Hyperoplosbare groepen

Kiliç, A.Y.

HYPEROPLOSBARE GROEPEN

A. YASIR KILIÇ

Bachelorscriptie Wiskunde
Begeleider: prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden

23 augustus 2013

INHOUDSOPGAVE

1 INLEIDING

Zij G een groep. We noemen G *oplosbaar* als er een niet-negatief geheel getal t bestaat en een keten van ondergroepen

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\},$$

zodanig dat voor alle $i = 0, \ldots, t-1$ de groep G_{i+1} normaal is in G_i en G_i/G_{i+1} abels is. In deze bachelorscriptie zullen wij onze aandacht vestigen op een specifieke klasse van oplosbare groepen, de zogenaamde *hyperoplosbare* groepen.

Een groep G heet hyperoplosbaar wanneer er een keten zoals hierboven bestaat met de aanvullende eigenschappen dat voor alle $i = 0, \ldots, t-1$ de groep G_{i+1} normaal is in de hele groep G en G_i/G_{i+1} cyclisch is. Wij zullen ons in deze verhandeling voornamelijk beperken tot eindige hyperoplosbare groepen.

In hoofdstuk 2 behandelen we een aantal basiseigenschappen van hyperoplosbare groepen. Vervolgens zullen we de relatie van hyperoplosbare groepen met p-*groepen* bestuderen. Een p-groep (p is een priemgetal) is een groep waarvan de orde gelijk is aan p^i met i een niet-negatief geheel getal. We zullen zien dat elke p-groep hyperoplosbaar is, en dat een hyperoplosbare groep isomorf is met een *herhaald semidirect product* van eindig veel p-groepen. Wat we onder een herhaald semidirect product verstaan zullen we in hoofdstuk 3 uitleggen, en we laten zien dat dit begrip een natuurlijke generalisatie is van een semidirect product van twee groepen. Een van de hoofdresultaten van deze scriptie beschrijft welke herhaalde semidirecte producten hyperoplosbaar zijn.

Voor een groep G kunnen we inductief ondergroepen $G_{(0)}, G_{(1)}, \ldots$ definiëren door $G_{(0)} = G$ en $G_{(i+1)} = [G_{(i)}, G_{(i)}]$. Dan geldt: G is oplosbaar dan en slechts dan als er een niet-negatief geheel getal t bestaat waarvoor $G_{(t)} = \{1\}$. De vraag rijst of er een vergelijkbare toets bestaat of een groep hyperoplosbaar is. In de literatuur [1] kan men een toets vinden die voor een eindige groep G uitgaande van de triviale ondergroep $\{1\}$ een keten van stijgende ondergroepen construeert met de volgende eigenschap: G is hyperoplosbaar dan en slechts dan als G in deze keten voorkomt.

In hoofdstuk 4 zullen wij een toets voor eindige groepen presenteren waarmee we de zaken van 'bovenaf' aanpakken. Dat wil zeggen dat wij uitgaan van een eindige groep G en vervolgens een keten van dalende ondergroepen construeren die de volgende eigenschap heeft: G is hyperoplosbaar dan en slechts dan als $\{1\}$ in onze keten voorkomt.

2 HYPEROPLOSBAARHEID EN SYLOWFAMILIES

2.1 EIGENSCHAPPEN VAN HYPEROPLOSBARE GROEPEN

Een groep G heet *hyperoplosbaar* als er een $t \in \mathbf{Z}, t \geqslant 0$ en een keten van ondergroepen van G

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}$$

bestaan zodanig dat voor alle $i \in \{0, \ldots, t-1\}$ geldt: $G_i \trianglelefteq G$ en G_i/G_{i+1} is cyclisch. Een dergelijke keten noemen we een *hyperoplosbaarheidsketen* van G.

Lemma 2.1. Laat G hyperoplosbaar zijn en

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}$$

een hyperoplosbaarheidsketen van G. Laat $H, N \subseteq G$ ondergroepen zijn en $N \trianglelefteq G$. Dan geldt:

i. De groep H is hyperoplosbaar en de keten van ondergroepen

$$H = H \cap G_0 \supseteq H \cap G_1 \supseteq \ldots \supseteq H \cap G_t = \{1\}$$

is een hyperoplosbaarheidsketen van H.

ii. De groep G/N is hyperoplosbaar en de keten van ondergroepen

$$G/N = (NG_0)/N \supseteq (NG_1)/N \supseteq \ldots \supseteq (G_tN)/N = N/N$$

is een hyperoplosbaarheidsketen van G/N.

Bewijs. Het bewijs is rechttoe rechtaan en wordt aan de lezer overgelaten. □

Propositie 2.2. Elke eindige nilpotente groep G is hyperoplosbaar.

Bewijs. Zij $n = \#G$. We geven een bewijs met behulp van volledige inductie naar n. Voor $n = 1$ is de stelling triviaal, neem daarom aan dat $n > 1$. Merk op dat $Z(G) \neq \{1\}$ en kies een niet-triviaal element $z \in Z(G)$. Uit de inductiehypothese volgt dat $G/\langle z \rangle$ een hyperoplosbaarheidsketen heeft. Van de ondergroepen die in deze keten voorkomen kunnen we het inverse beeld nemen onder de kanonieke afbeelding $\pi : G \to G/\langle z \rangle$. Dit geeft vervolgens een keten

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \langle z \rangle$$

van ondergroepen die normaal zijn in G en waarvan ieder opeenvolgend quotiënt cyclisch is. Door de triviale groep erachteraan te plakken krijgen we een hyperoplosbaarheidsketen van G. □

Voor een priemgetal p definiëren we een p-*groep* als een groep waarvan de orde gelijk is aan p^i voor een zekere $i \in \mathbf{Z}, i \geqslant 0$. Het is welbekend dat p-groepen nilpotent zijn. Dus we hebben:

Gevolg 2.3. Zij p een priemgetal. Dan is elke p-groep hyperoplosbaar.

Het zij opgemerkt dat propositie 2.2 onjuist is als we ook oneindige groepen toelaten. Uit de definitie van hyperoplosbaarheid volgt namelijk rechtstreeks dat hyperoplosbare groepen eindig voortgebracht zijn. Er bestaan echter ook nilpotente groepen (zelfs abelse groepen) die niet eindig zijn voortgebracht.

Wij attenderen de lezer erop dat uit de hyperoplosbaarheid van $N \trianglelefteq G$ en G/N in het algemeen niet geconcludeerd kan worden dat G hyperoplosbaar is. De alternerende groep A_4 op vier elementen levert een tegenvoorbeeld:

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4.$$

De ondergroep V_4 is nilpotent (zelfs abels) en dus wegens propositie 2.2 hyperoplosbaar. Hetzelfde geldt voor A_4/V_4. Echter, A_4 is — zoals we verderop zullen zien — niet hyperoplosbaar.

Een ondergroep $N \subseteq G$ heet G-*hyperoplosbaar* wanneer N een hyperoplosbaarheidsketen

$$N = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_t = \{1\}$$

heeft waarvoor geldt: $N_i \trianglelefteq G$ voor alle $i \in \{0, \ldots, t-1\}$.

Propositie 2.4. Laat G een groep zijn en $N \trianglelefteq G$ een normale ondergroep. Dan geldt: G is hyperoplosbaar dan en slechts dan als N een G-hyperoplosbare groep is met G/N hyperoplosbaar.

Bewijs. [$\Rightarrow$] Dit volgt uit lemma 2.1.

[$\Leftarrow$] Beschouw een hyperoplosbaarheidsketen van N

$$N = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_t = \{1\}$$

met $N_i \trianglelefteq G$ voor alle $i \in \{0, \ldots, t-1\}$. Een hyperoplosbaarheidsketen van G/N induceert een keten

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = N$$

door inverse beelden te nemen onder de quotiëntafbeelding $G \to G/N$. Deze laatstgenoemde keten bestaat uit normale ondergroepen van G en opeenvolgende quotiënten zijn cyclisch. Door de keten voor N erachteraan te plakken krijgen we een hyperoplosbaarheidsketen van G. $\square$

Gevolg 2.5. Laat G_1 en G_2 hyperoplosbare groepen zijn. Dan geldt: $G = G_1 \times G_2$ is hyperoplosbaar.

