Grupos e Corpos

Prof. Lucas Calixto

Aula 4 - Subgrupos normais; grupos quocientes; homomorfismos; teoremas de isomorfismo

Subgrupos normais e grupos quocientes

Definição: Um subgrupo $N \leq G$ é normal se $gN = Ng \ \forall g \in G$, ou seja, N é normal se as classes laterais à esquerda à direita coincidem

Notação: Se $N \leq G$ é normal, escrevemos $N \lhd G$

Exemplo: G abeliano $\Rightarrow$ todo subgrupo é normal

Exemplo: Em S_3, $H = \{(1), (12)\}$ não é normal: se $g = (123)$

$$gH = \{g, (13)\}, \quad Hg = \{g, (23)\} \Rightarrow gH \neq Hg$$

Por outro lado, $N = \{(1), (123), (132)\}$ é normal:

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

Verifique os casos restantes e que N, $(12)N$ são as únicas classes laterais distintas

Teorema: Se $N \leq G$, então são equivalentes

1. $N \lhd G$
2. $gNg^{-1} \subset N, \ \forall g \in G$
3. $gNg^{-1} = N, \ \forall g \in G$

Prova: (1) $\Rightarrow$ (2) $\forall g \in G$, temos

$$gN = Ng \Rightarrow \forall n \in N, \ \exists \ n' \in N \text{ tal que } gn = n'g \Rightarrow gng^{-1} = n' \Rightarrow gNg^{-1} \subset N$$

(2) $\Rightarrow$ (3) $\forall n \in N, \forall g \in G$, escreva $g^{-1} = k$. Assim

$$n = g(g^{-1}ng)g^{-1} = g(knk^{-1})g^{-1} \in gNg^{-1} \Rightarrow N \subset gNg^{-1} \Rightarrow N = gNg^{-1}$$

(3) $\Rightarrow$ (1) $\forall g \in G$, temos

$$gNg^{-1} = N \Rightarrow gN = Ng \Rightarrow N \lhd G$$

$\blacksquare$

Grupos quocientes

Teorema: Se $N \lhd G$, então $G/N := \{gN \mid g \in G\}$ é um grupo, onde

$$(gN)(g'N) = gg'N, \ \forall g, g' \in G$$

Prova:

- Esse produto é bem definido:

Se $aN = a'N$ e $bN = b'N$, então existem $n_a, n_b \in N$ tais que $a = a'n_a$ e $b = b'n_b$

$$(aN)(bN) = abN = a'n_ab'n_bN = a'n_ab'N = a'n_aNb' = a'Nb' = a'b'N = (a'N)(b'N)$$

- associatividade segue da associatividade do produto de G
- eN é o elemento identidade
- se $gN \in G/N$, então $(gN)^{-1} = g^{-1}N$ ■

Note: $|G/N| = [G : N]$ e $|G| = |N|[G : N]$. Logo,

$$|G/N| = [G : N] = |G|/|N|$$

Exemplo: Vimos que $N = \{(1), (123), (132)\} \lhd S_3$, e que $G/N = \{N, (12)N\}$. Logo $G/N \cong \mathbb{Z}_2$

Exemplo: $3\mathbb{Z} \lhd \mathbb{Z}$, e se $n \in \mathbb{Z} \Rightarrow n = 3q + r$ com $0 \leq r < 3$. Logo

$$n + 3\mathbb{Z} = (r + 3q) + 3\mathbb{Z} = r + 3\mathbb{Z} \Rightarrow \mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

Exercício: Use o mesmo argumento para ver que $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \mid 0 \leq r < n\}$

Exemplo: Vimos que $D_n = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$ é gerado por r (rotação de $\frac{2\pi}{n}$) e s (reflexão que fixa o vértice 1), onde $r^n = id$, $s^2 = id$ e $srs = r^{-1}$

- $R_n = \langle r \rangle$ é subgrupo cíclico de D_n

- $srs^{-1} = srs = r^{-1} \in R_n \Rightarrow sr^k s^{-1} = (srs^{-1})^k = r^{-k} \in R_n \Rightarrow sR_n s^{-1} \subset R_n$

Logo, $r^k s R_n (r^k s)^{-1} = r^k s R_n s^{-1} r^{-k} \subset r^k R_n r^{-k} = R_n \Rightarrow R_n \lhd D_n$

