Hoofdstuk 4

Groepsconstructies

4.1 Direct product

We gaan nu bestuderen hoe we van 2 groepen een nieuwe groep kunnen maken of hoe we een groep kunnen schrijven als een product van 2 groepen met kleinere orde. Op die manier kunnen we op zoek naar de elementaire bouwstenen van de groepen. Zoals elk natuurlijk getal geschreven kan worden als een product van priemgetallen, zo zoeken we nu naar groepen waaruit elke groep is opgebouwd.

Definitie 4.1. Als H en K normaaldelers zijn van een groep G en $H \cap K = \{e\}$ en $HK = G$ dan noemt men G het direct product van H en K.

Notatie: $G = H \times K$. Men zegt ook dat G ontbonden is in H en K. Elk element van G is dan op een unieke manier te schrijven als een product van een element uit H en een element uit K. Want veronderstel dat $g = hk = h'k'$, dan is $h'^{-1}h = k'k^{-1} \in H \cap K$. Uit de definitie volgt dan dat $h'^{-1}h = k'k^{-1} = e$ en dus is $h = h'$ en $k = k'$.
Een verwante constructie is het uitwendig direct product. Als G_1 en G_2 groepen zijn met eenheidselementen e_1 en e_2, dan construeren we de verzameling $G' = G_1 \times G_2 = \{(g_1, g_2)$ met $g_1 \in G_1$ en $g_2 \in G_2\}$. De groepsbewerking wordt verder gegeven door:

$$(g_1, g_2).(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

Het is duidelijk dat de deelgroep $G_1 \times \{e_2\}$ congruent is met G_1 en dat de deelgroep $\{e_1\} \times G_2$ congruent is met G_2. Beide deelgroepen zijn normaal-

delers van G'. Nu is G' het direct product van beide deelgroepen volgens de definitie hierboven. Ook hier gebruiken we de notatie $G = H \times K$.
We bestuderen nu enkele eigenschappen van het direct product.

Stelling 4.2. *$A \times B \cong B \times A$.*

Bewijs. Definieer $\varphi : A \times B \to B \times A : (a, b) \mapsto (b, a)$. Het is duidelijk dat φ bijectief is. Het is ook een homomorfisme, want $\varphi((a, b).(c, d)) = \varphi((ac, bd)) = (bd, ac) = (b, a).(d, c) = \varphi((a, b)).\varphi((c, d))$. Bijgevolg is φ een isomorfisme en volgt het gestelde. □

Stelling 4.3. *$A \times (B \times C) \cong (A \times B) \times C$.*

Bewijs. Definieer $\varphi : A \times (B \times C) \to (A \times B) \times C : (a, (b, c)) \mapsto ((a, b), c)$. Het is duidelijk dat φ bijectief is. Het is ook een homomorfisme, want $\varphi((a, (b, c)).(d, (e, f))) = \varphi((ad, (b, c).(e, f)) = \varphi((ad, (be, cf)) = ((ad, be), cf)$ $= ((a, b).(d, e), cf) = ((a, b), c).((d, e), f) = \varphi((a, (b, c)).\varphi((d, (e, f))$. Bijgevolg is φ een isomorfisme en volgt het gestelde. □

Stelling 4.4. *De orde van $(a, b) \in A \times B$ is het kleinste gemene veelvoud van de ordes van a en b.*

Bewijs. Stel dat de orde van (a, b) gelijk is aan n, dan geldt $(a, b)^n = (e_1, e_2)$. Bijgevolg is $a^n = e_1$ en $b^n = e_2$. Maar dan is de orde van a een deler van n en ook de orde van b is een deler van n. Dus is n het kleinste gemene veelvoud van de ordes van a en b. □

Stelling 4.5. *$A \times B$ is abels als en slechts als A en B abels zijn.*

Bewijs. Het is evident dat als A en B abels zijn, $A \times B$ dit ook is. Veronderstel nu omgekeerd dat $A \times B$ een abelse groep is, dan is $(gh, e) = (g, e)(h, e) = (h, e)(g, e) = (hg, e)$ en dus is $gh = hg$. Bijgevolg is A een abelse groep. Analoog voor B. □

Voor abelse groepen kunnen we nu een belangrijke stelling formuleren die de groep gaat ontbinden in factoren met orde een priemmacht.