Bewijs. Observeer dat $G_1 \times \{1\} \subseteq G$ een G-hyperoplosbare groep is waarvoor de quotiëntgroep $G/(G_1 \times \{1\}) \cong G_2$ ook hyperoplosbaar is. Het gevraagde volgt nu uit propositie 2.4. □

Lemma 2.6. Zij G een eindige hyperoplosbare groep. Dan heeft G een hyperoplosbaarheidsketen

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}$$

met de eigenschap dat voor alle $i \in \{0, \ldots, t-1\}$ de index $p_i = \#(G_i/G_{i+1})$ priem is en voor alle $i, j \in \{0, \ldots, t-1\}$, $i < j$ geldt: $p_i \leqslant p_j$.

Bewijs. Beschouw een hyperoplosbaarheidsketen van G waarin twee opeenvolgende ondergroepen $H \supseteq K$ in voorkomen en zet $\#(H/K) = p_1 \cdots p_n$ met $p_1, \ldots, p_n$ niet noodzakelijkerwijs verschillende priemen. De cyclische groep H/K heeft een keten van karakteristieke ondergroepen

$$H/K = C_0 \overset{p_1}{\supseteq} C_1 \overset{p_2}{\supseteq} \ldots \overset{p_n}{\supseteq} C_n = \{1\}.$$

Deze correspondeert met een keten van normale ondergroepen in G

$$H = N_0 \overset{p_1}{\supseteq} N_1 \overset{p_2}{\supseteq} \ldots \overset{p_n}{\supseteq} N_n = K.$$

Hieruit volgt dat er een hyperoplosbaarheidsketen van G bestaat waarin ieder quotiënt van twee opeenvolgende ondergroepen een cyclische groep van priemorde is. Stel nu dat we in een dergelijke keten een deelketen $H \overset{q}{\supseteq} J \overset{p}{\supseteq} L$ tegenkomen met p, q priem en $p < q$. Merk op dat H/L een groep is van orde pq en dat deze een ondergroep K' van orde q heeft. Er geldt: $K' \trianglelefteq H/L$, immers de index van K' in H/L is de kleinste priemdeler van $\#(H/L)$. Omdat $\#K'$ en $\#(H/L)$ copriem zijn volgt dat K' zelfs een karakteristieke ondergroep is. Dit impliceert dat het inverse beeld K van K' onder $H \to H/L$ normaal is in G is met $H \overset{p}{\supseteq} K \overset{q}{\supseteq} L$. Uit het voorgaande volgt dat er een hyperoplosbaarheidsketen van G bestaat die voldoet aan het gevraagde. □

Gevolg 2.7. Zij G een eindige hyperoplosbare groep met $\#G > 1$ en q de grootste priemdeler van $\#G$. Dan heeft G een normale Sylow-q-ondergroep.

Bewijs. Laat q^e de grootste q-macht zijn die $\#G$ deelt. Beschouw een hyperoplosbaarheidsketen van G als in lemma 2.6, zeg

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}.$$

Dan is G_{t-e} een normale Sylow-q-ondergroep van G. □

Voorbeeld. Beschouw de alternerende groep A_4 op 4 elementen. Uit lemma 2.6 volgt gemakkelijk dat deze niet hyperoplosbaar is, immers A_4 bevat geen ondergroep van index 2.

Stelling 2.8. Zij G een hyperoplosbare groep. Dan is $G' = [G, G]$ nilpotent.

Bewijs. Beschouw een hyperoplosbaarheidsketen

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}.$$

Door elk van deze ondergroepen met G' te doorsnijden krijgen we wegens lemma 2.1 een hyperoplosbaarheidsketen van G':

$$G' = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_t = \{1\}.$$

Elk van de ondergroepen in de keten is een doorsnijding van twee normale ondergroepen van G, en daarom zelf ook normaal in G. Hieruit volgt dat we voor alle $i = 0, \ldots, t-1$ een conjugatiewerking van G op H_i/H_{i+1} hebben. De automorfismengroep van H_i/H_{i+1} is abels, dus deze werking factoriseert via G/G'. In het bijzonder geldt dat $H_i/H_{i+1} \subseteq Z(G'/H_{i+1})$. Dus de bovenstaande keten is een centrale rij voor G'. □

2.2 SYLOWFAMILIES

Zij G een eindige groep en $\mathcal{P}$ de verzameling priemgetallen. Een *Sylowfamilie* van G is een familie ondergroepen $(S_p)_{p \in \mathcal{P}}$ met de volgende eigenschappen:

- voor alle $p \in \mathcal{P}$ geldt: $S_p \subseteq G$ is een Sylow-p-ondergroep;
- voor alle $p, q \in \mathcal{P}, p < q$ geldt: S_p normaliseert S_q, i.e. voor alle $g \in S_p$ geldt: $gS_q g^{-1} = S_q$.

Lemma 2.9. Zij G een eindige groep, $(S_p)_{p \in \mathcal{P}}$ een Sylowfamilie van G en $\mathcal{P}' \subseteq \mathcal{P}$ een deelverzameling. Dan geldt: $\#\langle S_p : p \in \mathcal{P}' \rangle = \prod_{p \in \mathcal{P}'} \# S_p$ en de familie ondergroepen $(S'_p)_{p \in \mathcal{P}}$ met $S'_p = S_p$ als $p \in \mathcal{P}'$ en $S'_p = \{1\}$ als $p \notin \mathcal{P}'$ is een Sylowfamilie van $\langle S_p : p \in \mathcal{P}' \rangle$.

Bewijs. Het bewijs laten we aan de lezer over. □

Notatie. Zij $(S_p)_{p \in \mathcal{P}}$ een Sylowfamilie van G en $\mathcal{P}' \subseteq \mathcal{P}$ een deelverzameling. Met de notatie $(S_p)_{p \in \mathcal{P}'}$ zullen we de Sylowfamilie van $\langle S_p : p \in \mathcal{P}' \rangle \subseteq G$ aangeven die men verkrijgt door in $(S_p)_{p \in \mathcal{P}}$ alle Sylow-p-ondergroepen S_p met $p \notin \mathcal{P}'$ te vervangen door de triviale ondergroep.

Stelling 2.10 (Schur–Zassenhaus)**.** Zij G een eindige groep, $N \trianglelefteq G$ een normale ondergroep met $\#N$ en $\#(G/N)$ copriem. Dan heeft N een complement in G. Als we ook aannemen dat N of G/N oplosbaar is, dan is elk tweetal complementen van N geconjugeerd in G.

Bewijs. Zie [3, stelling 3.8 en 3.12]. □

Lemma 2.11. Zij G een eindige groep en $\mathcal{S} = (S_p)_{p \in \mathcal{P}}$ en $\mathcal{T} = (T_p)_{p \in \mathcal{P}}$ twee Sylowfamilies van G. Dan bestaat er een $g \in G$ zodanig dat voor alle $p \in \mathcal{P}$ geldt: $gS_pg^{-1} = T_p$.

Bewijs. Laat $n = \#G$. We bewijzen het lemma met behulp van volledige inductie naar n. De stelling is triviaal voor $n = 1$, dus neem aan dat $n > 1$ en laat q de grootste priemfactor van n zijn. Observeer dat S_q normaal is in G. Dan is S_q de unieke Sylow-q-ondergroep van G, dus we hebben $S_q = T_q$. Merk vervolgens op dat

$$H_{\mathcal{S}} = \langle S_p : p < q \rangle, \quad \text{en} \quad H_{\mathcal{T}} = \langle T_p : p < q \rangle,$$

complementen zijn van S_q in G wegens lemma 2.9. Omdat S_q oplosbaar is kunnen we stelling 2.10 toepassen, en hieruit volgt dat $gH_{\mathcal{S}}g^{-1} = H_{\mathcal{T}}$ voor een zekere $g \in G$. Dus $(gS_pg^{-1})_{p<q}$ en $(T_p)_{p<q}$ zijn Sylowfamilies voor $H_{\mathcal{T}}$. De inductiehypothese toegepast op $H_{\mathcal{T}}$ impliceert nu dat er een $h \in H_{\mathcal{T}}$ bestaat zodanig dat voor alle $p \in \mathcal{P}, p < q$ geldt: $h(gS_pg^{-1})h^{-1} = T_p$. Uit het voorgaande concluderen we dat $hg(S_q)(hg)^{-1} = S_q = T_q$ (wegens de normaliteit van S_q) en dat voor alle $p \in \mathcal{P}, p < q$ geldt: $(hg)S_p(hg)^{-1} = T_p$. Dit bewijst het gevraagde. □

Stelling 2.12. Zij G een eindige hyperoplosbare groep. Dan heeft G een Sylowfamilie.

