UNA CONEXIÓN ENTRE LOS NÚMEROS DE FERMAT Y LOS GRUPOS FINITOS

Diana Lucero Pinzón Ortiz

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2005

UNA CONEXIÓN ENTRE LOS NÚMEROS DE FERMAT Y LOS GRUPOS FINITOS

Diana Lucero Pinzón Ortiz

Monografía presentada como requisito para optar al título de Licenciada en Matemáticas

Director

Marlio Paredes Gutiérrez

Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2005

Con amor incondicional
a Nicolle Alejandra
inspiración de mi vida.

AGRADECIMIENTOS

Doy mi más profundo agradecimiento:

- A **Dios**, por todas las oportunidades que me ha dado para seguir adelante, por darme la sabiduría y fortaleza para afrontar cada prueba que ha puesto en mi camino.
- A **mis padres Luis José y Myriam Lucía y a mis hermanos Oscar, Carlos y Jorge**, quienes con ayuda, comprensión y con su apoyo incondicional y permanente, contribuyeron a la culminación de mi carrera.
- A **Edgar Giovanny**, quien con su gran cariño y confianza me llenó de fortaleza y me impulso a cumplir cada uno de mis objetivos.
- Al profesor **Marlio Paredes**, por su colaboración y por su acertada orientación durante el desarrollo en esta monografía.
- A **los profesores**, por su contribución en mi formación académica.
- A **mis familiares y amigos**, que de una u otra forma estuvieron conmigo, brindándome su compañía, ayuda y cooperación en el transcurso de mi carrera .
- A la **UIS**, institución que me dio la oportunidad de escalar otro peldaño en mi formación profesional.

TITULO: UNA CONEXIÓN ENTRE LOS NÚMEROS DE FERMAT Y LOS GRUPOS FINITOS[*]

AUTOR: PINZÓN ORTIZ Diana Lucero[**]

PALABRAS CLAVES: Grupos abelianos finitos, números de Fermat, subconjuntos de orden perfecto, grupo minimal SOP.

DESCRIPCIÓN

En este trabajo de monografía se analizan los grupos con subconjuntos de orden perfecto (SOP) los cuales hacen parte de la teoría de los **grupos abelianos finitos** y presentan un comportamiento muy especial, puesto que a partir de un grupo SOP dado podemos generar nuevos grupos con dicha propiedad; ya sean más grandes o más pequeños del grupo SOP dado. Estos grupos SOP más pequeños reciben el nombre de grupos SOP minimales.

Siendo precisamente estos grupos la base para el teorema principal, el cual afirma que existe un número finito de ellos salvo isomorfismos. En la demostración de este teorema se utilizan técnicas de teoría de números elemental y su conclusión es consecuencia directa de que el número F_5 es compuesto, donde este número hace parte de la secuencia numérica definida por Fermat más conocida como **los números de Fermat**.

El trabajo consta de tres capítulos: Preliminares, subconjuntos de orden perfecto y por último los números de Fermat y los grupos finitos. En el primer capítulo se recopilan los conceptos y resultados necesarios para el buen entendimiento de este trabajo. En el segundo capítulo se define la propiedad de tener subconjuntos de orden perfecto, algunos resultados básicos y diversos ejemplos. Al final de este capítulo se define un grupo con subconjuntos de orden perfecto que tienen una característica especial que es ser un grupo SOP minimal. Finalmente, en el tercer capítulo se presenta el teorema principal donde se hace evidente la conexión entre los números de Fermat y los grupos finitos.

---

[*]Monografía

[**]Facultad de Ciencias. Escuela de matemáticas. Director: Marlio Paredes Gutiérrez.

TITLE: A CONNECTION BETWEEN FERMAT NUMBERS AND FINITE GROUPS[*]

AUTHOR: PINZÓN ORTIZ Diana Lucero[**]

KEY WORDS: Finite abelian groups, Fermat numbers, perfect order subsets, minimal SOP group.

DESCRIPTION In this work, we study the groups with perfect order subsets (SOP) which are included in the theory of **finite abelian groups** and have some very special properties; because from a SOP group we can generate new groups with the same property bigger or smaller than the group SOP given. This smaller SOP groups are called minimal SOP group.

These groups are the base to the principal theorem which confirms that exists a finite number of them up to isomorphisms. In the proof of this theorem elementary number theory techniques are used and its conclusion is a direct consequence that the number F_5 is composite, and it is part of the number sequence defined by Fermat which is know as the **Fermat numbers.**

This work contain three chapters: Preliminaries, perfect order subsets, and the last, Fermat numbers and finite groups. The first chapter compiles concepts and requirements to understand this work. In the second chapter is defined the property about have perfect order subsets, some basic results and several examples. At the end of this chapter it is defined a group with perfect order subsets that have an special characteristic what is to be, a minimal SOP group. Finally, in the third chapter, it is presented the principal theorem in which the connection between Fermat numbers and finite groups is evident.

[*]Monograph

[**]Faculty of sciences. Mathematics school. Director: Marlio Paredes Gutiérrez.

Contenido

Introducción **1**

1. Preliminares **3**

1.1. Definiciones y ejemplos 3

1.2. El teorema de Lagrange 14

1.3. Subgrupos normales 16

1.4. Homomorfismos 19

1.5. Teorema fundamental de los grupos abelianos finitos 22

1.6. Números de Fermat 25

1.7. La función ϕ de Euler 26

2. Subconjuntos de orden perfecto **28**

2.1. Definiciones y propiedades 28

2.2. Tres teoremas importantes 35

3. Los números de Fermat y los grupos finitos **39**

3.1. Teorema principal 40

Bibliografía **47**

Introducción

Ninguna colección de números presenta tantos misterios como la de los números primos. La relativa facilidad con que es posible demostrar que hay una infinidad de ellos, contrasta con la enorme dificultad para encontrar una manera rápida y eficiente para comprobar que un número es primo.

