Tema7-AII.pdf

jaliriop

Álgebra II

2º Grado en Matemáticas

Facultad de Ciencias
Universidad de Granada

7 CLASIFICACIÓN DE GRUPOS ABELIANOS FINITOS.

25/11/19.

Notación: Al producto directo (interno) lo llamaremos suma directa (interna) $\times \rightsquigarrow \oplus$

Teorema 1 (clasificación de los p-grupos abelianos finitos):
Si A es un p-grupo abeliano finito con $|A| = p^n$, entonces A es isomorfo a una suma directa de p-grupos cíclicos de la forma $A \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \dots \oplus C_{p^{\beta_t}}$ donde $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$ y $\beta_1 + \beta_2 + \dots + \beta_n = n$
Además, esta expresión es única en el sentido de que si $A \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \dots \oplus C_{p^{\alpha_s}}$ con $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_s \geq 1$ y $\alpha_1 + \alpha_2 + \dots + \alpha_s = 1$, entonces $s = t$ y $\beta_i = \alpha_i \quad \forall i \in \{1, \dots, t\}$.
(Lo demostraremos más adelante).

Ejemplos:

- Si A es un 2-grupo con $|A| = 2^3 = 8$

$$3 \to \begin{cases} 3 \\ 2,1 \\ 1,1,1 \end{cases}$$

$$A \cong \begin{cases} C_8 \\ C_4 \oplus C_2 \\ C_2 \oplus C_2 \oplus C_2 \end{cases}$$

- Si A es un 3-grupo con $|A| = 3^4 = 81$

$$4 \to \begin{cases} 4 \\ 3,1 \\ 2,2 \\ 2,1,1 \\ 1,1,1,1 \end{cases}$$

$$A \cong \begin{cases} C_{81} \\ C_{27} \oplus C_3 \\ C_9 \oplus C_9 \\ C_9 \oplus C_3 \oplus C_3 \\ C_3 \oplus C_3 \oplus C_3 \oplus C_3. \end{cases}$$

Recordatorio: Si G es finito y todos sus p-subgrupos de Sylow son normales, entonces G es el producto directo de sus p-subgrupos.

Teorema 2 (Clasificación de grupos abelianos finitos: descomposición cíclica primaria): Sea A un grupo abeliano finito con $|A| = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ con p_i primos. Entonces A es isomorfo a una suma directa de grupos cíclicos de la forma

$$A \cong \bigoplus_{i=1}^{k} \left(\bigoplus_{j=1}^{t_i} C_{p_i^{n_{ij}}} \right)$$

donde $n_{i1} \geq n_{i2} \geq \dots n_{it_i} \geq 1$ y $n_{i1} + n_{i2} + \dots + n_{it_i} = r_i \quad \forall i$ y esta descomposición es única salvo el orden de los sumandos.

Esta descomposición se llama <u>descomposición cíclica primaria</u> de A y $\left\{ p_i^{n_{ij}} \mid \begin{array}{l} i \in \{1, \dots, k\} \\ j \in \{1, \dots t_i\} \end{array} \right\}$ es el conjunto de los llamados <u>divisores elementales de A</u>

DEMOSTRACIÓN:

Como A es abeliano, todos sus subgrupos son normales. En particular lo serán sus p_i-subgrupos de Sylow $P_1, P_2 \dots P_k$, que son únicos.

Entonces $A \cong P_1 \oplus P_2 \oplus \dots \oplus P_k$ donde $|P_i| = p_i^{r_i}$ $\forall i \in \{1, \dots, k\}$.

Ahora basta aplicar el Teorema 1 a cada sumando para obtener la descomposición anunciada.

Observación: La unicidad es consecuencia de la unicidad en el Teorema 1. 26/11/19

Observación: Cada P_i es la llamada <u>componente p_i-primaria de A</u>. $\forall i \in \{1, \dots, k\}$

Observación: Un grupo abeliano finito está completamente determinado, salvo isomorfismo, por su lista de divisores elementales. Esto es, dos grupos abelianos finitos del mismo orden son isomorfos si, y solo si, tienen los mismos divisores elementales.

