Grupos e Corpos

Prof. Lucas Calixto

Aula 5 - Grupos Abelianos Finitamente Gerados; Teorema de Jordan-Hölder; Grupos Solúveis

O que sabemos?

O que já sabemos dizer sobre G se G é abeliano?

- Se G é cíclico $\Rightarrow G \cong \mathbb{Z}$ se $|G| = \infty$, ou $G \cong \mathbb{Z}_n$ se $n = |G| < \infty$
- Se $|G| = p$ com p primo $\Rightarrow G \cong \mathbb{Z}_p$
- Se $mdc(m, n) = 1 \Rightarrow \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

Nessa aula veremos que muito mais do que isso pode ser dito:

$$G \text{ é abeliano finito } \Leftrightarrow G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

para $p_1, \ldots, p_k$ primos não necessariamente distintos

Definição: Para $X = \{g_i \mid i \in I\} \subset G$, definimos

$$\langle X \rangle = \{g_1^{\epsilon_1} \cdots g_k^{\epsilon_k} \mid g_i \in X,\ \epsilon_i \in \{\pm 1\}\}$$

Proposição $\langle X \rangle$ é o menor subgrupo de G que contem X

Prova: Se $g, h \in \langle X \rangle$, então $g = g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}$, $h_1^{\tau_1} \cdots h_l^{\tau_l}$ e $h^{-1} = h_l^{-\tau_l} \cdots h_1^{-\tau_1}$ onde $g_i, h_j \in X$. Logo

$$gh^{-1} = g_1^{\epsilon_1} \cdots g_k^{\epsilon_k} h_l^{-\tau_l} \cdots h_1^{-\tau_1} \in \langle X \rangle \Rightarrow \langle X \rangle \leq G$$

Se $H \leq G$ e $X \subset H$, então obviamente $\langle X \rangle \subset H \Rightarrow \langle X \rangle$ é o menor subgrupo de G que contem X ■

$\langle X \rangle$ é chamado o subgrupo de G gerado por X

Os elementos $g \in X$ são chamados geradores de $\langle X \rangle$

Se $|X| < \infty$, dizemos que $\langle X \rangle$ é finitamente gerado

Exemplo: Todo grupo finito G é finitamente gerado, pois $G = \langle G \rangle$

Exemplo: Todo grupo cíclico é finitamente gerado

Exemplo: $\mathbb{Z} \times \mathbb{Z}_n$ é finitamente gerado, pois $\mathbb{Z} \times \mathbb{Z}_n = \langle (1,0), (0,1) \rangle$

Nem todo grupo é finitamente gerado

Exemplo: $\mathbb{Q}$ não é finitamente gerado. De fato, suponha $\mathbb{Q} = \langle p_1/q_1, \ldots, p_n/q_n \rangle$

$r \in \mathbb{Q} \Rightarrow r = k_1p_1/q_1 + \cdots + k_np_n/q_n = (k_1p_1q_2 \cdots q_n + \cdots + k_np_nq_1 \cdots q_{n-1})/q_1 \cdots q_n$

Seja p um primo tal que $p \nmid q_i \; \forall i$

Assim,

$$1/p = (k_1p_1q_2 \cdots q_n + \cdots + k_np_nq_1 \cdots q_{n-1})/q_1 \cdots q_n \Leftrightarrow p \text{ divide } q_1 \cdots q_n$$

o que claramente é uma contradição

Definição: Dizemos que G é um p-grupo (p primo) se a ordem de todo elemento de G é uma potencia de p

Exemplo: $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um 2-grupo

Exemplo: $\mathbb{Z}_4$ é um 2-grupo

Exemplo: $\mathbb{Z}_{27}$ é um 3-grupo

Teorema Fundamental dos Grupos Abelianos Finitos

TFGAF: Todo grupo abeliano finito é isomorfo a um produto direto da forma

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

para $p_1, \ldots, p_k$ primos não necessariamente distintos

Exemplo: Com o TFGAF em mãos podemos listar todos os grupos abelianos cuja ordem é $540 = 2^2 3^3 5$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

$\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

Lema 1: Se G é grupo abeliano finito, e $p \in \mathbb{N}$ é primo e divide $|G|$, então $\exists\, g \in G$ tal que $|g| = p$

