IMPORTANCIA DO PRODUTO "WREATH" PARA A TEORIA DE GRUPOS

SONIA GABRIELINA PASCHOLATI CARILE

ORIENTADOR

PROF. DR. JOHN EDMONDS DAVID

Dissertação apresentada ao Instituto de Matemática, Estatistica e Ciencia da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do titulo de Mestre em Matemática.

Este trabalho foi realizado com o auxílio financeiro da CAPES e FINEP;

A meus pais

e

José Archangelo

AGRADECIMENTOS

Ao Prof. John Edmonds David que, com sua segura orientação, permitiu a realização deste trabalho.

A meus pais, professores e colegas por seus estímulos e ensinamentos.

A meu irmão Sérgio, pelo auxílio prestado na datilografia dos manuscritos.

Aos funcionários da UNICAMP que colaboraram na impressão desta dissertação.

A CAPES e FINEP que, com seu apoio financeiro, tornaram possível a realização deste trabalho.

INDICE

I N T R O D U Ç Ã O

Segundo entrevista dada à imprensa pelo professor D. Gorenstein, da Universidade de Rugters, a principal linha de pesquisa, para a qual estão voltados os matemáticos que trabalham em grupos finitos, é a classificação dos grupos finitos simples. Acredita ele que nos próximos dez anos este problema estará solucionado.

Nesta dissertação contribuímos para mostrar a importância dessa linha de pesquisa para toda a teoria de grupos finitos, pois demonstramos que cada grupo finito pode ser imerso num produto "wreath" clássico de grupos simples.

Nosso principal objetivo neste trabalho foi criar condições para a prova do teorema de Kaloujnine - Krasner.

Nos capítulos iniciais apresentamos um resumo de conceitos e resultados básicos sobre semigrupos. Depois desenvolvemos a teoria de semigrupos agindo sobre conjuntos e semigrupos agindo sobre semigrupos. Nos capítulos 4 e 5, com base em ações de semigrupos, definimos produto direto e produto "wreath". No capítulo 6 apresentamos propriedades de ações de grupos e semigrupos, algumas envolvendo produto "wreath". Finalmente temos a decomposição de ações de semigrupo em produto "wreath", culminando com o teorema de Kaloujnine-Krasner, que trata da imersão de grupos finitos num produto "wreath" de grupos simples.

Tomamos como ponto de partida do nosso trabalho o artigo "Some Applications of the wreath product construction", de Charles Wells, usando uma notação uniformizada.

Demonstramos as proposições, observações e lemas seguintes, apenas enunciados por Wells:

Proposições: (6.7), (6.8), (6.9), (7.1), (9.2).

Observações: (5.9), (7.2.iv).

Lemas: (3.2), (3.7.14), (4.5), (4.6), (6.4).

Fizemos correção no enunciado de teorema (8.4), "Esquema de Decomposição", e corolários do mesmo. Detalhamos as demonstrações deles.

No capítulo 9 completamos a demonstração do corolário (9.13) e da proposição (9.2). Detalhamos a demonstração do teorema de Kaloujnine-Krasner e damos uma aplicação, usando o grupo dos quatérnios.

C A P I T U L O 1

DISCUSSÃO INTRODUTÓRIA SOBRE O PRODUTO "WREATH"

Nas situações a serem estudadas estarão envolvidos um conjunto X, um semigrupo S e uma função ϕ, onde $\phi: S \longrightarrow \{\text{operadores de } X\}$, tal que, $s \longrightarrow s\phi$.

(1.1.) <u>Exemplos</u>:

(1.1.1.) Em teoria de grupos, X é um espaço vetorial complexo e S um grupo, olhando-se $s\phi$ como uma matriz inversível.

(1.1.2.) Em muitas aplicações da teoria abstrata de grupos, X é o "conjunto por trás" de um grupo S e $s\phi$ é a multiplicação à direita por s.

(1.1.3.) Em combinatória, X é frequentemente uma estrutura combinatória (um gráfico por exemplo) e S é seu grupo de automorfismos.

Costuma-se parametrizar o conjunto X, de tal modo que a ação de S é analisada dentro de ações mais simples sobre os parâmetros, isto é, pode-se olhar X como um conjunto de vetores, no sentido mais amplo de n-uplas de algum produto cartesiano de conjuntos e descrever a ação de S, através das mudanças que faz nas coordenadas.

Em geral, o efeito de $s\phi$, sobre uma dada coordenada, depende de alguma ou todas as outras coordenadas. Frequentemente, pode acontecer que estas coordenadas estejam ordenadas de tal modo que o efeito de $s\phi$ em uma dada coordenada depende sómente daquela coordenada e das coordenadas que a seguem. A ação é dita, então, triangular.

Em muitas aplicações é conveniente tomar S como um semigrupo. Se S não é semigrupo ele é, usualmente, representado por um semigrupo livre ou, às vezes, pelo semigrupo gerado pelo conjunto de funções $s\phi$, com a composição funcional como operação.

O produto "wreath", como veremos, é descrito através de ações de semigrupos.

CAPITULO 2

SEMIGRUPOS

(2.1.) Definições:

(2.1.1.) Semigrupo. Um semigrupo é um conjunto S, munido de uma multiplicação associativa sobre S.

(2.1.2.) Unidade. Uma unidade em S é um elemento $1 \in S$, satisfazendo $1s = s1 = s$, para todo $s \in S$.

(2.1.3.) Monóide. Um monóide é um semigrupo com unidade.

(2.1.4.) Subsemigrupo. Um subsemigrupo de um semigrupo S é um subconjunto de S, fechado para a multiplicação.

(2.1.5.) $S^1 = S \cup 1$, onde S é semigrupo sem unidade e 1 é um elemento que não pertence a S, tal que, $1s = s1 = s$, para todo $s \in S$. Se S tem unidade $S^1 = S$.

(2.1.6.) Trans X. Seja X um conjunto. Trans X é o conjunto de todas as funções de X em X, juntamente com uma operação binária, composição de funções. Uma função em Trans X é chamada uma transformação de X.

(2.1.7.) Subgrupo. Seja S um semigrupo. G é subgrupo de S se G é subsemigrupo de S e G é grupo.

(2.1.8.) Sim X. É o subgrupo unitário de Trans X, constituído de todas as permutações de X, isto é, $1_{\text{Sim } X} = 1_{\text{Trans } X}$.

(2.1.9.) PF(X). É o monóide, constituído de todas as funções $f: A \subseteq X \longrightarrow X$. Trans $X \subset$ PF(X).

(2.1.10.) Zero de S. Seja S um semigrupo. Se $z \in S$ satisfaz $zs = sz = z$, para todo $s \in S$, então z é um zero de S.

(2.1.11.) Idempotente. Seja S um semigrupo. O elemento $e \in S$ é idempotente se $e^2 = e$.

(2.1.12.) Ideal à direita. Seja S um semigrupo. Um subconjunto I S é um ideal à direita se $is \in I$, para todo $i \in I$ e $s \in S$. Ideal à esquerda é definido de modo semelhante.

(2.1.13.) Homomorfismo de semigrupos. Sejam S e T, semigrupos. Uma função $\phi: S \longrightarrow T$ é um homomorfismo se $(s.s')\phi = s\phi \, . \, s'\phi$, para todo $s, s' \in S$.

(2.1.14.) Imagem homomórfica. Seja $\phi: S \longrightarrow T$ homomorfismo de semigrupos. T é imagem homomórfica de S, se ϕ é sobrejetora.

(2.1.15.) S "divide" T. Sejam S e T semigrupos. Dizemos que S "divide" T (S/T), se S é imagem homomórfica de um subsemigrupo de T.

(2.2.) Lema. Seja S um semigrupo finito e $s \in S$. Então alguma potência de s é idempotente.

Prova:

Sejam k e n os inteiros mínimos, tal que $0 < k < n$ e $s^k = s^n$. Então $s^{k+n-k} = s^k$.

Suponhamos que para algum inteiro $m \geqslant 0$, $s^{k+m(n-k)} = s^k$.

Então $s^{k+(m+1)(n-k)} = s^{k+m(n-k)} \cdot s^{(n-k)} = s^k . s^{(n-k)} =$
$= s^{k+n-k} = s^k$.

Assim, por indução, $s^{k+m(n-k)} = s^k$, para todos os inteiros $m \geqslant 0$.

Seja p um inteiro positivo, para o qual $k+p = m(n-k)$, para algum m.

Então s^{k+p} é idempotente, pois:

$$s^{k+p} = s^k \cdot s^p = s^{k+m(n-k)} \cdot s^p = s^{k+p} \cdot s^{m(n-k)} =$$
$$= s^{k+p} \cdot s^{k+p} = (s^{k+p})^2.$$

(2.2.1.) <u>Corolário</u>. Seja G' um semigrupo finito com um único elemento idempotente, e. Se e for identidade de G, então G é um grupo.

Prova:

Seja $e \in G$ o único idempotente de G e seja $x \in G$.

Pelo lema 3.2., $x^k = e$ para algum k.

Então x^{k-1} é o inverso de k, pois:

$$x^k = x \cdot x^{k-1} = x^{k-1} \cdot x = e .$$

Logo G é grupo.

(2.3.) <u>Lema</u>. Sejam: S um semigrupo finito, ϕ um homomorfismo de semigrupo, com domínio S e $S\phi$ um grupo. Então há um subgrupo G de S, tal que $G\phi = S\phi$. (Por definição G é subgrupo de S se G é subsemigrupo de S e G é grupo).

Prova:

Seja G um subsemigrupo minimal de S, tal que $G\phi = S\phi$.

Vamos mostrar que G é grupo.

Seja $e \in G$ um idempotente arbitrário, cuja existência é garantida por 3.2.

Então $e\phi$ é idempotente em $S\phi$:

$e\phi \cdot e\phi = (e.e)\,\phi = e\phi$

$e\phi$ é, portanto, a unidade de $S\phi$, pois o único idempotente num grupo é sua unidade.

Temos então que:

$(eGe)\phi = e\phi \cdot G\phi \cdot e\phi = e\phi \cdot S\phi \cdot e\phi = S\phi$,e assim pela minimalidade de G , $eGe = G$.

Como $(ege) = e(ege) = (ege)e = ege$, temos que G é um monóide com unidade e .

Como e é um idempotente arbitrário, então e é o único idempotente de G.

Pelo corolário 3.2.1., G é um grupo.

CAPITULO 3

AÇÕES DE SEMIGRUPOS

(3.1.) Definição. Uma ação à direita, por um semigrupo S em um conjunto X, é uma função:

$$X \times S \longrightarrow X \text{ , satisfazendo :}$$
$$(x,s) \longrightarrow xs.$$

$x(st) = (xs)t$, para todo $x \in X$, $s, t \in S$.

(3.2.) Lema. i) Uma ação determina um homomorfismo $\phi : S \longrightarrow \text{Trans } X$, definido por $x(s\phi) = xs$, $(x \in X,\ s \in S)$.

ii) Qualquer homomorfismo $\phi : S \longrightarrow \text{Trans } X$, determina uma ação em X por S , dada por $(x,s) \longrightarrow x(s\phi)$.