Por tanto, para determinar, salvo isomorfismo, todos los grupos abelianos finitos, de un determinado orden, basta calcular todas las posibles listas de divisores elementales

Ejemplo: Determinar, todos los grupos abelianos, salvo isomorfismo, de orden 360 dando para cada uno de ellos su descomposición cíclica primaria.

$360 = 2^3 \cdot 3^2 \cdot 5$

$2^3, 3^2, 5 \rightsquigarrow A \cong C_8 \oplus C_9 \oplus C_5$

$2^2, 2, 3^2, 5 \rightsquigarrow A \cong (C_4 \oplus C_2) \oplus C_9 \oplus C_5$

$2, 2, 2, 3^2, 5 \rightsquigarrow A \cong (C_2 \oplus C_2 \oplus C_2) \oplus C_9 \oplus C_5$

$2^3, 3, 3, 5 \rightsquigarrow A \cong C_8 \oplus (C_3 \oplus C_3) \oplus C_5$

$2^2, 2, 3, 3, 5 \rightsquigarrow A \cong (C_4 \oplus C_2) \oplus (C_3 \oplus C_3) \oplus C_5$

$2, 2, 2, 3, 3, 5 \rightsquigarrow A \cong (C_2 \oplus C_2 \oplus C_2) \oplus (C_3 \oplus C_3) \oplus C_5$

Recordatorio: $C_n \oplus C_m \cong C_{nm} \iff m.c.d(n,m) = 1$

Teorema 3 (clasificación de los grupos abelianos finitos: descomposición cíclica): Si A es un grupo abeliano finito, entonces A es isomorfo a una suma directa de grupos abelianos cíclicos de la forma

$$A \cong C_{d_1} \oplus C_{d_2} \oplus \dots \oplus C_{d_t}$$

donde $d_1, d_2, \dots, d_t$ son enteros positivos tales que $d_1 d_2 \dots d_t = |A|$ y $d_i \mid d_j$ si $j \leq i$. Además, esta descomposición es única en el sentido de que si $A \cong C_{m_1} \oplus C_{m_2} \oplus \dots \oplus C_{m_s}$ con $m_1 m_2 \dots m_s = |A|$ y $m_i \mid m_j$ si $j \leq i$, entonces $s = t$ y $m_i = d_i \ \forall i \in \{1, \dots, t\}$.

Esta descomposición de A es la llamada <u>descomposición cíclica</u> y la lista $d_1, d_2, \dots, d_t$ es la llamada lista de <u>factores invariantes</u> de A.

DEMOSTRACIÓN:

Supongamos que $|A| = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ con p_i primo $\forall i \in \{1, \dots, k\}$, y consideremos la descomposición cíclica primaria de A.

Ejemplo: $A \cong (C_{2^2} \oplus C_2) \oplus (C_3 \oplus C_3 \oplus C_3) \oplus C_5 \cong$

$$\cong (C_{2^2} \oplus C_2 \oplus C_{2^0}) \oplus (C_3 \oplus C_3 \oplus C_3) \oplus (C_5 \oplus C_{5^0} \oplus C_{5^0})$$

Sea $t = \max\{t_1, t_2, \dots, t_k\}$, y sea $n_{il} = 0$ con $t_i < l \leq t$.

Consideremos la matriz de tamaño $t \times k$ siguiente:

$$\begin{pmatrix} p_1^{n_{11}} & p_2^{n_{21}} & \cdots & p_k^{n_{k1}} \\ p_1^{n_{12}} & p_2^{n_{22}} & \cdots & p_k^{n_{k2}} \\ \vdots & \vdots & \ddots & \vdots \\ p_1^{n_{1t}} & p_2^{n_{2t}} & \cdots & p_k^{n_{kt}} \end{pmatrix}$$

Entonces $A \cong$ suma directa de los grupos abelianos cíclicos de orden las entradas de las columnas de esta matriz $\cong$

$\cong$ suma directa de los grupos abelianos cíclicos de orden las entradas de las filas de esta matriz

$= (C_{p_1^{n_{11}}} \oplus C_{p_2^{n_{21}}} \oplus \ldots \oplus C_{p_k^{n_{k1}}}) \oplus (C_{p_1^{n_{12}}} \oplus C_{p_2^{n_{22}}} \oplus \ldots \oplus C_{p_k^{n_{k2}}}) \oplus \ldots \oplus$