Prova: Indução em $n = |G|$

Se $n = 1$, OK

Suponha que o lema é verdade para todo grupo H tal que $|H| < n$

Se o único subgrupo próprio de G é $\{e\}$, então $G = \langle a \rangle, \ \forall a \in G \setminus \{e\}$

Assim, $\langle a \rangle = \langle a^k \rangle$ para todo $0 \leq k < |a|$, e temos

$$n = |a| = |a^k| = |a|/mdc(k, n) \Rightarrow mdc(k, n) = 1 \Rightarrow n \text{ é primo}$$

Logo, $n = p \Rightarrow |a| = p, \ \forall a \in G \setminus \{e\}$

Se G contem algum subgrupo não trivial H $\Rightarrow 1 < |H| < |G|$

Se $p \mid |H|$, então $\exists h \in H \subset G$ tal que $|h| = p$

Suponha que $p \nmid |H|$ e considere G/H

$|G| = |G/H||H| \Rightarrow p$ divide $|G/H| \Rightarrow \exists\ aH \in G/H$ tal que $|aH| = p$. Assim,

$$(aH)^p = a^pH = e_{G/H} = H \Rightarrow a^p \in H$$

Se $|H| = r \Rightarrow |a^p|$ divide $r \Rightarrow (a^p)^r = (a^r)^p = e$

Afirmação: $a^r \neq e$. De fato, suponha $a^r = e$

$p \nmid r \Rightarrow mdc(p, r) = 1 \Rightarrow \exists\ s, t \in \mathbb{Z}$ tal que $sp + tr = 1$. Logo,

$$a = a^{sp+tr} = a^{sp}a^{tr} = (a^p)^s(a^r)^t = (a^p)^s \in H \Rightarrow a \in H \text{ contradição}$$

Assim, $a^r \neq e$. Como $(a^r)^p = e$ temos que $|a^r|$ divide $p \Rightarrow |a^r| = p$ e $a^r \in G$ ■

Lema 2: Um grupo abeliano finito G é um p-grupo $\Leftrightarrow |G|$ é uma potencia de p

Prova: $(\Rightarrow)$ $|G| = p^n \Rightarrow$ para todo $g \in G$, $|g|$ divide $p^n \Rightarrow |g| = p^k \Rightarrow G$ é p-grupo

$(\Leftarrow)$ $|G| \neq$ potencia de $p \Rightarrow \exists\ q$ primo tal que $q \mid |G|$

Lema 1 $\Rightarrow \exists\ g \in G$ tal que $|g| = q \Rightarrow G$ não é p-grupo ■

Lema 3: Suponha que G é abeliano finito e $|G| = p_1^{n_1} \cdots p_k^{n_k}$ onde $p_i \neq p_j$ e $n_i > 0$. Então G é o produto direto interno de subgrupos $G_1, \ldots, G_k$ onde

$$G_i = \{g \in G \mid |g| = \text{potencia de } p_i\}$$

Prova: É fácil ver que cada G_i é subgrupo de G (exercício)

- $G = G_1 \cdots G_k$

Tome $g \in G$. $|g|$ divide $|G| \Rightarrow |g| = p_1^{m_1} \cdots p_k^{m_k} \Rightarrow$ os inteiros $a_i = |g|/p_i^{m_i}$ são coprimos

Logo, $\exists\ b_1, \ldots, b_k \in \mathbb{Z}$ tais que $b_1 a_1 + \cdots + b_k a_k = 1$. Assim

$$g = g^{b_1 a_1 + \cdots + b_k a_k} = g^{b_1 a_1} \cdots g^{b_k a_k}$$

$(g^{b_i a_i})^{p_i^{m_i}} = g^{b_i |g|} = e \Rightarrow g^{a_i b_i} \in G_i \Rightarrow G = G_1 \cdots G_k$

- $g_i g_j = g_j g_i,\ \forall g_i \in G_i,\ g_j \in G_j$ pois G é abeliano

- $G_i \cap \prod_{j \neq i} G_j = \{e\}$

Por conveniência, suponha $i = 1$ e tome $g_1 = g_2 \cdots g_k \in G_1 \cap G_2 \cdots G_k$

Se $|g_i| = p_i^{r_i} \Rightarrow g_1^{p_2^{r_2} \cdots p_k^{r_k}} = g_2^{p_2^{r_2}} \cdots g_k^{p_k^{r_k}} = e \Rightarrow p_1^{r_1} \mid p_2^{r_2} \cdots p_k^{r_k} \Rightarrow r_1 = 0 \Rightarrow g_1 = e$ ■