Prova:

i) ϕ é um homomorfismo, pois $x(s\phi \circ s'\phi) =$
$= (xs\phi)\ s'\phi = (xs)\ s'\phi = (xs)\ s' = x\ (ss') = x\ (ss'\phi)$.

ii) $(x,s) \longrightarrow x\,(s\phi)$ é uma ação pois:

$$x\,(st) = x\,(st\phi) = x\,(s\phi \circ t\phi) = (xs\phi)\,t\phi = (xs)\,t\ ,$$

para todo $x \in X$, $s,t \in S$.

(3.3.) <u>Notação</u>:

Ações serão denotadas por S^* ou (S, ϕ, X), onde

$\phi : S \longrightarrow \text{Trans } X$.

$(\text{Trans } X)^*$ e $(\text{Sim } X)^*$ denotam as ações de

Trans X e Sim X sobre X.

(3.4.) <u>Definição</u>: Uma ação à esquerda, por um semigrupo S, em um conjunto X, é uma função de $S \times X$ em X, satisfazendo:

$(st)\,x = s\,(tx)$, para todo $s,t \in S$, $x \in X$.

(3.5.) <u>Observações</u>:

Consideraremos apenas ações à direita, exceto quando especificado o contrário.

Se $S^* = (S, \phi, X)$ é uma ação, S é também chamado semi-autômato ou máquina e X pode ser chamado um S-conjunto ou S-operando.

(3.6.) <u>Exemplos de ações</u>:

(3.6.1.) Qualquer semigrupo de transformações de um conjunto X , age sobre X. Em particular qualquer grupo de permutações em X é exemplo de uma ação.

(3.6.2.) Qualquer semigrupo S age sobre seu próprio conjunto de elementos, pela multiplicação à direita. Esta ação será denotada por S_S.

(3.6.3.) Se I é um ideal à direita de S, então S age sobre I, pela multiplicação à direita. Esta ação será denotada por S_I.

(3.6.4.) Um grupo G, com subgrupo normal N, age sobre N à direita, colocando-se $n^g = g^{-1}ng$, para todo $g \in G$ e $n \in N$.

(3.7.) <u>Morfismo de ações</u>.

(3.7.1.) <u>Definição</u>. Sejam: $S^* = (S,\phi,X)$ e $T^* = (T,\Psi,Y)$. Um par (α, θ) é um morfismo de ações de S^* para T^* se:

i) $\alpha : S \longrightarrow T$ é homomorfismo.

ii) $\theta : X \longrightarrow Y$ é função.

iii) Para todo $s \in S$, o diagrama abaixo comuta:

$$\begin{tikzcd} X \arrow[r, "s\phi"] \arrow[d, "\theta"'] & X \arrow[d, "\theta"] \\ Y \arrow[r, "s\alpha\Psi"'] & Y \end{tikzcd}$$

Para todo $x \in X$, $s \in S$, $(x\theta)(s\alpha) = (xs)\,\theta$.

Dizemos, então, que $(S, \alpha\Psi, X\theta)$ é uma ação de S sobre $X\theta$.

(3.7.2.) <u>Definição</u>. Um morfismo (α, θ) é injetivo, (respectivamente sobrejetivo) se α e θ são ambas injetivas (respectivamente sobrejetivas).

(3.7.3.) <u>Definição</u>. S^* é uma subação de T^*, se α e θ são inclusões.

(3.7.4.) <u>Definição</u>. T é imagem homomórfica de um subsemigrupo de S, se há um morfismo sobrejetivo de ações, de uma subação de S em T, onde S^* e T^* são ações.

(3.7.5.) <u>Definição</u>. Um S-morfismo ou mapa equivariante de (S, ϕ, X) para (S, Ψ, Y) é um morfismo (α, θ), tal que:

i) $(xs)\,\theta = (x\theta)\,s$, para todo $x \in X$, $s \in S$.

ii) $\alpha = id_S$.

(3.7.6.) Definição. Morfismo de $G^* = (G,\phi,X)$, (Morf G^*), é morfismo de G^* para G^* .

(3.7.7.) Lema. O conjunto dos morfismos de $G^* = (G,\phi,X)$ é um semigrupo, com a operação de composição de funções: $(\alpha_1,\theta_1) \circ (\alpha_2,\theta_2) = (\alpha_1\circ\alpha_2 , \theta_1\circ\theta_2)$, para todo (α_1, θ_1) , $(\alpha_2, \theta_2) \in$ Morf G^*.

i) A propriedade de fechamento é válida para todos os morfismos de G^* , isto é:

$(\alpha_1, \theta_1) \circ (\alpha_2, \theta_2) = (\alpha_1\circ\alpha_2 , \theta_1\circ\theta_2)$, para todo

(α_1, θ_1) , $(\alpha_2, \theta_2) \in$ Morf G^* .

_ $\alpha_1\circ\alpha_2$ é homomorfismo como composição de homomorfismos.

_ $\theta_1\circ\theta_2$ é função como composição de funções.

Verifiquemos que $(xg)(\theta_1\circ\theta_2) = x(\theta_1\circ\theta_2).g(\alpha_1\circ\alpha_2)$, para todo $x\in X$, $g\in G$.

Como (α_1, θ_1) e $(\alpha_2, \theta_2) \in$ Morf G^* temos:

$$(xg)(\theta_1\circ\theta_2) = \left[(xg)\theta_1\right]\theta_2 = \left((x\theta_1)(g\alpha_1)\right)\theta_2 =$$

$$= \left((x\theta_1)\theta_2\right) \left((g\alpha_1)\alpha_2\right) = x(\theta_1\circ\theta_2) . g(\alpha_1\circ\alpha_2).$$

Logo $(\alpha_1 \circ \alpha_2, \theta_1 \circ \theta_2) \in$ Morf G^* .

ii) É válida a propriedade associativa para os morfismos de G^* .

Para todo (α_1, θ_1), (α_2, θ_2), $(\alpha_3, \theta_3) \in$ Morf G^* temos:

$$\big((\alpha_1, \theta_1) \circ (\alpha_2, \theta_2)\big) \circ (\alpha_3, \theta_3) = (\alpha_1 \circ \alpha_2, \theta_1 \circ \theta_2) \circ (\alpha_3, \theta_3) =$$

$$= \big((\alpha_1 \circ \alpha_2) \circ \alpha_3 \ , \ (\theta_1 \circ \theta_2) \circ \theta_3\big) = \big(\alpha_1 \circ (\alpha_2 \circ \alpha_3), \ \theta_1 \circ (\theta_2 \circ \theta_3)\big) =$$

$$= (\alpha_1, \theta_1) \circ \big((\alpha_2, \theta_2) \circ (\alpha_3, \theta_3)\big) .$$

(3.7.8.) <u>Definição</u>. Aut G^* , onde $G^* = (G, \phi, X)$, é o conjunto dos pares (α, θ) , tal que, $\alpha : G \longrightarrow G$ é isomorfismo, $\theta : X \longrightarrow X$ é bijeção e $(xg)\theta = (x\theta)(g\alpha)$, para todo $x \in X$, $g \in G$.

(3.7.9.) <u>Definição</u>. G-Aut $G^* = \{(id_G, \theta) \in \text{Aut } G^*\}$.

(3.7.10.) <u>Lema</u>. Os automorfismos de G^* formam um grupo sob a operação de composição.

i) Propriedade associativa-trivialmente válida

ii) Existência do elemento neutro

_ $(id_G , id_X) \in$ Aut G^*, pois, id_G é isomorfismo e id_X é bijeção.

_ (id_G , id_X) é o elemento neutro de Aut G^* , pois , para todo $(\alpha, \theta) \in$ Aut G^* temos:

$(id_G , id_X)(\alpha, \theta) = (id_G \circ \alpha , id_X \circ \theta) = (\alpha, \theta)$.

$(\alpha, \theta)(id_G , id_X) = (\alpha \circ id_G , \theta \circ id_X) = (\alpha, \theta)$.

iii) Existência do elemento inverso

Mostraremos que $(\alpha^{-1}, \theta^{-1}) = (\alpha, \theta)^{-1}$.

iii.1.) Primeiramente verificaremos que $(\alpha^{-1}, \theta^{-1}) \in$ Aut G^* .

_ $\alpha : G \longrightarrow G$, isomorfismo , $\Longrightarrow \exists \alpha^{-1} : G \longrightarrow G$, isomorfismo.

$\theta : X \longrightarrow X$, bijeção , $\Longrightarrow \exists \theta^{-1} : X \longrightarrow X$, bijeção.

_ Provaremos que $(xg)\theta^{-1} = (x\theta^{-1})(g\alpha^{-1})$, para todo $x \in X$, $g \in G$.

$(\alpha, \theta) \in$ Aut $G^* \Longrightarrow$ diagrama I comuta:

$$\begin{tikzcd} X \arrow[r, "g\phi"] \arrow[d, "\theta"'] \arrow[dr, phantom, "\mathrm{I}"] & X \arrow[d, "\theta"] \\ X \arrow[r, "(g\alpha)\phi"'] & X \end{tikzcd}$$

$(xg)\theta = (x\theta)\ (g\alpha)$, para todo $x \in X$ e $g \in G$.

Consideremos os diagramas abaixo:

$$\begin{tikzcd} X \arrow[r, "g\phi"] \arrow[d, "\theta^{-1}"'] \arrow[dr, phantom, "\mathrm{II}"] & X \arrow[d, "\theta^{-1}"] \\ X \arrow[r, "(g\alpha^{-1})\phi"'] \arrow[d, "\theta"'] \arrow[dr, phantom, "\mathrm{III}"] & X \arrow[d, "\theta"] \\ X \arrow[r, "(g\alpha^{-1})\alpha\phi"'] & X \end{tikzcd}$$

O diagrama III comuta:

$\left(x\ (g\alpha^{-1})\right)\theta \overset{(I)}{=} (x\theta)\ \left((g\alpha^{-1})\alpha\right) = (x\theta)g$, para todo $x \in X$ e $g \in G$.

Verifiquemos que o diagrama II comuta, isto é,

$(x\,\theta^{-1})\ (g\,\alpha^{-1}) = (xg)\,\theta^{-1}$, para todo $x \in X$ e $g \in G$.

$(xg\,\theta^{-1})\,\theta = xg$, para todo $x \in X$ e $g \in G$.

Seja $x\,\theta^{-1} = y$.

Como o diagrama III comuta, então :

$(yg\,\alpha^{-1})\,\theta = (y\,\theta\,)g \implies (x\,\theta^{-1}\,g\,\alpha^{-1})\,\theta = (x\,\theta^{-1}\,\theta\,)g = xg$,

para todo $x \in X$ e $g \in G$.

Então $(x\,\theta^{-1}\,g\,\alpha^{-1}) = (xg)\,\theta^{-1}$, para todo $x \in X$ e $g \in G$.

Logo $(\alpha^{-1}, \theta^{-1}) \in \text{Aut } G^{*}$.

iii.2.) Para todo $(\alpha, \theta\,) \in \text{Aut } G^{*}$, temos:

$(\alpha, \theta\,) \circ (\alpha^{-1}, \theta^{-1}) = (\alpha \circ \alpha^{-1}, \theta \circ \theta^{-1}) = (id_G\ ,\ id_X)$.

$(\alpha^{-1}, \theta^{-1}) \circ (\alpha, \theta) = (\alpha^{-1} \circ \alpha\ , \theta^{-1} \circ \theta) = (id_G\ ,\ id_X)$.

Por (iii.1.) e (iii.2.) concluimos que $(\alpha, \theta\,)^{-1} = (\alpha^{-1}, \theta^{-1})$.

