STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1963 - 003

Voordracht in de serie "Actualiteiten"

W. Kuyk

30 maart 1963

Delers van het kransprodukt

1963

ZW 1963-003

Voordracht in de serie "Actualiteiten"
door
W. KUYK.
30 maart 1963

Delers van het kransprodukt.

1. Inleiding.

Het kransprodukt is één van de manieren om, uitgaande van twee groepen A en B, nieuwe groepen te vormen (zie [1], [2] en [3]). Dit kransprodukt (notatie $A \wr B$) kan op verschillende manieren gedefinieerd worden, bijv. als permutatiegroep door uit te gaan van permutatiegroepen A en B, maar ook als abstracte groep.

In het eerste geval is de struktuur van $A \wr B$ afhankelijk van de representatie die voor B gekozen is. Kiest men echter voor B een representatie die (permutatie-)isomorf is met de reguliere representatie dan is $A \wr B$ isomorf met de abstracte groep $A \wr B$ (zie [2], §3).

Een tweede manier om uit A en B nieuwe groepen te vormen is het nemen van de groepuitbreidingen van A met B. G heet groepuitbreiding van A met B als G de groep A als normaaldeler bevat, met factorgroep B: $G / A \cong B$. We zullen o.a. bewijzen dat alle groepuitbreidingen G van A met B een kopie bezitten in de (abstracte) groep $A \wr B$.

2. Definitie $A \wr B$. Stelling.

Definitie: We representeren zowel A als B op de (rechts-) reguliere wijze. Het (onbeperkte) kransprodukt $A \wr B$ van A en B is dan de groep van alle permutaties p op het cartesische produkt $B \times A$, van de vorm,

(1) $$p(b,a) = (\bar{b}b, \bar{a}_b a) \quad , \qquad b \in B, a \in A,$$

waarbij voor elke $b \in B$, $\bar{a}_b$ een willekeurig element van A is welke een rechtstranslatie van de tweede coördinaten van de paren (b,a) bewerkt, terwijl voor verschillende b de keuzen van de $\bar{a}_b$ uit A onafhankelijk zijn. $\bar{b}$ is een willekeurig element uit B, welke een translatie van de eerste coördinaten van de paren (b,a) bewerkt.

We gaan gemakkelijk na dat de permutaties p_1 met $\bar{b}=1 \in B$, een normaaldeler P_1 in $A \wr B$ vormen die isomorf is met het (onbeperkte) direkte groepsprodukt $\prod_{b \in B} A_b$, waarbij voor elke $b \in B$ A_b een kopie is van A. De factorgroep naar P_1 is isomorf met B en de permutaties p_2 met $\bar{a}_b=1 \in A$, vormen een deler P_2 van $A \wr B$ welke isomorf is met B. De elementen p_2 kunnen als representaties van $A \wr B$ naar P_1 worden gekozen. We hebben $A \wr B = P_1 P_2$ en $A \wr B$ werkt transitief op $B \times A$.

We merken op dat het kransprodukt niet commutatief is, maar wel associatief. Voorts dat de boven gedefinieerde groep $A \wr B$ isomorf is met de abstract gedefinieerde $A \wr B$.

<u>Stelling 1</u>. Elke groepuitbreiding G van A met B bezit een kopie in $A \wr B$.

<u>Bewijs</u>: Laat G zodanig zijn dat $G/A \cong B$. Vat G op als de (rechtsreguliere) permutatiegroep van zijn elementen. Laat $\{ b_i' \ : i \in I \}$ een representantensysteem van G naar A voorstellen. De klassen $b_i'A$ worden onder de gekozen representatie van G gepermuteerd; deze permutaties vormen een groep die isomorf is met de reguliere representatie van B. Deze isomorfie induceert een indicering van de elementen van B: $B = \{ b_i \ : i \in I \}$, zodanig, dat als

$$b_i'a\ (b_i' \bmod A) = b_k' \bmod A \qquad \text{in } G \ ,$$

dan $\qquad b_1 . b_i = b_k \qquad$ in B .

De klassen $M_i = b_i' A$ zijn imprimitiviteitsgebieden van de permutatiegroep G. Want rechtstranslatie van de elementen van M_i onder voorvermenigvuldiging met een willekeurig element $b_1' a \in G$ geeft:

$$b_1' a M_i = b_1' a b_i' A = b_1' b_i' a^{(i)} A =$$

$$= b_k' a_{(i)} a^{(i)} A = M_k \quad , \tag{2}$$

waarbij $a^{(i)} = b_i'^{-1} a b_i'$ en $a_{(i)}$ factoren uit A gedefinieerd door $b_1' b_i' = b_k' a_{(i)}$. Gegeven de translatie $b_1' a$ zijn de elementen $a_{(i)} a^{(i)} \in A$ en de representant b_k' ondubbelzinnig bepaald door de representant b_i van M_i.