Es por esto, que muchos matemáticos han intentado idear una forma para hallar todos los números primos. En el siglo XVII, Pierre de FERMAT (1601-1665, Francia) definió la secuencia de los números $F_n = 2^{2^n} + 1$ para $n \geqslant 0$, conocidos hoy como **los números de Fermat**.

Fermat mostró que F_n es primo para cada $n \leqslant 4$ y conjeturó que F_n es primo para todo $n \in \mathbb{N}$. Casi cien años después Leonhard EULER (1707-1783, Suiza) demostró en 1732 que F_5 es un número compuesto, puesto que $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = (641)(6700417)$, y además no es el único número compuesto de la forma F_n.

Es precisamente el hecho de que F_5 sea un número compuesto el que nos interesa en este momento ya que nos brinda la posibilidad para resolver un problema relacionado con la teoría de grupos y más explícitamente los grupos abelianos finitos, cuya solución es consecuencia directa de este hecho y se basa en técnicas muy propias de la teoría de números elemental; haciéndose así evidente la conexión entre los números de Fermat y los grupos abelianos finitos.

El presente trabajo está basado en el artículo **A curious connection between Fer-**

mat numbers and finite groups ([3]), está organizado en tres capítulos: en el primer capítulo se recopilan algunas definiciones y resultados básicos de teoría de números y de teoría de grupos los cuales nos brindan la información necesaria que se usará en los siguientes dos capítulos.

En el segundo capítulo se presentan algunos aspectos generales de la teoría de los grupos abelianos finitos, se muestran varios ejemplos, se demuestran algunas propiedades básicas, se define y se analiza la propiedad de tener subconjuntos de orden perfecto y algunos resultados importantes para el siguiente capítulo.

Finalmente en el capítulo tres enunciaremos el teorema principal e incluiremos su respectiva demostración que hace parte de la teoría de grupos abelianos finitos, encontrando allí la aplicación de que el número F_5 es compuesto. Es por esto el interés que nos ocupa en este momento el conocer y dar a conocer la solución a este problema, ya que así podemos enlazar uno de los conceptos intuitivos más importantes en las matemáticas como lo son los grupos abelianos finitos con una de las disciplinas más fascinantes del universo matemático como lo es la teoría de números.

CAPÍTULO 1

Preliminares

1.1. Definiciones y ejemplos

Dados dos conjuntos G y A, toda aplicación definida en el conjunto producto $G \times G$ con valores en A se dice que es una **operación binaria** definida en G. Una operación binaria en G se dice **cerrada** si su recorrido es un subconjunto de G.

Definición 1.1. Un conjunto G con una operación binaria * en él definida se dice que es un **grupo** si cumple las siguientes propiedades:

G1. La operación binaria * es cerrada en G, esto es $g_1 * g_2 \in G$ para todo $g_1, g_2 \in G$.

G2. La operación binaria * es asociativa, esto es, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ para todo $g_1, g_2, g_3 \in G$.

G3. Existe un elemento neutro $e \in G$ tal que $e * g = g * e = g$ para todo $g \in G$.

G4. Para todo elemento $g \in G$ existe un elemento $g' \in G$ denominado inverso de g, tal que $g * g' = g' * g = e$. En adelante g' se denotará de la forma g^{-1}.

Si además la operación binaria * cumple con la propiedad conmutativa; es decir, $g_1 * g_2 = g_2 * g_1$ para todo $g_1, g_2 \in G$, diremos que $(G, *)$ es un **grupo abeliano o conmutativo** (el nombre de abeliano se debe al matemático noruego Niels H. Abel quien contribuyó a la unificación de la teoría de grupos).
El elemento e del axioma G3 es único y se llama identidad del grupo. El elemento g^{-1} del axioma G4 denominado inverso de g también es único respecto a la operación * (ver [2]).

Ejemplo 1.1. Dado un número entero positivo n, mostraremos que siempre existe al menos un grupo con n elementos. Para ello haremos uso del concepto de congruencia.

Definición 1.2. Sea n es un entero positivo, dados dos números enteros a y b, se dice a **es congruente con** b **módulo** n, y se simboliza mediante $a \equiv b(mod\, n)$ si su diferencia, $a - b$, es un múltiplo de n. Es decir, $a - b = kn$, para algún $k \in \mathbb{Z}$.

