

Groepentheorie (aanvulling)

B. J. J. Moonen

Deze tekst geeft een aanvulling op de syllabus Algebra 1 van Prof. G. van der Geer. Er is wel enige overlap met de in die syllabus behandelde stof.

[Versie van 20 april 2011]

HOOFDSTUK 12

Aanvullingen op eerdere hoofdstukken

12.1. Stel g en h zijn twee elementen van een groep G waarvan we de orde kennen. In het algemeen is het niet mogelijk om uit deze informatie de orde van het element gh te bepalen. Als g en h allebei eindige orde hebben, dan wil dat bijvoorbeeld nog niet zeggen dat ook gh eindige orde heeft. (Verzin zelf een voorbeeld.)

We kunnen aanmerkelijk meer zeggen als we aannemen dat g en h onderling commuteren.

12.2. Propositie. *Laten g en h twee commuterende elementen zijn in een groep G .*

- (i) *Als $m = \text{orde}(g)$ en $n = \text{orde}(h)$ allebei eindig zijn dan is $\text{orde}(gh)$ een deler van $\text{kgv}(m, n)$.
Als bovendien $\text{ggd}(m, n) = 1$ dan is $\text{orde}(gh) = \text{kgv}(m, n)$.*
- (ii) *Als precies één van de elementen g en h oneindige orde heeft dan heeft ook gh oneindige orde.*

Bewijs. (i) Laat $k = \text{kgv}(m, n)$. Dan is $(gh)^k = g^k h^k = e \cdot e = e$, dus $\text{orde}(gh)$ is een deler van k . Neem nu aan dat $\text{ggd}(m, n) = 1$ en laat $\ell = \text{orde}(gh)$. Passen we het vorige toe op de elementen g^{-1} en gh dan vinden we dat n een deler is van $\text{kgv}(m, \ell)$. (Merk op dat $\text{orde}(g^{-1}) = \text{orde}(g)$ en dat g^{-1} commuteert met gh .) Uit $\text{ggd}(m, n) = 1$ volgt dat n een deler is van ℓ . Op dezelfde manier zien we dat m een deler is van ℓ . Dus $\ell = \text{kgv}(m, n)$.

(ii) Stel g heeft eindige orde en h heeft oneindige orde. Schrijf $h = g^{-1} \cdot gh$. Als de orde van gh eindig zou zijn dan volgt uit (i) dat ook h eindige orde heeft; tegenspraak. \square

Als g en h allebei oneindige orde hebben, kan de orde van het element gh eindig zijn. Denk maar aan het geval dat g een element van oneindige orde is en dat $h = g^{-1}$.

12.3. Propositie. *Zij G een groep. Laten H_1 en H_2 ondergroepen zijn van G zo dat voldaan is aan de volgende voorwaarden:*

- (a) $H_1 \cap H_2 = \{e\}$;
- (b) voor alle $h_1 \in H_1$ en $h_2 \in H_2$ geldt dat $h_1 h_2 = h_2 h_1$;
- (c) H_1 en H_2 brengen samen de hele groep G voort.

Dan is de afbeelding $f: H_1 \times H_2 \rightarrow G$ gegeven door $f(h_1, h_2) = h_1 h_2$ een isomorfisme van groepen.

Bewijs. We gaan eerst na dat f een homomorfisme is. Hiertoe nemen we elementen $h_1, h'_1 \in H_1$ en $h_2, h'_2 \in H_2$; dan berekenen we:

$$f((h_1, h_2) \cdot (h'_1, h'_2)) = f(h_1 h'_1, h_2 h'_2) = h_1 h'_1 h_2 h'_2 \stackrel{(b)}{=} h_1 h_2 h'_1 h'_2 = f(h_1, h_2) \cdot f(h'_1, h'_2).$$

Dit laat zien dat f inderdaad een homomorfisme is. Als $(h_1, h_2) \in \text{Ker}(f)$ dan is $h_1 = h_2^{-1}$ een element van $H_1 \cap H_2$, dus uit (a) volgt dat $h_1 = h_2 = e$. Dit toont aan dat $\text{Ker}(f) = \{(e, e)\}$, zodat f injectief is. Het beeld $\text{Im}(f) \subset G$ is een ondergroep die zowel H_1 als H_2 bevat, dus uit (c) volgt dat $\text{Im}(f) = G$. De conclusie is dus dat f een bijectief homomorfisme is. \square

Zie Opgave 12.2 voor een variant.

Opgaven bij hoofdstuk 12.

Opgave 12.1. Zij $\pi: G \rightarrow H$ een homomorfisme van groepen. Een homomorfisme $s: H \rightarrow G$ heet een *snede van π* als $\pi \circ s = \text{id}_H$.

- (i) Laat zien dat er alleen een snede van π kan bestaan als π surjectief is. Laat ook zien dat een snede s noodzakelijk injectief is.
- (ii) Geef een snede van het homomorfisme $\det: \text{GL}_2(\mathbb{R}) \rightarrow \mathbb{R}^*$.
- (iii) Geef een snede van het teken-homomorfisme $\varepsilon: S_n \rightarrow \{\pm 1\}$, voor $n > 1$.
- (iv) Zij Q de quaterniongroep van orde 8. Het centrum van Q is de ondergroep $\{\pm 1\}$. Laat zien dat er geen snede bestaat van de canonieke afbeelding $Q \rightarrow Q/\{\pm 1\}$.

Opgave 12.2. Gegeven is een groep G met twee normaaldelers N_1 en N_2 zo dat $N_1 \cap N_2 = \{e\}$ en $\langle N_1, N_2 \rangle = G$. Bewijs dat $G \cong N_1 \times N_2$.

Opgave 12.3. Zij $G = G_1 \times G_2$ het product van twee groepen. We identificeren G_1 met de ondergroep van G bestaande uit alle elementen van de vorm (g_1, e_2) . Evenzo identificeren we G_2 met de ondergroep bestaande uit de elementen (e_1, g_2) . Zij $H \subset G$ een ondergroep zo dat $G_1 \subset H$. Bewijs dat $H \cong G_1 \times (G_2 \cap H)$.

HOOFDSTUK 13

Toepassingen van werkingen

13.1. Stelling van Cauchy. *Zij G een eindige groep. Als p een priemgetal is dat de orde van G deelt, dan heeft G een element van orde p .*

Bewijs. Laat $m = \#G$. Beschouw de verzameling

$$X := \{(g_1, g_2, \dots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}.$$

Het aantal elementen van X is gelijk aan m^{p-1} ; we kunnen immers g_1, \dots, g_{p-1} willekeurig kiezen in G en dan ligt g_p vast door de relatie $g_1 g_2 \cdots g_p = e$.