We vinden dus dat de verzamelingen M_i imprimitiviteits-gebieden zijn van G en G werkt transitief op de verzameling $\bigcup_{i \in I} M_i$ van zijn elementen.

Laat nu $A = \{ a_j : j \in J \}$ waarin J een zekere indexverzameling. Dan definieert de toevoeging

$$b_i' a_j \longleftrightarrow (b_i, a_j)$$

een één-één toevoeging van de (transitiviteits-)gebieden van de permutatiegroepen G en $A \wr B$.

We tonen aan dat een willekeurige permutatie uit G, dus van de elementen $b_i' a_j$, te verkrijgen is als het produkt van twee permutaties uit $A \wr B$ (van de overeenkomstige elementen-paren (b_i, a_j)).

Een permutatie (translatie) $b_1' a$ werkt op de M_i op de volgende wijze (2) : $b_i' a_j$ gaat over in $b_k' a_{(i)} a^{(i)} a_j$.

Deze permutatie brengen we over op de paren (b_i, a_j). Onderwerpen we (b_i, a_j) eerst aan een permutatie p_2, gegeven door

$$p_2(b_i,a_j) = (b_l b_i,a_j) = (b_k,a_j)$$

en het resultaat daarvan aan p_1, gegeven door

$$p_1(b_k,a_j) = (b_k,a_{(i)}a^{(i)}a_j) \quad ,$$

dan heeft p_1p_2 op (b_i,a_j) toegepast blijkbaar het zelfde effect als $b_l'a$, toegepast op de elementen $b_i'a_j$ uit G.

Daar de tweede coördinaten a_j van (b_k,a_j) bij vaste k onder p_1 met dezelfde factor $a_{(i)}a^{(i)}$ voorvermenigvuldigd worden en bovendien de eerste coördinaten invariant gelaten worden, is $p_1 \in P_1$. p_2 is element van P_2. Dus $p_1p_2 \in A \wr B$.

Opmerking: 1) Het directe groepsprodukt $A \times B$ van A en B is isomorf met de deler P_2A' van $A \wr B$, waarbij A' de diagonaal van P_1 voorstelt.

2) M.Tibiletti bewijst in verband met een geheel andere vraagstelling een bijzonder geval van stelling 1, nl. dat de groepen G die splitsen over A een kopie in $A \wr B$ bezitten.

3. <u>Delers van $A \wr B$ als Galoisgroep</u>.

Laat A en B eindige groepen zijn. Laat L een separabele Galoisuitbreiding zijn van een of ander lichaam K en M een separabele Galoisuitbreiding van L. Laat L/K resp. M/L de Galoisgroepen B en A bezitten. Laat N de kleinste normale lichaamsuitbreiding zijn van K die M bevat. Dan zijn er i.h.a. meerdere mogelijkheden voor de Galoisgroep G van N/K. We bewijzen dat, bij willekeurige B en voor een zekere klasse van groepen A, al deze groepen G een kopie in $A \wr B$ bezitten.

<u>Stelling 2</u>. Laat A een isomorfe representatie toelaten als een transitieve permutatiegroep A_r van een verzameling onbepaalden $\{X_1,\dots,X_r\}$, en laat er een lichaam k bestaan

met de eigenschap dat het deellichaam $k(A_r)$ van alle invarianten onder A_r in de zuiver transcendente uitbreiding $k(X_1,\dots,X_r)$ over k, zelf ook zuiver transcendent is over k, dan bezit, bij willekeurige B, elke groep G van de boven aangegeven soort, een kopie in $A \wr B$.

Bewijs: (schets) Breidt k uit toteen lichaam K', met de eigenschap dat K' een algebraïsche uitbreiding $K' \subset N'$ toelaat die algebraïsch disjunct is over k met $k(A_r)$ en zodanig dat N'/K' de Galoisgroep G bezit. Dit is altijd mogelijk door met transcendenten te werken. Laat K', L', M' en N' de lichamen zijn die overeenkomen met de lichamen K, L, M en N zoals boven aangegeven.

We tonen dan eerst aan dat N'/K' is voort te brengen door de nulwaarden van een n-de graads irreducibel polynoom ($n=r.s$; s = de orde van B) : $f(t) = t^n + a_1 t^{n-1} + \dots \in K'[t]$, dat over L' uiteenvalt in s irreducibele delers $f_1,\dots,f_s$ waarvan elke f_i de Galoisgroep A_r t.o.v. L' bezit.

