Grupos e Corpos

Prof. Lucas Calixto

Aula 3 - Teoremas de: Lagrange, Euler, Fermat, Cayley; Produtos diretos de grupos

Classes laterais

Fixe $H \leq G$

Se $g \in G$, definimos a classe lateral à esquerda de H associada a g como sendo

$$gH = \{gh \mid h \in H\}$$

A classe lateral à direita de H associada a g é

$$Hg = \{hg \mid h \in H\}$$

Note: se G é abeliano, as classes laterias à esquerda e à direita coincidem

Exemplo: As classes laterais de $\{0, 3\} = H \leq \mathbb{Z}_6$ são

$$0 + H = \{0, 3\} = 3 + H$$
$$1 + H = \{1, 4\} = 4 + H$$
$$2 + H = \{2, 5\} = 5 + H$$

Exemplo: Seja $S_3 = \{(1), (123), (132), (12), (13), (23)\}$ e $H = \{(1), (123), (132)\}$

As classes laterais à esquerda e à direita de H coincidem

$$(1)H = H(1) = (123)H = H(123) = (132)H = H(132) = H$$
$$(12)H = H(12) = (13)H = H(13) = (23)H = H(23) = \{(12), (13), (23)\}$$

Isso não vale para $K = \{(1), (12)\} \leq S_3$, já que, por exemplo

$$(23)K = \{(23), (132)\} \neq K(23) = \{(23), (123)\}$$

Lema: Se $H \leq G$ e $g_1, g_2 \in G$, então as condições a seguir são equivalentes

1. $g_1 H = g_2 H$
2. $H g_1^{-1} = H g_2^{-1}$
3. $g_1 H \subset g_2 H$
4. $g_1 \in g_2 H$
5. $g_1 H \cap g_2 H \neq \emptyset$
6. $g_1^{-1} g_2 \in H$

Observe: em todos os exemplos as classes laterais gH (ou Hg) particionam G, ou seja decompoem G em subconjuntos disjuntos

Teorema: Se $G \leq H$, então $G = \dot{\bigcup}_{g \in G} gH$ ($\dot{\bigcup}$ = união disjunta)

Prova: É obvio que $G = \bigcup_{g \in G} gH$ ($g = ge \in gH$)

Como $g_1H \cap g_2H \neq \emptyset \Rightarrow g_1H = g_2H$. Logo,

$$\bigcup_{g \in G} gH = \dot{\bigcup}_{g \in G} gH$$

■

Obs: O mesmo resultado vale para classes laterais à direita

Defina: O índice de H em G como sendo $[G : H] = |\{gH \mid g \in G\}|$

Proposição: $|\{gH \mid g \in G\}| = |\{Hg \mid g \in G\}|$

Prova: Defina $\phi : \{gH \mid g \in G\} \to \{Hg \mid g \in G\}$ tal que $\phi(gH) = Hg^{-1}$

ϕ é bem definida

$$g_1H = g_2H \Rightarrow Hg_1^{-1} = Hg_2^{-1} \Rightarrow \phi(g_1H) = \phi(g_2H)$$

ϕ é bijeção com inversa $\psi : \{Hg \mid g \in G\} \to \{gH \mid g \in G\}$, $\psi(Hg) = g^{-1}H$ ■

Proposição: $|H| = |gH|$

Prova: Defina $\phi : H \to gH$ tal que $\phi(h) = gh$

ϕ é bijeção com inversa $\psi : Hg \to H$, $\psi(hg) = h$ ■

Teorema (Lagrange): Se G é grupo finito, e $H \leq G$, então $|G| = [G : H]|H|$

Prova: Sejam $g_1H, \ldots, g_{[G:H]}H$ as classes laterais distintas de G (por definição de índice, temos exatamente $[G : H]$ dessas). Então

$$G = \dot{\bigcup}_{i=1}^{[G:H]} g_iH \Rightarrow |G| = \sum_{i=1}^{[G:H]} |g_iH| = [G : H]|H| \qquad \blacksquare$$

