9 Automorfismen en Automorfismegroepen : Totient product.

Def G groep, $\psi \in S(G)$ zdd ψ homomorfisme is.
Dan heet ψ een Automorfisme van G. De verzameling
$Aut(G) := \{ f \in S(G) \mid \forall x,y \in G : f(xy) = f(x)f(y) \}$

Opm is een o.g. van $S(G)$: $f,g \in Aut(G) \Rightarrow f,g$ bijectief en
$f(xy) = f(x)f(y)$, $g(xy) = g(x)g(y) \Longrightarrow g^{-1}$ bijectief, en via h.3 ook
$g^{-1}(xy) = g^{-1}(x)\, g^{-1}(y)$

(Immers $g(g^{-1}(xy)) = xy = g(g^{-1}(x))\, g(g^{-1}(y))$ en g is
homom, dus $= g(g^{-1}(x)\, g^{-1}(y))$, en g is injectief, dus
$g^{-1}(xy) = g^{-1}(x)\, g^{-1}(y)$ $\square$)

En dus $f \circ g^{-1}$ bijectief en $(f \circ g^{-1})(xy) = f(g^{-1}(xy)) = f(g^{-1}(x) g^{-1}(y))$
$= f(g^{-1}(x))\, f(g^{-1}(y)) = (f \circ g^{-1})(x) (f \circ g^{-1})(y) \Rightarrow f \circ g^{-1} \in Aut(G) \Rightarrow (H1')$
Bovendien $Id_G \in Aut(G)$ want $Id(xy) = xy = Id(x)\, Id(y)$
en Id_G is bijectief $G \to G \Longrightarrow H0$ $\square\square$

Def alle functies $\varphi_a : G \to G$ van de vorm $\varphi_a(x) := axa^{-1}$
zijn automorfismes (Ga na $axa^{-1}aya^{-1} = axya^{-1}$ en $\varphi_{a^{-1}}$ is inverse
van φ_a ihb is φ_a bijectief homom $G \to G$)

Opm En ze vormen een ondergroep van $Aut(G)$, geheten $Inn(G)$
de o.g. van <u>inwendige automorfismes</u>

$Inn(G) := \{ \varphi : G \to G \mid \exists a \in G : \forall x \in G : \varphi(x) = axa^{-1} \}$

St. 9.3 G groep. Dan is $Inn(G) \trianglelefteq Aut(G)$ en $Inn(G) \cong G / Z(G)$

Bew $Inn(G) \trianglelefteq Aut(G)$: Definieer $f : G \to Aut(G)$: door $f(a) := \varphi_a$
met $\varphi_a : G \to G$ door $\varphi_a(x) := axa^{-1}$. $f(G) = Inn(G)$ en $\varphi_a \circ \varphi_b = \varphi_{ab}$
dus f is homom. en daarmee is $Inn(G)$ bewezen een o.g. van $Aut(G)$
stel $\tilde{\varphi} \in Aut(G)$ en $\varphi_a \in Inn(G)$. Dan voor $x \in G$:
$(\tilde{\varphi} \circ \varphi_a \circ \tilde{\varphi}^{-1})(x) = \tilde{\varphi}(a \tilde{\varphi}^{-1}(x) a^{-1}) = \tilde{\varphi}(a)\, \tilde{\varphi}(\tilde{\varphi}^{-1}(x))\, \tilde{\varphi}(a)^{-1}$
$= \varphi_{\tilde{\varphi}(a)}(x)$ en $\tilde{\varphi}(a) \in G$, dus $\varphi_{\tilde{\varphi}(a)} \in Inn(G)$.
dus $\tilde{\varphi} \circ \varphi_a \tilde{\varphi} \in Inn(G)$ voor $\varphi_a \in Inn(G)$, $\tilde{\varphi} \in Aut(G)$.
Dus $Inn(G) \trianglelefteq Aut(G)$.