Esta relación de congruencia definida en el conjunto $\mathbb{Z}$ de los números enteros es reflexiva ya que para todo $a \in \mathbb{Z}$, $a - a = 0 = 0n$; también es simétrica ya que si $a - b = kn$, entonces $b - a = (-k)n$; finalmente es transitiva ya que si $a - b = kn$ y $b - c = sn$, tenemos que $a - c = (a - b) + (b - c) = kn + sn = (k + s)n$. Por lo tanto, la relación de congruencia es una relación de equivalencia.
Podemos por tanto, considerar el conjunto cociente de $\mathbb{Z}$ mediante esta relación de equivalencia, el cual se simboliza por $\mathbb{Z}_n$ y se denomina el conjunto de las clases de congruencia módulo n.
Los elementos del conjunto $\mathbb{Z}_n$ son, pues, clases de equivalencia que se denotan mediante $[a]$, donde

$$[a] = \{x \in \mathbb{Z} : x \equiv a(mod\, n)\},$$
$$[a] = \{x \in \mathbb{Z} : x = a + kn \text{ para algún } k \in \mathbb{Z}\}.$$

Dada una clase de equivalencia $[a] \in \mathbb{Z}_n$ siempre podemos elegir un representante x de $[a]$, de manera que $[a] = [x]$ y $0 \leqslant x < n$; solamente dividimos a entre n y tomamos x como el residuo de esta división. Entonces, podemos escribir:

$$\mathbb{Z}_n = \{[0], [1], [2], ...[n-1]\}.$$

Sobre $\mathbb{Z}_n$ se puede definir una suma de clases residuales por $[a] + [b] = [a + b]$.
Para mostrar que $(\mathbb{Z}_n, +)$ es grupo y además es abeliano debemos comprobar que:

1. La operación $[a] + [b] = [a + b]$ está bien definida.
   Si $[a] = [a']$ y $[b] = [b']$ entonces $a \equiv a'(mod\, n)$ y $b \equiv b'(mod\, n)$ por la definición de congruencia se deduce que existen números enteros r, s tal que $a - a' = rn$ y $b - b' = sn$. Por tanto, $(a + b) - (a' + b') = (a - a') + (b - b') = (r + s)n$. Luego $a + b \equiv a' + b'(mod\, n)$; es decir, $[a] + [b] = [a'] + [b']$.

2. Para demostrar que la operación es cerrada basta observar que por la misma definición la suma de dos clases $[a]$ y $[b]$ es nuevamente una clase ($[a + b]$).

3. La operación es asociativa.

$$([a] + [b]) + [c] = [a + b] + [c] = [a + b + c],$$
$$[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c].$$

4. Existe el elemento identidad de $\mathbb{Z}_n$.

   Debido a que $0 \equiv n(mod\, n)$, tenemos que $[0] = [n]$.Por lo tanto,

$$[a] + [0] = [a + 0] = [a],$$
$$[0] + [a] = [0 + a] = [a].$$

5. Para cada $[a]$ existe $[x]$ tal que $[a] + [x] = [x] + [a] = [0]$.
   Para probar esta propiedad es suficiente tomar $x = n - a$ pues en tal caso tenemos

$$[a] + [n - a] = [a + n - a] = [n] = [0],$$
$$[n - a] + [a] = [n - a + a] = [n] = [0].$$

6. La operación es conmutativa.

   Es fácil mostrar esta propiedad gracias a la conmutatividad en los números enteros.

$$[a] + [b] = [a + b],$$
$$[b] + [a] = [b + a] = [a + b].$$

Con la operación de suma de clases residuales módulo n, $(\mathbb{Z}_n, +)$ es un grupo abeliano. Así queda demostrado que para todo entero positivo n siempre existe un grupo con n elementos.

De ahora en adelante no se indicará más, salvo cuando sea necesario, la operación con respecto a la cual un conjunto es un grupo.

Definición 1.3. Si G es un grupo finito, entonces **el orden de** G es el número de elementos en G, el cual se simboliza $|G|$. En general, para cualquier conjunto finito S, $|S|$ es el número de elementos en S.

Ejemplo 1.2. En el ejemplo 1.1 vimos que $(\mathbb{Z}_n, +)$ es un grupo abeliano y está definido de la siguiente forma

$$\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}.$$

Luego el orden de $\mathbb{Z}_n$ es n.

Dado que un grupo G es un conjunto y existen subconjuntos de este, nos preguntamos ¿dentro de un grupo se encuentran subconjuntos que también cumplen está propiedad? La respuesta es sí, y este es el contenido de la siguiente definición.

Definición 1.4. Dado un grupo G y un subconjunto H no vacío de G, diremos que H es un **subgrupo de** G, si H es un grupo con respecto a la operación definida en G.

Puesto que la operación definida en G es asociativa, esta operación también será asociativa en cualquier subconjunto H de G; se tiene entonces que H es un subgrupo de G si se cumple las tres condiciones siguientes:

1. La operación definida en G es cerrada en H.

2. El elemento neutro de G pertenece a H.

3. Si $x \in H$, su inverso x^{-1}, también pertenece a H.

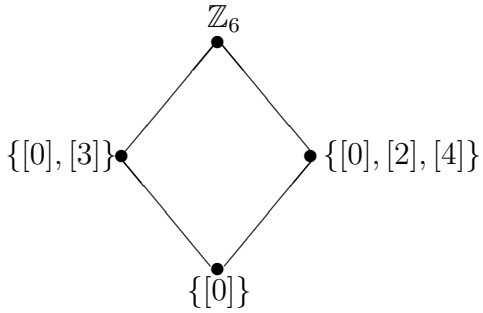
Ejemplo 1.3. Sea el grupo $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$
Realizando la tabla que describe la estructura del grupo nos será más fácil reconocer sus subgrupos.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Todo subgrupo de $\mathbb{Z}_6$ debe ser cerrado bajo la suma, debe contener $[0]$ el cual es el elemento identidad de $\mathbb{Z}_6$ y cada elemento del grupo debe tener su inverso dentro del subgrupo; por tanto, observando la tabla los únicos subgrupos de $\mathbb{Z}_6$ son:

- $\mathbb{Z}_6$
- $\{[0]\}$
- $\{[0], [3]\}$
- $\{[0], [2], [4]\}$

Es fácil ver que por ejemplo $\{[0], [4]\}$ no es subgrupo de $\mathbb{Z}_6$ pues $\{[0], [4]\}$ no es cerrado bajo la suma, ya que $[4] + [4] = [2] \notin \{[0], [4]\}$.
Un gráfico en el cual se representan todos los subgrupos de $\mathbb{Z}_6$ se llama el retículo de los subgrupos. A continuación observamos el retículo de $\mathbb{Z}_6$:



Puesto que todo conjunto es subconjunto de sí mismo, es claro que todo grupo es subgrupo de sí mismo. Por otra parte $\{e\}$ el conjunto formado por el elemento identidad de G también es subgrupo de G. De esta forma todo grupo G tiene al menos dos subgrupos G y $\{e\}$ conocidos como **el subgrupo impropio y el subgrupo trivial de** G respectivamente. Todos los otros subgrupos se denominan **subgrupos propios no triviales**.

Ejemplo 1.4. Del ejemplo anterior tenemos que:

- $\mathbb{Z}_6$ es el subgrupo impropio de $\mathbb{Z}_6$.
- $\{[0]\}$ es el subgrupo trivial de $\mathbb{Z}_6$.
- $\{[0],[3]\}$ y $\{[0],[2],[4]\}$ son los únicos subgrupos propios no triviales de $\mathbb{Z}_6$.

Se puede distinguir dentro de los conjuntos los términos minimal y menor cuando estos se aplican a un conjunto S que tenga alguna propiedad. Un subconjunto H de S es minimal con respecto a la propiedad si H tiene la propiedad y ningún subconjunto $K \subset H, K \neq H$ tiene la propiedad. Si H tiene la propiedad y $H \subseteq K$ para todo subconjunto K con la propiedad entonces H es el conjunto menor con la propiedad. Pueden haber muchos subconjuntos minimales, pero sólo un subconjunto menor. En el ejemplo 1.3 al observar el retículo de $\mathbb{Z}_6$ vemos que $\{[0],[3]\}$ y $\{[0],[2],[4]\}$ son todos los subgrupos no triviales minimales de $\mathbb{Z}_6$. Sin embargo, $\mathbb{Z}_6$ no contiene un subgrupo no trivial menor. Por otro lado, si estamos trabajando con elementos de un conjunto podemos distinguir términos en los elementos tales como máximo, mínimo, maximal y minimal.
En este caso, dado un conjunto A con una relación de orden $\leqslant$, un elemento $a \in A$ se dice:

a. **máximo**: si $b \leqslant a$ para todo $b \in A$.

b. **mínimo**: si $a \leqslant b$ para todo $b \in A$.

c. **maximal**: si $a \leqslant b$ implica que $b = a$.

d. **minimal**: si $b \leqslant a$ implica que $b = a$.

En un conjunto ordenado puede no haber máximos o mínimos, ni tampoco elementos maximales o minimales; pero si el máximo y el mínimo existen estos son únicos, pues si a y b son máximos en $(A, \leq)$ se tiene que $a \leq b$ y $b \leq a$ y, por tanto, $a = b$. Análogamente si a y b son mínimos.
Dentro del conjunto de los números naturales encontramos una propiedad muy importante conocida como el principio del mínimo ó el principio de la buena ordenación.
Principio de buena ordenación: Todo subconjunto no vacío de $\mathbb{N}$ posee un mínimo. (la demostración la encontramos en [5])

Teorema 1.1. *Sea G un grupo y sea $x \in G$. Entonces*

$$H = \{x^n : n \in \mathbb{Z}\}$$

es un subgrupo de G y es el menor subgrupo de G que contiene a x, esto es, cada subgrupo que contiene a x, contiene a H.

Demostración.
Puesto que $x^r \cdot x^s = x^{r+s}$ para $r, s \in \mathbb{Z}$, el producto en G de dos elementos de H está en H. Así, H es cerrado bajo la operación de grupo de G. Además, $x^0 = e$ de modo que $e \in H$ y para $x^r \in H$, $x^{-r} \in H$ y $x^{-r} \cdot x^r = e$. Todas las condiciones se satisfacen y, por tanto, H es subgrupo de G.
Claramente $x = x^1 \in H$. Para demostrar que es el menor tomamos un subgrupo que contenga a x, este debe contener a $x \cdot x$, lo que se denota por x^2. Entonces debe contener a $x^2 \cdot x$ lo que se denota por x^3. En general, debe contener a x^n. Estas potencias enteras positivas de x conforman un conjunto cerrado bajo la operación de G. Además, un subgrupo que contenga a x debe contener a x^{-1} y por tanto a $x^{-1} \cdot x^{-1}$, lo que se denota por x^{-2}, y en general debe contener a x^{-m} con $m \in \mathbb{Z}_+$. Por último, debe contener la identidad $e = x \cdot x^{-1}$. Por tanto, un subgrupo de G que contenga a x, debe contener todos los elementos x^n para todo $n \in \mathbb{Z}$. Es decir, un subgrupo que contenga a x debe contener a H. □

Definición 1.5. El subgrupo

$$H = \{x^n : n \in \mathbb{Z}\}$$

se llama **subgrupo de G generado por** x, y se simboliza mediante $\langle x \rangle$.

Definición 1.6. Dado un grupo G y un elemento $x \in G$, definimos **el orden de** x como el número de elementos que posee el subgrupo generado por x, si éste es finito.