Corolário: Se $g \in G$, então $|g|$ divide $|G|$

Corolário: Se $|G| = p$ com p primo, então $G = \langle g \rangle$ para qualquer $g \neq e$. Em particular, G é cíclico

Corolário: Se $K \leq H \leq G$, então $[G : K] = [G : H][H : K]$

Prova: Sabemos $|G| = [G : H]|H|$, $|H| = [H : K]|K|$ e $|G| = [G : K]|K|$. Logo

$$[G : H][H : K] = \frac{|G|}{|H|}\frac{|H|}{|K|} = \frac{|G|}{|K|} = [G : K] \qquad \blacksquare$$

$H \leq G \Rightarrow |H|$ divide $|G|$

Pergunta: se n divide $|G| \Rightarrow$ existe $H \leq G$ tal que $|H| = n$?

Proposição: A_4 não possui grupo com ordem 6

Prova: Suponha que tal H existe

$[G : H] = 2 \Rightarrow$ existem somente duas classes laterais distintas H e gH (qualquer $g \notin H$ funciona)

$g \notin H \Rightarrow gH = Hg \Rightarrow gHg^{-1} = H$

Sabemos que existem 8 3-ciclos em $A_4 \Rightarrow H$ contém um 3-ciclo

Assuma $(123) \in H$ (poderia ser qualquer outro) $\Rightarrow (123)^{-1} = (132) \in H$

Como $ghg^{-1} \in H$ para todo $h \in H$, temos que

$$(124)(123)(124)^{-1} = (124)(123)(142) = (243)$$
$$(243)(123)(243)^{-1} = (243)(123)(234) = (142)$$

pertencem a H

Logo, todos os elementos

$$(1), (123), (123)^{-1} = (132), (243), (243)^{-1} = (234), (142), (142)^{-1} = (124)$$

pertencem a $H \Rightarrow |H| \geq 7$ Contradição ■

Note: No exemplo anterior, a partir de (123), construimos todos os outros 3-cilos de S_4. Isso, não foi por acaso!

Proposição: Dois cíclos $\tau, \mu \in S_n$ tem o mesmo comprimento se e só se eles são conjugados por algum elemento de S_n, ou seja, existe $g \in S_n$ tal que $\mu = g\tau g^{-1}$

Prova: ($\Rightarrow$) Escreva

$$\tau = (a_1 \cdots a_k)$$
$$\mu = (b_1 \cdots b_k)$$

Defina $g \in S_n$ tal que $g(a_i) = b_i$ para todo i, e defina $g(x)$ de qualquer forma de modo que g seja bijeção

- $g\tau g^{-1}(b_i) = g\tau(a_i) = g(a_{i+1}) = b_{i+1} = \mu(b_i)$
- $x \neq b_i \ \forall i \Rightarrow g^{-1}(x) \neq a_i \ \forall i \Rightarrow g\tau g^{-1}(x) = gg^{-1}(x) = x = \mu(x)$

($\Leftarrow$) Escreva $\tau = (a_1 \cdots a_k)$, e tome $g \in S_n$ qualquer

Afirmação: $g\tau g^{-1} = (g(a_1) \cdots g(a_k))$

- $g\tau g^{-1}(g(a_i)) = g\tau(a_i) = g(a_{i+1})$
- $x \neq g(a_i) \ \forall i \Rightarrow g^{-1}(x) \neq a_i \ \forall i \Rightarrow g\tau g^{-1}(x) = gg^{-1}(x) = x$ ■

Teoremas de Fermat e de Euler

Definição: A função ϕ de Euler é a função $\phi : \mathbb{N} \to \mathbb{N}$ tal que $\phi(1) = 1$ e $\phi(n) = |\{1 \leq k < n \mid mdc(k, n) = 1|$

Lembrem: na Aula 1 provamos que $U(n) = \{a \in \mathbb{Z}_n \mid mdc(a, n) = 1\}$ junto com a multiplicação é grupo abeliano