Definieer een afbeelding $\alpha: X \rightarrow X$ door

$$\alpha(g_1, g_2, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1).$$

Merk op dat het rechterlid weer een element is van X , omdat

$$g_2 g_3 \cdots g_p g_1 = g_1^{-1} \cdot g_1 g_2 \cdots g_p \cdot g_1 = g_1^{-1} \cdot e \cdot g_1 = e.$$

Verder is duidelijk dat α injectief is, en omdat X eindig is, volgt dat α een bijectie is van X naar zichzelf, d.w.z., $\alpha \in S(X)$.

De permutatie α heeft orde p . Dit geeft ons een werking van de groep $\Gamma = (\mathbb{Z}/p\mathbb{Z})$ op de verzameling X door te stellen dat $(i \bmod p) \cdot x = \alpha^i(x)$. Het corresponderende homomorfisme $\Gamma \rightarrow S(X)$ wordt gegeven door $(i \bmod p) \mapsto \alpha^i$. Uit Propositie (8.9) volgt dat $\#X^\Gamma \equiv \#X \equiv 0 \pmod{p}$. Ook is duidelijk dat $\#X^\Gamma > 0$ want (e, e, \dots, e) is ten duidelijkste een vast punt in X onder de werking van Γ . We concluderen dat er nog tenminste één ander vast punt is. Dit is een element $x = (g_1, \dots, g_p) \in X$ met

$$(g_1, g_2, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1).$$

Hieruit volgt dat $g_1 = g_2 = \cdots = g_p$, dus x is van de vorm $x = (g, g, \dots, g)$ voor een element $g \in G$, met $g \neq e$. De conditie $g_1 g_2 \cdots g_p = e$ geeft dan dat $g^p = e$, dus de orde van g is een deler van p . Maar $g \neq e$ en p is een priemgetal, dus $\text{orde}(g) = p$. \square

We geven nog een tweede bewijs van de stelling:

Tweede bewijs. Met inductie naar $m = \#G$ mogen we aannemen dat de stelling waar is voor alle groepen van orde $< m$. (De start van de inductie is het triviale geval $m = 1$.)

Neem eerst aan dat G abels is. Kies een element $g \neq e$. Als $\text{orde}(g)$ deelbaar is door p , schrijf dan $\text{orde}(g) = pk$; in dat geval heeft g^k orde p . Als $p \nmid \text{orde}(g)$ dan is $G/\langle g \rangle$ een groep van orde $< m$ dus uit de inductiehypothese volgt dat er een element $\bar{h} \in G/\langle g \rangle$ is met orde p . De orde van \bar{h} is een deler van de orde van h , dus $p \mid \text{orde}(h)$. Schrijf $\text{orde}(h) = p\ell$; dan heeft h^ℓ orde p .

Vervolgens nemen we aan dat G niet abels is. In dit geval is $Z(G)$ een echte ondergroep van G . Als $\#Z(G)$ deelbaar is door p dan volgt uit de inductiehypothese dat $Z(G)$, en dus

ook G , een element van orde p heeft. Dus we mogen aannemen dat $\#Z(G)$ niet deelbaar is door p . Laat nu G op zichzelf werken door conjugatie. De vaste punten onder deze werking zijn precies de elementen van het centrum $Z(G)$. Omdat p een deler is van $\#G$ maar niet een deler van $\#Z(G)$, is er tenminste één baan $C(x) \subset G$ zo dat $\#C(x) > 1$ en $p \nmid \#C(x)$. De stabilisator $G_x \subset G$ is dan een echte ondergroep van G en p is een deler van $\#G_x = \#G/\#C(x)$. Uit de inductiehypothese volgt dan dat G_x , en dus ook G , een element van orde p heeft. \square

Als volgende gaan we bewijzen dat een groep van orde p^n met p een priemgetal altijd een niet-triviaal centrum heeft. (Zo'n groep van orde p^n noemen we een p -groep.) De werking die we gebruiken is de conjugatiewerking van G op zichzelf. Als toepassing zullen we de groepen van orde p^2 classificeren.

13.2. Propositie. *Zij G een eindige groep waarvan de orde een positieve macht is van een priemgetal p . Dan is het centrum $Z(G)$ niet triviaal, d.w.z., $Z(G) \neq \{e\}$.*

Bewijs. We laten G op zichzelf werken door conjugatie; zie Voorbeeld 3 in (8.2). Een element $x \in G$ is een vast punt onder deze werking wanneer voor alle $g \in G$ geldt dat $gxg^{-1} = x$. Dit betekent precies dat x een element is van het centrum $Z(G)$. Uit Propositie (8.9) volgt dat $\#Z(G) \equiv 0 \pmod{p}$. Anderzijds is duidelijk dat $\#Z(G) \geq 1$ want $e \in Z(G)$. Dus $\#Z(G) \geq p$. \square

13.3. Gevolg. *Zij G een groep van orde p^2 voor een priemgetal p . Dan is $G \cong \mathbb{Z}/p^2\mathbb{Z}$ of $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.*

Bewijs. Als G een element van orde p^2 heeft dan is $G \cong \mathbb{Z}/p^2\mathbb{Z}$ en we zijn klaar. Neem aan dat G niet cyclisch is. Alle elementen $g \neq e$ hebben dan orde p . Uit Propositie 13.2 volgt dat het centrum van G niet triviaal is. Kies een element $g \neq e$ in het centrum van G . Kies vervolgens een element h dat niet in de ondergroep $H_1 := \langle g \rangle$ zit en laat $H_2 = \langle h \rangle$. Merk op dat $H_1 \cong H_2 \cong \mathbb{Z}/p\mathbb{Z}$. We gaan na dat voldaan is aan de voorwaarden uit Propositie 12.3: (a) geldt omdat $h \notin H_1$, (b) geldt omdat $g \in Z(G)$ en (c) geldt omdat de ondergroep voortgebracht door H_1 en H_2 meer dan p elementen heeft en dus de hele groep G moet zijn. Toepassen van Propositie 12.3 geeft dat $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. \square

In het volgende hoofdstuk zullen we, onder bepaalde aannamen, de groepen van orde pq classificeren, waarbij p en q priemgetallen zijn. Een belangrijke stap daarbij is dat we in sommige gevallen van een ondergroep kunnen bewijzen dat deze een normaaldeeler is, enkel gebruik makend van informatie over de index van de ondergroep. Ook het bewijs van dit resultaat maakt gebruik van een werking, ditmaal de werking van G op de verzameling van nevenklassen G/H door linksvermenigvuldiging.