(3.7.11.) <u>Corolário</u>. O morfismo $(\alpha, \theta\,)$ tem inverso , se e somente se, α e θ são ambas bijetivas.

(3.7.12.) Os G-automorfismos de G^* formam um subgrupo dos automorfismos de G^*.

Prova:

$(\alpha, \theta) \in G - Aut\ G^* \Longrightarrow \alpha = id_G$.

Sejam $(1, \theta_1)$ e $(1, \theta_2) \in G - Aut\ G^*$.

Então:

$(1, \theta_1) \circ (1, \theta_2^{-1}) = (1 \circ 1, \theta_1 \circ \theta_2^{-1}) = (1, \theta_1 \circ \theta_2^{-1}) \in G\text{-}Aut\ G^*$.

Logo $G - Aut\ G^* \subset Aut - G^*$, como subgrupo.

(3.7.13.) <u>Lema</u>. Sejam: G um grupo de permutações e $C(G)$ = = centralizador de G em $Sim\ X$. A aplicação, $\Psi : G\text{-}Aut\ G^* \longrightarrow Sim\ X$, tal que, $(1, \theta)\Psi = \theta$, é isomorfismo sobre $C(G)$.

i) Se $(1, \theta) \in G\text{-}Aut\ G^* \Longrightarrow \theta$ é bijeção $\Longrightarrow \theta \in Sim\ X$.

ii) Ψ é homomorfismo

Para todo $(1, \theta_1)$, $(1, \theta_2) \in G - Aut\ G^*$,

$((1, \theta_1) \circ (1, \theta_2))\Psi = (1, \theta_1 \circ \theta_2)\Psi = \theta_1 \circ \theta_2$

$(1, \theta_1)\Psi \circ (1, \theta_2)\Psi = \theta_1 \circ \theta_2$

Logo: $\big((1,\theta_1) \circ (1,\theta_2)\big)\Psi = (1,\theta_1)\Psi \circ (1,\theta_2)\Psi$.

iii) Ψ é injeção

Se $(1,\theta_1)\Psi = (1,\theta_2)\Psi \Longrightarrow \theta_1 = \theta_2 \Longrightarrow (1,\theta_1) = (1,\theta_2)$.

iv) $\mathcal{I}m\,\Psi \subseteq C(G)$

Seja $\theta \in \mathcal{I}m(\Psi)$.

$(1,\theta) \in$ G-Aut $G^* \Longrightarrow xg\theta = x\theta g$, $\forall\, x \in X$, $\forall\, g \in G$.

Para todo $g \in G$, $g\theta = \theta g$. Então $\theta \in C(G)$.

v) $\mathcal{I}m\,\Psi = C(G)$.

Basta mostrar que $C(G) \subset \mathcal{I}m\,\Psi$.

Se $\theta \in C(G)$, $g\theta = \theta g \Longrightarrow xg\theta = x\theta g$, $\forall\, x \in X$

e $g \in G$.

Então $(1,\theta) \in G -$ Aut G^* e $(1,\theta)\Psi = \theta$.

(3.7.14.) <u>Lema</u>. Seja G um grupo de permutações. Os automorfismos de G^* podem ser identificados com o normalizador de G em Sim X , isto é, Aut-$G^* \cong N(G)$.

Prova:

Seja Ψ : Aut - $G^* \longrightarrow$ Sim X .
$(\alpha, \theta) \longrightarrow \theta$

i) Ψ é homomorfismo.

$$\big((\alpha_1, \theta_1) \circ (\alpha_2, \theta_2)\big)\Psi = (\alpha_1 \circ \alpha_2, \theta_1 \circ \theta_2)\Psi = \theta_1 \circ \theta_2 =$$

$$= (\alpha_1, \theta_1)\Psi \circ (\alpha_2, \theta_2), \forall (\alpha_1, \theta_1), (\alpha_2, \theta_2) \in \text{Aut} - G^*.$$

ii) Im $\Psi \subseteq N(G)$.

Seja $\theta \in \text{Im}\,\Psi$.

$xg\theta = x\theta g\alpha$, para todo $x \in X$ e $g \in G$.

Logo $g\theta = \theta g\alpha \Longrightarrow \theta^{-1} g\theta = \theta^{-1}(\theta g\alpha)$

$\theta^{-1} g\theta = g\alpha \in G \;\therefore\; \theta \in N(G) \Longrightarrow$ Im $\subseteq N(G)$.

iii) Im $\Psi = N(G)$.

Basta mostrar que $N(G) \subseteq \text{Im}\,\Psi$.

Seja $\theta \in N(G)$ e $\alpha : G \longrightarrow G$, o automorfismo definido por $g\alpha = \theta^{-1} g\theta$.

Para todo $x \in X$, $(x\theta)(g\alpha) = x(\theta g\alpha) = x(\theta\theta^{-1} g\theta) =$

$= xg\theta$. Então $(\alpha, \theta) \in$ Aut - G^*.

Portanto, $\theta \in \text{Im}\,\Psi$.

iv) Ψ é injeção.

Sejam (α_1, θ) e $(\alpha_2, \theta) \in$ Aut - G^*.

Para todo $x \in X$ e $g \in G$, $xg\theta = x\theta g\alpha_1$ e

$xg\theta = x\theta g\alpha_2$.

Logo $x\theta g\alpha_1 = x\theta g\alpha_2 \Longrightarrow \theta g\alpha_1 = \theta g\alpha_2 \Longrightarrow g\alpha_1 = g\alpha_2 \Longrightarrow \alpha_1 = \alpha_2$.

C A P I T U L O 4

PRODUTO SEMI-DIRETO

(4.1.) Definição:

i) Um semigrupo S age sobre um semigrupo E, à direita, se existe uma função $f : E \times S \longrightarrow E$, que leva $(e, s) \longrightarrow es$, tal que:

$$e(st) = (es)t, \quad (s,t \in S \; ; \; e \in E),$$

$$(e+f)s = es+fs, \quad (s \in S \; ; \; e,f \in E).$$

ii) Um semigrupo S age sobre um semigrupo E, à esquerda, se existe uma função $f : S \times E \longrightarrow E$, que leva $(s, e) \longrightarrow se$, tal que:

$$(st)e = s(te), \quad (s,t \in S \; ; \; e,f \in E).$$

$$s(e+f) = se+sf, \quad (s \in S \; ; \; e,f \in E).$$

(4.2.) Definição: Se o semigrupo S age sobre o semigrupo E, à esquerda, um novo semigrupo pode ser construido: o produto semi-direto de E por S , $(E \text{ sd } S)$, onde o conjunto sob $(E \text{ sd } S)$ é $(E \times S)$ e a multiplicação é definida por:

$$(e,s)\ (f,t) = (e + sf\ ,\ st)\ , \quad \text{para todo } e,f \in E$$

e $s,t \in S$.

Observação: $(E \text{ sd } S)$ é semigrupo, pois, para todo $e,f,g \in E$ e $s,t,u \in S$ temos:

$$\left[(e,s)\ (f,t)\right]\ (g,u) = (e + sf\ ,\ st)\ (g,u) =$$

$$= \Big((e + sf) + (st)g\ ,\ (st)u\Big).$$

Como E e S são semigrupos e S age sobre E à esquerda, $\Longrightarrow \Big((e + sf) + (st)g\ ,\ (st)u\Big) =$

$$= \Big(e + sf + s(tg)\ ,\ s(tu)\Big) = \Big(e + s(f + tg)\ ,\ s(tu)\Big) =$$

$$= (e,s)\ (f + tg\ ,\ tu) = (e,s)\ \left[(f,t)\ .\ (g,u)\right].$$

(4.3.) <u>Definição</u>. Sejam: S semigrupo, E monóide e 0_E, elemento neutro de E. Dizemos que S age sobre E, à esquerda, se S age sobre E, considerando apenas E como semigrupo, e $s0_E = 0_E$, para todo $s \in S$.

(4.4.) <u>Definição</u>. Seja $S^* = (S, \phi, X)$, ação à direita, onde S é monóide, com unidade 1_s e X é conjunto. Dizemos que a ação S^* é unitária, se:

$x\, 1_s = x$, para todo $x \in X$.

Então $1_s \phi = id_X$.

Vamos assumir que se S é grupo a ação por S é unitária.

Nota: Se S^* é ação à esquerda $\Longrightarrow 1_s\, x = x$, para todo $x \in X$.

(4.5.) <u>Lema</u>.

i) Se S e E são monóides, com unidades 1_s e 0_E , respectivamente, e a ação de S sobre E é unitária, então $(0_E , 1_s)$ é a unidade de $(E \text{ sd } S)$, que é também um monóide.

Prova:

Já foi verificado em 4.2. que $(E \text{ sd } S)$ é semigrupo.

Basta, portanto, mostrar que $(0_E , 1_s)$ é a unidade de $(E \text{ sd } S)$.

Para todo $(e,s) \in E \times S$, $(e,s)\ (0_E\ ,\ 1_s) =$

$= (e + s0_E\ ,\ s1_s) = (e + 0_E\ ,\ s) = (e,s)$ e

$(0_E\ ,\ 1_s)\ (e,s) = (0_E + 1_s \cdot e\ ,\ 1_s \cdot s) = (0_E + e,s) =$

$= (e,s)$.

ii) (E sd S) tem submonóides:

ii.1.) $E \times \{1_s\} \cong E$, $E \times \{1_s\} \subseteq (E \text{ sd } S)$.

ii.2.) $\{0_E\} \times S \cong S$, $\{0_E\} \times S \subseteq (E \text{ sd } S)$.

Prova:

ii.1.) $E \times \{1_s\} \cong E$.

A função $\alpha : E \longrightarrow E \times \{1_s\}$ é isomorfismo.
$e \longrightarrow (e\ ,\ 1_s)$

Como S^* é unitária e S monóide, temos:

$- \alpha(e_1) + \alpha(e_2) = (e_1,1_s)\ (e_2,1_s) = (e_1 + 1_s \cdot e_2, 1_s \cdot 1_s) =$

$= (e_1 + e_2\ ,\ 1_s) = \alpha\ (e_1 + e_2)$

$-\ \alpha(0_E) = (0_E\ ,\ 1_s) =$ unidade de $E \times \{1_s\}$.

$-\ \alpha$ é injetiva e sobrejetiva - trivialmente se verifica.

ii.2.) $\{0_E\} \times S \cong S$.

A função $\beta : S \longrightarrow \{0_E\} \times S$ é isomorfismo.
$s \longrightarrow (0_E\ ,\ s)$

$-\ \beta(s_1)\cdot\beta(s_2) = (0_E\ ,\ s_1)(0_E\ ,\ s_2) = (0_E + s_1 \cdot 0_E\ ,\ s_1 \cdot s_2) =$

$= (0_E + 0_E\ ,\ s_1 \cdot s_2) = (0_E\ ,\ s_1 \cdot s_2) = \beta(s_1 \cdot s_2)$

$-\ \beta(1_s) = (0_E\ ,\ 1_s) =$ unidade de $\{0_E\} \times S$.

$-\ \beta$ é injetiva e sobrejetiva - trivial

(4.6.) <u>Lema</u>. Se s é inversível em S , então:

i) $(0_E\ ,\ s^{-1})$ é o elemento inverso de $(0_E\ ,\ s)$ em $(E \text{ sd } S)$.