Observe: O grupo $U(n)$ tem ordem $\phi(n)$

Teorema (Euler): Se $a \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(a, n) = 1$, então $a^{\phi(n)} = 1 \ (mod\ n)$

Prova: Se $b \in \mathbb{Z}_n$ é um representante de a (i.e. $b \ (mod\ n) = a \ (mod\ n)$), então $b^{\phi(n)} = 1 \ (mod\ n)$ (pois nesse caso $b \in U(n)$ e portanto $|b|$ divide $|U(n)|$). Logo $a^{\phi(n)} = 1 \ (mod\ n)$

Pequeno Teorema de Fermat: Se $a \in \mathbb{Z}$, $p \in \mathbb{N}$ é primo e $p \nmid a$, então $a^{p-1} = 1 \ (mod\ p)$

Prova: $mdc(a, p) = 1 \Rightarrow a^{\phi(p)=p-1} = 1 \ (mod\ p)$

Isomorfismos

Definição: Dois grupos $(G, \cdot)$ e $(H, \circ)$ são isomorfos se existe uma bijeção $\phi : G \to H$ que preserva a operação dos grupos, isto é

$$\phi(a \cdot b) = \phi(a) \circ \phi(b), \quad \forall\ a, b \in G$$

A função ϕ é chamada isomorfismo e denotamos $G \cong H$

Usando isomorfismos, podemos pensar em vários grupos aditivos como grupos multiplicativos e vice-versa

Exemplo: $\mathbb{Z}_4 \cong \langle i \rangle = \{\pm 1, \pm i\} \leq \mathbb{C}^*$. De fato, $\phi : \mathbb{Z}_4 \to \langle i \rangle$, $\phi(k) = i^k$ é isomorfismo pois é bijeção e

$$\phi(m + n) = i^{m+n} = i^m i^n = \phi(m)\phi(n)$$

Exemplo: Cálculo 1 $\Rightarrow exp : \mathbb{R} \to \mathbb{R}^+$, $\exp(x) = e^x$ define uma bijeção

Identifique os conjuntos $\mathbb{R}^+$ e $\{e^x \mid x \in \mathbb{R}\}$ usando exp

$(\mathbb{R}^+, \cdot)$, onde $e^x e^y = e^{x+y}$ (produto usual) é um grupo abeliano (cheque!)

$\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y) \Rightarrow$ exp é iso $\Rightarrow (\mathbb{R}, +) \cong (R^+, \cdot)$

Exemplo: Vimos que $H = \{2^n \mid n \in \mathbb{Z}\} \subset \mathbb{Q}^*$ é subgrupo

A função $\phi : \mathbb{Z} \to H$, $\phi(n) = 2^n$ é claramente bijeção. Além disso,

$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n) \Rightarrow \mathbb{Z} \cong H$

Existir uma bijeção entre dois grupos não é suficiente para que esses grupos sejam isomorfos

Exemplo: $|S_3| = \mathbb{Z}_6 \Rightarrow \exists$ bijeção entre os grupos. Contudo, $S_3 \ncong \mathbb{Z}_6$

Um dos problemas aqui é que $\mathbb{Z}_6$ é abeliano e S_3 não é abeliano

Se existe $\phi : \mathbb{Z}_6 \to S_3$ um iso, então todo $a \in S_3$ é dá forma $\phi(m_a)$ para algum $m_a \in \mathbb{Z}$. Logo, para todo $a, b \in S_3$ temos

$$ab = \phi(m_a)\phi(m_b) = \phi(m_a + m_b) = \phi(m_b + m_a) = \phi(m_b)\phi(m_a) = ba$$

Isso impica S_3 abeliano Contradição

Proposição Se $\phi : G \to H$ é iso de grupos, então

1. $\phi^{-1} : H \to G$ é iso
2. $|G| = |H|$
3. G é abeliano $\Rightarrow$ H é abeliano
4. G é cíclico $\Rightarrow$ H é cíclico

