Introdução a Teoria dos Grupos – MAT 113 – Pós Mat – UFABC-QS2020.2

TEOREMA:

SEJA M GRUPO ABELIANO (ESCRITO ADITIVAMENTE)
O SUBGRUPO $\langle x_1, x_2, \ldots, x_k \rangle$ DE M, GERADO PELOS
ELEMENTO $x_1, \ldots, x_m$ DE M CONSISTE DOS ELEMENTOS
$\sum_i m_i x_i$, $m_i \in \mathbb{Z}$. UM SUBCONJUNTO $\{x_1, \ldots, x_k\}$ DE M É UMA BASE
PARA M SE ELE GERA M E

$$m_1 x_1 + m_2 x_2 + \ldots + m_k x_k = 0 \Rightarrow m_i x_i = 0, \ \forall i$$
$$m_i \in \mathbb{Z}$$

ENTÃO: $M = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \cdots \oplus \langle x_k \rangle$.

LEMA: SUPONHA $x_1, x_2, \ldots, x_k$ GERAM M. PARA QUAISQUER $c_1, c_2, \ldots, c_k \in \mathbb{N}$, COM $\text{mdc}(c_1, c_2, \ldots, c_k) = 1$, EXISTEM GERADORES $y_1, y_2, \ldots, y_k$ PARA M TAIS QUE $y_1 = c_1 x_1 + c_2 x_2 + \ldots + c_k x_k$.

DEM: INDUÇÃO EM $s = c_1 + c_2 + \ldots + c_k$.

O LEMA CERTAMENTE VALE SE $s = 1$. SUPONHA $s > 1$.

ENTÃO PELO MENOS, DOIS DOS c_i's SÃO NÃO NULOS, SUPONHA $c_1 \geq c_2 > 0$.

AGORA. $\cdot$ $\{x_1, x_2 + x_1, x_3, \ldots, x_k\}$ GERAM M.

$\cdot$ $\text{mdc}(c_1 - c_2, c_2, c_3, \ldots, c_k) = 1$. E

$(c_1 - c_2) + c_2 + c_3 + \ldots + c_k < s$

LOGO, PELA H. INDUÇÃO, EXISTEM GERADORES $y_1, \ldots, y_k$ PARA M T.Q.

$$y_1 = (c_1 - c_2) x_1 + c_2 (x_1 + x_2) + c_3 x_3 + \ldots + c_k x_k$$
$$= c_1 x_1 + c_2 x_2 + \ldots + c_k x_k$$

easy office

TEOREMA: TODO GRUPO COMUTATIVO FINITAMENTE GERADO M POSSUI UMA BASE, PORTANTO ELE É UMA SOMA DIRETA DE GRUPOS CÍCLICOS.

DEM: INDUÇÃO NO NÚMERO DE GERADORES DE M.

SE M É GERADO POR UM ELEMENTO, O RESULTADO É TRIVIAL.

SUPONHA QUE O RESULTADO REQUERE PELO MENOS $k>1$ GERADORES.

ENTRE OS CONJUNTOS GERADORES $\{x_1, \dots, x_k\}$ DE M, ESCOLHA UM DE MODO QUE A ORDEM DE x_1 É A MENOR POSSÍVEL. MOSTRAREMOS QUE $M = \langle x_1 \rangle \oplus \langle x_2, \dots, x_k \rangle$.

A HIPÓTESE DE INDUÇÃO, DÁ UMA BASE PARA $\langle x_2, \dots, x_k \rangle$ QUE JUNTO COM $\{x_1\}$ DÁ UMA BASE PARA M. O RESULTADO SEGUE.

SE M NÃO É A SOMA DIRETA DE $\langle x_1 \rangle$ e $\langle x_2, \dots, x_k \rangle$, ENTÃO EXISTE UMA RELAÇÃO $m_1 x_1 + m_2 x_2 + \dots + m_k x_k = 0$ COM $m_1 x_1 \neq 0$.

APÓS MUDAR O SINAL DE ALGUNS x_i's, PODEMOS SUPOR $m_1, \dots, m_k \in \mathbb{N}$ E $m_1 < ord(x_1)$. SEJA $d = mdc(m_1, \dots, m_k) > 0$ E SEJA $c_i = \frac{m_i}{d}$.

PELO LEMA, EXISTE UM CONJUNTO GERADOR $y_1, \dots, y_k$ TAL QUE $y_1 = c_1 x_1 + c_2 x_2 + \dots + c_k x_k$.

MAS $d y_1 = m_1 x_1 + m_2 x_2 + \dots + m_k x_k = 0$.

E $d \leq m_1 < \operatorname{ord}(x_1)$. CONTRADIZENDO A ESCOLHA DE $\{x_1, \dots, x_k\}$!

