Ejercicios GyA - Cap 5

Jose Antonio Lorencio Abril

5 Grupos Abelianos Finitos

5.1 Sumas directas

5.1.1 Demostrar las siguientes afirmaciones sobre un grupo abeliano A

1. **Toda subfamilia de una familia independiente de subgrupos de A es independiente.**

   Esto es muy sencillo. Sea $\{B_i : i \in I\}$ una familia independiente, y sea $J \subset I$. Sabemos que si $\sum_{i\in I} b_i = 0 \implies b_i = 0,\ \forall i$. Si suponemos que $\sum_{j\in J} b_j = 0$ pero no todos los b_j son 0, entonces esta misma suma añadiendo los $b_k : k \in I \setminus J$ todos a 0, da 0, por lo que el b_j anterior debe ser $0\#$.

2. **Una familia de subgrupos es independiente precisamente si toda subfamilia finita suya lo es.**

   Como los elementos de $\sum_{i\in I} B_i$ tienen la forma $\sum_{i\in I} b_i$, con $b_i \in B_i$ y todos nulos excepto una cantidad finita, entonces si toda subfamilia finita es independiente, la familia total ha de serlo. Pues si una suma da 0, a lo sumo una cantidad finita de elementos pueden ser no nulos, pero estos están en una subfamilia finita, que es independiente, por lo que son todos nulos.

3. **Si la familia $\{B_i : i \in I\}$ de subgrupos de un grupo abeliano A es independiente y otro subgrupo B_0 de A verifica $B_0 \cap (\oplus_{i\in I} B_i) = 0$, entonces la familia $\{B_0\} \cup \{B_i : i \in I\}$ también es independiente.**

   Supongamos que $\sum_{i\in I\cup\{0\}} b_i = 0$. Entonces:

   - $b_0 = 0 \implies \sum_{i\in I} b_i = 0 \implies b_i = 0,\ \forall i \in I \implies b_i = 0,\ \forall i \in I \cup \{0\}$ ✓
   - $b_0 \neq 0 \implies \sum_{i\in I} b_i = -b_0 \implies -b_0 \in \oplus_{i\in I} B_i \implies b_0 \in \oplus_{i\in I} B_i \implies B_0 \cap (\oplus_{i\in I} B_i) \neq 0\#$

   Por lo que la suma da 0 de forma única y la familia es independiente.

4. **Si $A = \oplus_{i\in I} B_i$ entonces cada B_j es un sumando directo de A con complemento $\oplus_{i\neq j} B_i$.**

   Es evidente que $A = B_j \oplus (\oplus_{i\neq j} B_i)$, falta ver que la intersección es 0. Pero, si la intersección no es 0, si llamamos $0 \neq b_j \in B_j \cap (\oplus_{i\neq j} B_i)$, entonces $b_j - b_j = 0 = 0 + (0 + ... + 0)$ de forma que encontramos dos maneras de expresar el 0 como suma de elementos de estos conjuntos $\#$ Contradicción, pues la familia es independiente.

5. **Si $A = B \oplus C$ y $B = B_1 \oplus ... \oplus B_n$ y $C = C_1 \oplus ... \oplus C_m$, entonces $A = B_1 \oplus ... \oplus B_n \oplus C_1 \oplus ... \oplus$**

$$A = B \oplus C = B_1 \oplus ... \oplus B_n \oplus C_1 \oplus ... \oplus C_m$$

6. **Si $A = B \oplus C$ entonces la aplicación $A \to C$ dada por $b + c \mapsto c$ es un homomorfismo suprayectivo de grupos con núcleo B. En particular $C \simeq \frac{A}{B}$.**

   Está bien definida por la unicidad de la representación de los elementos de A como suma de elementos de B y C.

   ¿Es homomorfismo? Sean $x, y \in A \implies x = b_1 + c_1,\ y = b_2 + c_2$, entonces

   $$f(x+y) = f(b_1 + b_2 + c_1 + c_2) = c_1 + c_2 = f(b_1 + c_1) + f(b_2 + c_2) = f(x) + f(y) \checkmark$$

   ¿Es suprayectiva? Sí, dado $c \in C,\ c = f(0 + c)$.

   ¿El núcleo es B?

   $$f(b + c) = 0 \iff c = 0 \iff b + c = b \in B$$

   La isomorfía nos la da el primer teorema de isomorfía para grupos.