$\ldots \oplus (C_{p_1^{n_{1t}}} \oplus C_{p_2^{n_{2t}}} \oplus \ldots \oplus C_{p_k^{n_{kt}}})$

Llamemos ahora

$d_1 = p_1^{n_{11}} p_2^{n_{21}} \ldots p_k^{n_{k1}}$

$d_2 = p_1^{n_{12}} p_2^{n_{22}} \ldots p_k^{n_{k2}}$ $\Rightarrow$ $A \cong C_{d_1} \oplus C_{d_2} \oplus \ldots \oplus C_{d_t}$

$\vdots$ donde los d_i satisfacen las

$d_t = p_1^{n_{1t}} p_2^{n_{2t}} \ldots p_k^{n_{kt}}$ condiciones del enunciado.

La unicidad es consecuencia de las unicidades de los Teoremas 1 y 2

Ejemplo: Sea A un grupo abeliano finito de orden 360. Dar sus posibles descomposiciones cíclicas.

$360 = 2^3 \cdot 3^2 \cdot 5$

D.C.P. | D.C.

$2^3, 3^2, 5 \rightsquigarrow A \cong C_8 \oplus C_9 \oplus C_5 \Rightarrow (2^3 \;\; 3^2 \;\; 5) =$

$\Rightarrow A \cong C_{360}$

$2^2, 2, 3^2, 5 \rightsquigarrow A \cong C_4 \oplus C_2 \oplus C_9 \oplus C_5 \Rightarrow \begin{pmatrix} 2^2 & 3^2 & 5 \\ 2 & 1 & 1 \end{pmatrix} \Rightarrow$

$\Rightarrow A \cong C_{180} \oplus C_2$

$2, 2, 2, 3^2, 5 \rightsquigarrow A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5 \Rightarrow \begin{pmatrix} 2 & 9 & 5 \\ 2 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix} \Rightarrow$

$\Rightarrow A \cong C_{90} \oplus C_2 \oplus C_2$

$2^3, 3, 3, 5 \rightsquigarrow A \cong C_8 \oplus C_3 \oplus C_3 \oplus C_5 \Rightarrow \begin{pmatrix} 8 & 3 & 5 \\ 1 & 3 & 1 \end{pmatrix} \Rightarrow$

$\Rightarrow A \cong C_{120} \oplus C_3$

$2^2, 2, 3, 3, 5 \Rightarrow A \cong C_4 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5 \Rightarrow \begin{pmatrix} 4 & 3 & 5 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow$

$\Rightarrow A \cong C_{60} \oplus C_6$

$2, 2, 2, 3, 3, 5 \Rightarrow A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5 \Rightarrow \begin{pmatrix} 2 & 3 & 5 \\ 2 & 3 & 1 \\ 2 & 1 & 1 \end{pmatrix} \Rightarrow$

$\Rightarrow A \cong C_{30} \oplus C_6 \oplus C_2$

Ejemplo: orden 48

$48 = 2^4 \cdot 3$

$2^4, 3 \rightsquigarrow A \cong C_{16} \oplus C_3 \cong C_{48}$

$\begin{pmatrix} 16 & , 3 \end{pmatrix} \quad d_1 = 48$

$2^3, 2, 3 \rightsquigarrow A \cong C_8 \oplus C_2 \oplus C_3 \cong C_{24} \oplus C_2$

$\begin{pmatrix} 8 & 3 \\ 2 & 1 \end{pmatrix} \quad \begin{matrix} d_1 = 24 \\ d_2 = 2 \end{matrix}$

$2^2, 2^2, 3 \rightsquigarrow A \cong C_4 \oplus C_4 \oplus C_3 \cong C_{12} \oplus C_4$

$\begin{pmatrix} 4 & 3 \\ 4 & 1 \end{pmatrix} \quad \begin{matrix} d_1 = 12 \\ d_2 = 4 \end{matrix}$

$2^2, 2, 2, 3 \rightsquigarrow A \cong C_4 \oplus C_2 \oplus C_2 \oplus C_3 \cong C_{12} \oplus C_2 \oplus C_2$