13.4. Propositie. *Zij H een ondergroep van een groep G , van eindige index $n = [G : H]$. Dan bestaat er een normaaldeeler $N \triangleleft G$ met $N \subset H$, zo dat $[G : N]$ een deler is van $n!$.*

Bewijs. We laten G werken op de verzameling $X = G/H$ van linkernevenklassen van H in G door linksvermenigvuldiging; zie Voorbeeld 4 in (8.2). Deze werking wordt gegeven door een homomorfisme $\rho: G \rightarrow S(X)$. Zij N de kern van dit homomorfisme. Merk op dat de stabilisator van de nevenklasse eH precies de ondergroep H is, zodat $N \subset H$. De Eerste Isomorfiestelling geeft een isomorfisme van G/N met het beeld van ρ , en dit is een ondergroep van de groep

$S(X)$. Omdat $S(X)$ orde $n!$ heeft, volgt uit de Stelling van Lagrange dat $[G : N]$ een deler is van $n!$. \square

13.5. Opmerking. De normaaldeler $N = \text{Ker}(\rho)$ die we in het bewijs gevonden hebben, is de grootste normaaldeler van G die bevat is in H en er geldt

$$N = \bigcap_{g \in G} gHg^{-1}.$$

Immers, als $g \in G$ dan is de stabilisator van de nevenklasse $gH \in X$ de ondergroep gHg^{-1} , zodat de kern van ρ inderdaad gelijk is aan de doorsnede van alle gHg^{-1} . (Merk op dat gHg^{-1} alleen afhangt van de nevenklasse gH .) Als M nu een willekeurige normaaldeler van G is met $M \subset H$, dan is $M = gMg^{-1}$ ook bevat in gHg^{-1} , voor elke $g \in G$. Daaruit volgt dat $M \subset N$, dus $N = \text{Ker}(\rho)$ is inderdaad de grootste normaaldeler die bevat is in H .

13.6. Gevolg. Zij G een eindige groep. Zij p het kleinste priemgetal dat $\#G$ deelt. Als $H \subset G$ een ondergroep is van index p , dan is H een normaaldeler van G .

Bewijs. Volgens Propositie 13.4 is er een normaaldeler $N \triangleleft G$ die bevat is in H en zo dat $[G : N]$ een deler is van $p!$. Anderzijds weten we uit de Stelling van Lagrange dat $[G : N]$ een deler is van $\#G$. De aanname dat p het kleinste priemgetal is dat $\#G$ deelt, impliceert dat $\text{ggd}(p!, \#G) = p$. Dus $[G : N]$ is een deler van p , en uit $[G : N] = [G : H] \cdot [H : N] = p \cdot [H : N]$ volgt dat $[H : N] = 1$, d.w.z., $N = H$. \square

13.7. Voorbeeld. Zij G een groep van orde pq , waarbij p en q twee priemgetallen zijn. Neem aan dat $p \leq q$, zodat p het kleinste priemgetal is dat $\#G$ deelt. Volgens de Stelling van Cauchy bestaat er een element $g \in G$ van orde q . De door g voortgebrachte ondergroep $N = \langle g \rangle$ heeft index p , en is dus een normaaldeler van G . De quotiëntgroep G/N heeft orde p . Merk op dat $N \cong \mathbb{Z}/q\mathbb{Z}$ en $G/N \cong \mathbb{Z}/p\mathbb{Z}$. Wanneer we bovendien aannemen dat $p \nmid q - 1$, dan is de groep G noodzakelijk abels. We zullen dit bewijzen in Stelling 14.14.

Opgaven bij hoofdstuk 13.

Opgave 13.1. Zij G een groep.

- (i) Gegeven zijn twee ondergroepen H_1 en H_2 van eindige index in G . Bewijs dat $H_1 \cap H_2$ weer eindige index heeft in G en dat

$$[G : H_1 \cap H_2] \leq [G : H_1] \cdot [G : H_2].$$

- (ii) Laten N_1 en N_2 normaaldelers zijn van G . Bewijs dat $N_1 \cap N_2$ weer een normaaldeler is en dat $G/(N_1 \cap N_2)$ isomorf is met een ondergroep van $(G/N_1) \times (G/N_2)$.

Opgave 13.2. Zij G een eindige groep. Zij $H \subset G$ een ondergroep van index n zo dat $\#H$ onderling ondeelbaar is met $(n - 1)!$. Laat zien dat H een normaaldeler is.

Opgave 13.3. Gegeven zijn een groep G en een geheel getal n zo dat voor alle $g, h \in G$ geldt dat $(gh)^n = g^n h^n$.

(i) Definieer

$$G^{[n]} := \{g^n \mid g \in G\} \quad \text{en} \quad G_{[n]} := \{g \in G \mid g^n = e\}.$$

Bewijs dat $G^{[n]}$ en $G_{[n]}$ normaaldelers zijn van G en dat $G/G_{[n]} \cong G^{[n]}$.

- (ii) Toon aan dat ook voor alle $g, h \in G$ geldt dat $(gh)^{1-n} = g^{1-n}h^{1-n}$. [*Hint*: gebruik de relatie $(hg)^n = h \cdot (gh)^{n-1} \cdot g$.]
- (iii) Bewijs dat de elementen van de vorm $g^{n(n-1)}$ onderling allemaal commuteren.

HOOFDSTUK 14

Automorfismen en semidirecte producten

14.1. Als G en H groepen zijn, dan schrijven we $\text{Hom}(G, H)$ voor de verzameling van homomorfismen van G naar H .

In het algemeen heeft de verzameling $\text{Hom}(G, H)$ geen verdere structuur. Dat wordt anders wanneer H abels is, want homomorfismen naar een abelse groep kunnen we bij elkaar optellen. Om dit verder uit te werken, beschouwen we een additief geschreven abelse groep A . Als $\varphi, \psi: G \rightarrow A$ homomorfismen zijn, kunnen we een nieuw homomorfisme

$$\varphi + \psi: G \rightarrow A$$

definiëren door de regel $(\varphi + \psi)(g) = \varphi(g) + \psi(g)$. Het is gemakkelijk na te gaan dat dit inderdaad weer een homomorfisme is. Omdat A abels is, is de inverse $-\text{id}: A \rightarrow A$ een homomorfisme (vgl. Opgave 8 uit Hoofdstuk 5), zodat ook $-\varphi = -\text{id} \circ \varphi$ een homomorfisme is.