7. **Si B es un sumando directo de A, cualquier complemento directo suyo es isomorfo a $\frac{A}{B}$. Por tanto, aunque un sumando directo puede tener distintos complementos directos, todos ellos son isomorfos entre sí.**

   Consecuencia directa del apartado anterior.

5.1.2 Sea A un grupo abeliano. Demostrar que als siguientes condiciones son equivalentes para un subconjunto X de A.

1. **X es linealmente independiente sobre $\mathbb{Z}$, es decir, si $k_1, ..., k_n$ son enteros y $k_1x_1 + ... + k_nx_n = 0$ con $x_1, ..., x_n$ elementos distintos de X entonces $k_1 = ... = k_n = 0$**

2. **Todo elemento de X tiene orden infinito y la familia de grupos cíclicos $\{\langle x \rangle : x \in X\}$ es independiente**

5.1.3 Sea V un espacio vectorial sobre el cuerpo de los números complejos y consideremos V como grupo aditivo. Demostrar que un subconjunto de V es linealmente independiente sobre $\mathbb{Z}$ si, y solo si, lo es sobre $\mathbb{Q}$.

' $\implies$ ' Si lo es sobre $\mathbb{Z}$, lo es también sobre $\mathbb{Q}$.

' $\impliedby$ ' Si lo es sobre $\mathbb{Q}$, eso quiere decir que si $\sum_{i \in I} q_i v_i = 0 \implies q_i = 0,\ \forall i$. Cada v_i tendrá coeficientes en $\mathbb{Q}$, pero si multiplicamos por el mcm de los denominadores, el vector será proporcional y estará en $\mathbb{Z}$. Llamemos a estos vectores v_i', claramente son independientes en $\mathbb{Z}$, pues de no serlo, tampoco lo serían en $\mathbb{Q}$ los v_i.

5.1.4 Decidir sobre la verdad o falsedad de las siguientes afirmaciones para el caso en que $A = (\mathbb{Z}^n, +)$.

1. **Todo subconjunto linealmente independiente de A tiene a lo sumo n elementos.**

   Verdadero, $\mathbb{Z}$ no puede ponerse como suma directa de subgrupos. Al ser abeliano, todo subgrupo es cíclico, por lo que es generado por algún elemento. Pero en $\mathbb{Z}$, dados dos elementos, la intersección de los subgrupos generados por estos no es 0, pues están todos los múltiplos comunes de ambos elementos. Entonces, los únicos conjuntos linealmente independientes que podemos tomar son de la forma $\{\mathbb{Z}^{m_i}\},\ \sum_i m_i \leq n$.

2. **Todo subconjunto generador de A tiene al menos n elementos.**

   Verdadero, el menor generador que podemos encontrar es $\{\langle 1,0,...,0\rangle, \langle 0,1,0,...,0\rangle, ..., \langle 0,...,0,1\rangle\}$. Ya que no puede haber un único elemento que genere el producto cartesiano.

   Por ejemplo, supongamos que $\mathbb{Z}\times\mathbb{Z} = \langle a,b\rangle$, entonces $b = ka$, luego

   - Si $a \neq b$, entonces$(b,b) = (ka,b) \notin \langle a,b\rangle$, pues $kb \neq b$
   - Si $a = b$, entonces $2 = ka$, $5 = ma$, y así $(2,5) = (ka,ma) \notin \langle a,a\rangle$

3. **Todo subconjunto linealmente independiente de A con n elementos es conjunto generador de A.**

   Falso. $\{\langle 2,0,...,0\rangle, \langle 0,2,0,...,0\rangle, ..., \langle 0,...,0,2\rangle\}$ tiene n elementos, es linealmente independiente, pero no es generador, pues $(1,0,...,0)$ no está en el conjunto que genera.

4. **Todo subconjunto generador de A con n elementos es linealmente independiente.**

   Un conjunto generador debe poder expresar todo elemento de A como suma de elementos de sus subconjuntos. Por ser A abeliano, todo subgrupo es cíclico. Luego lo genera un elemento. Entonces para todo $(x_1,...,x_n) \in A$, se tiene que

$$\begin{cases} k_1a_{11} + k_2a_{21} + ... + k_na_{n1} = x_1 \\ k_1a_{12} + k_2a_{22} + ... + k_na_{12} = x_2 \\ ... \\ k_1a_{1n} + k_2a_{2n} + ... + k_na_{nn} = x_n \end{cases}$$