Lema 4: Seja G um p-grupo abeliano finito, e seja $g \in G$ um elemento cuja ordem é máxima. Então, $G \cong \langle g \rangle \times K$ para algum $K \leq G$

Prova: Lema 2 $\Rightarrow |G| = p^n$ para algum n

Indução sobre n

$n = 1 \Rightarrow |G| = p \Rightarrow G = \langle g \rangle \ \forall g \in G \setminus \{e\} \Rightarrow G \cong \langle g \rangle \times \{e\}$

Suponha que o resultado valha para qualquer grupo L tal que $|L| = p^l$ com $l < n$

Seja $g \in G$ elemento cuja ordem é máxima, digamos $|g| = p^m \Rightarrow a^{p^m} = e, \ \forall a \in G$

Se $G = \langle g \rangle$, OK

Suponha $\langle g \rangle \neq G$ e tome $h \in G \setminus \langle g \rangle$ cuja ordem é mínima. Defina $H = \langle h \rangle$

- $\langle g\rangle \cap H = \{e\}$

Se $|H| = p$, então

$$\langle g\rangle \cap H \leq H \Rightarrow \langle g\rangle \cap H = \{e\} \text{ ou } H \Rightarrow \langle g\rangle = \{e\}, \text{ pois } h \notin \langle g\rangle$$

Afirmamos que $|H| = p$. Basta construir um elemento em $G \setminus \{e\}$ cuja ordem é p (essa é a mínima possível)

Note: $|h^p| = |h|/mdc(p, |h|) = |h|/p \Rightarrow |h^p| < |h|$. A construção de $H \Rightarrow h^p \in \langle g\rangle \Rightarrow h^p = g^r$

Logo, $(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e$ (pois $a^{p^m} = e, \ \forall a \in G$) $\Rightarrow |g^r| < p^m = |g|$

Assim, $|g^r| = |g|/mdc(r, |g|) = p^m/mdc(r, p^m) < p^m \Rightarrow mdc(r, p^m) = p^l$, $l > 0 \Rightarrow r = ps$ para algum $s \Rightarrow h^p = g^r = g^{ps}$

Defina $a = g^{-s}h$. Se $a \in \langle g\rangle \Rightarrow g^s a = h \in \langle g\rangle$ contradição $\Rightarrow a \notin \langle g\rangle$

Note: $a^p = g^{-sp}h^p = g^{-sp}g^{sp} = e \Rightarrow |a| = p \Rightarrow |H| = p$, pela construção de H

- $|gH| = |g|$

$(gH)^{p^{m-1}} = g^{p^{m-1}}H = e_{G/H} = H \Rightarrow g^{p^{m-1}} \in H \Rightarrow g^{p^{m-1}} \in \langle g \rangle \cap H = \{e\}$

$\Rightarrow g^{p^{m-1}} = e$ (contradiz $|g| = p^m$) $\Rightarrow |gH| = |g| \Rightarrow gH$ tem ordem máxima em G/H

Por indução, $G/H \cong \langle gH \rangle \times \bar{K}$ para algum $\bar{K} \leq G/H$

Teorema de correspondência $\Rightarrow \bar{K} = K/H$ para algum $K \leq G$ tal que $H \subset K$. Logo,

$$G/H \cong \langle gH \rangle \times K/H$$

- $G = \langle g \rangle K$

$a \in G \Rightarrow aH = (gH)(k/H) = gkH \Rightarrow a \in gkH \subset gK$ (pois $H \subset K$)

- $\langle g \rangle \cap K = \{e\}$

$b = \langle g \rangle \cap K \Rightarrow bH \in \langle gH \rangle \cap K/H = \{e_{G/H}\} = H \Rightarrow b \in H \Rightarrow b \in \langle g \rangle \cap H = \{e\}$

- $ab = ba, \ \forall a \in \langle g \rangle, b \in K$ pois G é abeliano

Logo, G é o produto direto interno de $\langle g \rangle$ e $K \Rightarrow G \cong \langle g \rangle \times K$ ■

Teorema: Todo grupo abeliano finito é isomorfo a um produto direto da forma

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

para $p_1, \ldots, p_k$ primos não necessariamente distintos

Prova: Suponha que G é p-grupo $\Rightarrow |G| = p^n$. Tome $g \in G$ de ordem máxima