14.2. Propositie. *Zij G een groep en zij A een additief genoteerde abelse groep. Dan geeft de hierboven ingevoerde optelling $(\varphi, \psi) \mapsto \varphi + \psi$ de verzameling $\text{Hom}(G, A)$ de structuur van een abelse groep. Het eenheidselement van deze groep is het triviale homomorfisme $0: G \rightarrow A$, gegeven door de regel $0(g) = 0$ voor alle $g \in G$. De inverse van een homomorfisme $\varphi: G \rightarrow A$ in $\text{Hom}(G, A)$ is het homomorfisme $-\varphi$.*

Het eenvoudige bewijs van de propositie laten we als oefening over aan de lezer.

14.3. Opmerking. Zoals we hebben gezien in Propositie (10.4), factoriseert elk homomorfisme van een groep G naar een abelse groep A via de abels gemaakte groep $G^{\text{ab}} = G/[G, G]$. Anders gezegd: als $\pi: G \rightarrow G^{\text{ab}}$ het canonieke homomorfisme is, dan geeft $\varphi \mapsto \varphi \circ \pi$ een afbeelding $\text{Hom}(G^{\text{ab}}, A) \rightarrow \text{Hom}(G, A)$ en deze afbeelding is een isomorfisme van groepen.

14.4. Een homomorfisme van een groep G naar zichzelf noemen we een *endomorfisme* van G . We schrijven $\text{End}(G) := \text{Hom}(G, G)$ voor de verzameling van endomorfismen van G . Op deze verzameling is een binaire bewerking gedefinieerd door samenstelling van endomorfismen; immers, als φ en ψ endomorfismen van G zijn, dan is ook $\psi \circ \varphi$ een endomorfisme. Afgezien van het triviale geval dat $G = \{e\}$, is $\text{End}(G)$ met deze bewerking echter geen groep. Zie Opgave 14.5.

14.5. Voorbeelden. (a) Een homomorfisme $\varphi: \mathbb{Z} \rightarrow H$ wordt uniek bepaald door het element $h = \varphi(1)$, want met inductie zien we gemakkelijk in dat $\varphi(n) = h^n$ voor alle $n \in \mathbb{Z}$. Anderzijds is voor elke $h \in H$ de afbeelding $\varphi: \mathbb{Z} \rightarrow H$ gegeven door $\varphi(n) = h^n$ een homomorfisme. We vinden daarmee dat $\varphi \mapsto \varphi(1)$ een bijectie van verzamelingen $\text{Hom}(\mathbb{Z}, H) \rightarrow H$ geeft. Als speciaal geval hiervan vinden we dat $\text{End}(\mathbb{Z}) \cong \mathbb{Z}$, waarbij $k \in \mathbb{Z}$ correspondeert met het endomorfisme “vermenigvuldiging met k ”,

$$[k]: \mathbb{Z} \rightarrow \mathbb{Z}, \quad \text{gegeven door } m \mapsto km.$$

(Let op: zoals steeds is \mathbb{Z} de optelgroep van de gehele getallen; maar met km bedoelen we het product van de getallen k en m .)

(b) Zij $N \triangleleft G$ een normaaldeeler en zij $\pi: G \rightarrow G/N$ de canonieke afbeelding. Dan geeft $\psi \mapsto \psi \circ \pi$ een natuurlijke bijectie tussen $\text{Hom}(G/N, H)$ en de deelverzameling

$$\{\varphi: G \rightarrow H \mid \varphi(n) = e_H \text{ voor alle } n \in N\} \subset \text{Hom}(G, H).$$

Dit is gewoon een herformulering van de Homomorfiestelling.

(c) Combineren we (a) en (b) dan vinden we dat er voor elke groep H een bijectie is tussen $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, H)$ en de verzameling van elementen $h \in H$ waarvan de orde een deler is van n . In het bijzonder is $\text{End}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$, waarbij $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ correspondeert met het endomorfisme

$$[\bar{k}]: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad \text{gegeven door } (m \bmod n) \mapsto (km \bmod n).$$

14.6. Een bijectief endomorfisme van een groep G , noemen we een *automorfisme* van G . Anders gezegd: een automorfisme van G is een isomorfisme van G naar zichzelf. We schrijven $\text{Aut}(G)$ voor de verzameling van automorfismen van G . Per definitie is dit een deelverzameling van de verzameling $S(G)$ van alle permutaties van G .

14.7. Propositie. *Zij G een groep. Dan is $\text{Aut}(G)$ een ondergroep van $S(G)$.*

Bewijs. Dit volgt direct uit Propositie (5.11). □

14.8. Opmerking. Als we werken met automorfismen dan dreigt er soms wat notationale verwarring. Namelijk, als $\varphi: G \rightarrow G$ een automorfisme is, dan bedoelen we met φ^{-1} de inverse afbeelding; deze is ook weer een automorfisme van G . Deze inverse moet niet verward worden met de inverse in de groep G . Als $g \in G$ dan is $\varphi(g^{-1}) = \varphi(g)^{-1}$ maar dat is in het algemeen iets heel anders dan $\varphi^{-1}(g)$.

14.9. Als g een element is van een groep G dan is de afbeelding $\text{Inn}(g): G \rightarrow G$ gegeven door

$$\text{Inn}(g)(h) = ghg^{-1}$$

een automorfisme van G . We noemen $\text{Inn}(g)$ het *inwendige automorfisme* dat door g wordt gedefinieerd. (Engels: inner automorphism.) De relatie

$$g_1(g_2hg_2^{-1})g_1^{-1} = (g_1g_2)h(g_1g_2)^{-1}$$

laat zien dat voor elementen $g_1, g_2 \in G$ geldt dat $\text{Inn}(g_1) \circ \text{Inn}(g_2) = \text{Inn}(g_1g_2)$. Dit betekent dat de afbeelding

$$\text{Inn}: G \rightarrow \text{Aut}(G) \quad \text{gegeven door } g \mapsto \text{Inn}(g)$$

een homomorfisme van groepen is. Hieruit volgt dat de verzameling $\text{Inn}(G) \subset \text{Aut}(G)$ van alle inwendige automorfismen een ondergroep is van de automorfismengroep.