Stelling 4.6. *G eindig abels met orde ab en ggd(a,b)=1. Dan is $G \cong A \times B$, waarbij de orde van A gelijk is aan a en de orde van B gelijk is aan b.*

Bewijs. Als $a = 1$ of $b = 1$ dan is de stelling evident. Omdat de orde van G gelijk is aan ab, geldt $\forall g \in G : g^{ab} = e$. Construeer nu $A = \{g \in G : g^a = e\}$ en $B = \{g \in G : g^b = e\}$. Dit zijn deelgroepen van G, want als $x, y \in A$, dan is $(xy^{-1})^a = x^a.(y^a)^{-1} = e.e^{-1} = e$. Bijgevolg is $xy^{-1} \in A$. Analoog voor B. Rest ons te bewijzen dat $G = A \times B$. Omdat ggd(a,b)= 1 bestaan er gehele getallen $r, s : ra + sb = 1$. Dan is $g = g^1 = (g^r)^a.(g^s)^b$. Hierbij geldt dat $(g^r)^a \in B$ want $((g^r)^a)^b = (g^r)^{ab} = e$. Analoog is $(g^s)^b \in A$. Bijgevolg is elk element van G te schrijven als product van een element van A en van B, dus $G = AB$. Neem nu $x \in A \cap B$, dan moet de orde van x een deler zijn van a en van b. Maar ggd(a,b)=1, dus moet $x = e$. Bijgevolg is $G = A \times B$. Rest te bewijzen dat de orde van A gelijk is aan a en die van B gelijk is aan b. Hiervoor proberen we te bewijzen dat $|A|$ en b onderling ondeelbaar zijn. Stel dat dit niet zo is, dan bestaat er een priemgetal p dat een deler is van b en van $|A|$. Volgens de stelling van Cauchy bestaat er dan een $x \in A$ met $o(x) = p$. Anderzijds is de orde van x een deler van a en p kan a niet delen want het deelt b en de ggd(a,b)=1. Een tegenspraak en dus zijn $|A|$ en b onderling ondeelbaar. Analoog zijn de orde van B en a ook onderling ondeelbaar. Omdat we weten dat de orde van A een deler moet zijn van ab volgt hier uit dat de orde van A een deler moet zijn van a en dus is de orde van A gelijk aan a. Analoog is de orde van B gelijk aan b. □

Stelling 4.7. *Elke eindige abelse groep is het direct product van eindige abelse groepen van priemmacht grootte.*

Bewijs. Stel dat de orde van G gelijk is aan n, dan is de priemontbinding van $n = p_1^{e_1}.p_2^{e_2} \cdots .p_r^{e_r}$. Neem $a = p_1^{e_1}$ en $b = \frac{n}{a}$. We kunnen nu vorige stelling toepassen en schrijven dat $G = A \times B$ waarbij de orde van A gelijk is aan $p_1^{e_1}$ en de orde van B gelijk is aan B. We kunnen deze procedure herhalen op B. □

4.2 Semidirect product

We kunnen de definitie van het direct product veralgemenen door de voorwaarde dat beide deelgroepen normaaldelers moeten zijn, af te zwakken.

Definitie 4.8. Als H een normaaldeler en K een deelgroep is van een groep G en $H \cap K = \{e\}$ en $HK = G$ dan noemt men G het semidirect product van H en K.

Notatie: $G = H \rtimes K$. Men zegt ook dat G *gesplitst* wordt over H. Net zoals bij het direct product is elk element van G op een unieke manier te schrijven als product van een element van H en een element van K.

Stelling 4.9. *Als $G = H \rtimes K$ met H een normaaldeler en K een deelgroep van G, dan is $K \cong G/H$.*

Bewijs. Neem $f : K \to G/H : k \mapsto kH$. Het is duidelijk dat f een homomorfisme is. Nu is f ook injectief, want $f(k) = f(k') \Rightarrow kH = k'H \Rightarrow k^{-1}k' \in H$. Maar $k^{-1}k' \in K$ en $K \cap H = \{e\}$, dus is $k = k'$. Bovendien is f surjectief. Neem immmers $gH \in G/H$, dan is $g = kh$ op een unieke manier. Dus is $gH = khH = kH = f(k)$. Bijgevolg is f een isomorfisme en is het gestelde bewezen. □

Gevolg 4.10. *Als G het semidirect product is van een normaaldeler H en een deelgroep K, en H en K zijn beiden eindig, dan is de orde van G het product van de ordes van H en K.*

Gevolg 4.11. *G is het semidirect product van H en K met $K \cong G/H$ als $g : G \to G/H : g \mapsto gH$ splitst, met andere woorden als er een $s : G/H \to G$ bestaat zodat $g \circ s = I_{G/H}$. Men noemt s een sectie van g.*