Note: $k > 0 \Rightarrow r^k s = sr^{-k} \Rightarrow r^k s R_n = sr^{-k} R_n = sR_n \Rightarrow D_n/R_n = \{s, sR_n\} \cong \mathbb{Z}_2$

Obs: Nos exemplos anteriores, todos os subgrupos normais tem índice 2

Exercício: Prove que se $N \leq G$ e $[G : N] = 2$, então $N \lhd G$

Note: Exercício anterior $\Rightarrow A_n \lhd S_n$

$S_n/A_n = \{A_n, \sigma A_n \mid \sigma \in S_n$ é qualquer transposição$\} \cong \mathbb{Z}_2$

$$\begin{array}{c|cc} \cdot & A_n & \sigma A_n \\ \hline A_n & A_n & \sigma A_n \\ \sigma A_n & \sigma A_n & A_n \end{array} \qquad \cong \qquad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

- A_n cuida dos produtos pares de transposições
- σA_n cuida dos produtos ímpares de transposições

Grupos simples e simplicidade de A_n

Um grupo G é simples se seus únicos subgrupos normais são $\{e\}$ e G

Exemplo: $\mathbb{Z}_p$ com p primo é simples (todo elemento $\neq e$ é um gerador de $\mathbb{Z}_p$)

Objetivo: Provar que A_n com $n \geq 5$ é simples

Lema 3.1: Se $n \geq 3$, então A_n é gerado por 3-ciclos

Prova: Como A_n é gerado por produtos de quantidades pares de transposições, basta mostrarmos que qualquer produtor de 2 transposições é um produto de 3-ciclos. Como $(ab) = (ba)$, tais produtos podem ser:

- (todas entradas coincidem) $(ab)(ab) = id = (abc)(acb)$
- (só uma entrada coincide) $(ab)(ac) = (acb)$
- (todas as entradas são diferentes) $(ab)(cd) = (acb)(acd)$ ∎

Lema 3.2: Se $n \geq 3$, $N \lhd A_n$ e N contem algum 3-ciclo, então $N = A_n$

Prova: Afirmação: todo 3-ciclo é produto de 3-ciclos da forma (ijk), onde $i, j \in \{1, \ldots, n\}$ estão fixos, e k varia em $\{1, \ldots, n\}$

- i, j aparecem: $(iaj) = (ija)^2$; $(jai) = (ija)$; $(aij) = (ija)$
- só i apare: $(iab) = (ijb)(ija)^2$; $(aib) = (iab)^2$; $(abi) = (aib)^2$
- só j apare: $(jab) = (ijb)^2(ija)$; $(ajb) = (jab)^2$; $(abj) = (ajb)^2$
- nem i nem j apare: $(abc) = (ija)^2(ijc)(ijb)^2(ija)$

Logo, a Afirmação segue do lema anterior

$\exists\ (ija) \in N$, e

$$N \lhd A_n \Rightarrow N \ni ((ij)(ak))\,(ija)^2\,((ij)(ak))^{-1} = (ijk),\ \forall k \in \{1, \ldots, n\}$$

Afirmação $\Rightarrow N$ contém todos os 3-ciclos $\Rightarrow N = A_n$, pelo Lema 3.1 ■

Lema 3.3: Se $n \geq 5$ e $N \lhd A_n$, então N contem um 3-ciclo

Prova: Seja $\sigma \in N$ e escreva σ como produto de ciclos disjuntos

Temos os seguintes casos:

σ é ciclo de comprimento 3 $\Rightarrow$ OK

Um dos ciclos tem comprimento > 3 $\Rightarrow \sigma = \tau(a_1 \cdots a_r)$, $r > 3$

Todos os ciclos tem comprimento 2 ou 3

mais de um tem comprimento 3 $\Rightarrow \sigma = \tau(a_1a_2a_3)(a_4a_5a_6)$

somente um tem comprimento 3 $\Rightarrow \sigma = \tau(a_1a_2a_3)$, onde τ é produto de transposições disjuntas

todos tem comprimento 2 $\Rightarrow \sigma = \tau(a_1a_2)(a_3a_4)$, onde τ é o produto de uma quantidade par de transposições disjuntas

Um dos ciclos tem comprimento > 3 $\Rightarrow \sigma = \tau(a_1 \cdots a_r)$, $r > 3$

$$(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \in N \Rightarrow \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \in N$$