$G/Z(G) \cong \mathrm{Inn}(G)$: We bekijken weer het homom. f met beeld $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$. Beschouw de kern van f:

$a \in \mathrm{Ker}(f) \iff \varphi_a = id_G \iff \forall x \in G: axa^{-1} = x \iff \forall x \in G: ax = xa$

$\iff a \in Z(G)$. Dus $\mathrm{Ker}(f) = Z(G)$.

Toepassen van de 1e isomorfiestelling geeft nu $G/Z \cong \mathrm{Im}(f) = \mathrm{Inn}(G)$ ∎

Vb op S_3: Er zijn 3 elementen van orde 2, n.l. $(12), (23), (13)$. Een automorfisme φ is i.h.b. injectief dus $\text{orde}(\varphi(x)) = \text{orde}(x)$ $\forall x \in G$. Dus φ moet hier $\{(12), (23), (13)\}$ ook afbeelden op zichzelf en is dus beperkt op deze verz. een permutatie. Omdat $\langle (12), (23), (13) \rangle = S_3$, legt hiermee heel φ vast. Er zijn dus hoogst $6 = 3!$ mogelijkheden voor φ automorf.

Stel nu $\sigma \in S_3$, $\sigma \neq (1)$, dan $\sigma = (12), (13), (23), (123), (132)$

en steeds geldt: $(12)(23) = (123) \neq (132) = (23)(12) \Rightarrow (12), (23) \notin Z(S_3)$

$(13)(12) = (123) \neq (132) = (12)(13) \Rightarrow (13) \notin Z(S_3)$

$(123)(12) = (13) \neq (23) = (12)(123) \Rightarrow (123) \notin Z(G)$

$(132)(12) = (23) \neq (13) = (12)(132) \Rightarrow (132) \notin Z(G)$

oftewel $(1) \in Z(G)$ want $\sigma(1)\sigma^{-1} = \sigma\sigma^{-1} = (1) \Rightarrow (\sigma)(1) = (1)(\sigma)$

dus $\mathrm{Inn}(G) \cong G/Z(G) \Rightarrow \mathrm{Inn}(S_3) \cong S_3/\{(1)\} \cong S_3$

$\Rightarrow \# \mathrm{Inn}(S_3) = 6$ en $\mathrm{Inn}(S_3) \subseteq \mathrm{Aut}(G)$, met $\# \mathrm{Aut}(G) \leq 6$

Oftewel $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3) \cong S_3$ □

! Vb voor $\mathbb{Z}/n\mathbb{Z}$ geldt, omdat $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$, dat de keuze voor $\psi(\bar{1})$ elk automorfisme volledig vastlegt: $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$, dan

$$\psi(\bar{k}) = \psi(k\bar{1}) = k\psi(\bar{1}) = \bar{k} \cdot \psi(\bar{1})$$

merk op dat $\cdot$ hier niet de groepsbewerking is, en $k\bar{1}$ is additieve notatie voor $\underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{k \text{ termen}}$

Notatie:

	additief		multiplicatief
	0		e of 1
	$+$	bewerking	$\cdot$
	$(-a)$	inverse	a^{-1}
	$ka := a + (k-1)a$, $0a = 0$		$a^k := a \cdot a^{k-1}$, $a^0 = e$
	voor abelse Gr.		voor alg. groepen.

vervolg: omdat $\psi(\bar{k}) = \bar{k}\psi(\bar{1})$, neem $\psi(\bar{1}) =: \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ dan ligt ψ vast. Maar ψ is ^mu^ een automorfisme desda ψ bijectief is, dus welke $\bar{a}$ kunnen? Als ψ bijectief is, bestaat er een inverse ψ^{-1} zodat $\psi^{-1}(\psi(\bar{k})) = \psi^{-1}(\bar{a}\cdot\bar{k}) = \bar{1}$ $\forall k \in \mathbb{Z}/n\mathbb{Z}$ dit is desda er een inverse voor $\bar{a}$ is, dus desda $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$
Ook definieert elke $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ een andere $\psi_{\bar{a}} : \bar{x} \to \overline{ax}$ in $\mathrm{Aut}(\psi)$
Daarom is $f : (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ een bijectie, en ook geldt $f(\bar{a}\cdot\bar{b}) = f(\overline{ab}) = \varphi_{\overline{ab}} \Rightarrow \psi_{\overline{ab}}(\bar{x}) = \overline{ab}\bar{x} = \bar{a}(\bar{b}\bar{x})$
$= (\varphi_a \circ \varphi_b)(\bar{x})$ $\forall \bar{x} \in G \Rightarrow f(\overline{ab}) = f(\bar{a}) \circ f(\bar{b})$, dus f is een isomorfisme. Conclusie $(\mathbb{Z}/n\mathbb{Z})^* \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