SUPONHA QUE O RESULTADO REQUERE PELO MENOS $k > 1$ GERADORES.

ENTRE OS CONJUNTOS GERADORES $\{x_1, \dots, x_k\}$ DE M, ESCOLHA UM DE MODO QUE A ORDEM DE x_1 É A MENOR POSSÍVEL. MOSTRAREMOS QUE $M = \langle x_1 \rangle \oplus \langle x_2, \dots, x_k \rangle$.

A HIPOTESE DE INDUÇÃO, DÁ UMA BASE PARA $\langle x_2, \dots, x_k \rangle$ QUE JUNTO COM $\{x_1\}$ DÁ UMA BASE PARA M. O RESULTADO SEGUE.

SE M NÃO É A SOMA DIRETA DE $\langle x_1 \rangle$ e $\langle x_2, \dots, x_k \rangle$, ENTÃO EXISTE UMA RELAÇÃO $m_1 x_1 + m_2 x_2 + \dots + m_k x_k = 0$ COM $m_1 x_1 \neq 0$.

APÓS MUDAR O SINAL DE ALGUNS x_i's, PODEMOS SUPOR $m_1, \dots, m_k \in \mathbb{N}$ E $m_1 < \operatorname{ord}(x_1)$. SEJA $d = \operatorname{mdc}(m_1, \dots, m_k) > 0$ E SEJA $c_i = \frac{m_i}{d}$.

TEOREMA: SEJA M GRUPO ABELIANO f.g. NÃO NULO.
ENTÃO M PODE SER EXPRESSO COMO

$$M \cong C_{n_1} \times \dots \times C_{n_s} \times (C_\infty)^r.$$

PARA CERTOS INTEIROS $n_1, \dots, n_s \geq 2$ E $r \geq 0$. ALÉM DISSO:

(a) r É UNICAMENTE DETERMINADO POR M.

(b) OS n_i PODEM SER ESCOLHIDOS DE MODO QUE $n_1 \geq 2$, E $n_1 | n_2 \dots n_{s-1} | n_s$; E ELES SÃO UNICAMENTE DETERMINADOS POR M;

(c) OS n_i PODEM SER ESCOLHIDOS COMO POTÊNCIAS DE NÚMEROS PRIMOS, E ELES SÃO UNICAMENTE DETERMINADOS POR M.

$\to n_1, n_2, \dots, n_s \to$ FATORES INVARIANTES DE M

$\to M \cong C_{p_1^{e_1}} \times C_{p_2^{e_2}} \times \dots \times C_{p_t^{e_t}} \times (C_\infty)^r$, $p_1 \dots p_t$ PRIMOS

$\to$ DIVISORES ELEMENTARES DE M.

TEOREMA: SEJA M GRUPO ABELIANO f.g. NÃO NULO.
ENTÃO M PODE SER EXPRESSO COMO

$$M \cong C_{n_1} \times \cdots \times C_{n_s} \times (C_\infty)^r.$$

PARA CERTOS INTEIROS $n_1, \ldots, n_s \geq 2$ E $r \geq 0$.

DEM: (a) SEJA p PRIMO $p \nmid n_i$, $i = 1, \ldots, s$.

$$\frac{M}{pM} \cong \left(\frac{C_\infty}{pC_\infty}\right)^r \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^r$$

$\therefore$ r É A DIMENSÃO DE $\frac{M}{pM}$ COMO $\mathbb{F}_p$-ESPAÇO VETORIAL.

TEOREMA: SEJA M GRUPO ABELIANO f.g. NÃO NULO.

ENTÃO M PODE SER EXPRESSO COMO

$$M \cong C_{n_1} \times \cdots \times C_{n_s} \times (C_{\infty})^{r}.$$

PARA CERTOS INTEIROS $n_1, \ldots, n_s \geq 2$ E $r \geq 0$.

DEM (b, c): SE $mdc(m,n) = 1$ ENTÃO $C_m \times C_n \cong C_{mn}$. (*)

USAMOS (*) PARA DECOMPOR OS C_{n_i} COMO PRODUTO DE GRUPOS CÍCLICOS DE ORDEM POTÊNCIA DE PRIMO. APÓS ISSO, PODEMOS USAR (*) PARA OBTER UMA DECOMPOSIÇÃO COMO EM (b). POR EXEMPLO, $C_3 = \prod C_{p_i^{e_i}}$, O PRODUTO É SOBRE OS PRIMOS DISTINTOS ENTRE OS p_i E e_i É O MAIOR EXPOENTE PARA O PRIMO e_i...

UNICIDADE: PODEMOS SUPOR QUE M É DE TORÇÃO. ($\therefore r = 0$)

A DEMONSTRAÇÃO SEGUE DO CASO FINITO.