Prova:

$(0_E\ ,\ s)\ (0_E\ ,\ s^{-1}) = (0_E + s \cdot 0_E\ ,\ s \cdot s^{-1}) = (0_E + 0_E\ ,\ 1_s) =$

$= (0_E , 1_s)$. Também,

$$(0_E , s^{-1}) (0_E , s) = (0_E + s^{-1} . 0_E , s^{-1}s) = (0_E + 0_E , 1_s) =$$

$$= (0_E , 1_s) .$$

ii) Para todo $e \in E$, conjugando $(e , 1_s)$ por $(0_E , s)$ temos:

$$(0_E,s) (e,1_s) (0_E,s)^{-1} = (0_E + se , s1_s) (0_E , s^{-1}) =$$

$$= (se,s) (0_E,s^{-1}) = (se + s0_E , ss^{-1}) = (se , 1_s) .$$

Podemos, portanto, concluir que a ação à esquerda de um monóide sobre um monóide pode ser imerso em um monóide maior, em que os elementos inversíveis agem por conjugação.

(4.7.) <u>Corolário</u>. Sejam G e N grupos. A ação de G sobre N , à esquerda é o mesmo que conjugação em N sd G , de $(0_N , G)$ sobre $(N , 1_G)$.

Então a ação de grupos sobre grupos esta contida no produto semi-direto de grupos.

C A P I T U L O 5

PRODUTO "WREATH"

(5.1.) Definição. Sejam S semigrupo e Y conjunto.

S^Y = conjunto das funções de Y em S.

(5.2.) Definição. Para todo $y \in Y$, $F, G \in S^Y$, definimos $F + G \in S^Y$ como $y(F+G) = yF \cdot yG$.

(5.3.) Lema. S^Y é semigrupo sob a operação $(+)$.

i) S^Y é fechado para a operação $(+)$, (def. 5.2).

ii) $y\left((F+G)+H\right) = y(F+G) \cdot yH = (yF \cdot yG) \cdot yH =$

$= yF \cdot (yG \cdot yH) = yF \cdot \left[y(G+H)\right] = y\left(F + (G+H)\right)$.

(5.4.) Definição. Sejam: $T^* = (T, \psi, Y)$ e S semigrupo.

$y\,(tG) = (yt)\,G$, para todo $y \in Y$, $t \in T$ e $G \in S^Y$.

5.5. Lema. $S^Y \times T$, com a multiplicação abaixo definida, é semigrupo:

$$(F,t) \, . \, (G,u) = (F + tG,\ tu) \text{ , para todo } F,G \in S^Y,\ t,\ u \in T.$$

Prova:

i) $S^Y \times T$ é fechado para a operação acima definida.

Para todo $y \in Y$; $t,u \in T$; $F,G \in S^Y$ mostraremos que:

$$(F,t) \, . \, (G,u) = (F + tG,\ tu) \in S^Y \times T.$$

Como $yt \in Y$ e $G \in S^Y \Longrightarrow tG \in S^Y$.

$tG \in S^Y$ e $F \in S^Y \Longrightarrow F + tG \in S^Y$.

$u,t \in T$, semigrupo, $\Longrightarrow tu \in T$.

Logo $(F + tG,\ tu) \in S^Y \times T$.

ii) Propriedade associativa

Para todo $F, G, H \in S^Y$ e $t,u,v \in T$, temos:

$$\left[(F,t) \, . \, (G,u)\right] \, . \, (H,v) = (F + tG \ ,\ tu) \, . \, (H,v) =$$

$$= \Big((F + tG) + (tu)H \ , \ (tu)\ v\Big) \text{, Também,}$$

$$(F,t) \ . \ \Big[(G,u) \ . \ (H,v)\Big] = (F,t) \ . \ (G + uH \ , \ uv) =$$

$$= \Big(F + t(G + uH) \ , \ t(uv)\Big) \ .$$

i) Para todo $y \in Y$, temos:

$$y \ \Big(t(G + uH)\Big) = (yt) \ (G + uH) = (yt)G \ . \ (yt) \ (uH) =$$

$$= y(tG) \ . \ y\Big(t(uH)\Big) = y(tG) \ . \ y \ \Big((tu)H\Big).$$

ii) T semigrupo $\Rightarrow (tu)v = t(uv)$.

Logo:

$$\Big[(F,t) \ . \ (G,u)\Big] \ (H,v) = (F,t) \ \Big[(G,u) \ . \ (H,v)\Big] \ .$$

(5.6.) <u>Definição</u>. $S \text{ wr } T^* = (S^Y \text{ sd } T)$, com a multiplicação acima definida, onde S é semigrupo, Y conjunto, T semigrupo e $T^* = (T, \phi, Y)$.

(5.7.) <u>Definição</u>. Uma ação de semigrupo $S^* = (S, \phi, X)$ é leal se ϕ é injetiva, isto é:

$$(xs_1 = xs_2 \text{ para todo } x \in X) \Longrightarrow s_1 = s_2.$$

(5.8.) <u>Lema</u>. Se S^* é uma ação leal, então, a multiplicação em S é determinada por composição de funções.

Se $\phi : S \longrightarrow \text{Trans } X$ é injeção, então ϕ é isomorfismo sobre $(S\phi , o)$.

(5.9.) <u>Observação</u>.

Seja $Y = 1,2,\ldots,n$. Então $S \text{ wr } T^*$ pode ser representado por um semigrupo de matrizes com a operação de multiplicação. Se $(F,t) \in S \text{ wr } T^*$, define-se a $n \times n$ matriz $M(F,t)$, por:

$$M(F,t)_{i,j} = \begin{cases} iF & \text{se } j = it \\ 0 & \text{se } j \neq it \end{cases}$$

Seja $M(S^Y \times T) = \{ M(F,t) \text{ tal que } (F,t) \in S \text{ wr } T^* \}$.

i) A função $\gamma : S^Y \times T \longrightarrow M(S^Y \times T)$ é homomorfismo
$(F,t) \longrightarrow M(F,t)$

de semigrupos.

Sejam $M(F,t)$ e $M(G,u) \in M(S^Y \times T)$.

Então:

$$M(F,t)_{i,j} = \begin{cases} iF & \text{se } j = it \\ 0 & \text{se } j \neq it \end{cases}$$

$$M(G,u)_{i,j} = \begin{cases} iG & \text{se } j = iu \\ 0 & \text{se } j \neq iu \end{cases}$$

Verifiquemos que $\gamma(F,t) \cdot \gamma(G,u) = \gamma\big((F,t)\cdot(G,u)\big)$

$\gamma(F,t) \cdot \gamma(G,u) = M(F,t) \cdot M(G,u)$.

Logo: $\big(M(F,t) \cdot M(G,u)\big)_{i,j} = iF \cdot M(G,u)_{it,j}$.

$$\text{Mas} \quad iF \cdot M(G,u)_{it,j} = \begin{cases} iF\cdot(it)G & \text{se } j = (it)u \\ 0 & \text{se } j \neq (it)u \end{cases}$$

$$\text{Então} \quad M(F,t) \cdot M(G,u)_{i,j} = \begin{cases} i(F+tG) & \text{se } j = i(tu) \\ 0 & \text{se } j \neq i(tu) \end{cases}$$

Logo $\gamma(F,t) \cdot \gamma(G,u) = M(F,t) \cdot M(G,u) = M(F+tG,tu)$.

Também $\gamma\big((F,t)\cdot(G,u)\big) = M\big((F,t)\cdot(G,u)\big) = M(F+tG,tu)$.

Portanto $\gamma(F,t) \cdot \gamma(G,u) = \gamma\big((F,t)\cdot(G,u)\big)$.

ii) γ é isomorfismo se T^* é leal.

Se $M(F,t) = M(G,u)$ então $M(F,t)_{i,j} = M(G,u)_{i,j}$, $1 \leq i,j \leq n$.

Na linha i o único elemento diferente de $\underline{0}$ é o que está na coluna (it) para $M(F,t)$ e o que está na coluna (iu) para $M(G,u)$.

Como $\underline{O}$ não pertence a S, então $it = iu$ e $iF = iG$, para todo i. Portanto $F = G$.

Como T^* é leal então $t = u$.

Logo $\gamma(F,t) = \gamma(G,u) \Longrightarrow \gamma$ é injetora.

(5.10.) Definição. Produto "wreath".

Sejam : $S = (S, \phi, X)$ e $T = (T, \psi, Y)$ ações.

$S^* \text{ wr } T^*$ = produto "wreath" de S^* por T^*.

Por definição $S^* \text{ wr } T^* = (S \text{ wr } T^*, \Delta, X \times Y)$, onde:

$$\begin{aligned} \Delta : (X \times Y) \times (S \text{ wr } T) &\longrightarrow X \times Y \\ (x,y) \cdot (F,t) &\longrightarrow (x(yF), yt), \text{ para todo} \end{aligned}$$

$x \in X$, $y \in Y$, $t \in T$, e $F \in S^Y$.

(5.11.) Lema. O produto "wreath" é uma ação de $(S \text{ wr } T^*)$ sobre $X \times Y$.

Basta verificar que $(x,y)\,(F,t) \cdot (G,u) =$

$= (x,y)(F,t)\,(G,u)$.

$$\big((x,y)\,(F,t)\big)\,(G,u) = (x(yF),yt)\,(G,u) =$$

$$= \big(x(yF)\,(yt)G,\ (yt)u\big)$$

Por outro lado $(x,y)\big((F,t)\,(G,u)\big) =$

$$= (x,y)\,(F + tG, tu) = \big(x(y(F+tG)), y(tu)\big) =$$

$$= \big(x\,(yF) \cdot y(tG)\ , y(tu)\big)$$

S^* e T^* ações $\Longrightarrow \Big(x(yF \,.\, y(tG), y(tu)\Big) =$

$= \Big(x(yF) \,.\, (yt)G, (yt)u\Big)$.

Logo $\Big((x,y)\ (F,t)\Big)\ (G,u) = (x,y)\ \Big((F,t)\cdot(G,u)\Big)$ e o produto "wreath" , portanto, é ação.

(5.12.) Definição. Produto "wreath" clássico.

S wr T^* é chamado produto "wreath" clássico, quando $T = Y$ e a ação de T sobre Y é a multiplicação à esquerda.

C A P I T U L O 6

PROPRIEDADES DE AÇÕES DE SEMIGRUPOS E GRUPOS

(6.1.) <u>Definição</u>. Constituinte de S .

Seja $S = (S, \phi, X)$ uma ação de semigrupo. Constituinte de S é o semigrupo $S\phi$ de transformações sobre X .

(6.2.) <u>Observação</u>.

Se $S^* = (S, \phi, X)$ é uma ação de semigrupo e Y um subconjunto estável de X, então há uma natural ação (S, ϕ_Y, Y) e um morfismo (id_S , i_Y) de (S, ϕ_Y, Y) para (S, ϕ, X) que é uma injeção. Definimos $\phi_Y = \phi/Y$.

$$\begin{tikzcd} Y \arrow[r, "s\phi_Y"] \arrow[d, "i_Y"'] & Y \arrow[d, "i_Y"] \\ X \arrow[r, "s\, id_S\, \phi"'] & X \end{tikzcd}$$

(6.3.) <u>Definição</u>. S^* é transitiva se para todo par ordenado $(x,x') \in X \times X$, há algum $s \in S$, tal que, $xs = x'$. Se

$x \in X$, então : $xS = \{xs \mid s \in S\}$.