$n = 1 \Rightarrow G \cong \mathbb{Z}_p \Rightarrow$ OK

Suponha $n > 1$. Lema 4 $\Rightarrow G \cong \langle g \rangle \times K,$ para algum $K \leq G$

- $\langle g \rangle \cong \mathbb{Z}_{|g|} = \mathbb{Z}_{p^r}$
- $|K| = p^k < |G| = p^n \Rightarrow K \cong \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}}$ (por indução)

Logo, $G \cong \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}}$

Se $|G| = p_1^{n_1} \cdots p_k^{n_k}$, então Lema 3 $\Rightarrow G \cong G_1 \times \cdots \times G_k$, onde G_i é p_i-subgrupo

Resultado para cada $G_i \Rightarrow$ resultado para G $\blacksquare$

Teorema: Todo grupo abeliano finitamente gerado é isomorfo a um produto direto da forma

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} \times \mathbb{Z}^n$$

onde $p_1, \ldots, p_k$ são primos não necessariamente distintos, e $n \in \mathbb{N}$

Prova: Seja $G = \langle g_1, \ldots, g_k \rangle$

Se $|G| < \infty \Rightarrow$ OK, pelo slide anterior

Se $|G| = \infty \Rightarrow |g_i| = \infty$ para algum i

- Prove que $T(G) = \{g \in G \mid |g| < \infty\} \leq G$
- Prove que $G/T(G)$ é fin. ger. e todo elemento de $G/T(G)$ tem ordem infinita
- Prove que $G/T(G) \cong \mathbb{Z}^n$ para algum $n \in \mathbb{N}$
- Prove que $G \cong T(G) \times F$, onde $F \cong G/T(G)$

$T(G)$ é finito e abeliano $\Rightarrow$ o resultado segue do slide anterior ■

Séries de Composição

Uma serie subnormal de subrupos de um grupo G é uma cadeia de subgrupos $\{H_i\}$

$$G = H_n \supsetneq H_{n-1} \supsetneq \cdots \supsetneq H_1 \supsetneq H_0 = \{e\}$$

onde cada H_i é normal em H_{i+1}

Se cada H_i é normal em G, a série é chamada de serie normal

O comprimento de uma serie subnormal é a quantidade de inclusões próprias

Exemplo: G abeliano $\Rightarrow$ qualquer sequencia de subgrupos próprios de G é serie normal

Exemplo: Existem series subnormais que não são normais: em D_4 temos que

$$D_4 \supsetneq \{(1), (12)(34), (13)(24), (14)(23)\} \supsetneq \{(1), (12)(34)\} \supsetneq \{(1)\}$$

é subnormal mas não normal, pois $\{(1), (12)(34)\}$ não é normal em D_4

Se $\{H_i\}$ e $\{K_j\}$ são séries (sub)normais tais que $\{H_i\} \subset \{K_j\}$, dizemos que $\{K_j\}$ é um refinamento de $\{H_i\}$

Exemplo: A série

$$\mathbb{Z} \supsetneq 3\mathbb{Z} \supsetneq 9\mathbb{Z} \supsetneq 45\mathbb{Z} \supsetneq 90\mathbb{Z} \supsetneq 180\mathbb{Z} \supsetneq \{0\}$$

é um refinamento de

$$\mathbb{Z} \supsetneq 9\mathbb{Z} \supsetneq 45\mathbb{Z} \supsetneq 90\mathbb{Z} \supsetneq 180\mathbb{Z} \supsetneq \{0\}$$

Estudaremos uma série sub(normal) $\{H_i\}$ por meio dos quocientes $\{H_{i+1}/H_i\}$

Duas séries (sub)normais $\{H_i\}$ e $\{K_j\}$ são ditas isomorfas se:

- os seus comprimentos coincidem
- para cada i existe j_i tal que $H_{i+1}/H_i \cong K_{j_i+1}/K_{j_i}$