5.1.5 Demostrar que todo subgrupo de $\mathbb{Z}^n$ es isomorfo a $\mathbb{Z}^k$ para algún $k \leq n$.

5.1.6 Encontrar un subgrupo B de $A = \mathbb{Z}_{16}^*$ tal que $\frac{A}{B} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. ¿Cuántos subgrupos así eres capaz de encontrar? ¿Alguno de ellos es un sumando directo de A?

$$16 = 2^4 \implies \phi(16) = 16\frac{2-1}{2} = 8$$

El cardinal de $\mathbb{Z}_2 \times \mathbb{Z}_2$ es 4. Por tanto, B debe tener cardinal 2.
Los subgrupos de cardinal 2 son $\langle 15\rangle$, $\langle 7\rangle$ y $\langle 9\rangle$.

$$\frac{A}{\langle 15\rangle} = \{(1,15),(3,13),(5,11),(7,9)\}, \quad \frac{A}{\langle 7\rangle} = \{(1,7),(3,5),(9,15),(11,13)\}, \quad \frac{A}{\langle 9\rangle} = \{(1,9),(3,11),(5,13),(7$$

con tablas

	1	3	5	7		1	3	9	11		1	3	5	7
1	1	3	5	7	1	1	3	9	11	1	1	3	5	7
3		7	1	5	3		7	11	1	3		1	7	5
5			7	3	9			1	3	5			1	3
7				1	11				9	7				1

respectivamente.
La tabla de $\mathbb{Z}_2 \times \mathbb{Z}_2$ es

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$		$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$			$(0,0)$	$(1,0)$
$(1,1)$				$(0,0)$

Es decir, que la isomorfía es

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \frac{A}{\langle 9\rangle}$$

5.3.22 Un subgrupo propio H de un grupo G que no está contenido en ningún otro subgrupo propio de G se dice que es maximal en G. Para un grupo abeliano finito A, demostrar:

1. **Los subgrupos maximales son precisamente los de índice primo**
2. **A tiene exactamente 2 subgrupos maximales si y solo si A es cíclico y $|A|$ tiene exactamente dos divisores primos.**

5.4 Grupos indescomponibles y $p-$grupos

5.4.1 Demostrar que si G es un grupo finito, entonces $Exp(G) \mid |G|$. ¿En qué caso se daría la igualdad?

Se tiene que, $\forall a \in G,\ a^{Exp(G)} = 1$. Esto quiere decir que $|\langle a \rangle| = Exp(G)$, por el teorema de Lagrange, $Exp(G) \mid |G|$.

La igualdad se daría precisamente en el caso de que G es cíclico.

5.4.2 Sea G de período finito y sea H un subgrupo de G. Demostrar que $Exp(H)$ y $p(G/H)$ son divisores de $Exp(G)$. En particular, si $g \in G \implies |g| \mid Exp(G)$.

Evidentemente, $Exp(H) \leq Exp(G)$. Por el ejercicio anterior $Exp(H) \mid |H|$.

Está claro que $a^{Exp(H)} = 1,\ \forall a \in H$. Pero, también $a^{Exp(G)} = 1$.

Supongamos que $Exp(H) \nmid Exp(G)$, sabemos que no son coprimos, por lo anterior. Sea $d = mcd(Exp(H), Exp(G)) < Exp(H)$.

5.4.3 Demostrar que el período de un grupo finito, no necesariamente abeliano, es el mcm de los órdenes de sus elementos. Demostrar que si A es un grupo abeliano generado por un subconjunto finito X y todos los elementos de X tienen orden finito entocnes A es periódico y $Exp(A) = mcm(|x| : x \in X)$. Dar un ejemplo que muestre que esto último no se verifica en grupos no abelianos.

Sabemos que $a^{Exp(G)} = 1 \implies |a| \mid Exp(G)$. Esto ocurre para todo a, luego $mcm | Exp(G)$.

Pero, además

$$a^{mcm} = a^{|a|\frac{mcm}{|a|}} = 1^{\frac{mcm}{|a|}} = 1$$

Luego $Exp(G) \leq mcm$.

Por tanto, $Exp(G) = mcm$.

Si A es abeliano generado por un subconjunto finito, entonces sea $m = mcm(|x| : x \in X)$. Entonces $a^m = 1,\ \forall a \in A$

Y dado $g \in G$, se tiene que $g = a_1^{n_1} ... a_k^{n_k}$, luego G tiene menos elementos o tantos como $card(X)^m$, que es finito.

Además

$$g^m = a_1^{mn_1} ... a_k^{mn_k} = 1...1 = 1$$

Luego G es periódico.