(6.4.) Lema. S^* é transitiva, se e sómente se, $xS = X$, para todo x .

Prova:

$\Longrightarrow$

i) $xS = X$.

$X \subseteq xS$

S^* transitiva $\Longrightarrow \forall\ x' \in X$, $\exists\ s \in S$, tal que,

$x' = xs \in xS$.

$xS \subseteq X$, pois, S^* é ação de S sobre X .

$\Longleftarrow$

ii) S^* é transitiva.

Seja $(x , x') \in X \times X$.

Como $xS = X$, $\exists$ $s \in S$, tal que, $x' = xs \Longrightarrow S^*$ é transitiva.

(6.5.) Definição. Seja X um conjunto e $z \in X$. A função constante c_z é dada por: $c_z : X \longrightarrow X$

$$x \longrightarrow xc_z = z .$$

(6.6.) Definição. Seja $S^* = (S, \phi, X)$ uma ação leal de semigrupo.

S_X^c é o semigrupo $\langle S\phi \, , \, CX \rangle \subseteq \text{Trans } X$, onde CX é o semigrupo de funções constantes sobre X . Como S^* é leal pode-se identificar os elementos de S e $S\phi$. A ação natural de S_X^c sobre X é denotada por $(S_X^c)^*$.

S_X^{-c} é o subsemigrupo de $S\phi$, gerado pelas funções não constantes em $S\phi$. Se toda função em $S\phi$ é constante , $S_X^{-c} = id_X$, por convenção.

(6.7.) Proposição. Se S é um grupo e $S^* = (S, \phi, X)$ uma ação então:

i) S^* é leal $\Longleftrightarrow$ o único elemento de S , fixando tudo em X é a unidade de S .

ii) S^* é transitiva $\Longleftrightarrow xS = X$ para pelo menos um $x \in X$.

Prova:

i) $\Longrightarrow$

S grupo $\Longrightarrow S^*$ unitária $\Longrightarrow x1_s = x \, , \, \forall \, x \in X$.

Seja $s \in S$, tal que, $xs = x \, , \, \forall \, x \in X$.

$\therefore \quad x1_s = x = xs$.

$S^* \text{ leal} \Longrightarrow s = 1_s$.

$\Longleftarrow$

Se $\quad xs = xs' \Longrightarrow x(s\, s'^{-1}) = x \Longrightarrow s\, s'^{-1} = 1_s \Longrightarrow$
$\Rightarrow s = s' \Longrightarrow S^*$ é leal.

ii) $\Longrightarrow$

S^* transitiva $\Longrightarrow xS = X$, para todo $x \in X$.
(lema 6.4.)

$\Longleftarrow$

Por hipótese , $\exists\ x \in X$, tal que, $xS = X$.

Seja $(x', x'') \in X \times X$. Então existe s' e s'' , tal que , $x' = xs'$ e $x'' = xs''$.

$x' = xs' \Longrightarrow x = x'\, s'^{-1}$.

$x'' = xs'' \Longrightarrow x'' = (x' s'^{-1})\, s'' = x'\, (s'^{-1}\, s'') = x's$.

(6.8.) <u>Proposição</u>. Se S é um semigrupo e a multiplicação à direita é transitiva , então S^1 é grupo.

Basta verificar a existência do elemento inverso

Seja $(s\, ,\, 1_s) \in S \times S$.

S^* transitiva $\Longrightarrow \exists\, s' \in S$, tal que, $s\, s' = 1_s$.

Por outro lado, $(s\, s')\, (s'\, s) = s's$ e existe

$s'' \in S$, tal que, $(s' s) s'' = 1_s$.

$\therefore \quad s's = (s's)(s' s s'') = s' s s'' = 1_s$.

(6.9.) <u>Proposição</u>. Sejam $S^* = (S, \phi, X)$ e $T^* = (T, \psi, Y)$

i) Se S^* e T^* são unitárias $\Longrightarrow S^*$ wr T^* é unitária.

ii) Se S^* e T^* são ambas leais $\Longrightarrow S^*$ wr T^* é leal.

iii) Se S^* e T^* são ambas transitivas $\Longrightarrow S^*$ wr T^* é transitiva.

iv) Se S e T são ambos grupos $\Longrightarrow S$ wr T^* é grupo.

Prova:

i) Por definição S^* wr $T^* = (S^Y{}_{sd}\, T, \triangle, X \times Y)$.

i.1.) Verifiquemos que para qualquer $(F,t) \in S^Y{}_{sd}\, T$, $(F,t) \cdot (C_S , 1_T) = (F,t)$, sendo $C_S : Y \longrightarrow S$, tal que, $C_S (y) = 1_S$.

$(F,t)(C_S , 1_T) = (F + tC_S , t\, 1_T)$.

Para todo $y \in Y$, $y(F + tC_S) = yF \cdot y(tC_S) =$

$= yF \cdot (yt)\, C_S = yF \cdot 1_S = yF$.

Logo $F + tC_S = F \Longrightarrow (F,t) \cdot (C_S, 1_T) = (F , t . 1_T)$.

T^* unitária $\Longrightarrow t.1_T = t \Longrightarrow (F,\ t.1_T) = (F,t)$.

Verifica-se facilmente que $(C_S,1_T) \,.\, (F,t) = (F,t)$.

i.2.) Verifiquemos que $(x,y)\ (C_S\ ,\ 1_T) = (x,y)$, para todo $(x,y) \in X \times Y$.

$$(x,y)\ (C_S,\ 1_T) = \Big(x\ (yC_S)\ ,\ y\ 1_T\Big) = (x1_S\ ,\ y\ 1_T)\ .$$

S^* e T^* unitárias $\Longrightarrow (x1_S\ ,\ y\ 1_T) = (x,y)$.

Logo S^* wr T^* é unitária.

ii) Mostraremos que S^*wr T^* é leal, se S^* e T^* são leais.

Suponhamos que para todo $(x,y) \in X \times Y$, $F \in S^Y$ e $t \in T$, $(x,y)\ (F,t) = (x,y)\ (G,u)$.

$$\therefore \Big(x\ (yF)\ ,\ yt\Big) = \Big(x\ (yG)\ ,\ yu\Big)\ .$$

Como S^* e T^* são leais, se para todo x,y , $x\ (yF) = x\ (yG) \Longrightarrow yF = yG \Longrightarrow F = G$.

Para todo y , $yt = yu \Longrightarrow t = u$, pois T^* é leal.

$\therefore$ para todo $(x,y) \in X \times Y$, $(F,t) = (G,u) \Longrightarrow$

S^* wr T^* é leal .

iii) S^* e T^* transitivas $\Longrightarrow S^*$ wr T^* transitiva.

Mostraremos que para todo $(x_1, y_1), (x_2, y_2) \in X \times Y$, $\exists\ (F,t) \in S^Y \times T$, tal que, $(x_1,y_1)(F,t) = (x_2, y_2)$.

S^* e T^* transitivas $\Longrightarrow \exists s \in S$, tal que, $x_1 s = x_2$ e $\exists\ t \in T$, tal que, $y_1 t = y_2$.

Seja $F : Y \longrightarrow S$, tal que, $F(y) = s$, $\forall\ y \in Y$.

$(x_1,y_1)(F,t) = \left(x_1(y_1F), y_1t \right) = (x_1s, y_1t) = (x_2, y_2)$.

iv) Mostraremos que são válidas as propriedades de grupo para S wr T^*.

_Propriedade associativa - trivialmente válida, pois $S^Y{}_{sd}\, T$ é semigrupo.

_Existência do elemento neutro
Provado em (6.9. i.1.) que o elemento neutro é $(C_S, 1_T)$.

_Existência do elemento inverso

Seja $(F,t) \in S^Y \times T$.

Definimos $G \in S^Y$ como $yG = \left((yt^{-1})F \right)^{-1}$.

Portanto se $y \in Y \Longrightarrow y(F + tG) = yF \cdot (yt)G =$

$= yF \left((yt)t^{-1}F \right)^{-1} = yF\,(yF)^{-1} = 1_S$.

Logo $(F,t)\,(G,t^{-1}) = id_{S^Y_{sd}\,T}$.

$(G,t^{-1})\,(F,t) = (G + t^{-1}F \, , 1_T)$.

Se $y \in Y$, $y(G + t^{-1}F) = yG \cdot yt^{-1}F =$

$= \left((yt^{-1})F \right)^{-1} \cdot (yt^{-1}F) = 1_S$.

CAPITULO 7

CONSIDERAÇÕES SOBRE S^Y e $S \text{ wr } T^*$

(7.1.) <u>Lema</u>. Seja Y um conjunto e S um semigrupo. Se (T,Ψ,Y) é uma ação de semigrupo à direita, há uma ação canônica à esquerda de T sobre S^Y, semigrupo, assim definida:

$$y(tG) = (yt)G \text{ , para todo } y \in Y \text{ , } t \in T \text{ e } G \in S^Y .$$

Verifiquemos que, realmente, temos uma ação.

i) Para todo $t_1, t_2 \in T$ e $F \in S^Y$, $(t_1 t_2)F =$

$$= t_1(t_2 F) \therefore y(t_1 t_2)F = (yt_1 t_2)F = (yt_1)t_2 \; F = (yt_1)(t_2 F),$$

para $y \in Y$.

ii) Para todo $y \in Y$, $t \in T$ e $F,G \in S^Y$,

$$y\Big(t(F+G)\Big) = (yt)(F+G) = (yt)F \cdot (yt)G = y(tF + tG) .$$

(7.1.1.) Exemplo:

Suponhamos $Y = \{1,2,\ldots,n\}$.

S^Y pode ser identificado com S^n , olhando $F:Y \longrightarrow S$, como uma n-upla $(1F, 2F, \ldots, nF)$.

A ação de T sobre S^Y pode ser escrita como:

$tF = t(s_1, s_2, \ldots, s_n) = (s_{1t}, s_{2t}, \ldots, s_{nt})$, para

todo $s_1, s_2, \ldots, s_n \in S$ e $t \in T$.

Então:

$(tt')F = t(t'F) = t\,(s_{1t'} , s_{2t'} , \ldots , s_{nt'})$.

Seja $s_i' = s_{it'}$.

$\therefore\ t(s_{1t'} , s_{2t'} , \ldots , s_{nt'}) = t(s_1' , s_2' , \ldots , s_n') =$

$= \left(s_{1t}' , s_{2t}' , \ldots , s_{nt}'\right) = \left(s_{1tt'} , s_{2tt'} , \ldots , s_{ntt'}\right)$.

$\therefore\ tt'\,(s_1, \ldots, s_n) = (s_{1tt'} , s_{2tt'} , \ldots , s_{ntt'}) =$

$= t\,(s_{1t'} , s_{2t'} , \ldots , s_{nt'})$.