Exemplo: As séries

$$\mathbb{Z}_{60} \supsetneq \langle 3 \rangle \supsetneq \langle 15 \rangle \supsetneq \{0\}$$
$$\mathbb{Z}_{60} \supsetneq \langle 4 \rangle \supsetneq \langle 20 \rangle \supsetneq \{0\}$$

são isomorfas, pois

$$\{\mathbb{Z}_{60}/\langle 3 \rangle \cong \mathbb{Z}_3, \langle 3 \rangle/\langle 15 \rangle \cong \mathbb{Z}_5, \langle 15 \rangle/\{0\} \cong \mathbb{Z}_4\}$$

e

$$\{\mathbb{Z}_{60}/\langle 4 \rangle \cong \mathbb{Z}_4, \langle 4 \rangle/\langle 20 \rangle \cong \mathbb{Z}_5, \langle 20 \rangle/\{0\} \cong \mathbb{Z}_3\}$$

Uma série de composição é uma série subnormal $\{H_i\}$, onde todos os quocientes H_{i+1}/H_i são simples. Uma série principal é uma série normal $\{H_i\}$, onde todos os quocientes H_{i+1}/H_i são simples

Exemplo: A série

$$\mathbb{Z}_{60} \supsetneq \langle 3 \rangle \supsetneq \langle 15 \rangle \supsetneq \langle 30 \rangle \supsetneq \{0\}$$

é uma série de composição, pois

$$\mathbb{Z}_{60}/\langle 3 \rangle \cong \mathbb{Z}_3, \quad \langle 3 \rangle/\langle 15 \rangle \cong \mathbb{Z}_5, \quad \langle 15 \rangle/\langle 30 \rangle \cong \mathbb{Z}_2, \quad \langle 30 \rangle/\{0\} \cong \mathbb{Z}_2$$

são todos simples

Note: $\mathbb{Z}_{60} \supsetneq \langle 2 \rangle \supsetneq \langle 4 \rangle \supsetneq \langle 20 \rangle \supsetneq \{0\}$ também é série de composição

Exemplo: Se $n \geq 5$, então a série

$$S_n \supsetneq A_n \supsetneq \{(1)\}$$

é uma série principal, pois $\{(1)\} \lhd A_n$, $A_n \lhd S_n$ e

$$S_n/A_n \cong \mathbb{Z}_2, \quad A_n/\{(1)\} \cong A_n$$

são simples

Exemplo: $\mathbb{Z}$ não admite série de composição. De fato, seja

$$\mathbb{Z} = H_n \supsetneq H_{n-1} \supsetneq \cdots \supsetneq H_1 \supsetneq H_0 = \{0\}.$$

Então $H_1 = k\mathbb{Z}$ para algum $k \in \mathbb{Z}$, e $H_1/H_0 \cong k\mathbb{Z}$ não é simples ($nk\mathbb{Z} \lhd k\mathbb{Z}$, $\forall n \in \mathbb{Z}$)

Séries de composição não são únicas (ex: $\mathbb{Z}_{60}$), contudo temos

Teorema (Jordan-Hölder) Quaisquer duas séries de composição de um grupo G são isomorfas

Corolário: Se G admite série de composição de comprimento finito, então qualquer série subnormal de G pode ser refinada à uma série de composição

Prova (Teorema): Sejam

$$G = H_n \supsetneq H_{n-1} \supsetneq \cdots \supsetneq H_1 \supsetneq H_0 = \{0\}$$
$$G = K_m \supsetneq K_{m-1} \supsetneq \cdots \supsetneq K_1 \supsetneq K_0 = \{0\}$$

duas séries de composição de G

Indução sobre o comprimento de uma serie de composição (qualquer uma)

Se $\{H_i\}$ tem comprimento 1, então G é simples. Nesse caso a única série de composição que existe é

$$G = H_1 \supsetneq H_0 = \{0\} \Rightarrow \text{OK}$$

Suponha que $\{H_i\}$ tem comprimento n e que o resultado valha para qualquer grupo que tenha uma série de composição de comprimento $< n$

Se $H_{n-1} = K_{m-1} \Rightarrow$ o resultado segue por indução

Assuma $H_{n-1} \neq K_{m-1} \Rightarrow H_{n-1}K_{m-1} = G$

- $H_i \cap K_{m-1}$ é normal em $H_{i+1} \cap K_{m-1}$
- $H_{n-1} \cap K_j$ é normal em $H_{n-1} \cap K_{j+1}$

Logo,

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_1 \cap K_{m-1} \supset H_0 \cap K_{m-1} = \{0\}$$
$$G = K_m \supset K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_{n-1} \cap K_1 \supset H_{n-1} \cap K_0 = \{0\}$$

são séries subnormais. Note:

$$\begin{aligned}(H_{i+1} \cap K_{m-1})/(H_i \cap K_{m-1}) &= (H_{i+1} \cap K_{m-1})/(H_i \cap (H_i \cap K_{m-1})) \\ &\overset{2^{\text{o}}\text{TI}}{\cong} (H_{i+1} \cap K_{m-1})H_i/H_i \\ &\lhd H_{i+1}/H_i\end{aligned}$$