In tegenstelling met het direct product, is het semidirect product van twee groepen meestal niet uniek. Als G en G' twee groepen zijn die isomorfe kopies bevatten van H als normaaldeler en K als deelgroep, en beiden zijn ze het semidirect product van H en K, dan moeten G en G' niet isomorf zijn. De extra informatie die we nodig hebben om de structuur van G uniek te bepalen bestaat uit een homomorfisme $\varphi : K \to Aut(H) : k \mapsto \varphi_k$ met $\varphi_k(h) = khk^{-1}$. Dit homomorfisme is de lijm waarmee je de twee deelgroepen samenhoudt.

Neem nu twee elementen hk en $h'k'$ van G, hoe moet je nu hun product en het inverse van hk schrijven in dezelfde vorm?
$(hk)(h'k') = h(kh'k^{-1})kk' = h\varphi_k(h')kk'$ en $(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1} = \varphi_{k^{-1}}(h^{-1})k^{-1}$.
Als we nu omgekeerd starten vanuit 2 groepen H en K en een homorfisme $\varphi : K \to Aut(H) : k \mapsto \varphi_k$ is er dan altijd een semidirect product te vinden op basis van deze informatie? De onderliggende verzameling is het product van H en K, dus $\{(h,k) : h \in H \text{ en } k \in K\}$ en de bewerking wordt gedefinieerd als:

$$(h,k)(h',k') = (h\varphi_k(h'), kk')$$

Het neutraal element is (e_H, e_K) en het inverse element is gegeven door

$$(h,k)^{-1} = (\varphi_{k^{-1}}(h^{-1}), k^{-1})$$

Deze bewerking is associatief:

$$\begin{aligned}((h,k)(h',k'))(h'',k'') =& (h\varphi_k(h'), kk')(h'',k'')\\ =& (h\varphi_k(h')\varphi_{kk'}(h''), kk'k'')\\ =& (h\varphi_k(h')\varphi_k(\varphi_{k'}(h'')), kk'k'')\\ =& (h\varphi_k(h'\varphi_{k'}(h'')), kk'k'')\\ =& (h,k)(h'\varphi_{k'}(h''), k'k'')\\ =& (h,k)((h',k')(h'',k''))\end{aligned}$$

(e_H, e_K) is het neutraal element, want $(h,k)(e_H,e_K) = (h\varphi_k(e_H), k) = (h,k)$.
$(\varphi_{k^{-1}}(h^{-1}), k^{-1})$ is het symmetrische element van (h,k), want
$(h,k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) = (hh^{-1}, e_K) = (e_H, e_K)$
We hebben dus een groep. Rest te bewijzen dat dit het semidirect product is van H en K. Net zoals bij het direct product kunnen we H identificeren met $H' = \{(h, e_K) : h \in H\}$ en K met $K' = \{(e_H, k) : k \in K\}$. Het is duidelijk dat $H' \cap K' = \{(e_H, e_K)\}$ en dat $G = H'K'$.
Is H' nu ook nog een normaaldeler van G?
$(e_H,k)(h,e_K)(e_H,k)^{-1} = (e_H,k)(h,e_K)(e_H,k^{-1}) = (\varphi_k(h),k)(e_H,k^{-1}) = (\varphi_k(h), e_K) \in H'$

Gevolg 4.12. *Het direct product $H \times K$ is het semidirect product met $\varphi : K \to Aut(H) : k \mapsto I_H$, want $(h,k)(h',k') = (h\varphi_k(h'), kk') = (hh', kk')$.*

Stelling 4.13. *$K' = \{(e_H, k) : k \in K\}$ is een normaaldeler van G als en slechts als φ het triviaal homomorfisme is.*

Bewijs. Stel dat $\varphi_k(h) \neq h$. Dan is: $(h, e_K)(e_H, k)(h, e_K)^{-1} = (h, e_K)(e_H, k)(h^{-1}, e_K) = (h, k)(h^{-1}, e_K) = (h\varphi_k^{-1}(h), k) \notin K'$. Dus als φ niet triviaal is, dan is K' niet normaal in G. Als omgekeerd, φ triviaal is, dan is G het direct product $H \times K$ en is K' normaal in G. □

Stelling 4.14. *Als φ niet triviaal is, dan is $H \rtimes K$ niet abels, zelfs al zijn H en K wel abels.*