$\begin{pmatrix} 4 & 3 \\ 2 & 1 \\ 2 & 1 \end{pmatrix} \quad \begin{matrix} d_1 = 12 \\ d_2 = 2 \\ d_3 = 2 \end{matrix}$

$2, 2, 2, 2, 3 \rightsquigarrow A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \cong C_6 \oplus C_2 \oplus C_2 \oplus C_2$

$\begin{pmatrix} 2 & 3 \\ 2 & 1 \\ 2 & 1 \\ 2 & 1 \end{pmatrix} \quad \begin{matrix} d_1 = 6 \\ d_2 = 2 \\ d_3 = 2 \\ d_4 = 2 \end{matrix}$

29/11/19

Observaciónes

- Si p es un primo tal que $p|n \Rightarrow \exists i \in \{1, \dots, t\} \mid p|d_i$
- si $p|d_i \Rightarrow p|d_j$ con $j \leq i$ (porque $d_i|d_j$)
- Si $p|d_i \Rightarrow p|d_1$ (cualquier primo que divida a n aparece en la factorización del primer factor invariante d_1)

Ejemplo: Si $|A| = n = p_1 p_2 \dots p_t$, hay un único factor invariante $d_1 = n \Rightarrow A \cong C_n \cong C_{p_1} \oplus C_{p_2} \oplus \dots \oplus C_{p_t}$

Ejemplo: Sea $|A| = 180 = 2^2\cdot 3^2\cdot 5$

- $d_1 = 2^2\cdot 3^2\cdot 5 \Rightarrow A \overset{D.C.}{\cong} C_{180} \overset{D.C.P}{\cong} C_4 \oplus C_9 \oplus C_5$

- $d_1 = 2\cdot 3^2\cdot 5$
  $d_2 = 2$ $\Rightarrow A \overset{D.C}{\cong} C_{90} \oplus C_2 \overset{D.C.P}{\cong} C_2 \oplus C_2 \oplus C_9 \oplus C_5$

- $d_1 = 2^2\cdot 3\cdot 5$
  $d_2 = 3$ $\Rightarrow A \overset{D.C}{\cong} C_{60} \oplus C_3 \overset{D.C.P}{\cong} C_4 \oplus C_3 \oplus C_3 \oplus C_5$

- $d_1 = 2\cdot 3\cdot 5$
  $d_2 = 2\cdot 3$ $\Rightarrow A \overset{D.C}{\cong} C_{30} \oplus C_6 \cong C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$

Teorema 1: $|A| = p^n$, $n \geq 1$

$A \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \dots \oplus C_{p^{\beta_t}}$ $\Big|$ $\beta_1 + \dots + \beta_t = n$, $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$

Definición: Si p es un primo, un p-grupo abeliano abeliano E se dice que es <u>p-elemental</u> si $x^p = 1$ $\forall x \in E$ ($\Rightarrow$ $o(x) = p$ $\forall x \neq 1$)

Ejemplo: $C_p \oplus C_p \oplus \dots \oplus C_p$ es p-elemental

(De hecho, si el Teorema 1 es cierto, todo grupo p-elemental es de esa forma).

Lema: Sea E un p-grupo abeliano finito p-elemental con $|E| = p^k$. Entonces $\forall x \in E$ $\exists M < E$ / $E \cong M \oplus \langle x\rangle$

DEMOSTRACIÓN:

Como E abeliano, $M \trianglelefteq E$, $\langle x\rangle \trianglelefteq E$

- Si $x = 1$, tomamos $M = E$ ($E \cong E \oplus 1$)
- Si $x \neq 1$, consideramos $\Sigma = \{H < E \mid x \notin H\}$
  $\Sigma \neq \emptyset$ porque $1 \in \Sigma$.

Tomemos $M \in \Sigma$ de grado mayor y consideramos E/M

$|E/M| = [E:M] \,\big|\, |E| = p^k \Rightarrow [E:M] = p^i$, $i > 0$ (si $i = 0$, $M = E$)

Veamos que $i = 1$. Para ello, supuesto que $i > 1$, veamos que llegamos a una contradicción con la maximalidad de M.

