a) \circ (d, c) = (b + ad, ac).$$

Er geldt hier niet $h_1 h_2 = h_2 h_1$, maar voor vaste $h_2 = a$ is de afbeelding $h_1 \mapsto h_2 h_1 h_2^{-1}$ een automorfisme van de normaaldeeler $H_1 = \mathbb{R}$ gegeven door $d \mapsto ad$.

Dit is een voorbeeld van een semi-direct product

(11.6) Definitie-Stelling. *Laat H en N twee groepen zijn en $\phi : H \rightarrow \text{Aut}(N)$ een homomorfisme. Het semi-directe product $N \rtimes_{\phi} H$ is de verzameling paren $\{(n, h) : n \in N, h \in H\}$ met als bewerking*

$$(n_1, h_1) \circ (n_2, h_2) = (n_1 \phi(h_1)(n_2), h_1 h_2).$$

Dit is een groep.

Bewijs. We moeten nagaan dat het semi-directe product een groep is. De associativiteit van de bewerking volgt uit het feit dat ϕ een homomorfisme is:

$$\begin{aligned} ((n_1, h_1) \circ (n_2, h_2)) \circ (n_3, h_3) &= (n_1 \phi(h_1)(n_2), h_1 h_2) \circ (n_3, h_3) \\ &= (n_1 \phi(h_1)(n_2) \phi(h_1 h_2)(n_3), (h_1 h_2) h_3) \end{aligned}$$

en

$$\begin{aligned} (n_1, h_1) \circ ((n_2, h_2) \circ (n_3, h_3)) &= (n_1, h_1) \circ (n_2 \phi(h_2)(n_3), h_2 h_3) = \\ &= (n_1 \phi(h_1)(n_2 \phi(h_2)(n_3)), h_1 (h_2 h_3)) \end{aligned}$$

wat hetzelfde is wegens

$$\phi(h_1)(n_2) \phi(h_1 h_2)(n_3) = \phi(h_1)(n_2 \phi(h_2)(n_3)).$$

Het eenheidselement is (e_N, e_H) en de inverse van (n, h) is $(\phi(h^{-1})(n^{-1}), h^{-1})$.

De notatie is $N \rtimes_{\phi} H$ of $H \ltimes_{\phi} N$. Soms wordt de werking van $\phi(h)$ op N geschreven als

$$n \mapsto n^{\phi(h)}.$$

Het volgende criterium is het analogon van (11.4) voor semi-directe producten.

(11.7) Stelling. *Laat G een groep zijn met ondergroepen N en H zodat*

- i) $N \triangleleft G$,
- ii) $G = NH$,
- iii) $N \cap H = \{e\}$.

Laat $\phi : H \rightarrow \text{Aut}(N)$ het homomorfisme zijn met $n \xrightarrow{\phi(h)} hnh^{-1}$. Dan is de afbeelding

$$\pi : N \rtimes_{\phi} H \longrightarrow G \quad \text{met } \pi((n, h)) = nh$$

een isomorfisme.

Bewijs. De afbeelding π is een homomorfisme; dit volgt uit de identiteit

$$n_1 h_1 n_2 h_2 = n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\phi(h_1)(n_2)} h_1 h_2.$$

voor elementen n_1, h_1, n_2, h_2 van G . De surjectiviteit en injectiviteit volgen als in het bewijs van (11.4).

(11.8) Voorbeeld.

- i) De groep van affine transformaties $f_{a,b} : x \mapsto ax + b$ is isomorf met het semi-directe product $\mathbb{R} \rtimes_{\phi} \mathbb{R}^*$ waarbij $\phi(a) : \mathbb{R} \rightarrow \mathbb{R}$ gegeven is door $b \mapsto ab$.
- ii) De diëdergroep D_n is het semi-directe product van een cyclische groep $N = \langle r \rangle$ van orde n en een cyclische groep $H = \langle s \rangle$ van orde 2 met de relatie $sr s^{-1} = r^{-1}$.

Opgaven

1) Laat G een eindige groep zijn met $\#G > 2$. Bewijs dat $\text{Aut}(G)$ tenminste twee elementen heeft.

2) Laat G een groep zijn en $n \in \mathbb{Z}_{\geq 1}$. Bewijs: de ondergroep

$$\langle \{g^n : g \in G\} \rangle$$

voortgebracht door de n -de machten van elementen van G is een karakteristieke ondergroep (dwz een ondergroep die onder ieder automorfisme van G in zich gaat).

3) Laat $\text{GL}_n(\mathbb{R})$ de groep van $n \times n$ matrices met determinant ongelijk 0. Laat verder

$$\text{SL}_n(\mathbb{R}) = \{M \in \text{GL}_n(\mathbb{R}) : \det(M) = 1\}.$$

Bewijs dat $\text{SL}_n(\mathbb{R})$ een normaaldeler is en dat $\text{GL}_n(\mathbb{R}) \cong \text{SL}_n(\mathbb{R}) \times \mathbb{R}^*$.

4) Laat $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ zijn met de bewerking

$$(x, y) \circ (x', y') = (x + (-1)^y x', y + y').$$

Bewijs dat dit een groep definieert. Schrijf G als een semi-direct product.

5) Laat N_1, \dots, N_k normaaldelers van een groep G zijn met $D = \bigcap_{i=1}^k N_i$ de doorsnede. Laat zien dat D een normaaldeler van G is en dat G/D isomorf is met een ondergroep van $G/N_1 \times \dots \times G/N_k$.

6) Laat G_1 en G_2 eindige groepen zijn met $\text{ggd}(\#G_1, \#G_2) = 1$. Bewijs dat geldt $\text{Aut}(G_1 \times G_2) \cong \text{Aut}(G_1) \times \text{Aut}(G_2)$.