Bewijs. Stel dat φ niet triviaal is, dus dat $\varphi_k(h) \neq h$. Dan is $(h, e_K)(e_H, k) = (h, k)$ en $(e_H, k)(h, e_K) = (\varphi_k(h), k)$. Bijgevolg is G niet abels. □

Als H een normaaldeler van een groep G is en G/H de quotiëntgroep, dan zouden we willen begrijpen in hoeverre we de structuur van G kunnen terugvinden uit de groepen H en G/H. Het is natuurlijk te optimistisch te verwachten dat G helemaal bepaald wordt door H en G/H; in het algemeen is aanvullende informatie nodig. Dit kan bijvoorbeeld aanvullende informatie zijn hoe elementen van G commuteren met elementen van H, zoals precies gemaakt wordt in de constructie van det semidirecte product. Het is in het algemeen echter niet zo dat G altijd een semidirect product is van H en G/H. We eindigen met een stelling die ons zegt wanneer 2 semidirecte producten isomorf zijn.

Stelling 4.15. *Zij H een normaaldeler van G en K een deelgroep van G. Als φ_1 en φ_2 twee homomorfismen zijn van K op $Aut(H)$ en $\varphi_2 = \varphi_1 \circ f$, waarbij f een automorfisme is van K, dan is $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.*

Bewijs. Definieer $\alpha : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K : (h, k) \mapsto (h, f^{-1}(k))$.
We tonen eerst aan dat α een homomorfisme is:

$$\begin{aligned}\alpha(h_1, k_1)\alpha(h_2, k_2) =& (h_1, f^{-1}(k_1))(h_2, f^{-1}(k_2)) \\ =& (h_1\varphi_2(f^{-1}(k_1), f^{-1}(k_1)f^{-1}(k_2)) \\ =& (h_1\varphi_1(k_1), f^{-1}(k_1k_2)) \\ =& \alpha((h_1, k_1)(h_2, k_2))\end{aligned}$$

Bovendien is α bijectief met inverse de afbeelding $(h, k) \mapsto (h, f(k))$. Dus is α een isomorfisme en is de stelling bewezen. $\square$

4.3 Groepsuitbreidingen

Het semidirect product is een veralgemening van het direct product. Zo kunnen we ook het semidirect product nog veralgemenen door de voorwaarde $H \cap K = \{e\}$ weg te laten.

Definitie 4.16. Een groep G is een groepsuitbreiding van H door K als H een normaaldeler is van G en $K \cong G/H$. We noteren:
$G = H \uparrow K$.

Een andere manier om een groepsuitbreiding weer te geven is via korte exacte rijen. Dit is een opeenvolging van 3 groepen met homomorfismen er tussen zodat het beeld van elk homomorfisme de kern is van het volgende homomorfsme.

Definitie 4.17. Een groep G is een groepsuitbreiding van H door K als er een korte exacte rij groepen bestaat:

$$1 \to H \xrightarrow{f} G \xrightarrow{g} K \to 1$$

Hierbij is f injectief, g surjectief en $bldf = kerg$.
Het directe product $H \times K$ kan ingepast worden in een korte exacte rij :

$$1 \to H \xrightarrow{f} H \times K \xrightarrow{g} K \to 1$$

met $f(h) = (h, 1)$ en $g(h, k) = k$.
Ook het semidirecte product kan ingepast worden in een korte exacte rij :

$$1 \to H \xrightarrow{f} H \rtimes K \xrightarrow{g} K \to 1$$

met ook hier $f(h) = (h, 1)$ en $g(h, k) = k$.
Rest ons nog te bewijzen dat beide definities equivalent zijn.

Stelling 4.18. *Beide definities van een groepsuitbreiding zijn gelijkwaardig.*

Bewijs. Als H een normaaldeler is van G dan bestaat er een korte exacte rij

$$1 \to H \xrightarrow{f} G \xrightarrow{g} G/H \to 1$$

waarbij f de inclusie is van H in G en g het homomorfisme dat elk element van G afbeeldt op zijn nevenklasse modulo H. Als we omgekeerd een willekeurige korte exacte rij hebben

$$1 \to H \xrightarrow{f} G \xrightarrow{g} K \to 1$$

dan is $H \cong f(H) = kerg$ en $K \cong G/kerg$. Dit induceert een isomorfisme $g' : G/kerg \to K$. We krijgen dan volgend schema dat commuteert:

$$\begin{array}{ccccccccc} 1 & \to & H & \xrightarrow{f} & G & \xrightarrow{g} & K & \to & 1 \\ & & \downarrow f & & \downarrow Id & & \downarrow g' & & \\ 1 & \to & f(H) & \to & G & \to & G/kerg & \to & 1 \end{array}$$