Ejemplo 1.5. Sea el grupo aditivo $\mathbb{Z}_3 = \{[0], [1], [2]\}$ entonces

- $\langle [0] \rangle = \{[0]\}$
- $\langle [1] \rangle = \{[1], [2], [0]\}$
- $\langle [2] \rangle = \{[2], [1], [0]\}$
  Luego
- [0] tiene orden 1.
- [1] tiene orden 3.
- [2] tiene orden 3.

El subgrupo generado por un elemento x y el orden de x se encuentran muy relacionados. A continuación, presentamos dos propiedades donde se hace evidente esta relación.

Teorema 1.2. *Sea G un grupo finito y x un elemento de G; existe un entero positivo n tal que $x^n = e$ y el subgrupo generado por x es:*

$$\langle x \rangle = \{x, x^2, x^3, ..., x^{n-1}, x^n = e\}.$$

Demostración.
Dado que G es un grupo finito, el conjunto $\{x, x^2, x^3, ..., x^k, ...\}$ debe tener repeticiones; existen pues enteros positivos i, j tal que $x^i = x^j$. De aquí se deduce que

$$e = x^i * x^{-i} = x^j * x^{-i} = x^{j-i}.$$

Como podemos suponer que $j > i$ tomamos $n = j - i$, aplicando el principio de la buena ordenación al conjunto $\{t \in \mathbb{N} | x^t = e\} \subseteq \mathbb{N}$ se puede escoger n como el menor entero positivo tal que $x^n = e$. Además

$$\langle x \rangle = \{x, x^2, ..., x^k, ..., x^{-1}, x^{-2}, ..., x^{-k}, ...\}.$$

Si $k > n$, por el algoritmo de la división tomamos $c, r \in \mathbb{N}$ tal que $k = cn + r$ con $0 \leqslant r < n$; entonces $x^k = x^{cn} \cdot x^r = x^r$. Esto nos dice que los elementos x^k, con $k > n$, pueden ser eliminados de $\langle x \rangle$ puesto que aparecen repetidos. De manera similar se puede razonar para probar que los elementos de la forma x^{-i} aparecen repetidos: basta tomar $c, r \in \mathbb{Z}$ tal que $-i = cn + r$ con $0 \leqslant r < n$. □

Teorema 1.3. *Si G es un grupo finito y x un elemento de G, el orden de x coincide con el menor entero positivo k tal que $x^k = e$, además $\langle x \rangle = \{x, x^2, ..., x^k = e\}$ y todos los elementos de este conjunto son distintos.*

Demostración.
De la proposición anterior existe k tal que $x^k = e$, por el principio de la buena ordenación tomamos k como el menor entero positivo que cumple $x^k = e$.
Debemos ver que $x, x^2, ..., x^{k-1}, x^k = e$ son todos distintos, en efecto, si tomamos $x^i = x^j$ con $1 \leqslant i < j \leqslant k$ tenemos que

$$x^{j-i} = x^j * x^{-i} = x^i * x^{-i} = e.$$

Lo cual es una contradicción, ya que $j - i < k$ y k es el menor entero positivo tal que $x^k = e$. Por lo tanto, $x^i \neq x^j$ para todo $1 \leqslant i < j \leqslant k$. □

Teorema 1.4. *Sea G un grupo y $x \in G$ un elemento de orden finito k; si m es un entero positivo tal que $x^m = e$, se tiene que k divide a m.*

Demostración.
Si $x^m = e$, escribimos $m = ck + r$ con $0 \leqslant r < k$, pot tanto, $e = x^m = x^{ck} \cdot x^r = e^c \cdot x^r = x^r$ como $0 \leqslant r < k$ y k es el menor entero positivo que satisface $x^k = e$, de la igualdad anterior se deduce que $r = 0$ y por tanto $m = ck$, lo que prueba que k divide a m. □

Definición 1.7. Un grupo G se dice **cíclico** si existe al menos un elemento $x \in G$ tal que el subgrupo generado por x es G, es decir; $\langle x \rangle = G$. En este caso x se denomina un **generador** de G.

Ejemplo 1.6. $(\mathbb{Z}_n, +)$ es un grupo cíclico con generador [1].

Existen propiedades importantes acerca de la teoría de los grupos cíclicos, y este es el contenido de los siguientes resultados.

Teorema 1.5. *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración.
Sea G un grupo generado por el elemento g y H un subgrupo de G. Si $H = \{e\}$ entonces $H = \langle e \rangle$. Si $H \neq \{e\}$ entonces existe k entero positivo tal que $g^k \in H$; consideremos m como el más pequeño de los k enteros positivos; este mínimo existe debido al principio de la buena ordenación.
Como $g^m \in H$ y H es un subgrupo de G, se deduce que $\langle g^m \rangle \subset H$. Para demostrar la otra inclusión consideremos un elemento h de H; como h es también un elemento de G y G es cíclico existe un entero s tal que $h = g^s$, por el algoritmo de la división(ver [5]) podemos escribir $s = cm + r$ con $0 \leqslant r < m$; entonces $h = g^s = g^{cm} \cdot g^r$, de donde se deduce que $g^r = g^s \cdot (g^m)^{-c} = h(g^m)^{-c}$ como tanto h como g^m son elementos de H, deducimos que g^r es también un elemento de H. Como r es un entero no negativo más pequeño que m, de la definición de m se deduce que $r = 0$; entonces

$$h = g^s = g^{cm} = (g^m)^c \in \langle g^m \rangle.$$

Por lo tanto, $H \subset \langle g^m \rangle$. Esto demuestra que $H = \langle g^m \rangle$ y, en consecuencia, H es cíclico. □