St. 9.6 G groep, $N \trianglelefteq G$. Dan beperkt een inwendig automorfisme $\varphi_a : x \longrightarrow axa^{-1}$, $G \to G$ tot N, en is er de functie $f : G \to \mathrm{Aut}(N)$ door $f(a) := \varphi_a|_N$, en dit is een groepshomomorfisme

Bew zij $\varphi_a : G \to G$ door $\varphi_a(x) := axa^{-1}$, dan voor $n \in N$ geldt $\forall a \in G$: $ana^{-1} \in N$, dus $\varphi_a(n) \in N$, dus je kunt $\varphi_a : G \to G$ beperken tot $\varphi_a|N : N \to N$.
Bovendien is φ_a een automorfisme op N, want $m, n \in N \Rightarrow \varphi_a|_N(mn) = amna^{-1}$
$= ama^{-1}ana^{-1} = \varphi_a|_N(m)\,\varphi_a|_N(n)$, en omdat $\varphi_{ab} = \varphi_a \circ \varphi_b$, dus voor alle $g \in G$, geldt zeker $(\varphi_a|N) \circ (\varphi_b|N) = \varphi_{ab}|N$ voor dus alle $n \in N$,
ihb is $\varphi_a|N$ een bijectie met $(\varphi_a|N)^{-1} = \varphi_{a^{-1}}|N$
En ook $f(ab) = (\varphi_{ab}|N) = (\varphi_a|N) \circ (\varphi_b|N) = f(a) \circ f(b)$

Vervolg 9.6 Als N abels is, is er een groepshomomorfisme $g : G/N \to \mathrm{Aut}(N)$ door $g(aN) := f(a)$ voor elke $aN \in G/N$

Bew Als we kunnen aantonen dat $N \subseteq \mathrm{Ker}(f)$, kunnen we de homomorfiestelling toepassen met $g := \bar{f}$.
N is abels, dus $n, m \in N \Rightarrow nm = mn$
Dus als $n \in N$, dan $\forall m \in N$: $nm = mn$, dus $\forall m \in N$: $nmn^{-1} = m$
dus $\forall m \in N$: $(\varphi_n|N)(m) = m$, dus $\varphi_n|N = \mathrm{id}_N$, de eenheid op $\mathrm{Aut}(N)$
en $\mathrm{Ker}(f) = \{n \in N \mid f(n) = \mathrm{id}_N\}$ dus als $n \in N$ dan
$\varphi_n|N = \mathrm{id}_N$ dus $f(n) = \mathrm{id}_N$ dus $n \in \mathrm{Ker}(f)$ $\} \Rightarrow N \subseteq \mathrm{Ker}(f)$

dus pas 7.1 toe met homom. $f: G \to Aut(N)$
en $N \trianglelefteq G$ met $N \subseteq Ker(f)$, dan is er een (unieke) $g: G/N \to Aut(N)$
zdd $g(aN) = f(a)$ $\forall aN \in G/N$ en deze is welgedefinieerd
en een homomorfisme.