Hiermee is duidelijk te zien dat de gegeven korte exacte rij eigenlijk hetzelfde is dan de korte exacte rij die ontstaat door een normaaldeler f(H). □

Een eindige groep is ofwel enkelvoudig ofwel een uitbreiding van twee kleinere groepen. Als we een volledige lijst hebben van de enkelvoudige groepen en als we inzicht hebben in groepsuitbreidingen, dan begrijpen we alle eindige groepen. Dus is één van de basisproblemen in de groepentheorie het bepalen van alle groepsuitbreidingen van H door K of met andere woorden het bepalen van alle groepen G die in een korte exacte rij tussen H en K kunnen geplaatst worden. Hierbij zijn H en K enkelvoudige groepen. Er is altijd minstens 1 groep tussen H en K te plaatsen, namelijk het (semi)directe product van H en K. Omdat de constructie van korte exacte rijen met (semi)directe producten gekend is, worden ze als triviaal beschouwd. Het is dus belangrijk te herkennen of een korte exacte rij afkomstig is van een (semi)direct product. Vandaar volgende twee stellingen:

Stelling 4.19. *Als* $1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta} K \to 1$ *een korte exacte rij is dan zijn volgende uitspraken equivalent:*

1. *Er bestaat een homomorfisme* $\alpha' : G \to H$ *zodat voor alle* $h \in H$ *geldt dat* $\alpha'(\alpha(h)) = h$.
2. *Er bestaat een isomorfisme* $\theta : G \to H \times K$ *zodat onderstaand schema commuteert:*

$$\begin{array}{ccccccccc} 1 & \to & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \to & 1 \\ & & \downarrow Id & & \downarrow \theta & & \downarrow Id & & \\ 1 & \to & H & \to & H \times K & \to & K & \to & 1 \end{array}$$

Bewijs. Definieer $\theta : G \to H \times K : g \mapsto (\alpha'(g), \beta(g))$. We tonen aan dat θ een isomorfisme is:

1. Omdat α' en β homomorfismen zijn is θ dat ook.
2. θ is injectief, want als $\theta(g) = (1, 1)$, dan is $\alpha'(g) = 1$ en $\beta(g) = 1$. Bijgevolg zit g in $ker\beta = bld\alpha$ en bestaat er een $h \in H$ met $g = \alpha(h)$. Maar omdat $\alpha'(g) = 1$ is $\alpha'(\alpha(h)) = 1$ en dus is $h = 1$ en bijgevolg is $g = \alpha(1) = 1$.
3. θ is ook surjectief. Stel $(h, k) \in H \times k$. Omdat β surjectief is, bestaat er een $g \in G : \beta(g) = k$. Omdat $ker\beta = bld\alpha$ is de algemene vorm van een element dat op k wordt afgebeeld door β, gegeven door $g.\alpha(x)$ met $x \in H$. Zoek nu x zodat $\alpha'(g.\alpha(x)) = h$, want dan is er inderdaad een element $g.\alpha(x)$ dat op (h, k) wordt afgebeeld door θ. Neem $x = \alpha'(g)^{-1}h$.

Rest nog te bewijzen dat het schema commuteert. Bekijken we eerst het eerste vierkant. Als we, vertrekkend bij H linksom gaan dan wordt h afgebeeld op $(h,)$. Gaan we rechtsom dan wordt h afgebeeld op $\theta(\alpha(h)) = (\alpha'(\alpha(h)), \beta(\alpha(h))) = (h, 1)$. Neem nu het tweede vierkant. Gaan we, vertrekkend van G linksom, dan wordt g afgebeeld op $\beta(g)$. Rechtsom wordt g eveneens afgebeeld op $\beta(g)$.
Nu moeten we nog de andere kant bewijzen. Er bestaat een isomorfisme θ tussen G en $H \times K$ zodat het gegeven schema commuteert. Definieer dan $\alpha'(g)$ als de eerste cordinaat van $\theta(g)$. Omdat θ een homomorfisme is, is ook

α' een homomorfisme. Uit het commuteren van het eerste vierkant in het schema volgt dat $(\alpha'(\alpha(h)), \beta(\alpha(h))) = (h, 1)$ en dus is $\alpha'(\alpha(h)) = h$. $\square$

Stelling 4.20. *Als* $1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta} K \to 1$ *een korte exacte rij is dan zijn volgende uitspraken equivalent:*