Prova: (1): Obviamente ϕ^{-1} é bijeção. Além disso,

$$\begin{aligned}\phi^{-1}(h_1h_2) &= \phi^{-1}(\phi(\phi^{-1}(h_1))\phi(\phi^{-1}(h_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(h_1)\phi^{-1}(h_2))) \\ &= \phi^{-1}(h_1)\phi^{-1}(h_2)\end{aligned}$$

(2) Óbvia

(3) Exercício

(4) $G = \langle g \rangle \Rightarrow H = \langle h = \phi(g) \rangle$, pois se $a \in H$ temos

$$a = \phi(g^n) = \phi(g)^n = h^n$$

■

Caracterização de grupos cíclicos

Teorema: Se G é cíclico e $|G| = \infty$, então $G \cong \mathbb{Z}$

Prova: Suponha $G = \langle g \rangle$ e defina $\phi : \mathbb{Z} \to G$, $\phi(n) = g^n$.

Afirmação: ϕ é iso

- sobrejetividade: se $h \in G$, então $h = g^n = \phi(n)$
- injetividade: suponha $m \neq n$

$$\phi(m) = \phi(n) \Leftrightarrow g^m = g^n \Leftrightarrow g^{n-m} = e \Rightarrow |G| = |g| < \infty$$

- $\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$ ■

Teorema (Exercício): Se G é cíclico e $|G| = n$, então $G \cong \mathbb{Z}_n$

Corolário: Se G é arbitrário e $|G| = p$ com p primo, então $G \cong \mathbb{Z}_p$

Prova: Vimos que $|G| = p$ implica G cíclico

Teorema de Cayley

Note: Se G é grupo e $g \in G$, então $\lambda_g : G \to G$, $\lambda_g(h) = gh$ é permutação de G

$\overline{G} = \{\lambda_g \mid g \in G\} \subset S_G$ é subgrupo de S_G

- $\lambda_e = id$
- $\lambda_g^{-1} = \lambda_{g^{-1}}$
- $\lambda_g \lambda_h = \lambda_{gh}$

Teorema (Cayley): A função $\lambda : G \to \overline{G}$, $\lambda(g) = \lambda_g$ é isomorfismo

Prova:

- λ é bijetora, pois $\alpha(\lambda_g) = g$ é a inversa de λ
- $\lambda(gh) = \lambda_{gh} = \lambda_g \lambda_h = \lambda(g)\lambda(h)$ ■

Produtos de grupos

Suponha $(G, \cdot)$ e $(H, \circ)$ grupos

O conjunto $G \times H$ munido do produto

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$$

é um grupo (cheque!)

O grupo $G \times H$ é o produto direto externo de G e H

A mesma construção pode ser aplicada para n grupos: $\prod G_i = G_1 \times \cdots \times G_n$

Se $G_1 = \ldots = G_n = G$, denotamos $G_1 \times \cdots \times G_n$ por G^n

Exemplo: $(\mathbb{R}^2, +)$ onde

$$(a, b) + (c, d) = (a + c, b + d)$$

é um grupo. Note: o grupo $\mathbb{R}^2$ é simplesmente $\mathbb{R} \times \mathbb{R}$

Exemplo: Os grupos $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_4$ não são isomorfos

Se $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ fosse um tal isomorfismo, então $\phi(1)$ deveria ter ordem 4 (isomorfismos preservam ordem de grupos, e ordem de elementos)

Todos elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ tem ordem 1 ou 2

Exemplo: O grupo $\mathbb{Z}_2^n$ é muito importante em ciência da computação

Óbvio que $|G \times H| = |G||H|$

Teorema: Se $g \in G$ tem ordem r, $h \in H$ tem ordem $s \Rightarrow |(g,h)| = mmc(r,s)$

Prova: Seja $m = mmc(r,s)$ e $n = |(g,h)|$

$$(g,h)^m = (g^m, h^m) = (e_G, e_H) \Rightarrow n \text{ divide } m \Rightarrow n \leq m$$

$(e_G, e_H) = (g,h)^n = (g^n, h^n) \Rightarrow r$ divide n e s divide $n \Rightarrow n$ é múltiplo de r e de $s \Rightarrow n \geq m$