Bewijs. Zij $n = \#G$. We geven een bewijs met behulp van volledige inductie naar n. Voor $n = 1$ is de bewering triviaal, dus stel dat $n > 1$ en laat q de grootste priemdeler van n zijn. Wegens gevolg 2.7 heeft G een normale Sylow-q-ondergroep S_q. De stelling van Schur-Zassenhaus (stelling 2.10) impliceert dat S_q een complement H heeft in G. Er geldt dat H hyperoplosbaar is (gebruik lemma 2.1), en uit de inductiehypothese volgt dan dat H een Sylowfamilie $\mathcal{S}'$ heeft. Door in deze Sylowfamilie de triviale Sylow-q-ondergroep te vervangen door S_q verkrijgen we een Sylowfamilie van G. □

3 SEMIDIRECTE PRODUCTEN

In paragraaf 2 van dit hoofdstuk zullen we de definitie van het semidirecte product veralgemenen zodat we ook kunnen spreken over semidirecte producten van meer dan twee groepen (of zelfs oneindig veel groepen). Ter motivatie echter beginnen wij in de volgende paragraaf met een definitie van het semidirecte product van twee groepen. Ten slotte laten wij in de laatste paragraaf zien welke herhaalde semidirecte producten hyperoplosbaar zijn.

3.1 SEMIDIRECT PRODUCT VAN TWEE GROEPEN

Laat N en H groepen zijn en $\phi : H \to \mathrm{Aut}(N)$ een homomorfisme (we noteren $\phi(h)(n)$ met ${}^h n$). We definiëren een categorie $\mathcal{C}$ waarvan een *object* bestaat uit een groep G tezamen met groepshomomorfismen $\nu : N \to G$ en $\eta : H \to G$ die voldoen aan de voorwaarde dat voor alle $h \in H, n \in N$ geldt:

$$\nu({}^h n) = \eta(h)\nu(n)\eta(h)^{-1}.$$

In het vervolg zullen we ν en η met het lege symbool weergeven (i.e. het beeld van $n \in N$ en $h \in H$ in G noteren we als respectievelijk n en h). Laat G en G' twee objecten zijn uit $\mathcal{C}$. Een *morfisme* van G naar G' is een groepshomomorfisme $f : G \to G'$ zodanig dat het onderstaande diagram commuteert.

$$\begin{tikzcd} & N \arrow[dl] \arrow[dr] & \\ G \arrow[rr, "f"] & & G' \\ & H \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Een *semidirect product van* N *en* H *met betrekking tot* ϕ is een object G uit deze categorie dat de volgende universele eigenschap bezit: voor ieder object G' uit $\mathcal{C}$ is er een uniek morfisme van G naar G'.

Stelling 3.1. Het semidirecte product G van N en H met betrekking tot $\phi\colon H \to \mathrm{Aut}(N)$ bestaat. Bovendien geldt: het tripel bestaande uit G en de homomorfismen $N \to G$ en $H \to G$ is uniek op een uniek isomorfisme na.

Bewijs. De uniciteit volgt uit een welbekend categorisch argument. De existentie is eenvoudig te bewijzen. Men kan bijvoorbeeld G definiëren door voortbrengers en relaties. Als voortbrengersverzameling hebben we dan de disjuncte vereniging van N en H; als relaties hebben we enerzijds de groepsrelaties uit N en H, anderzijds de relaties van de vorm $hnh^{-1}({}^hn)^{-1}$ waarbij $h \in H$ en $n \in N$. $\square$

Stelling 3.1 rechtvaardigt dat we voortaan spreken over *het* semidirecte product van N en H met betrekking tot ϕ. We noteren dit semidirecte product ook wel met $N \rtimes_\phi H$ (of simpelweg met $N \rtimes H$; de context maakt dan duidelijk wat het bijbehorende homomorfisme $H \to \mathrm{Aut}(N)$ is).

Het bovenstaande bewijs is zonder meer correct maar geeft ons geen enkel idee over de structuur van $N \rtimes H$. Een vruchtbaarder aanpak is om een semidirect product te construeren. De klassieke constructie wordt gegeven door een geschikte vermenigvuldiging te definiëren op de verzameling $N \times H$. Ter motivatie van wat zal volgen laten wij hier een andere constructie zien.

Constructie van het semidirecte product.
Beschouw de verzameling $\Omega = N \times H$ en laat $\nu : N \to \mathrm{Sym}(\Omega)$ en $\eta : H \to \mathrm{Sym}(\Omega)$ gegeven zijn door

$$\nu(n)(m,k) = (nm,k), \qquad \eta(h)(m,k) = ({}^hm, hk),$$

met $n \in N, h \in H$ en $(m,k) \in \Omega$. Het is makkelijk te verifiëren dat de bovenstaande afbeeldingen trouwe acties van N en H definiëren op Ω. Zet $N_0 = \nu[N]$ en $H_0 = \eta[H]$, dus we hebben $N \cong N_0$ en $H \cong H_0$, en laat $G = \langle N_0, H_0 \rangle$. We zullen hierna ν en η met het lege symbool noteren. Voor alle $n \in N, h \in H$ en alle $(m,k) \in \Omega$ geldt:

$$\begin{aligned}
\left(hnh^{-1}\right)(m,k) &= (hn)\left({}^{h^{-1}}m, h^{-1}k\right)\\
&= h\left(n\,{}^{h^{-1}}m, h^{-1}k\right)\\
&= \left({}^hnm, k\right)\\
&= \left({}^hn\right)(m,k)
\end{aligned}$$

Dus volgt: $hnh^{-1} = {}^hn$. We zien dat $N_0 \trianglelefteq G$ en $G = N_0H_0$. Stel nu dat $n = h$ voor een zekere $n \in N$ en $h \in H$. Dan geldt

$$(n,1) = n(1,1) = h(1,1) = (1,h).$$

Dus $n = h = \mathrm{id}_\Omega$ en we hebben dat $N_0 \cap H_0 = \{\mathrm{id}_\Omega\}$. Uit het voorgaande volgt gemakkelijk dat ieder element van G op unieke wijze te schrijven is als een product nh.

Beschouw nu een groep G' en homomorfismen $N \to G'$ en $H \to G'$ (die we met het lege symbool zullen noteren) zodanig dat $hnh^{-1} = {}^hn$ in G'. De afbeelding $f : G \to G' : nh \mapsto nh$ is welgedefinieerd. Het is makkelijk te verifiëren dat f een groepshomomorfisme is. Bovendien is duidelijk dat f het enige homomorfisme $G \to G'$ is zodat het diagram

$$\begin{tikzcd} & N \arrow[dl] \arrow[dr] & \\ G \arrow[rr, "f"] & & G' \\ & H \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commuteert. We concluderen dat G het semidirecte product van N en H met betrekking tot ϕ is. $\square$

Observeer dat de afbeelding $G \to \Omega$ gegeven door $nh \mapsto (n,h)$ een bijectie is. Via deze bijectie kunnen we een groepsstructuur transporteren naar Ω. De geïnduceerde groepsbewerking op Ω wordt dan gegeven door

$$(n,h)\cdot(n',h') = (n^h n', hh'),$$

en dit komt overeen met de klassieke constructie van het semidirecte product. Men kan zich afvragen wat het nut is geweest om de groep $\mathrm{Sym}(\Omega)$ te betrekken voor de bovenstaande constructie. Het antwoord is simpel: we hoeven niet meer de groepsaxioma's te verifiëren. Deze aanpak zal vooral in de volgende paragraaf zijn meerwaarde tonen.