1. *Er bestaat een homomorfisme* $\beta' : K \to G$ *zodat voor alle* $k \in K$ *geldt dat* $\beta(\beta'(k)) = k$.
2. *Er bestaat een homomorfisme* $\varphi : K \to Aut(H)$ *en een isomorfisme* $\theta : G \Rightarrow H \rtimes K$ *zodat onderstaand schema commuteert:*

$$\begin{array}{ccccccccc} 1 & \to & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \to & 1 \\ & & \downarrow Id & & \downarrow \theta & & \downarrow Id & & \\ 1 & \to & H & \to & H \rtimes K & \to & K & \to & 1 \end{array}$$

Bewijs. Voor $k \in K$ en $h \in H$ is $\beta'(k)\alpha(h)\beta'(k^{-1})$ een element van de kern van β, want $\beta(\beta'(k)\alpha(h)\beta'(k^{-1}) = \beta(\beta'(k))\beta(\alpha(h))\beta(\beta'(k^{-1})) = k.1.k^{-1} = 1$. Nu is $ker\beta = \alpha$, dus bestaat er een $h' \in H$ zodat $\alpha(h') = \beta'(k)\alpha(h)\beta'(k^{-1}$. Omdat α injectief is , zal h' uniek zijn. Definieer nu $\varphi_k(h) = h'$ en $\varphi : K \to Aut(H); k \mapsto \varphi_k$. We bewijzen nu dat φ het gevraagde homomorfisme is:

1. Neem $k = 1$ in de betrekking $\alpha(h') = \beta'(k)\alpha(h)\beta'(k^{-1}$. Dan is $\alpha(h) = \alpha(\varphi_1(h))$ en wegens de injectiviteit van α is dan $h = \varphi_(h)$. Bijgevolg is φ_1 het identiek homomorfisme van H.

2. We bewijzen dat φ_k een homomorfisme is van H. Uit $\alpha(h') = \beta'(k)\alpha(h)\beta'(k^{-1})$ volgt dat $\alpha(\varphi_k(h_1h_2)) = \beta'(k)\alpha(h_1h_2)\beta'(k^{-1})$ of $\beta'(k)\alpha(h_1)\beta'(k^{-1})\beta'(k)\alpha(h_2)\beta'(k^{-1}) = \alpha(\varphi_k(h_1h_2))$.
Maar dan is $\alpha(\varphi_k(h_1)).\alpha(\varphi_k(h_2)) = \alpha(\varphi_k(h_1)\varphi_k(h_2))$.
Uit de injectiviteit van α volgt dan dat $\varphi_k(h_1h_2) = \varphi_k(h_1)\varphi_k(h_2)$.

3. Nu bewijzen we dat φ een homomorfisme is. We weten dat $\beta'(k_1k_2)\alpha(h)\beta'(k_1k_2)^{-1} = \alpha(\varphi_{k_1k_2}(h))$.
Dan is $\beta'(k_1)\beta'(k_2)\alpha(h)\beta'(k_2)^{-1}\beta'(k_1)^{-1} = \alpha(\varphi_{k_1k_2}(h))$.
Hieruit volgt dat $\beta'(k_1)\alpha(\varphi_{k_2}(h)\beta'(k_1)^{-1} = \alpha(\varphi_{k_1k_2}(h))$
of $\alpha(\varphi_{k_1}(\varphi_{k_2}(h))) = \alpha(\varphi_{k_1k_2}(h))$. Uit de injectiviteit van α volgt dan het gestelde.

Definieer nu $\gamma : h \rtimes k \to G$ via $\gamma(h,k) = \alpha(h)\beta'(k)$. We tonen aan dat γ een isomorfisme is.

1. γ is een homomorfisme, want $\gamma((h_1,k_1)(h_2,k_2)) = \gamma(h_1\varphi_{k_1}(h_2), k_2k_2) = \alpha(h_1\varphi_{k_1}(h_2))\beta'(k_1k_2) = \alpha(h_1)\alpha(\varphi_{k_1}(h_2))\beta'(k_1)\beta'(k_2) = \alpha(h_1)\beta'(k_1)\alpha(h_2)\beta'(k_2) = \gamma(h_1,k_1)\gamma(h_2,k_2)$.