14.10. Propositie. *De ondergroep $\text{Inn}(G) \subset \text{Aut}(G)$ van inwendige automorfismen is isomorf met $G/Z(G)$ en is een normaaldeeler van $\text{Aut}(G)$.*

Bewijs. Als $g \in G$ dan is het inwendige automorfisme $\text{Inn}(g)$ de identiteit op G dan en slechts dan als $g \in Z(G)$. Dus $\text{Ker}(\text{Inn}) = Z(G)$ en toepassen van de Eerste Isomorfiestelling geeft dat $G/Z(G) \xrightarrow{\sim} \text{Inn}(G)$. Als φ een automorfisme is van G dan geldt voor alle $h \in G$ dat

$$(\varphi \circ \text{Inn}(g) \circ \varphi^{-1})(h) = \varphi(g\varphi^{-1}(h)g^{-1}) = \varphi(g)h\varphi(g)^{-1} = \text{Inn}(\varphi(g))(h).$$

Dit toont aan dat $\varphi \circ \text{Inn}(g) \circ \varphi^{-1} = \text{Inn}(\varphi(g))$ weer een inwendig automorfisme is; dus $\text{Inn}(G) \triangleleft \text{Aut}(G)$. \square

14.11. Opmerking De quotiëntgroep $\text{Aut}(G)/\text{Inn}(G)$ heet de *uitwendige automorfismengroep van G* , notatie $\text{Out}(G)$. (Engels: outer automorphisms.) De terminologie is een beetje misleidend, want de elementen van $\text{Out}(G)$ zijn geen automorfismen maar zijn klassen van automorfismen.

14.12. Voorbeelden. (a) Als $k \neq 0$ dan is het endomorfisme $[k]$ van \mathbb{Z} . Het beeld van $[k]$ is de ondergroep $k\mathbb{Z} \subset \mathbb{Z}$; dit is alleen de hele groep wanneer $k = \pm 1$. We vinden dat $\text{Aut}(\mathbb{Z}) = \{\pm \text{id}\}$.

(b) Zoals we hierboven hebben gezien, is $\text{End}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$, waarbij de klasse $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ correspondeert met het endomorfisme $[\bar{k}]: (m \bmod n) \mapsto (km \bmod n)$. Het beeld van het endomorfisme $[\bar{k}]$ is de ondergroep $(k\mathbb{Z}/n\mathbb{Z}) \subset (\mathbb{Z}/n\mathbb{Z})$. Dus

$$[\bar{k}] \text{ is bijjectief} \iff [\bar{k}] \text{ is surjectief} \iff \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*.$$

(De eerste equivalentie geldt omdat de groep eindig is.) De automorfismen van $\mathbb{Z}/n\mathbb{Z}$ zijn dus de afbeeldingen $[\bar{k}]$ met $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$. Omdat $[\bar{l}] \circ [\bar{k}] = [\bar{\ell k}]$ vinden we een isomorfisme van groepen $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

(c) Een automorfisme van een groep behoudt de ordes van elementen. In S_3 zijn er drie elementen van orde 2, namelijk (12) , (13) en (23) . Als $\varphi \in \text{Aut}(S_3)$ dan permuteert φ deze drie elementen; dit geeft een homomorfisme $\text{Aut}(S_3) \rightarrow S_3$. Dit homomorfisme is injectief, want S_3 wordt voortgebracht door de drie genoemde elementen. Anderzijds is het centrum van S_3 triviaal, dus de groep $\text{Inn}(S_3)$ van inwendige automorfismen is isomorf met S_3 . De conclusie is dat $\text{Inn}(S_3) = \text{Aut}(S_3) \cong S_3$. Algemener is het voor $n > 2$ waar dat $S_n \cong \text{Inn}(S_n) = \text{Aut}(S_n)$, behalve voor $n = 6$; in dat geval heeft $S_6 \cong \text{Inn}(S_6)$ index 2 in $\text{Aut}(S_6)$.

14.13. Zij N een normaaldeeler van een groep G . Als $g \in G$ dan hebben we een automorfisme $\gamma_g \in \text{Aut}(N)$ door $\gamma_g(n) = gng^{-1}$; dit automorfisme is dus niets anders dan de beperking van $\text{Inn}(g)$ tot N . Het automorfisme γ_g beschrijft in hoeverre het element g commuteert met de elementen van N . Merk op dat γ_g in het algemeen geen inwendig automorfisme van N is, want g hoeft geen element te zijn van N .

De afbeelding $g \mapsto \gamma_g$ definieert een homomorfisme $\gamma: G \rightarrow \text{Aut}(N)$. De kern van dit homomorfisme is de ondergroep

$$Z_G(N) := \{g \in G \mid gn = ng \text{ voor alle } n \in N\};$$

deze ondergroep heet de *centralisator van N in G* . Merk op dat $Z(G) \subset Z_G(N)$ en dat $Z_G(N) = G$ dan en slechts dan als $N \subset Z(G)$.

14.14. Stelling. *Zij G een groep van orde pq waarbij p en q twee priemgetallen zijn. Neem aan dat $p < q$ en dat p geen deler is van $q - 1$. Dan is $G \cong \mathbb{Z}/pq\mathbb{Z}$.*

Bewijs. Kies elementen $g \in G$ van orde p en $h \in G$ van orde q . (Het bestaan van dergelijke elementen wordt gegarandeerd door de Stelling van Cauchy.) Merk op dat g en h samen de hele groep G voortbrengen.

Uit Gevolg 13.6 weten we dat de ondergroep $N := \langle h \rangle$ een normaaldeler is van G . Verder weten we dat $N \cong \mathbb{Z}/q\mathbb{Z}$, zodat $\text{Aut}(N) \cong (\mathbb{Z}/q\mathbb{Z})^*$; dit is een groep van orde $q - 1$. Beschouw nu het homomorfisme $\gamma: G \rightarrow \text{Aut}(N)$. De orde van γ_g is een deler van $p = \text{orde}(g)$. Anderzijds volgt uit de Stelling van Lagrange dat $\text{orde}(\gamma_g)$ ook een deler is van $q - 1 = \#\text{Aut}(N)$. Omdat p geen deler is van $q - 1$ volgt dat $\gamma_g = \text{id}_N$. In het bijzonder commuteert g met het element h , en uit Propositie 12.2 volgt dat het element gh orde $\text{kgv}(p, q) = pq$ heeft. Dus G is cyclisch van orde pq . \square

14.15. De voorwaarde dat p geen deler is van $q - 1$ kan niet gemist worden; bijvoorbeeld: voor een oneven priemgetal q is de diëdergroep D_q een niet-abelse groep van orde $2q$.