Teorema 1.6. *Todo grupo cíclico es abeliano.*

Demostración.
Sea G un grupo cíclico y sea a un elemento generador de G, es decir

$$G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}.$$

Si g_1 y g_2 son dos elementos cualesquiera de G, existen enteros r y s tales que: $g_1 = a^r$ y $g_2 = a^s$. Entonces

$$g_1 \cdot g_2 = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = g_2 \cdot g_1,$$

de modo que G es abeliano. □

Cuando el orden del grupo cíclico es finito se puede decidir el orden de cada uno de sus elementos a partir del orden del grupo; además, en este caso, el número de subgrupos del grupo coincide con el número de divisores del orden del grupo. A continuación se enunciará el teorema básico con respecto a los generadores de subgrupos para los grupos cíclicos finitos.

Teorema 1.7. *Sea G un grupo y x un elemento de G de orden n; el orden de x^k es $n/(n,k)$ donde (n,k) es el máximo común divisor de n y k. En particular, si k divide a n, x^k tiene orden n/k.*

Demostración.
Sea d el máximo común divisor de n y k; existen, por tanto, dos números enteros a y b tales que $n = ad$ y $k = bd$. A partir de aquí podemos escribir:

$$(x^k)^{n/d} = x^{ka} = x^{bda} = (x^n)^b = e.$$

De donde se deduce que el orden de x^k es un divisor de n/d.
Sea c el orden de x^k; como $x^{kc} = e$, deducimos que n es un divisor de kc y por tanto n/d es un divisor de $(k/d)c$; puesto que n/d y k/d son primos entre sí (ver [5]), se ha de tener que n/d divide a c. De esta manera queda probado el resultado deseado. □

La siguiente afirmación es consecuencia inmediata del resultado anterior.

Corolario 1.1. *Si G es un grupo cíclico y $|G| = n$ entonces G posee tantos generadores como enteros positivos hay menores que n y primos relativos con n.*

Demostración.
Como G es un grupo cíclico, entonces existe $x \in G$ tal que x es un elemento generador de G. Por tanto,

$$\text{orden}(x) = n.$$

Además por la definición de generado de x tenemos que:

$$\langle x \rangle = \{x, x^2, ..., x^n = e\},$$

estando en este conjunto todos los elementos distintos de G. Ahora supongamos que existe $1 \leqslant r < n$ tal que x^r es también un generador de G, entonces

$$\text{orden}(x^r) = n.$$

Por el teorema anterior tenemos que

$$\text{orden}(x^r) = \tfrac{n}{(n,r)}.$$

Aplicando la propiedad transitiva a la igualdad de orden(x^r) obtenemos que

$$n = \tfrac{n}{(n,r)}.$$

Para que esta igualdad sea cierta es necesario que $(n, r) = 1$. Es decir; que n y r sean primos relativos. Recíprocamente, si $(n, r) = 1$ veamos que x^r es un generador de G para lo cual basta probar que $G \subseteq \langle x^r \rangle$. Sea $g \in G$. Como $G = \langle x \rangle$ existe $m \in \mathbb{Z}$ tal que $g = x^m$. Ahora como $(n, r) = 1$, existen $t, s \in \mathbb{Z}$ tales que $1 = nt + rs$ y se tiene: $g = x^m = (x^m)^1 = (x^m)^{nt+rs} = (x^n)^{mt} \cdot (x^r)^s = e \cdot (x^r)^s = (x^r)^s \in \langle x^r \rangle$ □

1.2. El teorema de Lagrange

A continuación demostraremos un teorema elemental y muy importante en el estudio de los grupos finitos, como lo es el teorema de Lagrange. Previamente será necesario estudiar la cardinalidad de las clases de equivalencia y la relación determinada por un subgrupo.

Definición 1.8. Sea G un grupo finito, sea H un subgrupo de G y x un elemento cualquiera de G. Se llama **clase a la derecha según el subgrupo H generada por** x al subconjunto Hx de G dada por

$$Hx = \{hx : h \in H\}.$$

De forma similar se llama **clase a la izquierda según el subgrupo H generada por** x al subconjunto xH de G dado por

$$xH = \{xh : h \in H\}.$$

La clase lateral a la derecha será utilizada sólo cuando sea necesario, de lo contrario, utilizaremos la clase lateral a la izquierda.

Teorema 1.8. *Si G es un grupo finito, H un subgrupo de G y x es un elemento de G, el número de elementos de xH coincide con el número de elementos de H.*

Demostración.

$$Sea\ f : H \mapsto xH$$
$$h \mapsto xh$$

Debemos ver que f es biyectiva, es decir que f es inyectiva y sobreyectiva.

a. Si $f(h_1) = f(h_2)$ para $h_1, h_2 \in H$ entonces $xh_1 = xh_2$. Por la propiedad cancelativa por izquierda que se cumple en los grupos se tiene que $h_1 = h_2$.

b. Si $xh \in xH$, basta observar que $f(h) = xh$ debido a la definición de f, para tener que f es sobreyectiva.