2. γ is injectief, want als $\gamma(h,k) = 1$, dan is $\alpha(h)'(k) = 1$ en door toepassing van β krijgen we dan $\beta(\alpha(h))\beta(\beta'(k)) = \beta(1) = 1$. Bijgevolg is $1.k = 1$ en dus is $k = 1$. Maar dan is $\alpha(h)\beta'(1) = 1$ en dus is $\alpha(h) = 1$. Omdat α injectief is, volgt hieruit dat ook $h = 1$.

3. γ is ook surjectief. Neem $g \in G$. We zoeken nu $h \in H$ en $k \in K$ zodat $\gamma(h,k) = \alpha(h)\beta'(k) = g$. Door toepassing met β vinden we dat $\beta(g) = \beta(\alpha(h))\beta(\beta'(k)) = 1.k = k$. Dus definieer $k = \beta(g)$. Rest ons $h \in H$ te zoeken zodat $g = \alpha(h)\beta'(k)$ of $\alpha(h) = g\beta'(k^{-1}) = g\beta'(\beta(g)^{-1})$. Nu is $Im\alpha = ker\beta$, dus h bestaat als $g\beta'(\beta(g)^{-1}) \in Ker\beta$. We berekenen $\beta(g\beta'(\beta(g)^{-1}))$. Dit is gelijk aan $\beta(g)\beta(\beta'(\beta(g)^{-1})) = \beta(g)\beta(g)^{-1} = 1$. hiermee is aangetoond dat $g\beta'(\beta(g)^{-1})$ in $ker\beta$ zit.

Definieer tenslotte $\theta = \gamma^{-1}$. Dit is het gevraagde isomorfisme. Rest ons nu nog te bewijzen dat het gegeven schema commuteert. Bekijken we het eerste vierkant. Als we, vertrekkend van H linksom gaan dan wordt h afgebeeld op $\alpha(h)$. Gaan we rechtsom, dan wordt h afgebeeld op $\gamma(h,1) = \alpha(h)\beta'(1) = \alpha(h)$. Neem nu het tweede vierkant en vertrekken we bij $H \rtimes K$. Linksom wordt (h,k) afgebeeld op $\beta(\gamma(h,k)) = \beta(\alpha(h))\beta(\beta'(k)) = k$. Rechtsom wordt (h,k) ook afgebeeld op k.
Nu moeten we nog de andere kant bewijzen.Als er een isomorfisme θ bestaat, definieer dan $\beta' : K \to G : k \mapsto \theta^{-1}(1,k)$. Dit is een homomorfisme want θ en $k \mapsto (1,k)$ zijn ook homomorfismen. Bovendien volgt uit het commuteren van het diagram dat $\beta(\beta'(k)) = k$. Hiermee is het gestelde bewezen. □

Definitie 4.21. Als $1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta} K \to 1$ een korte exacte rij is, die voldoet aan de voorwaarden van vorige stelling, dan zeggen we dat de groepsuitbreiding *splitst*

Een gesplitste korte exacte rij correspondeert dus met een semidirect product. Merk ook op dat als G abels is dat de voorwaarden uit de twee vorige stellingen equivalent zijn.

4.4 Gekruiste producten

Hoe vormen we nu met twee groepen H en K zo een groepsuitbreiding $H \uparrow K$?

Definitie 4.22. Een gekruist systeem van groepen is een viertal (H, K, α, f) waarbij H en K groepen zijn en α en f functies met $\alpha : K \to AutH$ en $f : K \times K \to H$. Bovendien geldt:

$$\alpha_{g_1}(\alpha_{g_2}(h)) = f(g_1, g_2)\alpha_{g_1 g_2}(h)f(g_1, g_2)^{-1}$$

$$f(g_1, g_2)f(g_1 g_2, g_3) = \alpha_{g_1}(f(g_2, g_3))f(g_1, g_2 g_3)$$

Het gekruiste systeem is genormaliseerd als $f(1, 1) = f(1, g) = f(g, 1) = 1$. We noemen α een zwakke groepswerking of zwakke groepsactie en f een α-cocykel. We werken verder enkel met genormaliseerde gekruisde systemen. Met behulp van dit gekruiste systeem kunnen we een groepsstruktuur leggen op de productverzameling HK

Stelling 4.23. *$H\#_\alpha^f K = HK$ met $(h_1, g_1).(h_2, g_2) = (h_1.\alpha_{g_1}(h_2).f(g_1, g_2), g_1 g_2)$ is een groep.*