3.2 HERHAALDE SEMIDIRECTE PRODUCTEN

Zij $(I, \leqslant)$ een totaal geordende verzameling, $(G_i)_{i \in I}$ een familie groepen en $\Phi = (\phi_{ij})_{i,j \in I, i<j}$ een familie groepshomomorfismen $\phi_{ij} : G_i \to \mathrm{Aut}(G_j)$. Voor alle $i, j \in I, i < j$ en $x \in G_i$ en $y \in G_j$ voeren we de volgende notatie in: ${}^x y = \big(\phi_{ij}(x)\big)(y)$. We definiëren vervolgens een categorie $\mathcal{C}$. Een *object* van $\mathcal{C}$ bestaat uit een groep G tezamen met een familie homomorfismen $\pi_i : G_i \to G$ zodanig dat voor alle $i, j \in I, i < j$ en voor alle $x \in G_i, y \in G_j$ geldt:

$$\pi_i(x)\pi_j(y)\pi_i(x)^{-1} = \pi_j({}^x y).$$

Hierna noteren we de afbeeldingen π_i met het lege symbool. Voor twee objecten G en G' uit $\mathcal{C}$ definiëren we een *morfisme* van G naar G' als een groepshomomorfisme $G \to G'$ zodanig dat voor alle $i \in I$ het onderstaande diagram commuteert.

$$\begin{tikzcd} G \arrow[rr, "f"] & & G' \\ & G_i \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Een *herhaald semidirect product van* $(G_i)_{i\in I}$ *met betrekking tot* Φ is een object G uit deze categorie dat de volgende universele eigenschap bezit: voor ieder object G' uit $\mathcal{C}$ is er een uniek morfisme van G naar G'. Voor het gemak zullen we soms kortweg van een herhaald semidirect product van de groepen $(G_i)_{i\in I}$ spreken als dit niet tot verwarring leidt.

Stelling 3.2. Laat $I, (G_i)_{i\in I}$ en Φ zijn zoals hierboven. Dan bestaat het herhaalde semidirecte product G van de familie $(G_i)_{i\in I}$ met betrekking tot Φ. Bovendien geldt: het paar bestaande uit G en de familie homomorfismen $G_i \to G$ is uniek op een uniek isomorfisme na.

Bewijs. Het bewijs is analoog aan dat van stelling 3.1. Voor de existentie definiëren we G door voortbrengers en relaties. Als voortbrengersverzameling nemen we de disjuncte vereniging van de groepen G_i; als relaties nemen we voor alle $i \in I$ de groepsrelaties uit G_i, en voor alle $i, j \in I, i < j$ de relaties van de vorm $xyx^{-1}({}^{x}y)^{-1}$ waarbij $x \in G_i$ en $y \in G_j$. □

Wegens de bovenstaande stelling spreken we vanaf nu over *het* herhaalde semidirecte product van de groepen $(G_i)_{i\in I}$, en noteren dit met $G = \rtimes_{i\in I} G_i$ (dit is uiteraard een incomplete notatie omdat de onderlinge acties van de groepen niet worden aangegeven; de context maakt duidelijk welke onderlinge acties betrokken zijn). Verder is het makkelijk in te zien dat als $\#I = 2$, de definitie van een herhaald semidirect product overeenkomt met het semidirecte product van twee groepen. In het geval dat I eindig is zullen we ook de notatie $G_1 \rtimes \ldots \rtimes G_n$ hanteren.

Het is a priori niet duidelijk hoe we over de elementen van G moeten nadenken. Het onderstaande voorbeeld maakt duidelijk dat in het algemeen *niet* geldt dat de natuurlijke homomorfismen $G_i \to \rtimes_{i\in I} G_i$ injectief zijn.

Voorbeeld. Zij $A = \langle a\rangle, B = \langle b\rangle$ en $C = \langle c\rangle$ cyclische groepen van respectievelijk ordes $7, 3$ en 2. De werking van B op A wordt gegeven door ${}^{b}a = a^2$, en C werkt op A en B door inversie. Beschouw vervolgens het herhaalde semidirecte product $G = A \rtimes B \rtimes C$ met betrekking tot deze acties. Er geldt in G dat

$$\begin{aligned}
{}^{c}({}^{b}a) &= {}^{c}(a^2) = a^5;\\
{}^{c}({}^{b}a) &= c(bab^{-1})c^{-1} = (cbc^{-1})(cac^{-1})(cb^{-1}c^{-1})\\
&= {}^{({}^{c}b)}({}^{c}a) = {}^{b^{-1}}(a^{-1}) = a^3.
\end{aligned}$$

Dus in de groep G hebben we dat $a^5 = a^3$ en hieruit volgt $a = 1$. We zien dat het natuurlijke homomorfisme $A \to G$ triviaal is.

Lemma 3.3. Laat $I, (G_i)_{i\in I}, \Phi$ en $\mathcal{C}$ zijn zoals hierboven en zij G het herhaalde semidirecte product van $(G_i)_{i\in I}$ met betrekking tot Φ. Dan geldt: elk element $g \in G$ is te schrijven als een eindig (en mogelijkerwijs leeg) product

$$x_{i_1} \cdots x_{i_n},$$

zodanig dat $i_1, \ldots, i_n \in I, i_1 > \ldots > i_n$ en dat voor alle $j = 1, \ldots, n$ geldt: $x_{i_j} \in G_{i_j}$ en $x_{i_j} \neq 1$ in G_{i_j}.

Bewijs. Laat H de ondergroep van G zijn voortgebracht door de beelden van G_i in G. Observeer dat H ook een object uit $\mathcal{C}$ is en dat de inclusie $H \to G$ een morfisme in $\mathcal{C}$ is. Hieruit volgt gemakkelijk dat H ook de universele eigenschap van G heeft en wegens stelling 3.2 zijn H en G isomorf in $\mathcal{C}$. Maar dan wordt G voortgebracht door de beelden van G_i in G en we concluderen dat $H = G$.

Het voorgaande impliceert dat elk element uit G geschreven kan worden als een eindig (en mogelijkerwijs leeg) product van elementen $x_i \in G_i$ met $i \in I$. In dit product kunnen we het eenheidselement weglaten; voor $i \in I$ en $x, y \in G_i$ kunnen we xy vervangen door z met $z = xy \in G_i$; voor $i, j \in I, i < j$ en $x \in G_i, y \in G_j$ kunnen we xy vervangen door ${}^x y x$. Door het voorgaande herhaaldelijk toe te passen zien we dat elk element van G de gevraagde schrijfwijze heeft. □

Stelling 3.4. Laat $I, (G_i)_{i \in I}, \Phi$ en $\mathcal{C}$ zijn zoals hierboven en beschouw een object G uit $\mathcal{C}$ met de eigenschap dat elk element $g \in G$ op *unieke* wijze te schrijven is als een eindig (en mogelijkerwijs leeg) product

$$x_{i_1} \cdots x_{i_n},$$

zodanig dat $i_1, \ldots, i_n \in I, i_1 > \ldots > i_n$ en dat voor alle $j = 1, \ldots, n$ geldt: $x_{i_j} \in G_{i_j}$ en $x_{i_j} \neq 1$ in G_{i_j}. Dan geldt: $G = \rtimes_{i \in I} G_i$.

Bewijs. Laat $H = \rtimes_{i \in I} G_i$, dan volgt uit de universele eigenschap van H dat er een uniek morfisme $f : H \to G$ in $\mathcal{C}$ is. Uit lemma 3.3 volgt dat elk element uit H geschreven kan worden als $x_{i_1} \cdots x_{i_n}$, met $i_1, \ldots, i_n \in I, i_1 > \ldots > i_n$ en voor alle $j = 1, \ldots, n : x_{i_j} \in G_{i_j}$ en $x_{i_j} \neq 1$ in G_{i_j}. Deze schrijfwijze is (ook) in H uniek omdat dit anders in tegenspraak zou zijn met de unieke schrijfwijze in G. Dus f is een isomorfisme en hieruit volgt het gevraagde. □

Stelling 3.5. Laat $I, (G_i)_{i \in I}$ en Φ zijn zoals hierboven. Dan zijn de onderstaande beweringen equivalent.

i. In $\rtimes_{i \in I} G_i$ is elk element op een *unieke* wijze te schrijven als een eindig (en mogelijkerwijs leeg) product

$$x_{i_1} \cdots x_{i_n},$$

zodanig dat $i_1, \ldots, i_n \in I, i_1 > \ldots > i_n$ en dat voor alle $j = 1, \ldots, n$ geldt: $x_{i_j} \in G_{i_j}$ en $x_{i_j} \neq 1$ in G_{i_j}.

ii. Voor alle $i \in I$ is het natuurlijke homomorfisme $G_i \to \rtimes_{i \in I} G_i$ injectief.

iii. Voor alle $i, j, k \in I, i < j < k$ en voor alle $x \in G_i, y \in G_j, z \in G_k$ geldt de onderstaande gelijkheid in G_k:

$$^{x}(^{y}z) = {}^{(^{x}y)}(^{x}z).$$

Bewijs. [$i \Rightarrow ii$] Dit is triviaal.