Por lo tanto, f es biyectiva, como se quería demostrar. □

Definición 1.9. Sea G un grupo y H un subgrupo de G; diremos que dos elementos $x, y \in G$ están relacionados mediante H y escribiremos

$$x \equiv y(H) \qquad sii \qquad x^{-1}y \in H.$$

Teorema 1.9. *Sea G un grupo y H un subgrupo de G; la relación definida anteriormente es una relación de equivalencia y la clase de equivalencia de un elemento x de G en esta relación coincide con xH.*

Demostración.
Puesto que H es un subgrupo de G tenemos

a. $x^{-1}x = e \in H$ para todo $x \in G$; por tanto $x \equiv x(H)$ y queda probada la propiedad reflexiva.

b. Si $x \equiv y(H)$ se tiene que $x^{-1}y \in H$ como H es subgrupo de G, $y^{-1}x = (x^{-1}y)^{-1} \in H$ y por tanto, $y^{-1}x \in H$ luego $y \equiv x(H)$ con lo que se cumple la propiedad simétrica.

c. Sean ahora x, y, z elementos de G, y suponga que $x \equiv y(H)$ y $y \equiv z(H)$, se tiene que $x^{-1}y \in H$ y $y^{-1}z \in H$ y puesto que H es un subgrupo de G, $x^{-1}z = (x^{-1}y)(y^{-1})z \in H$ con lo que queda demostrada la propiedad transitiva.

Sea ahora $x \in G$; si $[x]$ representa la clase de equivalencia de x, se tiene que

$$[x] = \{y \in G : x \equiv y(H)\} = \{y \in G : x^{-1}y \in H\},$$
$$\{y \in G : y \in xH\} = \{xh : h \in H\} = xH.$$

□

Teorema 1.10. ***(Teorema de Lagrange.)*** *Si G es un grupo finito y H un subgrupo de G, el número de elementos de H divide al número de elementos de G.*

Demostración.
Puesto que la relación dada en la definición 1.9 es una relación de equivalencia en G, se tiene que las clases de equivalencia de esta relación establecen una partición de G. Debido al teorema 1.9 estas clases de equivalencia coinciden con xH, por tanto, tenemos que

$$G = (x_1H) \bigcup (x_2H) \bigcup ... \bigcup (x_mH)$$

donde $x_j \in G$ y $x_iH \bigcap x_jH = \varnothing$ si $i \neq j$ y $j = 1, 2, ..., m$. Como todos los conjuntos x_jH poseen $|H|$ elementos (teorema 1.7).

$$|G| = |x_1H| + |x_2H| + ... + |x_mH| = m|H|$$

Lo cual demuestra el teorema. □

La importancia del Teorema de Lagrange reside, básicamente en permitir saber de antemano cuántos elementos es posible que haya en cada uno de sus subgrupos. No obstante, este teorema no garantiza que cada grupo de orden n tenga al menos un subgrupo por cada divisor de n. Más exactamente, el recíproco del Teorema de Lagrange no es verdadero para un grupo cualquiera, sólo se cumple para grupos cíclicos y para grupos abelianos. El caso abeliano se encuentra explícito en el teorema de Cauchy el cual se demostrará más adelante.

1.3. Subgrupos normales

Definición 1.10. Un subgrupo H de un grupo se dice **normal**, y escribiremos $H \triangleleft G$, si $(xH)(yH) = (xy)H$, para todo $x, y \in G$.

Definición 1.11. Si H es un subgrupo de G podemos considerar **el conjunto cociente** G/H, que es el conjunto de las clases de equivalencia que se obtienen al definir en G la relación de equivalencia módulo H dada por la definición 1.9,

$$x \equiv y(H) \qquad sii \qquad x^{-1}y \in H.$$

El siguiente teorema muestra que si H es un subgrupo normal de G, el conjunto G/H si se puede dotar con una estructura de grupo.

Teorema 1.11. *Sea G un grupo y H un subgrupo normal de G, la operación $(xH)(yH) = (xy)H$ define en el conjunto cociente G/H una estructura de grupo. Este grupo recibe el nombre de* ***grupo cociente de G sobre H.***

Demostración.
Debemos verificar en primer lugar que la operación de clases de equivalencia está bien definida en G/H, si x' es un representante de xH y y' es un representante de yH entonces $x'y' \in (xH)(yH) = (xy)H$, por ser H un subgrupo normal de G.
La propiedad asociativa de esta operación es una consecuencia de la asociatividad de G, puesto que

$$((xH)(yH))(zH) = (xy)H(zH) = (xy)zH = x(yz)H = (xH)((yH)(zH)).$$

El elemento neutro es $H = eH$ donde e es el neutro de G, puesto que

$$(xH)(eH) = (xe)H = (x)H \text{ y } (eH)(xH) = (ex)H = (x)H,$$

para todo $xH \in G/H$.
Finalmente, si $xH \in G/H$, $x^{-1}H$ es su inverso, donde x^{-1} denota el inverso de x en G, puesto que se tienen las siguientes igualdades

$$(xH)(x^{-1}H) = (xx^{-1})H = (e)H = H,$$
$$\text{y}$$
$$(x^{-1}H)(xH) = (x^{-1}x)H = (e)H = H.$$

□

La definición dada de subgrupo normal de un grupo aparece de manera natural al tratar de definir la estructura de grupo en el conjunto cociente; sin embargo, la verificación de que un subgrupo dado es normal resulta bastante tediosa a partir de la definición. La siguiente proposición nos da condiciones equivalentes de normalidad.

Teorema 1.12. *Si G es un grupo y H es un subgrupo de G, las siguientes condiciones son equivalentes:*

i. H es un subgrupo normal de G.

ii. $xHx^{-1} \subset H$ para todo $x \in G$.

iii. $xH = Hx$ para todo $x \in G$, es decir, las clases de equivalencia por la izquierda y por la derecha coinciden.