TOEPASSING 9.6

St. 9.7 (a) p priem G groep met $\# G = p^2$. Dan ofwel
$G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$, ofwel
$G \cong (\mathbb{Z}/p^2\mathbb{Z})$

(b) p, q priem, $p > q$ en $q \nmid (p-1)$. Dan
als $\# G = pq$ geldt (altijd) $G \cong (\mathbb{Z}/pq\mathbb{Z})$

Bew we bewijzen (a) en (b) tegelijk. Zij $\# G$ pq (in geval
(a) nemen we $p = q$) en q deelt niet $p-1$ (als $p = q$
geldt dit ook)
Omdat p een priemdeler van $\# G$ is, is er wegens de
st. van Cauchy een ondergroep H met $\# H = p$, en
dan geldt ook $[G : H] = q$, dus omdat q de kleinste priemdeler
van $\# G$ is geldt wegens Gevolg 8.2 dat H een normaaldeler is
H is cyclisch want de orde van H is een priemgetal, dus
$H \cong \mathbb{Z}/p\mathbb{Z}$ en dus is H abels, waardoor wegens 9.6
een homomorfisme $g: G/H \to Aut(H)$ bestaat zodat $g(aN) = \varphi_a|_N$
$H \cong \mathbb{Z}/p\mathbb{Z}$, dus $Aut(H) \cong (\mathbb{Z}/p\mathbb{Z})^*$ en $(\mathbb{Z}/p\mathbb{Z})^*$ heeft orde $p-1$
want $\varphi(p) = p-1$ voor p priem. $g(G/H)$ is een o.g. van $Aut(H)$
dus $\# g(G/H)$ deelt $p-1$, maar ook geldt voor
$G/H \trianglerighteq Ker(g)/H$ wegens 3e Is.st dat $(G/H/(Ker(g)/H) \cong g(G/H)$
dus $\# g(G/H) = [G/H : Ker(g)/H]$, een deler van $\# G/H$
$= [G : H] = q$, dus $\# g(G/H)$ deelt $p-1$ en q, dus
deelt $ggd(p-1, q) = 1$. Dus $g(G/H) = \{id_H\}$

Dus $\forall aH \in G/H : \varphi_a|_H = id_H$ dus
$\forall a \in G$ $\forall h \in H$: $aha^{-1} = h$ $\Rightarrow$ $\forall a \in G : \forall h \in H : ah = ha$

Kies dan $a \in G$ met $a \notin H$. Dan is aH voortbrenger van $G/H \, (\cong \mathbb{Z}/q\mathbb{Z})$, dus met $f: x \longmapsto xH$ het canonieke homom geldt nu $q = \text{orde}(aH) = \text{orde}(f(a))$ deelt $\text{orde}(a)$
dus $\text{orde}(a) = pq$ of $\text{orde}(a) = q$. Als $\text{orde}(a) = pq$, dan $\langle a \rangle = G$
dus $G \cong \mathbb{Z}/pq\mathbb{Z}$ en we zijn klaar.

Neem dus $\text{orde}(a) = q$. We passen nu 3.23 toe op $H_1 := \langle a \rangle$ en $H_2 := H$

Controleer: (1) $H_1 \cap H_2 = \{e\}$

(2) $h_1 h_2 = h_2 h_1$ voor $\forall h_1 \in H_1, h_2 \in H$

(3) elke $g \in G$ kan als $g = h_1 h_2$ worden geschreven $h_1 \in H_1, H_2 \ni h_2$

(1): $a \in G$, $a \notin H$, Dus $x \in \langle a \rangle \cap H \Rightarrow x = a^n, 1 \leq n \leq q$ en $x \in H$
dus $\exists_n : a^n \in H$, $1 \leq n \leq q$, $a \notin H$ stel $n \neq q$, dus $a^n \neq e$.
Dan $a^n \in H$, $(a^n)^{-1} \in H$ via (H2), maar $a^q = e$ dus dit is a^{q-n}
dus $a^{n-q} = (a^{q-n})^{-1} \in H$ via (H2). En omdat q priem is,
is $\text{ggd}(q,n) = 1$ omdat $n \neq q$, dus er zijn x, y zdd $xn + yq = 1$
dus nu omdat $a^{n-q}, a^n \in H$ ook $(a^{n-q})^{-y}(a^n)^{y+x} \in H$
via herhaald toepassen (H1), en $(a^{n-q})^{-y}(a^n)^{y+x} = a^{-yn+yq+yn+nx}$
$= a^{xn+yq} = a^1 = a \in H \Longrightarrow \perp$ dus $n = q$, dus $a^n = e$.
dus $x = e \}$ dus $x \in \langle a \rangle \cap H \overset{(\Leftarrow)}{\Rightarrow} x = e$ dus $\langle a \rangle \cap H = \{e\}$