[$i \Rightarrow ii$] Laat $i, j, k \in I, i < j < k$ zijn en $x \in G_i, y \in G_j, z \in G_k$. In $\rtimes_{i \in I} G_i$ geldt dat

$$^{x}(^{y}z) = xyzy^{-1}x^{-1} = (xyx^{-1})(xzx^{-1})(xyx^{-1})^{-1} = {}^{(^{x}y)}(^{x}z).$$

Uit de injectiviteit van $G_k \to \rtimes_{i \in I} G_i$ volgt nu het gevraagde.

[$iii \Rightarrow i$] Laat Ω de deelverzameling van het directe product $\Pi_i G_i$ zijn bestaande uit families $(a_k)_{k \in I}$ met $a_k \in G_k$ zodanig dat $a_k \neq 1$ voor slechts eindig veel indices $k \in I$. Het is makkelijk in te zien dat voor alle $i \in I$ de afbeelding $\pi_i : G_i \to \mathrm{Sym}(\Omega)$ gedefinieerd door

$$(\pi_i(x)a)_k = \begin{cases} a_k & \text{als } k < i; \\ xa_k & \text{als } k = i; \\ {}^{x}a_k & \text{als } k > i, \end{cases}$$

met $x \in G_i$ en $a = (a_k)_{k \in I} \in \Omega$ een trouwe actie van G_i op Ω is. Dus voor alle i geldt $G_i \cong \pi_i[G_i]$ en we definiëren $G = \langle \pi_i[G_i] : i \in I \rangle$. In het vervolg noteren we de acties π_i met het lege symbool. Voor alle $i, j \in I, i < j, x \in G_i, y \in G_j$ en $a = (a_k)_{k \in I} \in \Omega$ geldt dat

$$\left(xyx^{-1}a\right)_k = \begin{cases} a_k & \text{als } k < i; \\ x\left(x^{-1}a_k\right) = a_k & \text{als } k = i; \\ {}^{x}\left({}^{x^{-1}}a_k\right) = a_k & \text{als } i < k < j; \\ {}^{x}\left(y\left({}^{x^{-1}}a_k\right)\right) = (^{x}y)\left({}^{xx^{-1}}a_k\right) = (^{x}y)a_k & \text{als } k = j; \\ {}^{x}\left({}^{y}\left({}^{x^{-1}}a_k\right)\right) = {}^{(^{x}y)}\left({}^{xx^{-1}}a_k\right) = {}^{(^{x}y)}a_k & \text{als } k > j. \end{cases}$$

Dus we zien dat $xyx^{-1} = {}^{x}y$.

Merk op dat elk element uit G geschreven kan worden als een (mogelijkerwijs leeg) product van een eindig aantal elementen $x_i \in G_i$ met $i \in I$. In dit product kunnen we het eenheidselement weglaten; voor $i \in I$ en $x, y \in G_i$ kunnen we xy vervangen door z met $z = xy \in G_i$; voor $i, j \in I, i < j$ en $x \in G_i, y \in G_j$ kunnen we xy vervangen door ${}^{x}yx$. Door het voorgaande herhaaldelijk toe te passen zien we dat elk element van G geschreven kan worden als $x_{i_1} \cdots x_{i_n}$ met $i_1, \ldots, i_n \in I, i_1 > \ldots > i_n$ en voor alle $j = 1, \ldots, n : x_{i_j} \in G_{i_j}$ en $x_{i_j} \neq 1$. Stel nu dat we van een element twee van dergelijke schrijfwijzen hebben, zeg $x_{i_1} \cdots x_{i_n} = y_{j_1} \cdots y_{j_m}$. Zet $1_\Omega = (1_k)_{k \in I}$, dan geldt:

$$x_{i_1} \cdots x_{i_n} 1_\Omega = y_{j_1} \cdots y_{j_m} 1_\Omega,$$

en door coördinaten te vergelijken zien we dat $n = m$ en $i_1 = j_1, \ldots, i_n = j_n$ en $x_{i_1} = y_{i_1}, \ldots, x_{i_n} = y_{i_n}$. Dus deze schrijfwijze is uniek. Uit stelling 3.4 volgt nu dat $G = \rtimes_{i \in I} G_i$. Dit bewijst het gevraagde. □

Stelling 3.6. Laat $I, (G_i)_{i \in I}$ en Φ zijn zoals hierboven en zij G het herhaalde semidirecte product van $(G_i)_{i \in I}$ met betrekking tot Φ. Noteer het beeld van G_i in G met H_i. Dan geldt: voor alle $i, j \in I, i < j$ hebben we een conjugatieactie $\psi_{ij} : H_i \to H_j$ en de groep G tezamen met de inclusies $H_i \to G$ is het herhaalde semidirecte product van de familie $(H_i)_{i \in I}$ met betrekking tot $\Psi = (\psi_{ij})_{i,j \in I, i<j}$.

Bewijs. Voor $i \in I$ en $x \in G_i$ noteren we het beeld van x in $H_i \subseteq G$ met $\overline{x}$. Voor $i, j \in I, i < j$ noteren we de werking van $x \in G_i$ op $y \in G_j$ met ${}^x y$.

Laat $i, j \in I$ zijn met $i < j$ en kies $x \in G_i, y \in G_j$. Dan geldt: $\overline{x}\,\overline{y}\,\overline{x}^{-1} = \overline{{}^x y}$. Dus we hebben een conjugatieactie $\psi_{ij} : H_i \to \mathrm{Aut}(H_j)$.

Zij G' een groep en stel dat we voor alle $i \in I$ een homomorfisme $\pi_i : H_i \to G'$ hebben zodanig dat voor alle $i, j \in I, i < j$ en $x \in G_i, y \in G_j$ geldt:

$$\pi_i(\overline{x})\pi_j(\overline{y})\pi_i(\overline{x})^{-1} = \pi_j(\overline{{}^x y}). \qquad (*)$$

Observeer dat we voor alle $i \in I$ een homomorfisme $G_i \to G'$ krijgen door het homomorfisme $G_i \to H_i$ samen te stellen met π_i. Uit $(*)$ en de universele eigenschap van G volgt dat er een uniek homomorfisme $G \to G'$ bestaat die $\overline{x} \in H_i$ afbeeldt op $\pi_i(\overline{x})$. Hieraan kunnen we zien dat G (ook) het semidirecte product van de familie $(H_i)_{i \in I}$ is met betrekking tot $\Psi = (\psi_{ij})_{i,j \in I, i<j}$. □

Voorbeelden. 1. Laat A, B en C groepen zijn en stel dat de homomorfismen $\phi : A \to \mathrm{Aut}(B)$ en $\phi' : B \rtimes_\phi A \to \mathrm{Aut}(C)$ gegeven zijn. Via restrictie geeft ϕ' aanleiding tot homomorfismen $\chi : B \to \mathrm{Aut}(C)$ en $\psi : A \to \mathrm{Aut}(C)$. Het herhaalde semidirecte product $C \rtimes B \rtimes A$ met betrekking tot $\{\phi, \chi, \psi\}$ is wegens stelling 3.4 isomorf met de groep $C \rtimes_{\phi'} (B \rtimes_\phi A)$.

2. Een concreet geval van het vorige voorbeeld doet zich voor bij de groep $I_2(\mathbf{R})$ van vlakke isometrieën. De ondergroep $T \subseteq I_2(\mathbf{R})$ van translaties is normaal in $I_2(\mathbf{R})$ en de ondergroep $O_2(\mathbf{R}) \subseteq I_2(\mathbf{R})$ van orthogonale afbeeldingen vormt een complement van T in $I_2(\mathbf{R})$. De ondergroep van rotaties $SO_2(\mathbf{R}) \subseteq O_2(\mathbf{R})$ is normaal in $O_2(\mathbf{R})$ en de ondergroep $\langle\sigma\rangle$ voortgebracht door een willekeurige orthogonale spiegeling $\sigma \in O_2(\mathbf{R})$ vormt een complement van $SO_2(\mathbf{R})$ in $O_2(\mathbf{R})$. We zien dat

$$I_2(\mathbf{R}) \cong T \rtimes O_2(\mathbf{R}) \cong T \rtimes \Big(SO_2(\mathbf{R}) \rtimes \langle\sigma\rangle\Big) \cong T \rtimes SO_2(\mathbf{R}) \rtimes \langle\sigma\rangle.$$