Om de constructie van semidirect producten, die we hierna gaan behandelen, goed te begrijpen, is het instructief om nog eens naar het bewijs van de stelling te kijken, en te analyseren waarom dit bewijs alleen maar werkt als $p \nmid (q - 1)$. We vergelijken twee gevallen met elkaar: groepen van orde $10 = 2 \cdot 5$ (de stelling gaat niet op) versus groepen van orde $15 = 3 \cdot 5$ (stelling gaat wel op). We proberen voor groepen van orde 10 het argument zo lang mogelijk te volgen:

<i>groep van orde 10:</i>	<i>groep van orde 15:</i>
Stap 1: kies $g \in G$ van orde 2; kies $h \in G$ van orde 5.	kies $g \in G$ van orde 3; kies $h \in G$ van orde 5.
Stap 2: $N := \langle h \rangle$ is een normaaldeler; $N \cong \mathbb{Z}/5\mathbb{Z}$ en $\text{Aut}(N) \cong (\mathbb{Z}/5\mathbb{Z})^*$.	$N := \langle h \rangle$ is een normaaldeler; $N \cong \mathbb{Z}/5\mathbb{Z}$ en $\text{Aut}(N) \cong (\mathbb{Z}/5\mathbb{Z})^*$.
Stap 3: $\gamma_g \in \text{Aut}(N)$ is een automorfisme met $\gamma_g^2 = \text{id}$.	$\gamma_g \in \text{Aut}(N)$ is een automorfisme met $\gamma_g^3 = \text{id}$.
Stap 4: twee mogelijkheden: (a) $\gamma_g = \text{id}$, (b) $\gamma_g: h \mapsto h^{-1}$	de enige mogelijkheid is dat $\gamma_g = \text{id}$
Stap 5: (a) $gh = hg$; we vinden $G \cong \mathbb{Z}/10\mathbb{Z}$; (b) $gh = h^{-1}g$; we vinden $G \cong D_5$.	$gh = hg$; we vinden $G \cong \mathbb{Z}/15\mathbb{Z}$.

Het essentiële verschil tussen beide gevallen is dus, dat er bij een groep van orde 10 de mogelijkheid is om een niet-triviaal homomorfisme $\gamma: \langle g \rangle \rightarrow \text{Aut}(\langle h \rangle)$ te kiezen, wat uitdrukt dat we een groepsstructuur kunnen hebben waarbij de elementen g en h niet met elkaar commuteren.

14.16. Constructie. Zij gegeven een tweetal groepen N en H en een homomorfisme $\varphi: H \rightarrow \text{Aut}(N)$. We schrijven φ_h (in plaats van $\varphi(h)$) voor het beeld van een element h . Op de verzameling $N \times H$ definiëren we een bewerking door

$$(n_1, h_1) \star (n_2, h_2) := (n_1 \cdot \varphi_{h_1}(n_2), h_1 \cdot h_2). \quad (1)$$

14.17. Stelling. De verzameling $N \times H$ met de door (1) gegeven bewerking is een groep. Het eenheidselement van deze groep is (e_N, e_H) . De inverse van een element (n, h) is het element $(\varphi_h^{-1}(n^{-1}), h^{-1})$.

Bewijs. Het bewijs is een eenvoudige controle van de axioma's die we aan de lezer overlaten. \square

14.18. Definitie. De groep met onderliggende verzameling $N \times H$ en groepswet gegeven door (1) heet het *semidirecte product* van N en H met betrekking tot het homomorfisme φ . We noteren deze groep met $N \rtimes_{\varphi} H$. Als uit de context duidelijk is welk homomorfisme φ we bedoelen dan schrijven we gewoon $N \rtimes H$.

Als $\varphi: H \rightarrow \text{Aut}(N)$ het triviale homomorfisme is (d.w.z., $\varphi_h = \text{id}_N$ voor alle $h \in H$) dan is $N \rtimes_{\varphi} H$ het gewone product $N \times H$. We zullen hieronder een aantal interessantere voorbeelden bespreken.

14.19. Opmerkingen. Beschouw een semidirect product $G = N \rtimes_{\varphi} H$ zoals hierboven geconstrueerd.

(i) De afbeelding $i_N: N \rightarrow G$ gegeven door $n \mapsto (n, e_H)$ is een injectief homomorfisme. Het beeld is de ondergroep van G bestaande uit alle elementen van de vorm (n, e_H) . In wat volgt identificeren we deze ondergroep met N via het homomorfisme i_N .

(ii) De afbeelding $\pi: G \rightarrow H$ gegeven door $\pi(n, h) = h$ is een surjectief homomorfisme. De kern van dit homomorfisme is precies N . Derhalve is N een normaaldeler van G en de Eerste Isomorfiestelling geeft dat $G/N \cong H$.

(iii) De afbeelding $i_H: H \rightarrow G$ gegeven door $h \mapsto (e_N, h)$ is een injectief homomorfisme. Deze afbeelding is een snede van π , d.w.z., $\pi \circ i_H = \text{id}_H$. Het beeld van i_H is de ondergroep van G bestaande uit alle elementen van de vorm (e_N, h) . We identificeren deze ondergroep met H via het homomorfisme i_H .

(iv) Elk element $g \in G$ kan, met de voorgaande identificaties, worden geschreven als $g = nh$ met $n \in N$ en $h \in H$. Hierbij zijn n en h uniek bepaald door g . Elementen van N worden vermenigvuldigd zoals in de groep N , elementen van H worden vermenigvuldigd zoals in de groep H ; tenslotte is er de commutatieregel $h \cdot n = \varphi_h(n) \cdot h$. Deze regels leggen G helemaal vast.

Voordat we voorbeelden geven van semidirecte producten, bewijzen we een handig criterium waarmee we kunnen aantonen dat een groep isomorf is met een semidirect product. Dit resultaat is een generalisatie van Propositie 12.3.

14.20. Propositie. Zij G een groep. Stel we hebben een ondergroep $H \subset G$ en een normaaldeler $N \triangleleft G$ die voldoen aan de volgende voorwaarden:

- (a) $H \cap N = \{e\}$;
- (b) H en N brengen samen de hele groep G voort.

Zij $\varphi: H \rightarrow \text{Aut}(N)$ het homomorfisme gegeven door $\varphi_h(n) = hnh^{-1}$. (Met andere woorden, φ is de beperking van het homomorfisme $\gamma: G \rightarrow \text{Aut}(N)$ uit 14.13 tot de ondergroep H .) Dan is de afbeelding $f: N \rtimes_{\varphi} H \rightarrow G$ gegeven door $f(n, h) = nh$ een isomorfisme van groepen.