(2) We hadden reeds $\forall g \in G \; \forall x \in H: ax = xa$, dus i.h.b.
$\forall x \in \langle a \rangle \; \forall y \in H: \; xy = yx$

(3) Dit volgt uit het nader te formuleren (iso) homomorfisme $\ell: H_1 \times H_2 \to G$
definiëren $\ell(h_1, h_2) := h_1 h_2$, dan zien we
$\ell((h_1, h_2) \cdot (h_1', h_2')) = \ell(h_1 h_1', h_2 h_2') = h_1 \underline{h_1' h_2} h_2' = h_1 \underline{h_2 h_1'} h_2'$
$= \ell(h_1, h_2) \cdot \ell(h_1', h_2')$ dus ℓ is homom.

Verder $\text{Ker}(\ell) = \{(x,y) \in H_1 \times H_2 \mid \ell(x,y) = e\}$
dus $(x,y) \in \text{Ker}(\ell) \Rightarrow H_1 \ni x = y^{-1} \in H_2$ en dus $x, y \in H_1 \cap H_2 = \{e\}$
dus $(x,y) = (e,e)$, eenheid op $H_1 \times H_2$, dus triviale kern $\Rightarrow$ ℓ injectief.
Bovendien $\#(H_1 \times H_2) = \#\langle a \rangle \cdot \# H = pq = \# G$,
dus omdat $\text{Im}(\ell) \subseteq G$ en $\#\text{Im}(\ell) = \underbrace{\#(H_1 \times H_2)}_{= \# G}$ wegens injectiviteit
moet wel gelden $\text{Im}(\ell) = G$, dus ℓ is surjectief.
ℓ is dus isomorfisme, dus $G \cong \langle a \rangle \times H$ en $\langle a \rangle \cong \mathbb{Z}/q\mathbb{Z}$,
$H \cong \mathbb{Z}/p\mathbb{Z}$ dus $G \cong (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ $\square$

Opm De voorwaarde dat $q \nmid p-1$ is nodig om te bewijzen
dat $g(G/H) = id_H$. Deze kan ook niet gemist worden:
zie voor tegenvoorbeelden: D_p voor $q=2$

Def 9.8 $\tau : H \to Aut(N)$, twee groepen N en H, τ een groepshomom.
Dan definiëren we het <u>semidirecte product</u> $N \rtimes_\tau H$
van H met N (niet van N met H!) met betrekking tot τ
Als: de verzameling $N \times H$ met bewerking $(N\times H)\times(N\times H) \to N\times H$

$$(n_1, h_1)\cdot(n_2,h_2) := (n_1 \cdot (\tau(h_1))(n_2), h_1 h_2)$$

Dit levert een groep op: neem $(n_1,h_1), (n_2,h_2), (n_3,h_3) \in N \rtimes_\tau H$

(G1): $((n_1,h_1)\cdot(n_2,h_2))\cdot(n_3,h_3) = (n_1\cdot\tau(h_1)(n_2), h_1h_2)\cdot(n_3,h_3)$
$= ((n_1\cdot\tau(h_1)(n_2))\cdot\tau(h_1h_2)(n_3), (h_1h_2)h_3) =$

$(n_1,h_1)\cdot((n_2,h_2)\cdot(n_3,h_3)) = (n_1,h_1)\cdot(n_2\cdot\tau(h_2)(n_3), h_2h_3)$
$= (n_1\cdot\tau(h_1)(n_2\cdot\tau(h_2)(n_3)), h_1(h_2h_3))$
$= (n_1\cdot(\tau(h_1)(n_2)\cdot\tau(h_1)(\tau(h_2)(n_3))), (h_1h_2)h_3)$
$= ((n_1\cdot\tau(h_1)(n_2))\cdot\underline{(\tau(h_1)\circ\tau(h_2))}(n_3), (h_1h_2)h_3)$
$= ((n_1\cdot\tau(h_1)(n_2))\cdot\tau(h_1h_2)(n_3), (h_1h_2)h_3)$
$= ((n_1,h_1)\cdot(n_2,h_2))\cdot(n_3,h_3)$