Como H_{i+1}/H_i é simples, temos uma das possibilidades:

- $(H_{i+1} \cap K_{m-1})H_i/H_i = H_{i+1}/H_i \Rightarrow (H_{i+1} \cap K_{m-1})/(H_i \cap K_{m-1})$ simples
- $(H_{i+1} \cap K_{m-1})H_i/H_i = \{e_{H_{i+1}/H_i}\} \Rightarrow (H_{i+1} \cap K_{m-1}) = (H_i \cap K_{m-1})$

Além disso,

$$H_{n-1}K_{m-1} = G \Rightarrow H_{n-1}/(H_{n-1} \cap K_{m-1}) \overset{2^{\text{o}}\text{TI}}{\cong} (H_{n-1}K_{m-1})/K_{m-1} = G/K_{m-1}$$

Assim, deletando os termos iguais da série

$$H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_1 \cap K_{m-1} \supset H_0 \cap K_{m-1} = \{0\}$$

obtemos uma série de composição de H_{n-1}

Indução $\Rightarrow$ essa série é isomorfa a série $H_{n-1} \supsetneq \cdots \supsetneq H_1 \supsetneq H_0 = \{0\}$

Logo, as séries

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_1 \cap K_{m-1} \supset H_0 \cap K_{m-1} = \{0\}$$
$$G = H_n \supset H_{n-1} \supsetneq \cdots \supsetneq H_1 \supsetneq H_0 = \{0\}$$

são isomorfas

O mesmo argumento prova que as séries

$$G = K_m \supset K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_{n-1} \cap K_1 \supset H_{n-1} \cap K_0 = \{0\}$$
$$G = K_m \supset K_{m-1} \supsetneq \cdots \supsetneq K_1 \supsetneq K_0 = \{0\}$$

são isomorfas

Finalmente, observe

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_1 \cap K_{m-1} \supset H_0 \cap K_{m-1} = \{0\}$$
$$G = K_m \supset K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_{n-1} \cap K_1 \supset H_{n-1} \cap K_0 = \{0\}$$

Indução $\Rightarrow$ as séries destacadas são isomorfas

Para os pedaços que faltam, temos os seguintes quocientes:

- 1º: G/H_{n-1} e $H_{n-1}/(H_{n-1} \cap K_{m-1}) \overset{2^{\text{o}}\text{TI}}{\cong} (H_{n-1}K_{m-1})/K_{m-1} = G/K_{m-1}$
- 2º: G/K_{m-1} e $K_{m-1}/(H_{n-1} \cap K_{m-1}) \overset{2^{\text{o}}\text{TI}}{\cong} (H_{n-1}K_{m-1})/H_{n-1} = G/H_{n-1}$

Logo, as séries

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_1 \cap K_{m-1} \supset H_0 \cap K_{m-1} = \{0\}$$
$$G = K_m \supset K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_{n-1} \cap K_1 \supset H_{n-1} \cap K_0 = \{0\}$$

são isomorfas

Como essas séries são isomorfas as séries originais, o resultado segue ■

Grupos Solúveis

Um grupo G é dito solúvel se este que admite uma série subnormal $\{H_i\}$ tal que todos os quocientes H_{i+1}/H_i são abelianos

Exemplo: O grupo S_4 é solúvel, pois

$$S_4 \supset A_4 \supset \{(1), (12)(34), (13)(24), (14)(23)\} \supset \{(1)\}$$

é série subnormal cujos quocientes são abelianos

Exemplo: Para $n \geq 4$, temos que

$$S_n \supset A_n \supset \{(1)\}$$

é uma série de composição com quocientes não abelianos

Assim, se S_n admitisse uma série subnormal cujos quocientes são abelianos, essa série poderia ser refinada a uma série de composição cujos quocientes continuariam abelianos (por que?). Isso contradiz o teorema de Jordan-Hölder

Obs: Grupos solúveis são importantes na aplicação de teoria de Galois para encontrar soluções de equações polinomiais

Lista de exercícios

Cap 13: 2, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20, 21