Note

$$\begin{aligned}
\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} &= \sigma^{-1}(a_1a_2a_3)\sigma(a_3a_2a_1) \\
&= (a_r \cdots a_1)\tau^{-1}(a_1a_2a_3)\tau(a_1 \cdots a_r)(a_3a_2a_1) \\
&= (a_r \cdots a_1)(a_1a_2a_3)(a_1 \cdots a_r)(a_3a_2a_1) \\
&= (a_1a_3a_r) \in N \Rightarrow N \text{ contém um 3-ciclo}
\end{aligned}$$

Todos os ciclos tem comprimento 2 ou 3

mais de um tem comprimento 3 $\Rightarrow \sigma = \tau(a_1a_2a_3)(a_4a_5a_6)$

$$(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N \Rightarrow \sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N$$

Note

$$\begin{aligned}
\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} &= (a_6a_5a_4)(a_3a_2a_1)\tau^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6) \\
&= (a_6a_5a_4)(a_3a_2a_1)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6) \\
&= (a_1a_4a_2a_6a_3) \in N \Rightarrow \text{ de volta ao caso anterior}
\end{aligned}$$

somente um tem comprimento 3 $\Rightarrow \sigma = \tau(a_1a_2a_3)$, onde τ é produto de transposições disjuntas $(\Rightarrow \tau^{-1} = \tau)$

$$\sigma^2 = \tau(a_1a_2a_3)\tau(a_1a_2a_3) = (a_1a_2a_3)(a_1a_2a_3) = (a_1a_3a_2) \in N \Rightarrow OK$$

todos tem comprimento 2 $\Rightarrow \sigma = \tau(a_1a_2)(a_3a_4)$, onde τ é o produto de uma quantidade par de transposições disjuntas $(\Rightarrow \sigma^{-1} = \sigma)$

$$(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \in N \Rightarrow \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \in N$$

Note

$$\begin{aligned}\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} &= \tau(a_1a_2)(a_3a_4)(a_1a_2a_3)\tau(a_1a_2)(a_3a_4)(a_3a_2a_1)\\ &= (a_1a_3)(a_2a_4) \in N\end{aligned}$$

$n \geq 5 \Rightarrow \exists b \in \{1, \ldots, n\} \setminus \{a_1, a_2, a_3, a_4\}$. Se $\mu = (a_1a_3b)$, então

$$\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) \in N$$

$$\Rightarrow \mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) = (ba_3a_1)(a_1a_3)(a_1a_3b)(a_1a_3) = (a_1a_3b) \in N$$

$\Rightarrow N$ contém um 3-ciclo ■

Simplicidade de A_n para $n \geq 5$

Teorema: Se $n \geq 5$, então A_n é simples

Prova: Suponha $n \geq 5$ e $N \lhd A_n$

Lema 3.3 $\Rightarrow N$ contém um 3-ciclo

Lema 3.2 $\Rightarrow N = A_n \Rightarrow A_n$ é simples ■

Homomorfismos

Um homomorfismo entre $(G, \cdot)$ e $(H, \circ)$ é uma função $\phi : G \to H$ tal que

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2),\ \forall g_1, g_2 \in G$$

Note: Um isomorfismo é um homomorfismo bijetor

Exemplo: Se $g \in G$, então $\phi : \mathbb{Z} \to G$, $\phi(n) = g^n$ é homomorfismo:

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

Note: $\operatorname{im}\phi = \phi(\mathbb{Z}) = \langle g \rangle \leq G$

Exemplo: $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ é homomorfismo:

$$\det(gh) = \det(h)\det(h)$$

Exemplo: $\exp : \mathbb{R} \to T = \{z \in \mathbb{C}^* \mid |z| = 1\}$, $\exp(x) = e^{ix}$ é homomorfismo:

$$e^{i(x+y)} = e^{ix}e^{iy}$$

Proposição: Se $\phi : G \to H$ é um homomorfismo, então

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = \phi(g)^{-1}, \ \forall g \in G$
3. $K \leq G \Rightarrow \phi(K) \leq H$
4. $L \leq H \Rightarrow \phi^{-1}(L) = \{g \in G \mid \phi(g) \in L\} \leq G$; $L \lhd H \Rightarrow \phi^{-1}(L) \lhd G$