3. Zij K een lichaam, K^* de eenhedengroep van K en $\mathrm{Aut}(K)$ de groep van lichaamsautomorfismen van K. Laat Φ de verzameling zijn bestaande uit de werking van K^* op K door linksvermenigvuldiging

en de natuurlijke werkingen van $\mathrm{Aut}(K)$ op K en K^*. Beschouw de ondergroep $G \subseteq \mathrm{Sym}(K)$ bestaande uit afbeeldingen $x \mapsto a\sigma(x) + b$ met $b \in K, a \in K^*$ en $\sigma \in \mathrm{Aut}(K)$. Definieer de onderstaande groepshomomorfismen:

$$\begin{array}{lll} K \to G & K^* \to G & \mathrm{Aut}(K) \to G \\ b \mapsto [\tau_b : x \mapsto x + b], & a \mapsto [\rho_a : x \mapsto ax], & \sigma \mapsto \sigma. \end{array}$$

Voor alle $b \in K, a \in K^*$ en $\sigma \in \mathrm{Aut}(K)$ geldt:

$$\rho_a \tau_b \rho_a^{-1} = \tau_{ab}, \quad \sigma\tau_b\sigma^{-1} = \tau_{\sigma(b)}, \quad \sigma\rho_a\sigma^{-1} = \rho_{\sigma(a)}.$$

Verder is het eenvoudig te bewijzen dat elk element uit G op unieke wijze geschreven kan worden als een product $\tau_b\rho_a\sigma$. Uit stelling 3.4 volgt nu dat $G = K \rtimes K^* \rtimes \mathrm{Aut}(K)$.

4. Zij G een eindige groep die een Sylowfamilie $(S_p)_{p\in\mathcal{P}}$ heeft. Laat Φ de verzameling conjugatieacties $S_p \to \mathrm{Aut}(S_q)$ zijn met $p < q$, en $\pi_p : S_p \to G$ de inclusieafbeelding. Observeer dat voor een priem p de groepen S_p en $\langle S_q : q \in \mathcal{P}, q > p\rangle$ van coprieme orde zijn, dus volgt $S_p \cap \langle S_q : q \in \mathcal{P}, q > p\rangle = \{1\}$. Verder is het duidelijk dat $G = \langle S_p : p \in \mathcal{P}\rangle$. Hieruit volgt gemakkelijk dat elk element van G op een unieke manier geschreven kan worden als een product $x_{p_1} \cdots x_{p_n}$ waarbij $p_1, \ldots, p_n \in \mathcal{P}, p_1 > \ldots > p_n$ en voor alle $j = 1, \ldots, n : x_{p_j} \in S_{p_j}$ en $x_{p_j} \neq 1$. Uit stelling 3.4 volgt dat $G = \rtimes_{p\in\mathcal{P}} S_p$. Wegens stelling 2.12 hebben we in het bijzonder dat iedere eindige hyperoplosbare groep als een herhaald semidirect product van zijn Sylowondergroepen geschreven kan worden.

3.3 FRATTINI-ONDERGROEP EN p-GROEPEN

Zij G een groep. We noemen een ondergroep H van G *maximaal* wanneer G precies twee ondergroepen heeft die H omvatten. De *Frattini-ondergroep* van G definiëren we als de doorsnijding van alle maximale ondergroepen van G en noteren deze met $\Phi(G)$. Wanneer G geen maximale ondergroepen heeft, is deze lege doorsnijding gelijk aan G. Uit de definitie volgt direct dat $\Phi(G)$ een karakteristieke ondergroep van G is. Het onderstaande lemma geeft een andere beschrijving van de Frattini-ondergroep.

Lemma 3.7. Zij G een groep. Dan geldt $x \in \Phi(G)$ dan en slechts dan als voor iedere deelverzameling $S \subseteq G$ met $G = \langle x, S\rangle$ geldt dat $G = \langle S\rangle$.

Bewijs. Zie [2, hoofdstuk III, stelling 3.2]. □

Voor met name p-groepen blijkt het nuttig te zijn om de Frattini-ondergroep te bestuderen.

Lemma 3.8. Zij p een priemgetal en G een p-groep. Dan geldt: $\Phi(G) = [G, G]G^p$, waarbij G^p de ondergroep van G is voortgebracht door de p-de machten van G.

Bewijs. Zie [2, hoofdstuk III, stelling 3.14]. □

Gevolg 3.9. Zij p een priemgetal en G een p-groep. Dan is $G/\Phi(G)$ een elementair abelse p-groep

Propositie 3.10 (P. Hall)**.** Laat p een priemgetal zijn, G een p-groep en stel dat $\#\big(G/\Phi(G)\big) = p^d$. Dan geldt: de orde van de kern van de natuurlijke afbeelding $\mathrm{Aut}(G) \to \mathrm{Aut}\big(G/\Phi(G)\big)$ is een deler van $\big(\#\Phi(G)\big)^d$.

Bewijs. Kies $a_1, \ldots, a_d \in G$ zodanig dat $\langle \overline{a_i} : 1 \leqslant i \leqslant d \rangle = G/\Phi(G)$ met $\overline{a_i} = a_i\Phi(G) \in G/\Phi(G)$. Laat K de kern van de natuurlijke afbeelding $\mathrm{Aut}(G) \to \mathrm{Aut}\big(G/\Phi(G)\big)$ zijn. Dan werkt K op elke linkernevenklasse $a_i\Phi(G)$ en dus ook (puntsgewijs) op de verzameling $S = \prod_{i=1}^{d} a_i\Phi(G)$. Stel nu dat $\sigma \in K$, $x = (x_1, \ldots, x_n) \in S$ en dat $\sigma \cdot x = x$. Uit lemma 3.7 volgt dat

$$\begin{aligned} G &= \langle a_i, \Phi(G) : i = 1, \ldots, d \rangle = \langle x_i, \Phi(G) : i = 1, \ldots, d \rangle \\ &= \langle x_i : i = 1, \ldots, d \rangle. \end{aligned}$$

Omdat σ ieder element x_i vasthoudt, concluderen we dat $\sigma = \mathrm{id}_G$. Dus $\#K = \#(K \cdot x)$ en we zien dat de verzameling S uiteen valt in banen van lengte $\#K$. Dit impliceert dat $\#K$ een deler is van $\#S = \#\big(\Phi(G)\big)^d$. □

Laat p een priemgetal zijn en G een p-groep. We definiëren de *onderste p-centrale rij* van G door $G_0 = G$ en $G_{i+1} = G_i^p[G, G_i]$ voor $i \geqslant 0$ waarbij G_i^p de ondergroep is voortgebracht door de p-de machten van G_i. Het is duidelijk dat G_i een karakteristieke ondergroep van G is voor alle i.

Lemma 3.11. Zij p een priemgetal, G een p-groep en $(G_i)_{i=0}^{\infty}$ de onderste p-centrale rij van G. Dan geldt: er is een $t \in \mathbf{Z}, t \geqslant 0$ met $G_t = \{1\}$.

Bewijs. Uit de hyperoplosbaarheid van G volgt dat er een $t \in \mathbf{Z}, t \geqslant 0$ en een hyperoplosbaarheidsketen bestaat:

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_t = \{1\},$$

Met behulp van inductie laten we zien dat voor alle $i = 0, \ldots, t$ geldt: $G_i \subseteq H_i$. Het geval $i = 0$ is triviaal. Stel dat $G_i \subseteq H_i$, dan volgt

$$G_{i+1} = G_i^p[G, G_i] \subseteq H_i^p[G, H_i] \subseteq H_{i+1}.$$

Voor de laatste inclusie gebruiken we dat $\#\mathrm{Aut}(H_i/H_{i+1}) = p - 1$ zodat de conjugatiewerking van G op H_i/H_{i+1} triviaal is. Hiermee is de inductiestap gezet en zijn we klaar. Dus volgt $G_t = \{1\}$. □

3.4 HYPEROPLOSBARE SEMIDIRECTE PRODUCTEN

Een natuurlijke vraag die opkomt is of elke groep met een Sylowfamilie ook hyperoplosbaar is. Het onderstaande voorbeeld laat zien dat het antwoord op deze vraag negatief luidt.