5.4.4 Para un grupo arbitrario G, denotamos por $t(G)$ el conjunto de los elementos de orden finito de G. Demostrar que si A es un grupo abeliano entonces $t(A)$ es un subgrupo de A y $t(A) = \oplus_{p\in\mathbb{P}} t_p(A)$. Dar un ejemplo de un grupo G en el que $t(G)$ no sea un subgrupo de G.

- 1 tiene orden finito ✓
- Sean $a, b \in t(A)$ con $a^n = 1,\ b^m = 1$, entonces

$$(ab)^{nm} = abab...ab = aa...ab...bb = a^n b^m = 1\checkmark$$

- Si $a^n = 1 \implies 1 = a^{-n} = \left(a^{-1}\right)^n < \checkmark$

La segunda parte no la tengo clara

5.4.6 Demostrar que el grupo aditivo $(A, +)$ de un anillo A es de torsión precisamente si la característica de A es diferente de 0. Si A es un dominio, demostrar que las condiciones son equivalentes a que $t(A) \neq 0$. En particular, si A es dominio entonces $t(A)$ es 0 ó A. Calcular $t(\mathbb{Z}[X]/(2X))$.

A es de torsión $\implies na = 0,\ \forall a \in A \implies car(A)\,|n \implies car(A) \neq 0$
Si $car(A) \neq 0 \implies car(A)\,a = 0,\ \forall a \in A \implies A$ es de torsión.

5.5 Descomposiciones primarias e invariantes

5.5.1 Demostrar que si $(d_1, ..., d_k)$ es la lista de factores invariantes de un grupo entonces el exponente de A es d_1.

El exponente es el mcm de los órdenes de los elementos de A, pero también d_1 lo es.

5.5.2 Demostrar que, si $n \in \mathbb{Z}^+$ es libre de cuadrados, entonces todo grupo abeliano finito de orden n es cíclico.

Por ser libre de cuadrados, es $n = p_1...p_k$, con p_i primo.
Si $k = 1$, es cíclico y ya está.
Si $k > 1$, el teorema de Cauchy asegura que $\forall i,\ \exists a_i / |a_i| = p_i$.
Entonces

$$A = t_{p_1}(A) \oplus ... \oplus t_{p_k}(A) = \langle a_1\rangle \oplus ... \oplus \langle a_k\rangle$$

es una descomposición primaria, y

$$\mathbb{Z}_n = \langle p_1\rangle \oplus ... \oplus \langle p_k\rangle$$

luego las listas de divisores elementales serán iguales y se tiene la isomorfía. Por tanto, A es cíclico.

5.5.3 Sea p un número primo. Demostrar que, salvo isomorfismos, los únicos grupos de orden p^2 son $\mathbb{Z}_{p^2}$y $\mathbb{Z}_p \times \mathbb{Z}_p$.

Para todo $a \in A$, se tiene que $|a|\,|p^2$. Por tanto, $|a| \in \left\{1, p, p^2\right\}$.

Por otro lado, $Exp(A) = mcm\{|a| : a \in A\}$. No puede ser $Exp(A) = 1$ porque entonces el grupo sería trivial.

Entonces $Exp(A) \in \left\{p, p^2\right\}$. Si es p^2, entonces hay algún elemento con orden p^2, porque si no todos tendrían orden $1, p$ y el mcm sería p. Por lo que ese elemento genera A y es cíclico e isomorfo a $\mathbb{Z}_p$.

Si es p, entonces $A/\langle a\rangle$ tiene orden p y se tiene que hay $b \notin \langle a\rangle$ con $A = \langle a\rangle_p \oplus \langle b\rangle_p \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

5.5.4 Describir, salvo isomorfismos, los grupos abelianos de órden 8. Ver las isomorfías para $\mathbb{Z}_{15}^*,\ \mathbb{Z}_{16}^*,\ \mathbb{Z}_{20}^*,\ \mathbb{Z}_{24}^*,\ \mathbb{Z}_{30}^*$.

Los elementos pueden tener orden 1,2,4,8.

Si algún elemento tiene orden 8, entonces es cíclico y es isomorfo a $\mathbb{Z}_8$.