Prova: (1): $\phi(e_G)e_H = \phi(e_G)$ e $\phi(e_G)\phi(e_G) = \phi(e_G)$. Logo,

$$\phi(e_G)e_H = \phi(e_G)\phi(e_G) \Rightarrow \phi(e_G) = e_H$$

(2): para todo $g \in G$, temos

$$\begin{aligned} \phi(g)\phi(g^{-1}) &= \phi(gg^{-1}) = \phi(e_G) = e_H \\ \phi(g^{-1})\phi(g) &= \phi(g^{-1}g) = \phi(e_G) = e_H \\ &\Rightarrow \phi(g)^{-1} = \phi(g^{-1}) \end{aligned}$$

(3): $e_G \in K \Rightarrow \phi(e_G) = e_H \in \phi(K) \Rightarrow \phi(K) \neq \emptyset$. Se $\phi(k_1), \phi(k_2) \in \phi(K)$, então

$$\phi(k_1)\phi(k_2)^{-1} = \phi(k_1)\phi(k_2^{-1}) = \phi(k_1k_2^{-1}) \in \phi(K) \Rightarrow \phi(K) \leq G$$

(4): $\phi(e_G) = e_H \in L \Rightarrow e_G \in \phi^{-1}(L) \Rightarrow \phi^{-1}(L) \neq \emptyset$. Se $g_1, g_2 \in \phi^{-1}(L)$, então

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} \in L \Rightarrow g_1 g_2^{-1} \in \phi^{-1}(L) \Rightarrow \phi^{-1}(L) \leq G$$

Prove que $L \lhd H \Rightarrow \phi^{-1}(L) \lhd G$ ■

Definição: O núcleo (ou kernel) de um homomorfismo $\phi : G \to H$ é

$$\ker \phi = \phi^{-1}(\{e_H\}) = \{g \in G \mid \phi(g) = e_H\}$$

Corolário: Se $\phi : G \to H$ é homomorfismo, então $\ker \phi \lhd G$

Proposição: Um homomorfismo $\phi : G \to H$ é injetivo $\Leftrightarrow \ker \phi = \{e_G\}$

Prova: $(\Rightarrow)$ ϕ é injetivo $\Rightarrow |\phi^{-1}(\{h\})| = 1, \ \forall h \in H \Rightarrow |\phi^{-1}(\{e_H\})| = 1$

$e_G \in \ker \phi \Rightarrow \phi = \{e_G\}$

$(\Leftarrow)$

$$\phi(g_1) = \phi(g_2) \Rightarrow \phi(g_1)\phi(g_2^{-1}) = e_H \Rightarrow \phi(g_1 g_2^{-1}) = e_H \Rightarrow g_1 g_2^{-1} = e_G \Rightarrow g_1 = g_2 \quad ■$$

Corolário: Se $\phi : G \to H$ é homomorfismo injetivo, então $G \cong \phi(G)$

Exemplo: $SL_n(\mathbb{R}) = \{g \in GL_n(\mathbb{R}) \mid \det g = 1\} \lhd GL_n(\mathbb{R})$

Exemplo: O kernel do homomorfismo $\exp : \mathbb{R} \to \mathbb{C}^*$, $\exp(x) = e^{ix} = \cos(x) + i\sin(x)$ é $\{2n\pi \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$

Exemplo: Se $\phi : \mathbb{Z}_7 \to \mathbb{Z}_{12}$ é homomorfismo, então

$$\ker\phi \leq \mathbb{Z}_7 \Rightarrow \ker\phi = \{0\} \text{ ou } \mathbb{Z}_7$$

e

$$\operatorname{im}\phi \leq \mathbb{Z}_{12} \Rightarrow \operatorname{im}\phi = \{0\},\ \mathbb{Z}_2,\ \mathbb{Z}_3,\ \mathbb{Z}_4,\ \mathbb{Z}_6,\ \mathbb{Z}_{12}$$

- $\ker\phi = \{0\} \Rightarrow \mathbb{Z}_7 \operatorname{im}\phi \Rightarrow \mathbb{Z}_7 \leq \mathbb{Z}_{12}$ (contradição)

Logo, $\ker\phi = \mathbb{Z}_7 \Rightarrow \phi(n) = 0\ \forall n \in \mathbb{Z}_7 \Rightarrow \phi$ é o homomorfismo trivial

Teoremas de isomorfismo

Sabemos que

$$\begin{aligned}\{\text{homomorfismos cujo domínio é } G\} &\to \{N \lhd G\}\\ \phi &\mapsto \ker\phi\end{aligned}$$