Logo, $m = n$ ■

Corolário: Se $g_i \in G_i$ tem ordem $r_i \Rightarrow (g_1, \ldots, g_n) \in \prod G_i$ tem ordem $mmc(r_1, \ldots, r_n)$

Exemplo: Tome $(8, 56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$. Sabemos que

$|8| = 12/mdc(8, 12) = 12/4 = 3$ (lembrem: $8 = 8 \cdot 1$ (ou 1^8) e $|1| = 12$ em $\mathbb{Z}_{12}$)

$|56| = 60/mdc(56, 60) = 60/4 = 15$

Logo, $|(8, 56)| = mmc(3, 15) = 15$

Exemplo: Diferente do exemplo do slide anterior, temos $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

Afirmamos que $\mathbb{Z}_2 \times \mathbb{Z}_3$ é cíclico (logo o resultado segue, pois $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$)

Prove $\mathbb{Z}_3 \times \mathbb{Z}_3 = \langle (1, 1) \rangle$

Teorema: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow mdc(m,n) = 1$

Prova: ($\Rightarrow$) Suponha $mdc(m,n) = d > 1$. Como $mn = mdc(m,n)mmc(m,n)$ (prove), temos $mn/d = mmc(m,n) \Rightarrow m$ divide mn/d e n divide mn/d

Logo, $(a,b)^{mn/d} = (a^{mn/d}, b^{mn/d}) = (0,0) \Rightarrow \nexists\ (a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ de ordem mn

Logo, $\mathbb{Z}_m \times \mathbb{Z}_n \ncong \mathbb{Z}_{mn}$

($\Leftarrow$) Como $mdc(m,n) = 1$ e $mn = mdc(m,n)mmc(m,n)$, temos que

$$|(1,1)| = mmc(m,n) = mn$$

Portanto $\langle (1,1) \rangle = \mathbb{Z}_m \times \mathbb{Z}_n \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ é cíclico de ordem mn

Assim, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ ■

Corolário: $\Pi_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k} \Leftrightarrow mdc(n_i, n_j) = 1\ \forall i \neq j$. Em particular, se $m = p_1^{r_1} \cdots p_k^{r_k}$ com p_i primo e $p_i \neq p_j$, então

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

Produto direto interno

Pergunta: Quando um grupo pode ser escrito como produto direto de alguns de seus subgrupos próprios?

Exemplo: Note que $H = \{(x, 0) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ e $K = \{(0, y) \in \mathbb{R}^2 \mid y \in \mathbb{R}\}$ são subgrupos próprios de $\mathbb{R}^2$, e além disso $HK = \{hk \mid j \in H,\ k \in K\} = \mathbb{R}^2$

Definição: G é o produto direto interno de subgrupos $H, K \leq G$ se valem:

- $G = HK = \{hk \mid h \in H,\ k \in K\}$
- $H \cap H = \{e\}$
- $hk = kh$ para todo $h \in H$, $k \in K$

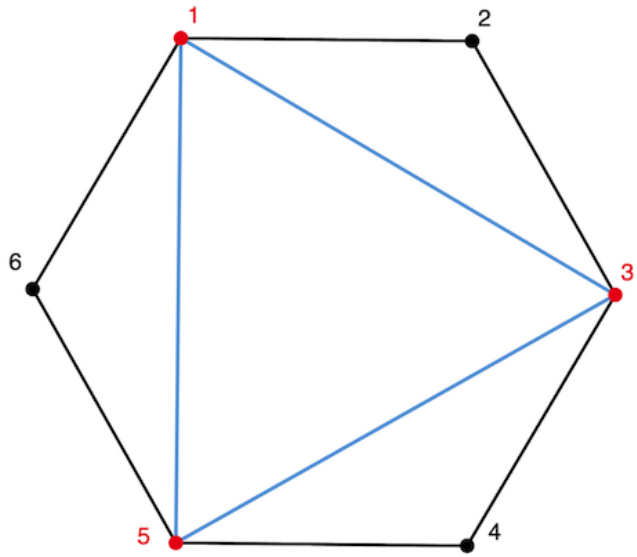
Exemplo: $U(8) = \{1, 3, 5, 7\} \subset \mathbb{Z}_8$ é o produto direto interno de

$$H = \{1, 3\} \quad \text{e} \quad K = \{1, 5\}$$

Exemplo: $D_6 = \{id, r, \ldots, r^5, s, rs, \ldots, r^5 s\}$ é o produto direto interno de