Consideramos entonces que $|E/M| = [E:M] = p^i$, $i > 1$.

Como $|E/M|$ también es p-elemental $\Rightarrow$

$\Rightarrow \exists\, yM \in E/M$ con $o(yM) = p$ y tal que $yM \notin \langle xM \rangle$ $\left(\langle xM \rangle \not\subseteq E/M \right)$

Además, $xM \notin \langle yM \rangle$ porque si $xM \in \langle yM \rangle \Rightarrow$

$\Rightarrow \langle xM \rangle = \langle yM \rangle$ al tener ambos el mismo orden $p \Rightarrow$

$\Rightarrow yM \in \langle xM \rangle$ CONTRADICCIÓN.

Consideramos ahora la proyección $\begin{aligned} q: E &\longrightarrow E/M \\ e &\longmapsto eM \end{aligned}$ y

$q^*(\langle yM \rangle) < E$, que verifica:

- $x \notin q^*(\langle yM \rangle)$ Si $x \in q^*(\langle yM \rangle) \Rightarrow q(x) = xM \in \langle yM \rangle$ CONTRADICCIÓN
- $M \subsetneq q^*(\langle yM \rangle)$ porque $y \notin M$ (ya que $o(yM) = p$) pero $y \in q^*(\langle yM \rangle)$ (ya que $q(y) = yM \in \langle yM \rangle$).

Por tanto, $q^*(\langle yM \rangle) \in \sum$ y es "mayor" que M.

CONTRADICCIÓN.

Por tanto $[E:M] = p \Rightarrow p = \dfrac{|E|}{|M|} \Rightarrow |M| = p^{k-1}$

Además, por el 2º Teorema de isomorfía, $\dfrac{M\langle x \rangle}{\langle x \rangle} \cong \dfrac{M}{M \cap \langle x \rangle}$,

pero $M \cap \langle x \rangle = 1$. Veamos esto:

Si $\exists\, x^j \in M$, $o(x) = p$ $\Rightarrow \langle x^j \rangle = \langle x \rangle < M \Rightarrow x \in M$ CONTRADICCIÓN

Por tanto, $|M\langle x \rangle| = |M| \cdot |\langle x \rangle| = p^{k-1} \cdot p = p^k \Rightarrow$

$$\left.\begin{aligned} \Rightarrow M\langle x \rangle &= E \\ M \cap \langle x \rangle &= 1 \end{aligned}\right\} \Rightarrow E \cong M \oplus \langle x \rangle$$

DEMOSTRACIÓN DEL TEOREMA 1:

Haremos inducción sobre n con $|A| = p^n$

- Si $n = 1 \Rightarrow A \cong C_p$ con $t = 1$ y $\beta_1 = 1$
- Supongamos $n > 1$ y el resultado cierto para todo grupo abeliano finito de orden p^m con $m < n$ y demostrémoslo para n.

Consideremos la aplicación $\begin{aligned} \varphi: A &\longrightarrow A \\ x &\longmapsto x^p \end{aligned}$ (homomorfismo porque A es abeliano).

Sea $K = \ker(\varphi) = \{x \in A \mid x^p = 1\} < A$ y $H = \mathrm{Im}(\varphi) = \{x^p \mid x \in A\} < A$

Se tiene entonces que:

- K y A/H son p-elementales
  K es claro y si $xH \in A/H$ $\quad (xH)^p = x^pH = H$
- Por el 1er Teorema de isomorfía
  $A/K \cong H \Rightarrow [A:K] = |H|$
- $|A/K| = [A:H] = \frac{|A|}{|H|} = \frac{|A|}{[A:K]} = |K|$

Como A es un p-grupo $\Rightarrow K \neq 1$ por el Teorema de Cauchy.

Por tanto, $[A:H] = |K| \neq 1 \Rightarrow H \lneq A \Rightarrow |H| = p^m$, $m < n$

Por hipótesis de inducción:

$H \cong C_{p^{\gamma_1}} \oplus C_{p^{\gamma_2}} \oplus \dots \oplus C_{p^{\gamma_r}}$ con $\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_r \geq 1$, $\gamma_1 + \gamma_2 + \dots + \gamma_r = m$

Elegimos $h_1, h_2, \dots, h_r \in H$ tales que $\langle h_i \rangle \cong C_{p^{\gamma_i}}$

Por tanto $o(h_i) = p^{\gamma_i}$ $\forall i \in \{1, \dots r\}$.