We gebruiken dat τ een homom. is en $\tau(h)$ ook weer.
dus $\tau(h_1)\circ\tau(h_2) = \tau(h_1h_2)$ en $\tau(h)(n_1)\cdot\tau(h)(n_2)$
$= \tau(h)(n_1n_2)$

(G2) eenheid is (e_N, e_H): $\tau(e_H) = id_H$
$(e_N,e_H)\cdot(n,h) = (e_N\cdot\tau(e_H)(n), e_Hh) = (e_N\cdot id_H(n), e_Hh)$
$= (n,h)$.

(G3) inverse van (n,h) is $(\tau(h^{-1})(n^{-1}), h^{-1})$ want
$(\tau(h^{-1})(n^{-1}), h^{-1})\cdot(n,h) = (\tau(h^{-1})(n^{-1})\cdot\tau(h^{-1})(n), h^{-1}h)$
$= (\tau(h^{-1})(n^{-1}n), h^{-1}h) = (\tau(h^{-1})(e_N), e_H)$
$= (e_N, e_H)$ want $\tau(h^{-1}) \in Aut(N)$ dus
$\tau(h^{-1})(e_N) = e_N$

Eigenschappen :

(a) voor $\tau: h \mapsto id_N \quad \forall h \in H$, de triviale afb, is $N \rtimes_\tau H$ gewoon het directe product.

(c) $\pi_H : (N \rtimes_\tau H) \to H$ door $\pi_H : (n,h) \mapsto h$ is surjectief en homomorfisme, want $\pi_H((n_1,h_1)\cdot(n_2,h_2)) = \pi_H((n_1 \cdot \tau(h_1)(n_2), h_1 \cdot h_2))$
$= h_1 h_2 = \pi_H((n_1,h_1)) \cdot \pi_H((n_2,h_2))$. Bovendien $Ker(\pi_H) = N \rtimes_\tau \{e\}$
Dus $N \rtimes_\tau \{e\}$ is een normaaldeler van $N \rtimes_\tau H$, vandaar ook het teken $\rtimes$, vgl: $\triangleleft$
De 1e Isomorfiestelling geeft nu: $(N \rtimes_\tau H)/(N \rtimes_\tau \{e\}) \cong (\{e\} \rtimes_\tau H)$

Overigens $N \rtimes_\tau \{e\} = N \times \{e\}$, want
$(n,e)\cdot(n',e) = (nn',e)$ in $N \times \{e\}$ en in $N \rtimes_\tau \{e\}$
is $(n,e)\cdot(n',e) = (n \cdot \tau(e)(n'), ee) = (n \cdot id_N(n'), e) = (nn',e)$

Opm vaak schrijft men N in plaats van $N \rtimes_\tau \{e\}$
en H in plaats van $\{e\} \rtimes_\tau H$

Vb $D_n \cong \{1,s\} \ltimes_\tau \{1, r, r^2, \dots r^{n-1}\}$ door
$\tau: 1 \mapsto id_N, \quad s \mapsto (r^i \mapsto r^{-i}), \; r^i \in N$
voor $H = \{1,s\}$, $N = \{1, r^2, \dots r^{n-1}\}$
Isomorfisme $f: D_n \to H \ltimes_\tau N$ door $f(sr^i) = (s, r^i)$
en $f(r^i) = (1, r^i)$ $\square$

— Een o.g. $N \subseteq G$ is normaaldeler als $\varphi(N) = N \quad \forall \varphi \in Inn(G)$

Def Een o.g. $N \subseteq G$ heet karakteristiek als $\varphi(N) = N \quad \forall \varphi \in Aut(G)$

Opm karakteristiek $\Rightarrow$ normaaldeler want $Inn(G) \subseteq Aut(G)$
(sterker nog, ook al is dat hier niet van belang, $Inn(G) \triangleleft Aut(G)$)