Si ningún elemento tiene orden 8:

- No puede ocurrir que todos tengan orden 1, el grupo sería trivial
- Si algún elemento tiene orden 4, entonces $A/\langle a\rangle$ tiene orden 2, y $A \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$
- Si ningún elemento tiene orden 4, entonces $A \simeq \mathbb{Z}_2 \times c_2 \times \mathbb{Z}_2$

$\mathbb{Z}_{15}^*$: $|2| = 4$ y ninguno tiene orden 8. Es isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$

$\mathbb{Z}_{16}^*$: $|3| = 4$ y ninguno tiene orden 8. Es isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$

$\mathbb{Z}_{20}^*$: $|3| = 4$ y ninguno tiene orden 8. Es isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$

$\mathbb{Z}_{24}^*$: todos tienen orden 2. Es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$\mathbb{Z}_{30}^*$: $|3| = 4$ y ninguno tiene orden 8. Es isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$

5.5.5 Grupos abelianos de órdenes 12,16,20,24 salvo isom.

- $12 = 2^2 \cdot 3$. Los grupos son $\mathbb{Z}_{12}$ y $\mathbb{Z}_6 \times \mathbb{Z}_2$
- $16 = 2^4$. Los grupos son $\mathbb{Z}_{16},\ \mathbb{Z}_8 \times \mathbb{Z}_2,\ \mathbb{Z}_4 \times \mathbb{Z}_4,\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $20 = 2^2 \cdot 5$. Los grupos son $\mathbb{Z}_{20}$ y $\mathbb{Z}_{10} \times \mathbb{Z}_2$
- $24 = 2^3 \cdot 3$. Los grupos son $\mathbb{Z}_{24},\ \mathbb{Z}_2 \times \mathbb{Z}_{12},\ \mathbb{Z}_4 \times \mathbb{Z}_6,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$

5.5.6 Calcular todos los grupos abelianos de orden 420 salvo isomorfismos y sus descomposiciones invariantes y primarias.

$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$

Los grupos son $\mathbb{Z}_{420}$ y $\mathbb{Z}_2 \times \mathbb{Z}_{210}$.

- $\mathbb{Z}_{420}$ descomposición primaria: $\mathbb{Z}_{420} \simeq \mathbb{Z}_4 \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_7 = \langle 1 \mod 4\rangle_4 \times \langle 1 \mod 5\rangle_5 \times \langle 1 \mod 7\rangle_7 \times \langle 1 \mod 3\rangle_3 = \langle 105\rangle_4 \times \langle 336\rangle_5 \times \langle 120\rangle_7 \times \langle 280\rangle_3$

  Descomposición invariante: $\mathbb{Z}_{420}$

- $\mathbb{Z}_2 \times \mathbb{Z}_{210}$ primaria: $t_2(\mathbb{Z}_2) \times t_2(\mathbb{Z}_{210}) \times t_3(\mathbb{Z}_{210}) \times t_5(\mathbb{Z}_{210}) \times t_7(\mathbb{Z}_{210}) = \mathbb{Z}_2 \times \langle 105\rangle_2 \times \langle 70\rangle_3 \times \langle 160\rangle_5 \times \langle 120\rangle_7$

  La invariante queda

  $$\mathbb{Z}_{210} \times \mathbb{Z}_2$$

5.5.7 Demostrar el recíproco del Teorema de Lagrange para grupos abelianos finitos. Es decir, demostrar que un grupo abeliano de orden n tiene un subgrupo de orden m para divisor m de n.

Podemos suponer que A es un $p-$grupo para algún p primo, porque en el caso general, si $n = |A| = p_1^{a_1}...p_k^{a_k}$, entonces $A = t_{p_1}(A) \oplus ... \oplus t_{p_k}(A)$. Si se cumple para cada $t_p(A)$, sea $m : m|n \implies m = p_1^{b_1}...p_k^{b_k}$, $0 \le b_i \le a_i$. Tomo un subgrupo $B_i \subset t_{p_i}(A) : |B_i| = p^{b_i}$ y $\oplus_i^k B_i$ tiene orden m.

Si A es $p-$grupo, $A = \langle x_1\rangle_{p_1^{a_1}} \oplus ... \oplus \langle x_k\rangle_{p_k^{a_k}}$, $m|\,|A| = p^n \implies m = p^l,\ 0 \le l \le n$. Tomo, para $i = 1, ..., k$, $b_i :\ 0 \le b_i \le a_i$ y $\sum_{i=1}^k b_i = l$. Como $\langle x_i\rangle$ es cíclico, $\exists y_i \in \langle x_i\rangle : |\langle y_i\rangle| = p^{b_i}$ y, por lo tanto $\oplus_1^k \langle y_i\rangle$ tiene orden m.