(7.2.) Observações:

Sejam (S, ϕ, X) e (T, Ψ, Y) ações. Consideremos $S \text{ wr } T^*$. Então:

i) S é chamado semigrupo de baixo de $S \text{ wr } T^*$ e T semigrupo de cima.

ii) S^Y é chamado semigrupo de base.

iii) Quando S e T são monóides, S^Y e T são canonicamente subsemigrupos de $S \text{ wr } T^*$ e S está encaixado em $S \text{ wr } T^*$ de várias maneiras. Um particular exemplo disto é o "encaixe diagonal", levando $s \in S$ sobre $M(F_S, 1_T)$. O "encaixe diagonal" leva S sobre as matrizes escalares, onde $S \text{ wr } T^*$ é escrito como um semigrupo de matrizes. S^Y corresponde à matriz diagonal.

$$s \longrightarrow F_s \longrightarrow (F_s, 1_T) \longrightarrow M(F_s, 1_T), \text{ onde :}$$

$$M(F_s, 1_T)_{i,j} = \begin{cases} M(F_s, 1_T)_{i,i} = iF_s = s, & j = i \\ \\ M(F_s, 1_T)_{i,j} = 0, & i \neq j \end{cases}$$

Então $M(F_s, 1_T) = s.I$

iv) Quando S e T são grupos, então S^Y é um subgrupo normal de $S \text{ wr } T^* = S^Y \text{ sd } T$ e a ação Ψ é conjugação de S^Y pela cópia canônica de T em $S \text{ wr } T^*$. $\left(T \cong \{0_S\} \times T \right)$.

_ $S^Y \subseteq S^Y \text{ sd } T$

$S^Y \cong S^Y \times \{1_T\} \subseteq S^Y \text{ sd } T$.

_ $S^Y \trianglelefteq S \text{ wr } T^*$

Afirmamos que $(G,t)(F,1_T)(G,t)^{-1} \in S^Y$, para todo $G,F \in S^Y$, t, $1_T \in T$.

$$(G,t)^{-1} = \left((t^{-1} G)^{-1}, t^{-1}\right), \quad G \in S^Y, \quad t \in T.$$

$$(G,t)(F,1_T)(G,t)^{-1} = (G,t)(F,1_T)\left((t^{-1} G)^{-1}, t^{-1}\right) =$$

$$= (G+tF, t1_T)\left((t^{-1}G)^{-1}, t^{-1}\right) = \left((G+tF) + t(t^{-1}G)^{-1}, tt^{-1}\right) \Longrightarrow$$

$$\Longrightarrow \left((G+tF) + t(t^{-1} G)^{-1}\right) \in S^Y.$$

_ A ação Ψ de S^Y pela cópia canônica de T em $S \text{ wr } T^*$ é conjugação de S^Y pela cópia canônica de T.

Para todo $F \in S^Y$ e t, t^{-1}, $1_T \in T$, temos:

$$(1_S, t)\,(F, 1_T)\,(1_S, t^{-1}) = (1_S + tF, t1_T)\,(1_S, t^{-1}) =$$

$$= \left((1_S + tF) + t1_T, tt^{-1}\right).$$

Para todo y, $y\left((1_S + tF) + t1_T\right) = (y1_T) \cdot \left(y(tF)\right) \cdot y(t1_T) =$

$= 1_S \cdot y(tF) \cdot 1_S = y(tF)$.

Logo: $\left((1_S + tF) + 1_T, tt^{-1}\right) = (tF, 1_T)$.

C A P I T U L O 8

ESQUEMA DE DECOMPOSIÇÃO

(8.1.) <u>Decomposição de S^* ou imersão de S^* em M^* wr N^*</u>.

Sejam: $S^* = (S, \phi, X)$, $M^* = (M, \Psi, Y)$ e $N^* = (N, \rho, P)$, ações.

S^* é dita imersa em M^* wr N^* se divide M^* wr N^*, isto é, se existe um morfismo sobrejetivo, $(\alpha, \theta): T^* \longrightarrow S^*$, onde T^* é alguma subação de M^* wr N^*.

Se (α, θ) é morfismo injetivo dizemos que S^* está homomorficamente imerso em M^* wr N^*.

(8.2.) <u>Definição</u>. S^* - partição de X.

Seja $S^* = (S, \phi, X)$. Uma S^*_ partição de X

é uma partição de X, tal que:

$$\Pi = \left\{ X_i \subseteq X, \text{ tal que, } \overset{\circ}{\cup} X_i = X \text{ e para } \forall\ i, \right.$$
$$\left. j \;/\; X_i S = X_j \right\}.$$

(8.3.) <u>Definição</u>. Sistema de coordenadas.

Seja $S^* = (S, \phi, X)$ uma ação de semigrupo e Π uma S^* _ partição de X .

Um sistema de coordenadas para Π é um par ordenado (M^*, W) , onde $M^* = (M, \Psi, Y)$ e $W = \left\{ \beta_B \right\}_{B \in \Pi}$, $\beta_B : B \longrightarrow Y$, injeção, tal que, dado $s \in S$ e $B \in \Pi$:

$$M_B^s = \left\{ m \in M \;/\; (x\beta_B)\, m = (xs)\beta_{Bs} \,,\ x \in B \right\} \neq \phi \ .$$

(8.4.) <u>Teorema</u>. Esquema de Decomposição.

Sejam: $S^* = (S, \phi, X)$ uma açaõ leal de semigrupo, com π uma S^*_ partição de X e (M^*, W) um sistema de coordenadas.

Então S^* divide M^* wr $\overline{S}^*$, onde $\overline{S}$ é, por definição, o constituinte de $(S^{\pi})^*$ e $\overline{S}^* = (\overline{S}, \text{trans}, \pi)$.

Para provar este teorema basta, então, encontrar um morfismo sobrejetivo $(\alpha, \theta) : T^* \longrightarrow S^*$, onde T^* é alguma subação de M^* wr $\overline{S}^* = (M \text{ wr } \overline{S}^*, \Delta, Y \times \pi)$.

Prova:

Parte I - Definiremos $T \subseteq M^{\pi} \times S$; T^* e mostraremos que T^* é subação de M^* wr $\overline{S}^*$.

Parte II - Mostraremos que (α, θ), definido na parte I, é morfismo sobrejetivo de ações.

Parte I

i) Sejam as funções:

i.1.) $\lambda : X \longrightarrow Y \times \pi$

$x \longrightarrow (x\beta_B, B)$, $x \in B \in \pi$.

λ é injetiva : $(x\beta_B\ ,\ B) = \left(y\beta_{B'}\ ,\ B'\right) \Longrightarrow B = B' \Longrightarrow$

$x = y$, pois β_B é injetiva.

i.2.) $\theta = \lambda^{-1} : \operatorname{Im}\lambda \longrightarrow X$.

ii) Seja $M_B^s = \left\{ m \in M \mid (x\beta_B)\, m = xs\,\beta_{Bs},\ x \in B \right\}$.

Sejam: $s \in S$, $F_s : \pi \longrightarrow M$, tal que, $BF_s \in M_B^s$

e $\bar{s}$ é o correspondente de s em $\bar{S}$. ($\bar{s} \in \operatorname{Trans}\pi$, com

$B\bar{s} = Bs$).

Para todo $x \in B$, $B \in \pi$, mostraremos que:

ii.1.) $\left[(x\beta_B\ ,\ B)\ (F_s\ ,\ \bar{s})\right] \in \operatorname{Im}\lambda$.

ii.2.) $\left[(x\beta_B\ ,\ B)\ (F_s\ ,\ \bar{s})\right]\theta = xs$.

Usando a definição de produto "wreath", definição F_s e definição S^* _ partição temos:

$(x\beta_B, B)(F_s, \bar{s}) = \left(x\beta_B\,(BF_s)\ ,\ B\bar{s} \right) \in Y \times \pi$ e

$BF_s \in M_B^s$.

$$\left(x\beta_B\,(BF_s)\,,\,B\bar{s}\right) = \left((xs)\,\beta_{Bs}\,,\,B\bar{s}\right) =$$

$$= \left((xs)\,\beta_{Bs}\,,\,Bs\right) \in \operatorname{Im}\lambda\,,$$ o que prova (ii.1.).

Como $\theta = \lambda^{-1}$ temos:

$$\left((xs)\,\beta_{Bs}\,,\,Bs\right)\theta = xs\,.$$

Portanto:

$$\left((x\beta_B,\,B)\,(F_s,\bar{s})\right)\theta = xs\,,$$ o que prova (ii.2.) .

iii) <u>Lema</u>. Seja $T = \left\{ (F,z) \mid z \in \bar{S} \text{ e } \exists\, s \in S \mid \bar{s} = z \text{ e } F\colon \Pi \longrightarrow M\,,\text{ com } BF \in M_B^s \right\}$. Dado $(F,z) \in T$, $\exists!\; s \in S \mid \bar{s} = z$ e $BF \in M_B^s$, $B \in \Pi$.

Prova:

Suponhamos $\bar{s} = \bar{s}' = z$ com $BF \in M_B^s$, $BF \in M_B^{s'}$, $B \in \Pi$.

$(x\beta_B\,,\,B)\,(F,\bar{s})\,\theta = xs$ e $(x\beta_B,\,B)\,(F,\bar{s})\theta = xs'$,

para todo $x \in B$. Como $\bigcup_{\Pi} B = X$, $xs = xs'$, $\forall\; x \in X$.

Como S^* é leal $\Longrightarrow s = s'$.

Definição. Pelo lema anterior podemos definir

$\alpha : T \longrightarrow S$, com $(F,z)\alpha = s$, onde $s \in S$, $\bar{s} = z$ e

$BF \in M_B^s$, $B \in \Pi$.

iv) T^* é subação de M^* wr $\bar{S}^*$, onde $T^* = (T, \delta, \mathrm{Im}\,\lambda)$,

$\mathrm{Im}\,\lambda \subseteq Y \times \Pi$ e $\delta = \Delta|_T$.

Prova:

iv.1.) $M_B^s \cdot M_{Bs}^{s'} \subseteq M_B^{ss'}$, onde:

$$M_B^s = \{ m \in M \mid (x\beta_B)\, m = (xs)\, \beta_{Bs'},\ x \in B \},$$

$$M_{Bs}^{s'} = \{ m' \in M \mid (x\beta_B)\, m' = (xs')\, \beta_{Bss'},\ x \in B \},$$

$$M_B^{ss'} = \{ m'' \in M \mid (x\beta_B)\, m'' = (xss')\, \beta_{Bss'},\ x \in B \}.$$

Sejam $m \in M_B^s$ e $m' \in M_{Bs}^{s'}$.

$$(x\beta_B)\,(mm') = \big((xs)\,\beta_{Bs}\big)\, m' = (x\,s\,s')\,\beta_{Bss'} .$$

Logo $m \,.\, m' \in M_B^{ss'}$.

iv.2.) T é fechado em relação à multiplicação.

$(F,\bar{s}) \,.\, (F',\bar{s}') = (F+\bar{s}F' \,,\, \bar{s}.\bar{s}')$, para todo

$(F,\bar{s})$, $(F',\bar{s}') \in T$, $BF \in M_B^s$, $BF' \in M_B^{s'}$.

$B(F + \bar{s}F') = BF \,.\, B\,\hat{s}\,F' \in M_B^s \,.\, M_{Bs}^{s'} \subseteq M_B^{ss'}$, para

todo $\bar{B} \in \Pi$.

Logo:

$(F,\bar{s}) \,.\, (F',\bar{s}') = (F+\bar{s}F',\overline{ss'}) \in T.$

iv.3.) Conclusão: T é subsemigrupo de M wr $\bar{S}^*$.

T age sobre $\mathrm{Im}\,\lambda$. (ii.1).

Logo T^* é subação de M^* wr $\bar{S}^*$.