Voorbeeld. Beschouw het lichaam $\mathbf{F}_{25}$ van 25 elementen en laat $\xi_3 \in \mathbf{F}_{25}^*$ een primitieve derde eenheidswortel zijn. We laten de groep $\langle \xi_3 \rangle$ werken op de optelgroep $\mathbf{F}_{25}^+$ door vermenigvuldiging en vormen het semidirecte product $G = \mathbf{F}_{25}^+ \rtimes \langle \xi_3 \rangle$ met betrekking tot deze werking. Het is duidelijk dat G een Sylowfamilie heeft. Echter, G is niet hyperoplosbaar. Stel dat dit namelijk wel het geval is, dan bevat G wegens lemma 2.6 een normale ondergroep N van orde 5. Dus we hebben een actie $\langle \xi \rangle \to \mathrm{Aut}(N)$. Merk nu op dat $\mathrm{Aut}(N)$ een cyclische groep van orde 4 is. Dus de actie is triviaal en dat levert een tegenspraak.

Stelling 3.12 (Maschke)**.** Zij G een groep en k een lichaam waarvan de karakteristiek geen deler is van #G. Dan geldt: de groepenring $k[G]$ is semisimpel.

Bewijs. Zie [4, hoofdstuk XVIII, stelling 1.2]. □

Lemma 3.13. Zij p een priemgetal en A een abelse groep van exponent een deler van $p-1$. Dan geldt: elk simpel $\mathbf{F}_p[A]$-moduul heeft orde p.

Bewijs. Zij V een simpel $\mathbf{F}_p[A]$-moduul en $x \in V, x \neq 0$. Beschouw vervolgens het moduulhomomorfisme $\mathbf{F}_p[A] \to V : r \mapsto rx$. Omdat V simpel is, is het homomorfisme surjectief. Dus we hebben een moduulisomorfisme $\mathbf{F}_p[A]/M \cong V$ voor een zeker ideaal $M \subseteq \mathbf{F}_p[A]$. De simpliciteit van V impliceert dat $M \subsetneq \mathbf{F}_p[A]$ een maximaal ideaal is. Maar dan is $\mathbf{F}_p[A]/M$ een lichaam, en de aanname op de exponent van A impliceert dat het Frobeniushomomorfisme als de identiteit hierop werkt. Dus we hebben een lichaamsisomorfisme $\mathbf{F}_p[A]/M \cong \mathbf{F}_p$ en hieruit volgt het gevraagde. □

Stelling 3.14. Zij G een groep en $(S_p)_{p \in \mathcal{P}}$ een Sylowfamilie van G. Laat voor alle p het homomorfisme $\phi_p : \langle S_q : q < p \rangle \to \mathrm{Aut}(S_p)$ gegeven zijn door conjugatie. Dan geldt: G is hyperoplosbaar dan en slechts dan als voor iedere p het beeld van ϕ_p abels is en van exponent een deler van $p-1$.

Bewijs. [⇒] Het volstaat om de bewering te bewijzen voor de grootste priemdeler van #G, zeg l. Zet $V = S_l/\Phi(S_l)$, dan is V een $\mathbf{F}_l$-vectorruimte wegens lemma 3.7. Beschouw de samenstelling

$$\langle S_q : q < l \rangle \xrightarrow{\phi_l} \mathrm{Aut}(S_l) \xrightarrow{\psi} \mathrm{Aut}(V),$$

waarbij ψ de natuurlijke afbeelding is. Laat A het beeld zijn van ϕ_l. Uit propositie 3.8 volgt dat $\ker \psi$ een l-groep is. Hieruit volgt dat de natuurlijke werking van A op V trouw is. De hyperoplosbaarheid van $G/\Phi(S_l)$ impliceert dat er een $n \in \mathbf{Z}, n \geqslant 0$ en een keten van $\mathbf{F}_l[A]$-deelmodulen

$$\{0\} = V_0 \overset{l}{\subseteq} V_1 \overset{l}{\subseteq} \ldots \overset{l}{\subseteq} V_n = V,$$

bestaan zodanig dat iedere index $\#(V_{i+1}/V_i)$ gelijk is aan l. Observeer dat l geen deler is van $\#A$, dus uit de stelling van Maschke (stelling 3.12) volgt dat $\mathbf{F}_l[A]$ semisimpel is. Dit impliceert dat V als $\mathbf{F}_l[A]$-moduul isomorf is met

$$V_n/V_{n-1} \oplus \ldots \oplus V_1/V_0.$$

Elk van de termen hierboven is een cyclische groep van orde l. Hieruit volgt gemakkelijk dat A abels is en van exponent een deler van $l-1$.

[$\Leftarrow$] We geven een bewijs met behulp van inductie naar het aantal priemfactoren van $\#G$. Laat l wederom de grootste priemdeler zijn van $\#G$. We laten zien dat S_l een G-hyperoplosbare ondergroep van G is. Beschouw de onderste l-centrale rij van S_l

$$S_l = H_0 \supsetneq H_1 \supsetneq \ldots \supsetneq H_t = \{1\}.$$

We zullen deze keten vervolgens verfijnen met normale ondergroepen in G zodanig dat we een hyperoplosbaarheidsketen voor S_l verkrijgen.

Zet $V = H_i/H_{i+1}$ voor een zekere $i \in \{0, \ldots, t-1\}$, dan is V een niet-triviale $\mathbf{F}_l$-vectorruimte. Laat A het beeld zijn van ϕ_l en beschouw de natuurlijke werking van A op V. We zien dat V een $\mathbf{F}_l[A]$-moduul is. Zij $V' \subsetneq V$ een maximaal deelmoduul, dan is V/V' een simpel $\mathbf{F}_l[A]$-moduul en lemma 3.13 impliceert dat $\#(V/V') = l$. Door dit argument te herhalen zien we dat er een $n \in \mathbf{Z}, n \geqslant 0$ en een keten van $\mathbf{F}_l[A]$-modulen

$$V = V_0 \overset{l}{\supseteq} V_1 \overset{l}{\supseteq} \ldots \overset{l}{\supseteq} V_n = \{0\}$$

bestaan zodanig dat elke index $\#(V_j/V_{j+1})$ (voor $j = 0, \ldots, n-1$) gelijk is aan l. Neem het inverse beeld van elk van de deze deelmodulen onder het homomorfisme $\pi : H_i \to H_i/H_{i+1}$. Dit levert een keten van ondergroepen in G:

$$H_i = N_0 \overset{l}{\supseteq} N_1 \overset{l}{\supseteq} \ldots \overset{l}{\supseteq} N_n = H_{i+1},$$

waarbij elke index eveneens gelijk is aan l. Observeer dat de conjugatiewerking van S_l op H_i/H_{i+1} triviaal is. Daarnaast zijn voor $j = 0, \ldots, n$ de ondergroepen N_j stabiel onder de werking van A. Hieruit volgt: $N_j \trianglelefteq G$ voor alle j. Op deze wijze kunnen we elk van de inclusies $H_i \supseteq H_{i+1}$ verfijnen met normale ondergroepen en we concluderen hieruit dat S_l een G-hyperoplosbare ondergroep van G is.

De inductiehypothese toegepast op G/S_l laat zien dat G/S_l hyperoplosbaar is. Propositie 2.4 bewerkstelligt nu de hyperoplosbaarheid van G. $\square$

4 EEN TOETS VOOR HYPEROPLOSBAARHEID

Gedurende deze hele paragraaf zal G een *eindige groep* voorstellen. We beginnen met het beschrijven van een toets voor hyperoplosbaarheid die we in de literatuur hebben aangetroffen. Een element $g \in G$ heet een *gegeneraliseerd centrumelement* als voor alle Sylowondergroepen $P \subseteq G$ geldt: $\langle g \rangle P = P \langle g \rangle$. Vervolgens definiëren we het gegeneraliseerde centrum $Z_{\text{Gen}}(G)$ van G als de ondergroep voortgebracht door de gegeneraliseerde centrumelementen.

Beschouw de keten van stijgende ondergroepen $K_i \subseteq G$ ($i \in \mathbf{Z}, i \geqslant 0$) met $K_0 = \{1\}$ en K_i het inverse beeld van $Z_{\text{Gen}}(G/K_{i-1})$ onder $G \to G/K_{i-1}$ (voor $i \geqslant 1$).

Het *gegeneraliseerde hypercentrum* $Z^*_{\text{Gen}}(G)$ van G is de vereniging $\bigcup_{i \geqslant 0} K_i$. We hebben de volgende stelling:

Stelling 4.1. Er geldt: G is hyperoplosbaar dan en slechts dan als $Z^*_{\text{Gen}}(G) = G$.