5.5.8 Sean L, M, N grupos abelianos finitos con $L \oplus N \simeq M \oplus N$. Demostrar que $L \simeq M$.

Por ser isomorfos, las descomposiciones primarias de $L \oplus N$ y de $M \oplus N$ son semejantes, además, la descomposición de $L \oplus N$ es la descomposición de L en suma directa con la de N, y lo mismo ocurre con la otra:

$$L_1 \oplus ... \oplus L_k \oplus N_1 \oplus ... \oplus N_m \simeq M_1 \oplus ... \oplus M_k \oplus N_1 \oplus ... \oplus N_m \implies L_1 \oplus ... \oplus L_k \simeq M_1 \oplus ... \oplus M_k$$

luego $L \simeq M$.

5.5.9 Calcular las descomposiciones primaria e invariante del grupo aditivo $\mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108}$, el grupo multiplicativo $\mathbb{Z}_{21}^* \times \mathbb{Z}_{27}^* \times \mathbb{Z}_{29}^*$ y el producto de ambos.

$20 = 2^2 \cdot 5$, $40 = 2^3 \cdot 5$, $108 = 2^2 3^3$, luego

$$\mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108} \simeq t_2(\mathbb{Z}_{20}) \oplus t_2(\mathbb{Z}_{40}) \oplus t_2(\mathbb{Z}_{108}) \oplus t_5(\mathbb{Z}_{20}) \oplus t_5(\mathbb{Z}_{40}) \oplus t_3(\mathbb{Z}_{108}) =$$

$$= \langle 5,0,0\rangle_4 \oplus \langle 0,25,0\rangle_8 \oplus \langle 0,0,77\rangle_4 \oplus \langle 16,0,0\rangle_5 \oplus \langle 0,16,0\rangle_5 \oplus \langle 0,0,28\rangle_{27}$$

O sea, que la descomposición primaria es

$$\begin{array}{lll} \mathbb{Z}_8 & \oplus\mathbb{Z}_4 & \oplus\mathbb{Z}_4 \\ \oplus\mathbb{Z}_{27} & & \\ \oplus\mathbb{Z}_5 & \oplus\mathbb{Z}_5 & \end{array}$$

Y la invariante es

$$\mathbb{Z}_{1080} \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_4$$

En el multiplicativo, tenemos que $\mathbb{Z}_{21}^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_7^* \simeq \langle -1,1\rangle_2 \times \langle 1,-1\rangle_2 \times \langle 1,2\rangle_3$, $\mathbb{Z}_{27}^* = \mathbb{Z}_{3^3}^*$, que tiene orden $2 \cdot 3^2$, luego $\mathbb{Z}_{27}^* \simeq \langle -1\rangle_2 \times \langle 4\rangle_9$ y, por último, $\mathbb{Z}_{29}^*$ tiene orden $28 = 2^2 \cdot 7$, y es $\mathbb{Z}_{29}^* \simeq \langle 17\rangle_4 \times \langle 25\rangle_7$, es decir

$$\mathbb{Z}_{21}^* \times \mathbb{Z}_{27}^* \times \mathbb{Z}_{29}^* \simeq \begin{array}{llll} \langle 1,1,17\rangle_4 & \times\langle 8,1,1\rangle_2 & \times\langle 1,-1,1\rangle_2 & \times\langle 13,1,1\rangle_2 \\ \times\langle 1,4,1\rangle_9 & \times\langle 16,1,1\rangle_3 & & \\ \times\langle 1,1,25\rangle_7 & & & \end{array} \simeq \langle 1,4,19\rangle_{252} \times \langle 2,1,1\rangle_6 \times \langle 1,-1,1\rangle_2 \times \langle 13$$

Para sacar la descomposición del producto, juntamos las descomposiciones primarias, teniendo en cuenta que $A \oplus B \simeq A \times B$. Entonces, si llamamos A a este grupo producto, es

$$A \simeq \begin{array}{lllllll} \mathbb{Z}_8 & \times\mathbb{Z}_4 & \times\mathbb{Z}_4 & \times\mathbb{Z}_4 & \times\mathbb{Z}_2 & \times\mathbb{Z}_2 & \times\mathbb{Z}_2 \\ \times\mathbb{Z}_{27} & \times\mathbb{Z}_9 & \times\mathbb{Z}_3 & & & & \\ \times\mathbb{Z}_5 & \times\mathbb{Z}_5 & & & & & \\ \times\mathbb{Z}_7 & & & & & & \end{array} \simeq \mathbb{Z}_{7560} \times \mathbb{Z}_{180} \times \mathbb{Z}_{12} \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