Bewijs. De gedefinieerde bewerking is associatief, want

$$\begin{aligned}((h_1, g_1).(h_2, g_2)).(h_3, g_3) &= (h_1.\alpha_{g_1}(h_2).f(g_1, g_2), g_1 g_2).(h_3, g_3)\\ &= (h_1.\alpha_{g_1}(h_2).f(g_1, g_2).\alpha_{g_1 g_2}(h_3).f(g_1 g_2, g_3), g_1 g_2 g_3)\\ &= (h_1.\alpha_{g_1}(h_2).\alpha_{g_1}(\alpha_{g_2}(h_3)).f(g_1, g_2).f(g_1 g_2, g_3), g_1 g_2 g_3)\\ &= (h_1.\alpha_{g_1}(h_2).\alpha_{g_1}(\alpha_{g_2}(h_3)).\alpha_{g_1}(f(g_2, g_3)).f(g_1, g_2 g_3), g_1 g_2 g_3)\\ &= (h_1, g_1)((h_2, g_2).(h_3, g_3))\end{aligned}$$

Het element $(1, 1)$ is het neutraal element, want $(h, g).(1, 1) = (h.\alpha_g(1).f(g, 1), g.1) = (h, g)$ en $(1, 1).(h, g) = (1.\alpha_1(h).f(1, g, 1).g) = (h, g)$.
Bovendien heeft elk element (h, g) een invers element: $(f(g^{-1}, g)^{-1}.\alpha_{g^{-1}}(h^{-1}), g^{-1})$. □

Gevolg 4.24. *Als (H, K, α, f) een gekruist systeem is, dan is $1 \to H \to H\#_\alpha^f K \to K \to 1$ met $i_H : H \to H\#_\alpha^f K : h \mapsto (h, 1)$ en $\pi_K : H\#_\alpha^f K \to K : (h, g) \mapsto g$ een exacte rij van groepen, met andere woorden $H\#_\alpha^f K$ is een groepsuitbreiding van H door K.*

Bestuderen we enkele speciale gevallen van dit gekruiste product:

1. Als α en f triviale afbeeldingen zijn, dus als $\alpha_g(h) = h$ en $f(g_1, g_2) = 1$, dan is het gekruiste product niets anders dan het direct product van de groepen H en K. Dus $H\#_\alpha^f G = H \times G$.

2. Als f triviaal is, dan moet volgens de definitie van een gekruist systeem, α een homomorfisme zijn en dan is $H\#_\alpha^f K = H \rtimes K$, het semidirecte product.

3. Als α triviaal is, dan moet $Imf \subseteq Z(H)$ en is $f(g_1, g_2)f(g_1g_2, g_3) = f(g_2, g_3)f(g_1, g_2g_3)$. Het gekruiste product wordt dan genoteerd door $H\#^f K$ en wordt het *gedraaide* product genoemd.

Elke groepsuitbreiding (E, i, π) van H door K is equivalent met een gekruist product. Omdat K eigenlijk een verzameling nevenklassen is modulo H, kunnen we van elke nevenklasse een willekeurige vertegenwoordiger nemen. Voor de klasse waarin het element g zit zou dit g kunnen zijn maar evengoed een ander element van die klasse. Noteer met $s(g)$ de gekozen vertegenwoordiger. Merk op dat g hier eigenlijk staat voor gH. We komen overeen om $s(1) = 1$ te nemen. Definieer verder :

$$\alpha : K \to Aut(H) : g \mapsto (\alpha_g : H \to H : h \mapsto s(g)hs(g)^{-1})$$

$$f : K \times K \to H : (g_1, g_2) \mapsto s(g_1)s(g_2)s(g_1g_2)^{-1}$$

Dan is (H, K, α, f) een gekruist systeem en $\theta : H\#_\alpha^f K \to E : (h, g) \mapsto i(h)s(g)$ een automorfisme.

De klassificatie van groepen kan nu dus beginnen. Als we alle enkelvoudige groepen kennen dan kennen we alle elementaire bouwstenen. Om bijvoorbeeld alle groepen van orde n te kennen zouden we n kunen ontbinden in priemfactoren en dan met enkelvoudige groepen met orde gelijk aan die priemfactoren proberen zoveel mogelijk groepen te bouwen. Maar zullen we dan alle groepen van orde n hebben? Stel dat er toevallig een enkelvoudige groep van orde n bestaat die we nog niet gevonden hadden! Het is dus beter om eerst op een andere manier alle groepen van orde n te bepalen en nadien deze groepen proberen te beschrijven als een product van enkelvoudige groepen. Vooraleer we hieraan gaan beginnen gaan we enkele eenvoudige verzamelingen van groepen bestuderen.