Bewijs. Zie [1, stelling 2.8.(i)]. □

In deze paragraaf zullen wij — gegeven een groep G — een keten van dalende ondergroepen $G_{(i)} \subseteq G$ (met $i \in \mathbf{Z}, i \geqslant 0$) definiëren zodanig dat het volgende geldt:

$$G \text{ hyperoplosbaar} \Leftrightarrow G_{(t)} = 1 \text{ voor een zekere } t \in \mathbf{Z}, t \geqslant 0.$$

Een dergelijke toets voor hyperoplosbaarheid hebben we in de literatuur niet kunnen vinden. We beginnen met het definiëren van een speciale operator op de verzameling van normale ondergroepen van G. Zij $H \trianglelefteq G$ een normale ondergroep. We definiëren een ondergroep $\Gamma(H) \subseteq G$ als volgt: als $H = \{1\}$, dan $\Gamma(H) = \{1\}$; als $H \neq \{1\}$, dan

$$\Gamma(H) = [G' G^{p-1}, H] H^p,$$

met p de kleinste priemdeler van $\#H$, $G' = [G, G]$, en G^n de groep voortgebracht door de n-de machten van elementen uit G. Dat $\Gamma(H)$ een ondergroep is volgt uit het onderstaande lemma.

Lemma 4.2. Laat $H, I \trianglelefteq G$ normale ondergroepen zijn met $H \supseteq I$. Stel dat $\#H > 1$ en laat p de kleinste priemdeler van $\#H$ zijn. Dan geldt:

i. $\Gamma(H) \trianglelefteq G$;

ii. $\Gamma(H) \subseteq H$ en $H/\Gamma(H)$ is een elementair abelse p-groep;

iii. $\Gamma(H) \supseteq \Gamma(I)$.

Bewijs. i. Merk hiervoor op dat $[G'G^{p-1}, H]$ en H^p normale ondergroepen van G zijn.

ii. Uit de normaliteit van H volgt dat $[A, H] \subseteq H$ voor elke ondergroep $A \subseteq G$. In het bijzonder geldt $[G'G^{p-1}, H] \subseteq H$. Uiteraard geldt $H^p \subseteq H$, dus $\Gamma(H) \subseteq H$. Verder volgt gemakkelijk uit de definitie van $\Gamma(H)$ dat $H/\Gamma(H)$ van exponent een deler van p is.

Rest ons aan te tonen dat $H/\Gamma(H)$ abels is. Er geldt $H = H^{p-1}$, immers elk element van H heeft een orde copriem met $p-1$ en is daarom te schrijven als een $(p-1)$-de macht van een element uit H. Hieruit volgt $H \subseteq G'G^{p-1}$. Dan geldt ook $[H, H] \subseteq \Gamma(H)$, en dus is $H/\Gamma(H)$ abels.

iii. Als $p \mid \#I$, dan is p ook de kleinste priemdeler van $\#I$ en volgt gemakkelijk dat $\Gamma(I) \subseteq \Gamma(H)$. Stel $p \nmid \#I$ en beschouw de quotiëntafbeelding $\pi : H \to H/\Gamma(H)$. Het beeld $\pi[I]$ heeft een orde die een deler is van $\#I$ en van $\#(H/\Gamma(H))$. Dit laatste getal is een macht van p wegens (ii), dus volgt $\#\pi[I] = 1$. Oftewel $\pi[I]$ is triviaal in $H/\Gamma(H)$ en $\Gamma(I) \subseteq I \subseteq \Gamma(H)$. □

We zullen vervolgens met G een keten van ondergroepen associëren. We definiëren inductief ondergroepen $G_{(i)} \subseteq G$ voor $i \in \mathbf{Z}_{\geqslant 0}$ door

$$G_{(0)} := G, \quad G_{(i)} := \Gamma(G_{(i-1)}) \ (i \geqslant 1).$$

Dit levert ons een keten

$$G = G_{(0)} \supseteq G_{(1)} \supseteq G_{(2)} \supseteq \ldots$$

bestaande uit normale ondergroepen van G.

Stelling 4.3. Er geldt: G is hyperoplosbaar dan en slechts dan als voor een zekere $t \in \mathbf{Z}, t \geqslant 0$ geldt: $G_{(t)} = \{1\}$.

Bewijs. [$\Rightarrow$] Beschouw een hyperoplosbaarheidsketen van G als in lemma 2.6, zeg

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}.$$

Met behulp van inductie naar i zullen we bewijzen dat $G_{(i)} \subseteq G_i$ voor alle $i = 0, \ldots, t$ zodat in het bijzonder $G_{(t)} = \{1\}$. Het geval $i = 0$ is triviaal. Stel dat de bewering waar is voor een zekere $i \in \{0, \ldots, t-1\}$. Definieer $p = [G_i : G_{i+1}]$ zodat p de kleinste priemdeler van G_i is en $\Gamma(G_i) = [G'G^{p-1}, G_i]G_i^p$. Omdat G_i/G_{i+1} cyclisch is van orde p volgt dat $G_i^p \subseteq G_{i+1}$. Beschouw vervolgens de conjugatiewerking $G \to \mathrm{Aut}(G_i/G_{i+1})$. Observeer dat $\mathrm{Aut}(G_i/G_{i+1})$ een cyclische groep van orde $p-1$ is, dus in het bijzonder abels en van exponent $p-1$. Hieruit volgt rechtstreeks dat $[G'G^{p-1}, G_i] \subseteq G_{i+1}$ en we concluderen dat

$$\Gamma(G_i) = [G'G^{p-1}, G_i]G_i^p \subseteq G_{i+1}.$$

Wegens onze inductiehypothese en lemma 4.2.iii hebben we nu dat

$$G_{(i+1)} = \Gamma(G_{(i)}) \subseteq \Gamma(G_i) \subseteq G_{i+1}.$$

Hiermee is de inductiestap gezet en zijn we klaar.

[$\Leftarrow$] Stel dat $N \trianglelefteq G$ een niet-triviale normale ondergroep is en p de kleinste priemdeler van $\#N$. Uit lemma 4.2.ii volgt dat $V := N/\Gamma(N)$ een vectorruimte over $\mathbf{F}_p$ is. Beschouw de conjugatiewerking van G op V en observeer dat deze op de onderstaande wijze factoriseert.

$$\begin{tikzcd} G \arrow[r] \arrow[d] & \mathrm{Aut}\,(V) \\ G/G'G^{p-1} \arrow[ur] & \end{tikzcd}$$

Zet $A := G/G'G^{p-1}$ en merk op dat A abels is en van exponent een deler van $p-1$. In het bijzonder is V een $\mathbf{F}_p[A]$-moduul. Stel dat $V \neq \{0\}$ en zij $V' \subseteq V$ een maximaal deelmoduul. Dan is V/V' een simpel $\mathbf{F}_p[A]$-moduul en wegens lemma 3.13 is zijn orde gelijk aan p. Door dit argument te herhalen zien we dat een zekere $n \in \mathbf{Z}, n \geqslant 0$ en een keten van deelmodulen

$$\{0\} = V_0 \overset{p}{\subseteq} V_1 \overset{p}{\subseteq} \ldots \overset{p}{\subseteq} V_n = V$$

bestaan waarbij elke index gelijk is aan p. Door van elk van deze deelmodulen het inverse beeld onder het homomorfisme $\pi : N \to N/\Gamma(N)$ te nemen, verkrijgen we een keten van normale ondergroepen in G:

$$\Gamma(N) = N_0 \overset{p}{\subseteq} N_1 \overset{p}{\subseteq} \ldots \overset{p}{\subseteq} N_n = N,$$

waarbij elke index eveneens gelijk is aan p.

Het bewijs is nu gemakkelijk af te maken. Als $t = 0$, dan volgt: $G = G_{(0)} = \{1\}$ en G is hyperoplosbaar. Als $t > 0$, dan kunnen we door achtereenvolgens N gelijk te nemen aan $G_{(0)}, G_{(1)}, \ldots, G_{(t-1)}$ en het bovenstaande toe te passen de oorspronkelijke keten $(G_{(i)})_{i=0}^{t}$ verfijnen tot een hyperoplosbaarheidsketen. $\square$

BIBLIOGRAFIE

[1] Ram K. Agrawal, *Generalized Center and Hypercenter of a Finite Group*, Proc. Amer. Math. Soc. **58** (1976), 13–21.

[2] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[3] I. Martin Isaacs, *Finite Group Theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008.

[4] S. Lang, *Algebra*, rev. 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.