Tenemos entonces que $H \cong \langle h_1 \rangle \oplus \langle h_2 \rangle \oplus \dots \oplus \langle h_r \rangle$

Como $H = Im(\varphi)$, $\exists\, g_1, g_2, \dots, g_r \in A$ tales que $\varphi(g_i) = g_i^{\,p} = h_i$

Como $o(h_i) = p^{\gamma_i} \Rightarrow o(g_i) = p^{\gamma_i + 1}$ $\forall i \in \{1, \dots, r\}$

Consideramos entonces $A_0 = \langle g_1, g_2, \dots, g_r \rangle < A$ siendo $H < A_0$, y se verifica

1 - $A_0 \cong \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \dots \oplus \langle g_r \rangle \Rightarrow |A_0| = p^{\gamma_1 + \gamma_2 + \dots + \gamma_r + r} = p^{m+r}$

2 - $A_0/H \cong \langle g_1 H \rangle \oplus \langle g_2 H \rangle \oplus \dots \oplus \langle g_r H \rangle$ y es p-elemental de orden p^r

3 - $H \cap K \cong \langle h_1^{p^{\gamma_1 - 1}} \rangle \oplus \langle h_2^{p^{\gamma_2 - 1}} \rangle \oplus \dots \oplus \langle h_r^{p^{\gamma_r - 1}} \rangle$ y es p-elemental de orden p^r

Entonces distinguimos dos casos:

<u>1er caso</u>: Si $K < H \Rightarrow K \cap H = K$ $\qquad$ 2/12/19

Usando 3-, $|K| = |K \cap H| = p^r \Rightarrow [A:H] = p^r$
Por 2-, $|A_0/H| = [A_0 : H] = p^r$
$\Big\}\ A_0 < A \Rightarrow A = A_0$

Utilizando 1-, $A \cong \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \dots \oplus \langle g_r \rangle \cong C_{p^{\gamma_1+1}} \oplus C_{p^{\gamma_2+1}} \oplus \dots \oplus C_{p^{\gamma_r+1}}$

y esa es la descomposición requerida porque como

$\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_r \Rightarrow \underbrace{\gamma_1 + 1}_{\beta_1} \geq \underbrace{\gamma_2 + 1}_{\beta_2} \geq \dots \geq \underbrace{\gamma_r + 1}_{\beta_r} \geq 1$

$\beta_1 + \beta_2 + \dots + \beta_r = \gamma_1 + 1 + \gamma_2 + 1 + \dots + \gamma_r + 1 = m + r = |A_0| = |A|$

<u>2º caso:</u> Si $K \not\subset H \Rightarrow \exists x \in K \mid x \notin H$

Consideremos la clase $xH \in A/H$, que es p-elemental.

Por tanto, $o(xH) = p$.

Ahora, por el lema previo aplicado a A/H y a $xH \in A/H$,

$\exists M/H < A/H \mid A/H = M/H \oplus \langle xH \rangle$ con $x \notin M$

Como $M/H \cap \langle xH \rangle = 1 \Rightarrow xH \notin M/H$ siendo $o(x) = p$ (pq $x \in K$)

Entonces $M \cap \langle x \rangle = 1$. Veamos esto:

Si $x^j \in M$ con $j > 0 \Rightarrow \langle x^j \rangle = \langle x \rangle \subseteq M \Rightarrow x \in M$ CONTRADICCIÓN.

Además, $|A/H| = |M/H| \cdot p \Rightarrow \frac{|A|}{|H|} = \frac{|M|}{|H|} \cdot p \Rightarrow |A| = |M| \cdot p \Rightarrow$

$\Rightarrow |A| = |M| \cdot |\langle x \rangle| = |M\langle x \rangle| \Rightarrow A = M\langle x \rangle \Rightarrow$

$\Rightarrow A \cong M \oplus \langle x \rangle$ con $\langle x \rangle \cong C_p$

y ahora basta aplicar inducción para M para obtener la descomposición requerida.