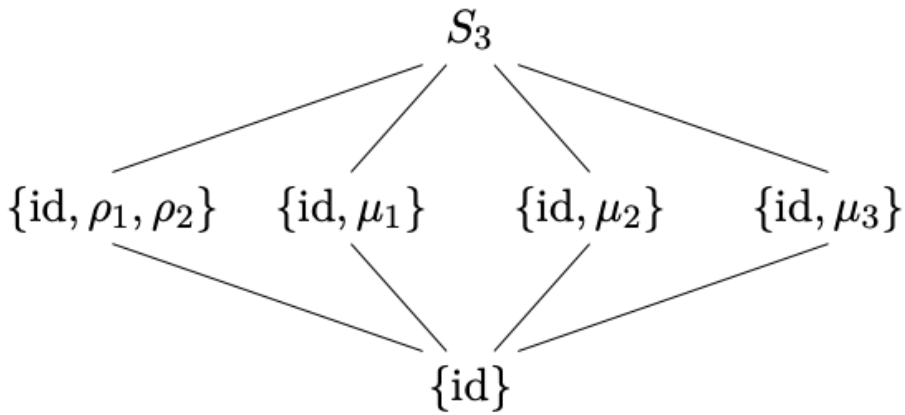
$$H = \{id, r^3\} \quad \text{e} \quad K = \{id, r^2, r^4, s, r^2 s, r^4 s\}$$

Além disso, $H \cong S_2 \cong \mathbb{Z}_2$ e $K \cong S_3$ (permutações dos vértices 1,3,5 do poligono de 6 lados)



Note: nem todo grupo é o produto direto interno de subgrupos próprios

Exemplo: S_3 (lembrem: S_3 = simetrias do triângulo equilátero) não é o produto direto de subgrupos próprios



- $S_3 = HK$ e $H \cap K = \{e\} \Rightarrow |H| = 3,\ |K| = 2 \Rightarrow H = \{id, \rho_1, \rho_2\}$

Como $\nexists\ \mu_i$ que comuta com todos $\rho_j \Rightarrow$ tal subgrupo K não existe

Teorema: Se G é produto direto interno de $H, K \leq G$, então $G \cong H \times K$

Prova: Defina $\phi : H \times K \to G$, $\phi(h, k) = hk$

Afirmação: ϕ e iso

- $G = HK \Rightarrow \phi$ é sobrejetiva
- $H \cap K = \{e\} \Rightarrow \phi$ é injetiva:

$$g = h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\} \Rightarrow h_1 = h_2,\ k_1 = k_2$$

Logo, ϕ é bijeção

- Como $hk = kh\ \forall\ h \in H,\ k \in K$, temos

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2k_2)$$

Logo, ϕ é iso ■

Exemplos: • $\mathbb{R}^2 \cong \mathbb{R} \times \mathbb{R}$

• $U(8) \cong H \times K$, onde $H = \{1, 3\},\ K = \{1, 5\} \leq U(8)$

• $D_6 \cong \mathbb{Z}_2 \times S_3$

G é o produto direto interno de subgrupos $H_1, \ldots, H_n \leq G$ se valem:

• $G = \prod H_i = \{h_1 \cdots h_n \mid h_i \in H_i\}$

• $h_i h_j = h_j h_i$ para todos $h_i \in H_i$, $h_j \in H_j$ e $i \neq j$

• $H_i \cap \prod_{j \neq j} H_j = \{e\}$

Teorema: Se G é o produto direto interno de $H_1, \ldots, H_n$, então $G \cong \prod H_i$