5.5.10 Grupos abelianos de órdenes 30, 60, 72, 90, 180, 360, 720, 1830.

- $30 = 2 \cdot 3 \cdot 5$, el único es $\mathbb{Z}_{30}$
- $60 = 2^2 \cdot 3 \cdot 5$, son $\mathbb{Z}_{60}$ y $\mathbb{Z}_2 \times \mathbb{Z}_{30}$
- $72 = 2^3 \cdot 3^2$, son $\mathbb{Z}_{72}$, $\mathbb{Z}_2 \times \mathbb{Z}_{36}$, $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18}$, $\mathbb{Z}_4 \times \mathbb{Z}_{18}$, $\mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_3$, $\mathbb{Z}_6 \times \mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$, $\mathbb{Z}_{24} \times \mathbb{Z}_3$ (quizás falte alguno)
- $90 = 2 \cdot 3^2 \cdot 5$, son $\mathbb{Z}_{90}$, $\mathbb{Z}_3 \times \mathbb{Z}_{30}$
- $180 = 2^2 \cdot 3^2 \cdot 5$, son $\mathbb{Z}_{180}$, $\mathbb{Z}_2 \times \mathbb{Z}_{90}$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{30}$, $\mathbb{Z}_3 \times \mathbb{Z}_{60}$, $\mathbb{Z}_6 \times \mathbb{Z}_{30}$
- $1830 = 2 \cdot 3 \cdot 5 \cdot 61$, solo es $\mathbb{Z}_{1830}$

5.5.12 Demostrar que la lista de factores invariantes de $\mathbb{Z}_n \oplus \mathbb{Z}_m$ es $(mcm(n,m),\ mcd(n,m))$ ó (nm).

Si n, m son coprimos, entonces, por el trm chino de los restos, $\mathbb{Z}_n \oplus \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ y es cíclico, por lo que su lista de factores invariantes es (nm).

Si n, m no son coprimos, entonces se tiene, si $d = mcd(n,m)$, que $\mathbb{Z}_n \simeq \mathbb{Z}_{\frac{n}{d}} \oplus \mathbb{Z}_d$ y $\mathbb{Z}_m \simeq \mathbb{Z}_{\frac{m}{d}} \oplus \mathbb{Z}_d$, luego $\mathbb{Z}_n \oplus \mathbb{Z}_m \simeq \mathbb{Z}_{\frac{n}{d}} \oplus \mathbb{Z}_d \oplus \mathbb{Z}_{\frac{m}{d}} \oplus \mathbb{Z}_d$, ahora bien, $\frac{n}{d}$ y $\frac{m}{d}$ sí que son coprimos, por lo que esto último es isomorfo a $\mathbb{Z}_{\frac{nm}{d^2}} \oplus \mathbb{Z}_d \oplus \mathbb{Z}_d$.

Si $d = p_1^{d_1}...p_k^{d_k}$ y $\frac{nm}{d^2} = p_1^{x_1}...p_k^{x_k}$, entonces, si $d_i \neq 0 \implies x_i = 0$, podemos suponer que los primeros m primos son los que tienen d_i no nulo, y la descomposición primaria (cambiando filas, esto no afectará a la invariante) queda

$$\begin{array}{cc} \langle a_{11}\rangle_{p_1^{d_1}} & \oplus \langle a_{12}\rangle_{p_1^{d_1}} \\ \multicolumn{2}{c}{...} \\ \oplus \langle a_{m1}\rangle_{p_m^{d_m}} & \oplus \langle a_{m2}\rangle_{p_m^{d_m}} \\ \oplus \langle a_{m+1,1}\rangle_{p_{m+1}^{x_{m+1}}} & \\ \multicolumn{2}{c}{...} \\ \oplus \langle a_{k,1}\rangle_{p_k^{x_k}} & \end{array}$$

y la descomposición invariante es

$$\langle a\rangle_{d\cdot\frac{nm}{d^2}} \oplus \langle b\rangle_d$$

pero $d\cdot\frac{nm}{d^2} = \frac{nm}{d} = mcm(n,m)$. Es decir, que la lista de factores invariantes es $(mcm(n,m),\ mcd(n,m))$.