Por outro lado, também temos

$$\begin{aligned}\{N \lhd G\} &\to \{\text{homomorfismos cujo domínio é } G\}\\ N &\mapsto \phi : G \to G/N,\ \phi(g) = gN \quad \text{(verifique)}\end{aligned}$$

Assim, existe uma correspondência

$$\{\text{homomorfismos cujo domínio é } G\} \longleftrightarrow \{N \lhd G\}$$

O homomorfismo $\phi : G \to G/N$ acima é chamado projeção canonica

Primeiro Teorema de Isomorfismo (1ºTI):

$$\psi : G \to H \text{ é homomorfismo} \Rightarrow G/\ker\psi \cong \psi(G)$$

Prova: Denote $N = \ker\psi$. Defina $\eta : G/N \to \psi(G)$, $\eta(gN) = \psi(g)$

- η é bem definida: se $g_1N = g_2N$ (ou $g_1 = g_2n$ para algum $n \in N$), então

$$\eta(g_1N) = \psi(g_1) = \psi(g_2n) = \psi(g_2)\psi(n) = \psi(g_2)e_H = \psi(g_2) = \eta(g_2N)$$

- η é homomorfismo:

$$\eta((g_1N)(g_2N)) = \eta(g_1g_2N) = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \eta(g_1N)\eta(g_2N) \qquad \blacksquare$$

- η é injetora:

$$\eta(gN) = e_H \Leftrightarrow \psi(g) = e_H \Leftrightarrow g \in N \Leftrightarrow gN = N = e_{G/N}$$

- η é sobrejetora:

$$\eta(G/N) = \psi(G)$$

Em resumo, temos o seguinte diagrama comutativo

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[d, "\phi"'] & H \\ G/N \arrow[ur, "\eta"'] & \end{tikzcd}$$

Corolário: Se $G = \langle g \rangle$ é cíclico, então um dos seguintes casos ocorre

1. $|G| = m$ e $G \cong \mathbb{Z}/m\mathbb{Z}$,
2. $|G| = \infty$ e $G \cong \mathbb{Z}$

Prova: Considere o homomorfismo $\phi : \mathbb{Z} \to G$, $\phi(n) = g^n$. Claramente, $\phi(\mathbb{Z}) = G$

(1): $|G| = m \Rightarrow |g| = m \Rightarrow \phi(mk) = (g^m)^k = e_G \ \forall k \in \mathbb{Z} \Rightarrow m\mathbb{Z} \subset \ker \phi$

Por outro lado,

$$\phi(n) = e_G \Leftrightarrow g^n = e_G \Leftrightarrow m|n \Leftrightarrow n \in m\mathbb{Z} \Rightarrow \ker \phi \subset m\mathbb{Z}$$

Logo, $\ker \phi = m\mathbb{Z}$, e 1°TI $\Rightarrow G \cong \mathbb{Z}/m\mathbb{Z}$

(2): $|G| = \infty \Leftrightarrow |g| = \infty \Leftrightarrow \phi$ é injetora. Logo, 1°TI $\Rightarrow \mathbb{Z} \cong G$ ∎

Segundo Teorema de Isomorfismo (2ºTI): Se $H \leq G$, $N \lhd G$, então

$$HN \leq G, \quad H \cap N \lhd H, \quad H/(H \cap N) \cong HN/N$$

Prova:

- $HN \leq G$: $e_G = e_G e_G \in HN \Rightarrow HN \neq \emptyset$. Se $h_1 n_1, h_2 n_2 \in HN$, então

$$(h_1 n_1)(h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 h_2^{-1} h_2 n_1 h_2^{-1} h_2 n_2^{-1} h_2^{-1} = h_1 h_2^{-1} n_1' n_2' \in HN$$

Logo, $HN \leq G$

- $H \cap N \lhd H$: $H \cap N \leq H$ (exercício), e se $n \in H \cap N$, $h \in H$, então

$$N \lhd G \Rightarrow hnh^{-1} \in N, \text{ e } H \leq G \Rightarrow hnh^{-1} \in H \Rightarrow hnh^{-1} \in N \cap H$$