Laat $k(A_r) = k(U_1,\dots,U_r)$, met $U_1,\dots,U_r$ algebraïsch onafhankelijk over k. Dan is het lichaam $K'(A_r)$ van alle invarianten onder A_r in $K'(X_1,\dots,X_r)$ identiek met $K'(U_1,\dots,U_r)$.

Neem s kopieën van de uitbreiding

$K'(U_1,..,U_r) \subset K'(X_1,..,X_r)$: $K'(U_{i1},..,U_{ir}) \subset K'(X_{i1},..,X_{ir})$ $(i=1,\dots,s)$, en wel zodanig dat $U_{11},\dots,U_{sr}$ (dus ook $X_{11},\dots,X_{sr}$) algebraïsch onafhankelijk zijn over K'. De elementen $X_{i1},\dots,X_{ir}$ zijn nulwaarden van een irreducibel polynoom $P_i(t) = (t-X_{i1}) \dots (t-X_{ir})$ over $K'(U_{i1},\dots,U_{ir})$ en $K'(U_{11},\dots,U_{sr}) = K'(U)$, met Galoisgroep $A_r^{(i)} \cong A_r$.

Men toont gemakkelijk aan dat $K'(X) = K'(X_{11},\dots,X_{sr})$ de Galoisgroep $A_r^{(1)} \times \dots \times A_r^{(s)}$ over K' bezit. Al deze beweringen blijven gelden indien we K' door L' vervangen, daar L' algebraïsch is over K'.

We stellen $U_{ik} = W_{1k} + W_{2k}\theta_i + \ldots + W_{sk}\theta_i^{s-1}$ ($i=1,\ldots,s$; $k=1,\ldots,r$), waarin $\theta_1,\ldots,\theta_s$ geconjugeerden over K' in L'. We krijgen $L'(U) = L'(W) = L'(W_{11},\ldots,W_{sr})$, en $W_{11},\ldots,W_{sr}$ zijn algebraïsch onafhankelijk over L' en K'.

Het produkt $P(t) = P_1(t) \ldots P_s(t)$ is nu een polynoom van de n-de graad over $K'(W)$ geworden, met Galoisgroep $A \wr B$ (bewijs analoog aan het bewijs van stelling 4 (pag.48) in W.Kuyk: Over het omkeerprobleem van de Galoistheorie, 1960, Amsterdam).

Het slot van het bewijs van de stelling is nu als volgt. We tonen aan dat het voortbrengende polynoom $f(t)$ van N'/K' met Galoisgroep G, zo te kiezen is dat het van $P(t)$ af te leiden is door in de coëfficienten van $P(t)$ de elementen W_{ik} te vervangen door geschikt gekozen $k_{ik} \in K'$.

Toepassing van (een modificatie van) een stelling in van der Waerden: Moderne Algebra I, § 61, geeft nu dat G een deler van $A \wr B$ moet zijn.

Opmerking: 1) Deze stelling geeft o.a. een ander bewijs van stelling 1, en wel voor het geval dat B willekeurig en eindig is, terwijl A aan de voorwaarde van stelling 2 voldoet.

2) De groepen A die voldoen aan de voorwaarde uit stelling 2, zijn bijv. de groepen die behoren tot de volgende klasse C:

(i) C bevat alle eindige abelse groepen.
(ii) C bevat alle eindige symmetrische groepen.
(iii) C bevat alle groepdelers van S_3 en S_4.
(iv) Als $G \in C$ en $H \in C$ dan $G \times H \in C$.
(v) Als $G \in C$ en $H \in C$ dan $G \wr H \in C$.

Voorts voldoen de eindige p-groepen en de eindige spiegelingsgroepen aan de gestelde voorwaarde.

De literatuur over de zuivere transcendentie van $k(A_r)$ wordt hier niet aangegeven. Vermeld worde slechts dat de resultaten hier genoemd, afkomstig zijn van E.Noether, F.Seidelmann, C.Chevalley, K.Masuda, W.Gaschütz en W.Kuyk.

Literatuur:

1 P.Hall - Proc. Lond. Math. Soc. 36 (1933).

2 M.Krasner - L.Kaloujnine - Acta Szeged 13, 14 (1950, 1951).

3 G.Baumschlag - Cambridge Phil. Soc. 55 (1959).

4 M.Tibiletti - Convz. Internaz. di Teoria Gruppi Finiti (Firenze, Rome 1960).