5.5.13 Demostrar que si A es un $p-$grupo abeliano que es la suma directa de n grupos cíclicos no triviales, entonces la ecuación $px = 0$ tiene exactamente p^n soluciones en A.

$A = \oplus_1^n \langle a_i\rangle_{p^{x_i}}$ con $a_i \neq 0\ \forall 1, ..., n \implies x_i > 0,\ \forall i$

- Si $y_i \in \langle a_i\rangle, y_j \in \langle a_j\rangle$ cumplen $py_i = 0,\ py_j = 0 \implies p(x_i + x_j) = 0$
- Si tengo p soluciones de $px = 0$ en cada $\langle a_i\rangle$, entonces tengo p^n soluciones en A
- Cada $\langle a_i\rangle$ tiene p soluciones:

  $px = 0 \implies |x|\,|p \implies |x| = 1$ *ó* p, la primera solución es $x = 0$. Buscamos ahora $|x| = 0$ y sabemos que $|\langle n\cdot a_i\rangle| = \frac{|a_i|}{mcd(n,a_i)} = \frac{p^{x_i}}{mcd(n,p^{x_i})} = p \iff mcd(n,p^{x_i}) = p^{x_i-1} \iff x = j\cdot p^{x_i-1},\ j = 1, ..., p-1$, pues a partir de ahí se repiten. Por tanto, hay p soluciones y lo tenemos.

5.5.14 Sea G un $p-$grupo abeliano finito en el que la ecuación $px = 0$ tiene a lo sumo p soluciones. Demostrar que G es cíclico. Demostrar que también es cíclico un grupo abeliano finito en el que la ecuación $px = 0$ tenga a lo sumo p soluciones para todo primo p.

G será suma directa de n grupos cíclicos, por lo que esa ecuación tendrá p^n soluciones. Por tanto, n es 1 y G es cíclico.

Para la segunda afirmación $G = t_{p_1}(G) \oplus ... \oplus t_{p_k}(G)$ con $p_1, ..., p_k$ primos distintos. Sea $s(p,G)$ el número de soluciones de $px = 0$ en G.

1. $s(p,G) = \prod_1^k s(p, t_{p_i}(G))$: similarmente a como hicimos en el ejercicio anterior

2. dado A un $p-$grupo, $s(q,G)=1$ si $q\neq p$ (q primo): $q\cdot 0=0 \implies$ al menos hay una solución.
   Si $g\in G\setminus\{0\}$, entonces $qg=0 \iff |g|=p^l|q \iff l=0$, por ser q primo#

3. $s(p_i,G)=s(p_i,t_{p_i}(G))$: evidente por 1 y 2

4. $t_{p_i}(G)$ cíclico para todo i:
   $s(p_i,t_{p_i}(G))=s(p_i,G)\leq p_i$, entonces la primera parte del ejercicio nos asegura que es cíclico

5. G cíclico

   Por el teorema chino de los restos, pues es suma directa de cíclicos con órdenes coprimos dos a dos

5.5.15 Sea A un grupo abeliano finito que satisface la siguiente propiedad: Para todo entero positivo n, el conjunto $\{a\in A: na=0\}$ tiene a lo sumo n elementos. Demostrar que A es cíclico. Deducir que todo subgrupo finito del grupo de unidades de un cuerpo es cíclico.

La primera parte es obvia teniendo en cuenta el ejercicio anterior.

Para la segunda, en notación multiplicativa, buscamos $x^n=1$ y esto tiene a lo sumo n soluciones, pues x^n-1 es un polinomio de grado n en un cuerpo.

5.5.16 Sea p primo. Demostrar que si G es un grupo abeliano finito en el que todo elemento no nulo tiene orden p, entonces $G\simeq\mathbb{Z}_p^n$ para algún n.

Sea $p^n=|G|$. Por hipótesis todo elemento de G es solución de $px=0$ (hay p^n soluciones). Descomponemos el grupo como

$$G=\oplus_1^k\langle a_i\rangle_{p^{x_i}}$$

por el 5.3.13, habrá p^k soluciones de $px=0$. Por tanto $k=n$. Como los $\langle a_i\rangle$ no son triviales, se debe cumplir $\sum_1^n x_i=n,\ x_i>0\ \forall i$, luego solo puede ser $x_i=1,\ \forall i$ y cada $\langle a_i\rangle$ tiene orden p, por lo que es isomorfo a $\mathbb{Z}_p$, y a$G=\oplus_1^n\langle a_i\rangle_p\simeq\mathbb{Z}_p^n$.