Parte II

Mostraremos, agora, que $(\alpha\,,\theta)$ é morfismo sobrejetivo de ações.

i) $\alpha : T \longrightarrow S$ é homomorfismo sobrejetivo.

_ α é sobrejetiva, pois, para cada $s \in S$ e todo $B \in \Pi$, $\exists\ m \in M_B^s$ e definimos $BF = m$. Então:

$(F,\bar{s}) \in T$ e $(F,\bar{s})\alpha = s$.

_ α é homomorfismo.

$(F,\bar{s})\alpha \,.\, (F',\bar{s}')\alpha = \bar{s} \,.\, \bar{s}'$ e $\big((F,s) \,.\, (F,s')\big)\alpha =$

$= (F + \bar{s}F' \,,\, \bar{s} \,.\, \bar{s}')\alpha = s \,.\, s'$, para todo $(F,\bar{s})$,

$(F',\bar{s}') \in T$.

ii) θ é sobrejetiva pois $\theta = \lambda^{-1}$.

iii) Mostraremos, agora, que o diagrama abaixo comuta, isto é, $(x\beta_B \,,\, B)\theta \,.\, (F,z)\alpha =$

$= (x\beta_B \,,\, B) \,.\, (F,z)\theta$, $z = \bar{s}$, para todo $x \in \mathcal{B}$,

e $(F,z) \in T$.

$$\begin{tikzcd}
\mathrm{Im}\,\lambda \arrow[r, "{(F,z)}"] \arrow[d, "\theta"'] & \mathrm{Im}\,\lambda \arrow[d, "\theta"] \\
X \arrow[r, "{s=(F,z)\alpha}"'] & X
\end{tikzcd}$$

$(x\beta_B, B)\theta \cdot (F,z)\alpha = xs$, pois $(x\beta_B , B) =$

$= \lambda(x)$ e $\theta = \lambda^{-1}$ e $(F,z)\alpha = s$.

Em (ii.2) já foi provado que:

$$\left((x\beta_B , B)\ (F,z)\right)\ \theta = xs.$$

Logo o diagrama acima comuta.

Conclusão:

Logo S^* é imagem homomórfica de T^* e S^* divide M^* wr $\bar{S}^*$.

(8.5.) Corolário. Seja $S^* = (S, \phi, X)$ uma ação leal de semigrupo , com Π uma S^*_ partição e sistema de coordenadas (M^*, W) , M^* leal , $M^* = (M,\Psi,Y)$ e as β_B bijeções. Então há uma imersão homomórfica de S^* em M^* wr $\bar{S}^*$.

Prova:

Basta verificar que (α , θ) é morfismo injetivo.

i) Verifiquemos que $\left| M_B^s \right| = 1$.

Sejam m' e $m'' \in M_B^s$.

Para $x \in B$ e $B \in \Pi$, temos:

$(x\beta_B)\, m' = xs\beta_{Bs}$ e $(x\beta_B)\, m'' = xs\beta_{Bs}$.

$\therefore\ (x\beta_B)\, m' = (x\beta_B)\, m''$.

Como $\beta_B : B \longrightarrow Y$ é sobre $\Longrightarrow m'\Psi = m''\Psi$.

M^* leal $\Longrightarrow m' = m''$ $\therefore$ $\left| M_B^s \right| = 1$.

ii) α é injetiva.

α é injetiva , pois, $\alpha^{-1}(s) = \left\{ (F,\bar{s}) \mid BF \in M_B^s \right\} \subseteq T$

e como $\left| M_B^s \right| = 1$, $\exists |$ F , tal que, $BF \in M_B^s$.

$\therefore$ $\left| \alpha^{-1}(s) \right| = 1$.

iii) Θ é injetiva , pois $\Theta = \lambda^{-1}$.

(8.6.) <u>Corolário</u>. Seja S^* uma ação leal de semigrupo onde Y é subconjunto estável de S e o conjunto $\Pi = \{Y\} \cup \{\{x\}\ ,\ x \in X - Y\}$ é uma S^* _ partição . Então S^* divide M^* wr $\bar{S}^*$, onde $M = (\langle \bar{S}_Y, CY \rangle$, trans, Y) .

Prova:

Y estável $\Longrightarrow$ para todo $s \in S$, $ys \in Y$.

Seja $y_o \in Y$ e seja $\beta_Y = id_Y$, $x\beta_{\{x\}} = y_o$, para $x \in X - Y$.

Se $s \in S$ e $B \in \Pi$, definimos :

$$m_B^s = \begin{cases} s\phi_Y\ , \text{ se } B = Y\ ,\quad \phi_Y = \text{ação de } S \text{ sobre } Y\ . \\ C_{xs}\ , \text{ se } B = \{x\}\ ,\quad x \in X - Y\ ,\quad xs \in Y\ . \\ C_{y_o}\ , \text{ se } B = \{x\}\ ,\quad x \in X - Y\ ,\quad xs \in X - Y\ . \end{cases}$$

Verifiquemos que m_B^s satisfaz as condições do teorema da decomposição.

i) $m_B^s \in S_Y^c = S\phi_Y \cup CY$, onde CY é o semigrupo das funções constantes de Y . Isso acontece pela própria definição de m_B^s .

ii) m_B^s satisfaz $(x\beta_B)\, m_B^s = (xs)\, \beta_{Bs}$.

$B = Y \Longrightarrow m_B^s = s\phi_Y \Longrightarrow (y\beta_Y)\, s\phi_Y = ys$ e

$(ys)\beta_{Ys} = ys\beta_Y = ys$.

$B = \{x\}$, $x \in X - Y$ e $xs \in Y$, $m^s_{\{x\}} = c_{xs}$.

$\left(x\beta_{\{x\}}\right) m^s_{\{x\}} = \left(x\beta_{\{x\}}\right) c_{xs} = y_o\, c_{xs} = xs = xs\beta_{Bs}$.

$B = \{x\}$, $x \in X - Y$ e $xs \in X - Y$, $m^s_{\{x\}} = c_{y_o}$.

$\left(x\beta_{\{x\}}\right) c_{y_o} = y_o$, $xs\beta_{xs} = y_o$, $xs \in X - Y$.

Estamos, portanto, nas condições do teorema da decomposição. Logo S^* divide M^* wr $\bar{S}^*$.

CAPITULO 9

DECOMPOSIÇÃO DE AÇÕES DE GRUPOS

Demonstraremos uma série de proposições que culminam no importante teorema de Kaloujnine - Krasner .

(9.1.) <u>Proposição</u>. Seja $G^* = (G, \phi, X)$ uma ação leal de grupo e π uma G^* _ partição. Suponhamos que a ação induzida por G sobre π é transitiva. Seja $Y \in \pi$ e $G_{(Y)}$, $(G_{(Y)} \neq \phi)$, o subgrupo de G que fixa Y como conjunto.

Seja $G^*_{(Y)} = (G_{(Y)}$, trans Y, Y) uma ação leal. Então G^* está homomórficamente imerso em $G^*_{(Y)}$ wr $(G^{\pi})^*$.

Prova:

i) Verifiquemos que se $Bg \subseteq B' \Longrightarrow Bg = B'$ $(B, B' \in \pi$ e $g \in G)$.

$Bg \subseteq B' \Longrightarrow Bgg^{-1} \subseteq B'g^{-1} \Longrightarrow B \subseteq B'g^{-1} \subseteq B'' \therefore \quad B = B''$ e

$B'g^{-1} = B \quad \therefore \quad B' = Bg$.

ii) $\beta_B : B \longrightarrow Y$, abaixo definida, é bijeção.

Como a ação de G sobre Π é transitiva , dados B e $Y \in \Pi$, sempre $\exists\ g_B$ tq. $Bg_B \subseteq Y$. Por (i) $\Longrightarrow Bg_B = Y$.

Para cada $B \in \Pi$, fixemos $g_B \in G$ tq. $Bg_B = Y$. Definimos então $\beta_B : B \longrightarrow Y$, por $x\beta_B = xg_B$, $x \in B$.

β_B é sobre $(Bg_B = Y)$ e é injetiva, pois, G é grupo .

iii) Mostraremos que $(g_B^{-1}\, h\, g_{Bh}) \in (G_{(Y)})_B^h$, onde $h \in G$, $B \in \Pi$.

Se $x \in B \in \Pi \Longrightarrow xh \in Bh \in \Pi$. Então:

$(xh)\beta_{Bh} = (xh)g_{Bh} = xg_B\, g_B^{-1}\, h\, g_{Bh} = (x\beta_B)\,(g_B^{-1}\, h\, g_{Bh})$.

$(xh)\beta_{Bh} \in Y \Longrightarrow (x\beta_B)\,(g_B^{-1}\, h\, g_{Bh}) \in Y$.

β_B sobre $\Longrightarrow \forall y \in Y$, $\exists\ x \in B$ tq. $x\beta_B = y$.

Logo, se $y \in Y$, $y(g_B^{-1}\, h\, g_{Bh}) \in Y \Longrightarrow$

$g_B^{-1}\, h\, g_{Bh} \in (G_{(Y)})_B^h$ e $(G_{(Y)})_B^h \neq \emptyset$, $\forall h \in G$.

Então $\left\{ G^*_{(Y)} , \{\beta_B\}_{B \in \Pi} \right\}$ é sistema de coordenadas que satisfaz as condições requeridas pelo Corolário (8.5.) .

Portanto G^* está homomórficamente imerso em $G^*_{(Y)}$ wr $\bar{G}^*$.

(9.1.1.) <u>Lema</u>. Se a ação $G^* = (G, \phi, X)$ é transitiva então a ação de G sobre Π é transitiva. (G = grupo) .

Prova:

Seja $(B,B') \in \Pi \times \Pi$.

G^* transitiva $\Longrightarrow \forall (x,x') \in B \times B'$, $\exists\, g \in G \mid xg = x'$

$\therefore$ $Bg \subseteq B'$.

Logo a ação de G sobre Π é transitiva.

(9.1.2.) <u>Observações</u>:

i) Se G é um grupo com subgrupo H , então G age transitivamente sobre o conjunto de cossets à direita Hg de

H , por $(Hg)g' = Hgg'$.

Para qualquer $(Hg, Hg') \in G/H$ temos: $(Hg)(g^{-1} g') = Hg'$.

ii) $G_G^* = (G, \text{trans}, G) = G$ agindo sobre si mesmo, pela multiplicação à direita.

(9.1.3.) <u>Corolário</u>. Seja G um grupo com subgrupo H . Então G_G^* está homomórficamente imerso em

$H_H^* \text{ wr } \bar{G}^*_{\Pi}$, onde $\bar{G}^*$ é o constituinte de G agindo sobre Π , sendo $\Pi = G/H$.

Prova:

Verifiquemos que estão satisfeitas todas as condições exigidas pela proposição (9.1.).

— G_G^* é leal.

Sejam g' e $g'' \in G$. Se $gg' = gg''$, para todo $g \in G \Longrightarrow g = g'$.

— $\bar{G}^*$ é transitiva .

Sejam $(Hg , Hg') \in G/H$. Como G é grupo $\Longrightarrow g'' = g^{-1} g'$. Logo $(Hg)\, g'' = Hg'$.

_ Seja $Y = H$, que é um bloco de G^*_G. O subgrupo de G que fixa H como conjunto é H mesmo. Então $G_{(Y)} = H$. Portanto $G^*_{(Y)} = (H, \text{trans}, H) = H^*_H$, que é leal.