Bewijs. Om te beginnen gaan we na dat f een homomorfisme is. Bekijk daartoe twee elementen

(n_1, h_1) en (n_2, h_2) van $N \rtimes_{\varphi} H$. Dan is

$$\begin{aligned} f((n_1, h_1) \star (n_2, h_2)) &= f(n_1 \cdot h_1 n_2 h_1^{-1}, h_1 \cdot h_2) \\ &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 h_1 n_2 h_2 = f(n_1, h_1) \cdot f(n_2, h_2). \end{aligned}$$

Dit toont aan dat f inderdaad een homomorfisme is. Als $(n, h) \in \text{Ker}(f)$ dan is $n = h^{-1}$ een element van $H \cap N$, dus uit (a) volgt dat $h = n = e$. Dit toont aan dat $\text{Ker}(f) = \{(e, e)\}$, zodat f injectief is. Het beeld van f is een ondergroep van G die H en N bevat, dus uit (b) volgt dat $\text{Im}(f) = G$. Daarmee is bewezen dat f een bijtief homomorfisme is. \square

14.21. Voorbeelden. (a) De diëdergroep D_n is isomorf met $(\mathbb{Z}/n\mathbb{Z}) \rtimes_{\psi} (\mathbb{Z}/2\mathbb{Z})$, waarbij

$$\psi: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z})$$

het homomorfisme is dat $(1 \bmod 2)$ stuurt naar het automorfisme $[-1]: (i \bmod n) \mapsto (-i \bmod n)$. Om dit in te zien, passen we de propositie toe op de ondergroepen $N = \langle r \rangle$ en $H = \langle s \rangle = \{\text{id}, s\}$ van D_n . Het is duidelijk dat is voldaan aan de voorwaarden (a) en (b). Het homomorfisme $\varphi: H \rightarrow \text{Aut}(N)$ stuurt s naar het automorfisme van N dat wordt gegeven door $r \mapsto srs^{-1} = r^{-1}$. Merk nu op dat $\mathbb{Z}/2\mathbb{Z} \cong H$ en dat $\mathbb{Z}/n\mathbb{Z} \cong N$ via $(i \bmod n) \mapsto r^i$. Onder deze identificaties correspondeert φ met ψ .

(b) Een afbeelding $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ heet een *affiene transformatie* als er een lineaire afbeelding $A: \mathbb{R}^n \rightarrow \mathbb{R}^n$ en een vector $b \in \mathbb{R}^n$ bestaan zo dat $f(x) = A(x) + b$ voor alle $x \in \mathbb{R}^n$. Met andere woorden, als we t_b schrijven voor de translatie over b , dan zijn de affiene transformaties van \mathbb{R}^n de afbeeldingen van de vorm $t_b \circ A$, met $A: \mathbb{R}^n \rightarrow \mathbb{R}^n$ een lineaire transformatie. De affiene transformatie $f = t_b \circ A$ is inverteerbaar dan en slechts dan als A inverteerbaar is.

We rekenen gemakkelijk na dat

$$(t_{b_2} \circ A_2) \circ (t_{b_1} \circ A_1) = t_{b_2 + A_2(b_1)} \circ (A_2 \circ A_1). \quad (2)$$

Dit ziet eruit als de rekenregel in een semidirect product!

We schrijven $\text{Aff}(\mathbb{R}^n)$ voor de verzameling van inverteerbare affiene transformaties van \mathbb{R}^n . Uit (2) volgt gemakkelijk dat voor $f = t_b \circ A$ in $\text{Aff}(\mathbb{R}^n)$ de inverse afbeelding gegeven wordt door $f^{-1} = t_{-A^{-1}(b)} \circ A^{-1}$. In het bijzonder zien we dat $\text{Aff}(\mathbb{R}^n)$ een ondergroep is van de permutatiegroep $S(\mathbb{R}^n)$.

De translaties t_b vormen een ondergroep van $\text{Aff}(\mathbb{R}^n)$ die isomorf is met de optelgroep \mathbb{R}^n . Het is gemakkelijk na te rekenen dat deze ondergroep een normaaldeler is. De lineaire afbeeldingen A vormen ook een ondergroep van $\text{Aff}(\mathbb{R}^n)$; deze ondergroep is de groep $\text{GL}_n(\mathbb{R})$ van inverteerbare $n \times n$ matrices. Uit Propositie 14.20 volgt dat $\text{Aff}(\mathbb{R}^n)$ isomorf is met het semidirecte product $\mathbb{R}^n \rtimes \text{GL}_n(\mathbb{R})$. Het homomorfisme $\varphi: \text{GL}_n(\mathbb{R}) \rightarrow \text{Aut}(\mathbb{R}^n)$ is gewoon de inclusie van $\text{GL}_n(\mathbb{R})$ in de automorfismengroep van \mathbb{R}^n .

(c) Neem $G = S_n$. We kunnen de propositie toepassen op de ondergroepen $H = \{\text{id}, (1\ 2)\}$ en $N = A_n$. Het corresponderende homomorfisme $\varphi: H \rightarrow \text{Aut}(A_n)$ stuurt $\alpha = (1\ 2)$ naar het automorfisme $\sigma \mapsto \alpha\sigma\alpha^{-1}$ van A_n . We vinden dat S_n een semidirect product is van A_n met $H \cong \mathbb{Z}/2\mathbb{Z}$.

14.22. Voorbeelden. De constructie van een semidirect product stelt ons ook in staat om vele “nieuwe” groepen te maken. Begin bijvoorbeeld met een abelse groep A ; we zullen voor A de multiplicatieve notatie gebruiken. Dan is de inverse $i_A: a \mapsto a^{-1}$ een automorfisme van orde ≤ 2 . Zij $H = \{1, s\}$ een multiplicatief geschreven groep van orde 2 (dus $s^2 = 1$ in H), en zij $\varphi: H \rightarrow \text{Aut}(A)$ het homomorfisme gegeven door $\varphi(s) = i_A$. Dit geeft ons een semidirect product $G := A \rtimes_{\varphi} H$; we noemen deze groep een *gegeneraliseerde diëdergroep*. De elementen van G zijn van de vorm $g = a$ of $g = as$, met $a \in A$. Elementen van A worden vermenigvuldigd volgens de regels van A ; verder geldt dat $s^2 = 1$ en dat $sa = a^{-1}s$ voor alle $a \in A$.

14.23. Als N een normaaldeler van een groep G is en G/N is de quotiëntgroep, dan zouden we willen begrijpen in hoeverre we de structuur van G kunnen terugvinden uit de groepen N en G/N . Het is natuurlijk te optimistisch te verwachten dat G helemaal bepaald wordt door N en G/N ; in het algemeen is aanvullende informatie nodig. Dit kan bijvoorbeeld aanvullende informatie zijn over hoe elementen van G commuteren met elementen van N , zoals precies gemaakt in de constructie van het semidirecte product. Het in het algemeen echter niet zo dat G altijd een semidirect product is van N en G/N . Het laatste resultaat van dit hoofdstuk geeft een eenvoudig criterium voor wanneer dit het geval is.