Logo, $H \cap N \lhd H$

- $H/(H \cap N) \cong HN$: Defina $\phi : H \to HN/N$, $\phi(h) = hN$

ϕ é homomorfismo (verifique!) e $hnN = hN = \phi(h) \Rightarrow \phi(H) = HN/N$

$\ker \phi = \{h \in H \mid hN = e_{G/N} = N\} = \{h \in H \mid h \in N\} = H \cap N$

Logo, 1ºTI $\Rightarrow H/(H \cap N) \cong HN/N$ ■

Teorema de correspondência: Se $N \triangleleft G$, então existe uma bijeção

$$\{H \leq G \mid N \subset H\} \longleftrightarrow \{K \leq G/N\}$$

$$H \xrightarrow{\Psi} \phi(H) = H/N \quad (\phi : G \to G/N,\ \phi(g) = gN)$$

$$\phi^{-1}(K) \xleftarrow{\Phi} K$$

Além disso, essa bijeção restringe a uma bijeção se trocarmos $\leq$ por $\triangleleft$

Prova: Que Ψ e Φ estão bem definidas é claro

Note: $N \leq H \Rightarrow hN \subset H,\ \forall h \in H$

$$\phi^{-1}(H/N) = \{g \in G \mid gN \in H/N\} = \{g \in G \mid\ \exists h \in H\ :\ gN = hN \subset H\} = H$$

Logo,

$$\Phi(\Psi(H)) = \Phi(H/N) = H$$

ϕ sobrejetora $\Rightarrow K = \phi(\phi^{-1}(K))$. Logo,

$$\Psi(\Phi(K)) = \Psi(\phi^{-1}(K)) = \phi(\phi^{-1}(K)) = K$$

Assim, $\Psi = \Phi^{-1}$ e temos a bijeção

Já sabemos que $K \lhd G/N \Rightarrow \phi^{-1}(K) \lhd G$

Por fim, afirmamos que $H \lhd G \Rightarrow H/N \lhd G/N$. De fato, se $gN \in G/N$ e $hN \in H/N$, então $ghg^{-1} = h' \in H$ e temos

$$(gN)(hN)(g^{-1}N) = ghg^{-1}N = h'N \in H/N \Rightarrow H/N \lhd G/N \qquad \blacksquare$$

3º Teorema de Isomorfismo (3ºTI): Se $N \lhd G$ e $N \leq H \lhd G$, então

$$\frac{G/N}{H/N} \cong G/H$$

Prova: Considere a composição

$$\psi : G \to G/N \to \frac{G/N}{H/N}, \; g \mapsto gN \mapsto (gN)H/N$$

ψ é sobrejetora, pois é composição de sobrejeções $\Rightarrow \psi(G) = \frac{G/N}{H/N}$

$$\psi(g) = (gN)H/N = e_{\frac{G/N}{H/N}} = H/N \Leftrightarrow gN \in H/N \Leftrightarrow gN = hN \subset H \Leftrightarrow g \in H$$

Logo,

$$\ker \psi = \{g \in G \mid (gN)H/N = e = H/N\} = \{g \in G \mid g \in H\} = H$$

Assim, $1^{\text{o}}\text{TI} \Rightarrow G/H \cong \psi(G) = \frac{G/N}{H/N}$ $\blacksquare$

Lembre que, se $N \lhd G$, então $|G/N| = |G|/|N|$

Exemplo: $m\mathbb{Z} \lhd \mathbb{Z}$, $mn\mathbb{Z} \lhd \mathbb{Z}$ e $mn\mathbb{Z} \leq m\mathbb{Z}$. Então

$$\mathbb{Z}/m\mathbb{Z} \cong \frac{\mathbb{Z}/mn\mathbb{Z}}{m\mathbb{Z}/mn\mathbb{Z}} \Rightarrow |\mathbb{Z}/m\mathbb{Z}| = \frac{|\mathbb{Z}/mn\mathbb{Z}|}{|m\mathbb{Z}/mn\mathbb{Z}|} \Rightarrow m = \frac{mn}{|m\mathbb{Z}/mn\mathbb{Z}|} \Rightarrow |m\mathbb{Z}/mn\mathbb{Z}| = n$$

Lista de exercícios:

Cap 10: 3, 4, 5, 6, 7, 9, 10, 11, 12

Cap 11: 3, 5, 11, 12, 13, 15, 16, 17

Lista de exercícios:

Cap 10: 3, 4, 5, 6, 7, 9, 10, 11, 12

Cap 11: 3, 5, 11, 12, 13, 15, 16, 17