Logo, pela proposição (9.1.) $\Longrightarrow G^*_G$ está homomórficamente imerso em $H^*_H \text{ wr } \bar{G}^*$.

Notemos que o corolário acima emerge G em $H \text{ wr } \bar{G}^*$, que é o grupo "atrás" de $H^*_H \text{ wr } \bar{G}^*$.

Como $H \text{ wr } G^* = \left(H^{G/H}\right) \text{ sd } \bar{G}^*$, temos que G está imerso em $\left(H^{G/H}\right) \text{ sd } \bar{G}^*$.

Se H age sobre X, como $\left(H^{G/H}\right) \text{ sd } \bar{G}^*$ age sobre $X \times G/H$, então G age sobre $X \times G/H$.

(9.2.) <u>Proposição</u>. Seja G um grupo com subgrupo normal H. Então $(\bar{G})^* \cong (G/H)^*_{G/H}$ e portanto $\bar{G} \cong G/H$.

Para isto basta verificar que o morfismo abaixo definido é isomorfismo sobre, isto é, α e θ são bijeções:

$$(\alpha, \theta) : \bar{G}^* \longrightarrow (G/H)^*_{G/H} \quad , \text{ tal que :}$$

i) $\theta = id_{G/H} \Longrightarrow \theta$ é bijeção.

ii) $\alpha : \bar{G} \longrightarrow G/H$, $\bar{G} \subseteq$ Trans G/H , tal que :

$\bar{g}\alpha = Hg$, sendo que $(Ha)\bar{g} = Hag$.

_ α está bem definida.

Se $a, f, g \in G$ e $\bar{f} = \bar{g}$, então $Ha\bar{f} = Ha\bar{g}$, isto é, $Haf = Hag$. Se $a=1 \Longrightarrow Hf = Hg$. Portanto $\bar{f}\alpha = \bar{g}\alpha$.

_ α é injetiva.

Sejam $\bar{f}$ e $\bar{g} \in \bar{G}$.

Se $\bar{f}\alpha = \bar{g}\alpha \Longrightarrow Hf = Hg \Longrightarrow gf^{-1} \in H$.

Seja $a \in G$. Como $H \triangle G$, $\left(a\,(gf^{-1})\,a^{-1}\right) \in H$.

Então $Ha\,g\,f^{-1}\,a^{-1} = H \Longrightarrow Hag = Haf \Longrightarrow \bar{g} = \bar{f}$.

_ α é sobre.

Seja $Hg \in G/H$. Para todo $g \in G$, $\exists\ \bar{g} \in \bar{G} \subseteq$ Trans G/H.
Portanto α é sobre.

_ α é homomorfismo.

$(\bar{g} \circ \bar{h})\alpha = \overline{g\,h}\alpha = H\,g\,h$.

$$(\bar{g}\alpha) \cdot (\bar{h}\alpha) = Hg \cdot Hh = Hgh$$

_ O diagrama abaixo comuta:

$$\begin{tikzcd} G/H \arrow[r, "\bar{g}"] \arrow[d, "\theta"'] & G/H \arrow[d, "\theta"] \\ G/H \arrow[r, "\bar{g}\alpha"'] & G/H \end{tikzcd}$$

$$(Ha)\bar{g}\,\theta = Hag = Ha \cdot Hg = (Ha\,\theta) \cdot (\bar{g}\alpha) .$$

Logo (α, θ) é isomorfismo sobre $\Longrightarrow (\bar{G})^* \cong (G/H)^*_{G/H}$.

(9.2.1.) <u>Corolário</u>. Seja G um grupo com subgrupo normal H . Então G é isomorfo a um subgrupo do produto "wreath" clássico H wr $(G/H)^*_{G/H} = H^{G/H}$ sd $(G/H)^*_{G/H}$.

Pelo corolário (9.1.3.) e pela proposição anterior

$\Longrightarrow G^*_G$ está homomorficamente imerso em H^*_H wr $(G/H)^*_{G/H} \Longrightarrow$

$\Longrightarrow$ G é isomorfo a algum subgrupo do produto "wreath"

$$H \text{ wr } (G/H)^*_{G/H} = H^{G/H} \text{ sd } (G/H)^*_{G/H} .$$

(9.2.2.) Observações:

i) Um grupo G é uma extensão de H por B se existe uma sequência exata $1 \to H \to G \to B \to 1$. Isto significa que há um monomorfismo de H em G e um epimorfismo de G sobre B , tal que a imagem do monomorfismo é exatamente o Kernel do epimorfismo.

O corolário anterior afirma que toda extensão G de H por B está imersa no produto "wreath" de H por B , isto é,

$$G \hookrightarrow H \text{ wr } (B_B)^* = H^B \text{ sd } (B_B)^* \quad , \text{ pois } \quad (B_B)^* \cong (G/H)^*_{G/H} .$$

ii) Seja G um grupo finito. Sabemos que existe uma sequência , não necessáriamente única, de subgrupo de G , $1 = N_o$, N_1 , N_2 , ... , $N_k = G$, com a propriedade que para $i = 0,1,\ldots, k-1$, N_i é um subgrupo normal de N_{i+1} e N_{i+1}/N_i é simples (não tem subgrupos normais não triviais). Além disso, o número de grupos simples, de um dado tipo de isomorfismo , é únicamente determinado. Esta sequência é chamada uma série de composição para G .

Então G é uma extensão de N_{k-1} por N_k / N_{k-1} ,

N_{k-1} é uma extensão de N_{k-2} por N_{k-1} / N_{k-2} e , em geral , N_i é uma extensão de N_{i-1} por N_i / N_{i-1} para $i = 1,2,3,\ldots, k$.

O teorema de Kaloujnine - Krasner segue-se do corolário (9.2.1.) por indução.

(9.3.) <u>Teorema de Kaloujnine - Krasner</u>

Um grupo finito pode ser imerso em um produto "wreath" clássico de grupo .simples.

Prova:

Seja $N_k = G \trianglerighteq N_{k-1} \trianglerighteq N_{k-2} \trianglerighteq N_{k-3} \trianglerighteq \ldots \trianglerighteq \{1\}$.

$$0 \longrightarrow N_{k-1} \longrightarrow G \longrightarrow N_k / N_{k-1} \longrightarrow 0$$

Pelo corolário anterior (9.2.1.) G está imerso em

$$N_{k-1} \text{ wr } \left(N_k \middle| N_{k-1} \right)^{*}_{N_k | N_{k-1}} .$$

Se $0 \longrightarrow N_{k-2} \longrightarrow N_{k-1} \longrightarrow N_{k-1} \big/ N_{k-2} \longrightarrow 0$, então :

N_{k-1} está imerso em N_{k-2} wr $\left(N_{k-1}\big|_{N_{k-2}}\right)^{*}_{N_{k-1}/N_{k-2}}$.

Então G está imerso em N_{k-1} wr $\left(N_k/_{N_{k-1}}\right)^{*}_{N_k/N_{k-1}}$

e N_{k-1} wr $\left(N_k/_{N_{k-1}}\right)^{*}_{N_k/N_{k-1}}$ está imerso em

$$\left(N_{k-2} \text{ wr } \left(N_{k-1}/_{N_{k-2}}\right)^{*}_{N_{k-1}/N_{k-2}}\right) \text{ wr } \left(N_k/_{N_{k-1}}\right)_{N_k/N_{k-1}} ,$$

pois se S_1 , S_2 , S_3 são conjuntos, S_3^* é ação, então

$$S_1 \text{ wr } S_3^* \subseteq S_2 \text{ wr } S_3^* .$$

Então se $N_{k-1} \subseteq N_{k-3}$ wr $\left(N_{k-2}\big|_{N_{k-3}}\right) \Longrightarrow$

$$N_{k-2} \text{ wr } \left(N_{k-1}\big|_{N_{k-2}}\right)^{*} \subseteq \left(N_{k-3} \text{ wr } \left(N_{k-2}/_{N_{k-1}}\right)^{*}\right) \text{ wr } \left(N_{k-1}/_{N_{k-2}}\right)^{*} . \therefore$$

$$\therefore \left(N_{k-2} \text{ wr } \left(N_{k-1} \Big/ N_{k-2} \right)^{*} \right) \text{ wr } \left(N_k \Big/ N_{k-1} \right)^{*} \subseteq$$

$$\subseteq \left(\left(N_{k-3} \text{ wr } N_{k-2} \Big/ N_{k-1} \right) \text{ wr } \left(N_{k-1} \Big/ N_{k-2} \right)^{*} \right) \text{ wr } \left(N_k \Big/ N_{k-1} \right)^{*} .$$

Continua-se o processo por indução.

<u>Exemplo</u>: Consideremos o grupo dos quatérnios Q, que tem 8 elementos e geradores $i, j, k,$ tal que $ij = k$, $jk = i$, $ki = j$, $i^2 = j^2 = k^2$.

Sabemos que $\{1\} \trianglelefteq \{1,-1\} \trianglelefteq \{1,-1,i,-i\} \trianglelefteq Q$.

Seja $N_o = \{1\}$, $N_1 = \{1,-1\}$, $N_2 = \{1,-1,i,-i\}$ e $N_3 = Q$.

Então: $N_3 / N_2 \cong \mathbb{Z}_2$, $N_2 / N_1 \cong \mathbb{Z}_2$, $N_o / N_1 \cong \mathbb{Z}_2$.

$N_3 / N_2 = \{1N_2 , jN_2\} \cong \mathbb{Z}_2$.

$N_2 / N_1 \cong \mathbb{Z}_2$ e $N_o / N_1 \cong \mathbb{Z}_2$.

$N_o \text{ wr } \mathbb{Z}_2 \cong \mathbb{Z}_2$.

Logo $Q \hookrightarrow \left(\mathbb{Z}_2 \text{ wr } \mathbb{Z}_2^{*}{}_{\mathbb{Z}_2} \right) \text{ wr } \mathbb{Z}_2^{*}{}_{\mathbb{Z}_2} = \tilde{G}$

$$\mathbb{Z}_2 \text{ wr } \mathbb{Z}_{2\,\mathbb{Z}_2}^{*} = \mathbb{Z}_2^{\mathbb{Z}_2} \text{ sd } \mathbb{Z}_2,$$ de ordem 8.

portanto $\tilde{G} = \left(\mathbb{Z}_2^{\mathbb{Z}^2} \text{ sd } \mathbb{Z}_2\right) \text{ sd } \mathbb{Z}_2$ e tem, portanto, ordem 128.

(9.3.1.) <u>Corolário</u>. Conhecendo-se o produto "wreath" e os grupos simples estarão conhecidos todos o grupos finitos.

B I B L I O G R A F I A

[1] DEAN, R.A.,Elementos de álgebra abstrata, Livros Técnicos e Científicos Editora S.A. (1971).

[2] GINZBURG, A., Algebraic Theory of Automata, Academic Press, New York, (1968).

[3] HERSTEIN, I.M., Tópicos de Álgebra, Editora da Universidade de São Paulo (1970).

[4] NEUMANM, B.H., Embedding theorems for semigroups, J. London Math. Soc., 34(1959).

[5] NEUMANM, P., On the structure of the standard wreath products of groups, Math. Z.,,84(1964).

[6] PETRICH, M., Introduction to Semigroups, Columbus, Ohio, (1973).

[7] WELLS, CHARLES; Some applications of the wreath product construction, The American Math. Monthly, 83(1975).