14.24. Propositie. *Zij G een groep. Zij $N \triangleleft G$ een normaaldeler, en zij $\pi: G \rightarrow G/N$ de canonieke afbeelding. Dan zijn de volgende twee eigenschappen equivalent:*

- (a) *Er is een snede $s: G/N \rightarrow G$ van π .*
- (b) *Er is een homomorfisme $\varphi: G/N \rightarrow \text{Aut}(N)$ en een isomorfisme $f: G \xrightarrow{\sim} N \rtimes_{\varphi} G/N$, zo dat $f(n) = (n, e)$ voor alle $n \in N$ en $(\pi \circ f^{-1})(e, gN) = gN$ voor alle $gN \in G/N$.*

(De voorwaarden in (b) drukken uit dat G een semidirect product is van N en G/N op zo'n manier dat de inclusie van N en de projectie op G/N de gegeven homomorfismen zijn.)

Bewijs. De implicatie (b) \Rightarrow (a) is duidelijk; vgl. (iii) in 14.19. Omgekeerd, als er een snede s bestaat, laat dan $H = \text{Im}(s)$. Er is voldaan aan de voorwaarden in Propositie 14.20 en dit geeft de gewenste beschrijving van G als een semidirect product van N en $H \cong G/N$. \square

Opgaven bij hoofdstuk 14.

Opgave 14.1.

- (i) Bepaal voor alle $n \geq 1$ alle homomorfismen $A_n \rightarrow \mathbb{C}^*$. [*Hint*: bepaal eerst A_n^{ab} .]
- (ii) Bepaal voor alle $n \geq 1$ alle homomorfismen $D_n \rightarrow \mathbb{C}^*$. [*Hint*: bepaal eerst D_n^{ab} .]

Opgave 14.2.

- (i) Laat zien dat $Z(S_4) = \{\text{id}\}$ en concludeer dat $S_4 \cong \text{Inn}(S_4)$.
- (ii) Zij φ een automorfisme van S_4 . Als $\sigma \in S_4$, laat zien dat σ en $\varphi(\sigma)$ hetzelfde cykeltype hebben. Concludeer dat φ de drie elementen

$$\alpha_1 := (12)(34), \quad \alpha_2 := (13)(24), \quad \text{en} \quad \alpha_3 := (14)(23)$$

onderling permuteert. Dit geeft een homomorfisme $\rho: \text{Aut}(S_4) \rightarrow S_3$.

Als $\sigma = (ab)$ een 2-cykel in S_4 is, dan schrijven we σ' voor de complementaire 2-cykel; hiermee bedoelen we de unieke 2-cykel $\sigma' = (cd)$ zo dat $\{1, 2, 3, 4\} = \{a, b, c, d\}$. (Dus $(13)' = (24)$, etc.) Merk op dat σ' de unieke 2-cykel $\neq \sigma$ is die commuteert met σ .

- (iii) Laat zien dat voor alle 2-cykels $\sigma \in S_4$ geldt dat $\varphi(\sigma') = \varphi(\sigma)'$.
- (iv) Als $\varphi \in \text{Ker}(\rho)$, laat zien dat voor alle 2-cykels σ geldt dat ofwel $\varphi(\sigma) = \sigma$, ofwel $\varphi(\sigma) = \sigma'$.
- (v) Toon aan dat $\#\text{Ker}(\rho) \leq 4$. [*Hint*: gebruik conjugatierelaties zoals $(13)(12)(13) = (23)$.]
- (vi) Bewijs dat $\text{Aut}(S_4) = \text{Inn}(S_4) \cong S_4$.

Opgave 14.3. Zij p een oneven priemgetal. Bij het vak Algebra 2 zullen we bewijzen dat de groep $(\mathbb{Z}/p\mathbb{Z})^*$ cyclisch is van orde $p - 1$, d.w.z., $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p - 1)\mathbb{Z}$. In deze opgave mag je gebruik maken van dit feit.

- (i) Zij G een groep van orde $2p$. Bewijs dat $G \cong \mathbb{Z}/2p\mathbb{Z}$ of $G \cong D_p$.
- (ii) Zij q een priemgetal dat $p - 1$ deelt. Bewijs dat er op isomorfie na precies één niet-abelse groep van orde pq bestaat.

Opgave 14.4. Een ondergroep $H \subset G$ heet een *karakteristieke ondergroep* als voor elk automorfisme $\varphi \in \text{Aut}(G)$ geldt dat $\varphi(H) = H$.

- (i) Laat zien dat een karakteristieke ondergroep een normaaldeeler is.
- (ii) Bewijs dat $[G, G]$ en $Z(G)$ karakteristieke ondergroepen zijn.
- (iii) Zij $H_n \subset G$ de ondergroep voortgebracht door alle n -de machten in G ; met andere woorden, $H = \langle g^n \mid g \in G \rangle$. Bewijs dat H een karakteristieke ondergroep is.
- (iv) Welke ondergroepen van de groep Q zijn normaaldeeler? En welke zijn karakteristiek?

Opgave 14.5. Zij G een groep. We beschouwen de verzameling $\text{End}(G)$ van endomorfismen van G met daarop de binaire bewerking \circ gegeven door samenstelling van endomorfismen.

- (i) Laat zien dat de bewerking \circ associatief is en een eenheidselement heeft.
- (ii) Laat zien dat $(\text{End}(G), \circ)$ geen groep is, tenzij $G = \{e\}$.

***Opgave 14.6.** Zij G een groep van orde 8 die niet abels is. Het doel van deze opgave is te bewijzen dat $G \cong D_4$ of $G \cong Q$.

- (i) Bewijs dat $\#Z(G) = 2$ en dat $G/Z(G) \cong V_4$.
- (ii) Bewijs dat de canonieke afbeelding $G \rightarrow G/Z(G) \cong V_4$ geen sectie heeft. Concludeer hieruit dat G een element van orde 4 heeft.
- (iii) Zij $g \in G$ een element van orde 4. Laat zien dat $Z(G) = \{e, g^2\}$.
- (iv) Kies een element $h \in G$ met $h \notin \langle g \rangle$. Laat zien dat $hgh^{-1} = g^{-1}$ en dat $\langle g, h \rangle = G$.
- (v) Bewijs dat $G \cong D_4$ als $\text{orde}(h) = 2$ en dat $G \cong Q$ als $\text{orde}(h) = 4$.

INDEX

affiene transformatie, 12

automorfisme, 8
inwendig, 8

centralisator, 9

diëdergroep
gegeneraliseerd, 13

endomorfisme, 7

gegeneraliseerde diëdergroep, 13

inwendig automorfisme, 8

semidirect product, 11
snede, 2