Demostración.
Demostraremos que $i) \Rightarrow ii), ii) \Rightarrow iii), iii) \Rightarrow i)$, con lo cual quedará demostrada la proposición.
Sea H un subgrupo normal de G; entonces $(xH)(x^{-1}H) = (xx^{-1})H = eH = H$ para todo $x \in G$; se tiene entonces que si $h \in H$, $xhx^{-1}h \in H$ y, por tanto, $xhx^{-1} \in Hh^{-1} \subseteq H$ luego $xHx^{-1} \subset H$, lo cual demuestra $ii)$.
Supongamos que $xHx^{-1} \subset H$ para todo $x \in G$; operando con x por la derecha se obtiene $xH \subset Hx$; aplicando la hipótesis a x^{-1} se obtiene $x^{-1}Hx \subset H$ y operando con x por la izquierda se obtiene $Hx \subset xH$; esto demuestra que las clases de equivalencia por la izquierda y por la derecha coinciden.
Finalmente, supongamos que $xH = Hx$ para todo $x \in G$; queremos demostrar que $(xH)(yH) = (xy)H$. Sean $x' \in xH$ y $y' \in yH$; se tiene $x' = xh_1$ y $y' = yh_2$ con $h_1, h_2 \in H$; entonces $x'y' = (xh_1)(yh_2)$ y, puesto que $Hy = yH$, existe $h' \in H$ tal que $h_1y = yh'$, con lo cual:

$$x'y' = (xh_1)(yh_2) = x(yh')h_2 = xy(h'h_2) \in (xy)H.$$

Esto prueba que $(xH)(yH) \subset (xy)H$. Sea ahora $(xy)h \in (xy)H$; entonces

$$(xy)h = (xe)(yh) \in (xH)(yH).$$

con lo cual se prueba la inclusión $(xy)H \subset (xH)(yH)$ y con ella la normalidad de H en G. □

Una consecuencia inmediata del resultado anterior es que todo subgrupo de un grupo abeliano es normal.

Corolario 1.2. *Si G es un grupo abeliano y H es un subgrupo de G, H es normal en G.*

Demostración.
Si H es un subgrupo de un grupo abeliano G, entonces para todo $x \in G$ y para todo $h \in H$ tenemos que $xhx^{-1} \in xHx^{-1}$ y $xhx^{-1} = xx^{-1}h = eh = h \in H$, luego $xHx^{-1} \subset H$. Por lo tanto, H es subgrupo normal de G. □

1.4. Homomorfismos

Definición 1.12. Sean $(G_1, *)$ y $(G_2, \circ)$ dos grupos y f una función de G_1 en G_2. La función f se dice que es **un homomorfismo de grupos** si para todo $x, y \in G_1$

$$f(x * y) = f(x) \circ f(y)$$

Es decir, si conserva las operaciones de los grupos entre los que está definida.

Si no es necesario especificar las operaciones de los grupos, la propiedad de homomorfismo se escribe $f(xy) = f(x)f(y)$.
Suponga que f es un homomorfismo de grupos

1. Si f es una función inyectiva, diremos que f es un **monomorfismo**.
2. Si f es una función sobreyectiva, diremos que f es un **epimorfismo**.
3. Si f es una función biyectiva, diremos que f es un **isomorfismo**.

Cuando existe un isomorfismo entre dos grupos G_1 y G_2, diremos que ambos grupos son isomorfos y escribiremos $G_1 \cong G_2$.

Teorema 1.13. *Si N es un subgrupo normal de un grupo G, entonces la función*

$$\gamma : G \mapsto G/N$$
$$a \mapsto aN$$

es un epimorfismo.

Demostración.
La demostración es consecuencia inmediata de la multiplicación de clases laterales en términos de la multiplicación de sus representantes.

$$\gamma(ab) = abN = (aN)(bN) = \gamma(a)\gamma(b)$$

Claramente se ve que γ es sobreyectiva. Por lo tanto, γ es un epimorfismo. □

Dentro de los homomorfismos y los grupos cocientes existe una conexión general que enunciaremos y probaremos en el teorema 1.15.

Definición 1.13. Sea f una función de un conjunto X en un conjunto Y y sea $A \subseteq X$ y $B \subseteq Y$. La imagen $f(A)$ en Y bajo f es $\{f(a) : a \in A\}$. La imagen inversa $f^{-1}(B)$ en X es $\{x \in X : f(x) \in B\}$.

El siguiente teorema proporciona algunas características estructurales preservadas bajo un homomorfismo.

Teorema 1.14. *Sea f un homomorfismo de grupo G en un grupo G'. Si e es el elemento identidad de G, entonces $f(e)$ es el elemento identidad de G' y si $a \in G$, entonces $f(a^{-1}) = (f(a))^{-1}$. Si H es un subgrupo de G, entonces $f(H)$ es un subgrupo de G' y H normal en G implica que $f(H)$ es normal en $f(G)$. Ahora, en la otra dirección, si K' es un subgrupo de G' entonces $f^{-1}(K')$ es un subgrupo de G y K' es normal en $f(G)$ implica que $f^{-1}(K')$ es normal en G.*

Demostración.
Sea f un homomorfismo de G en G'. Entonces, $f(a) = f(ae) = f(a)f(e)$ y análogamente $f(a) = f(ea) = f(e)f(a)$. De aquí se deduce que $f(e) = e'$ es el elemento identidad de G'.
Las ecuaciones $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ y $e' = f(e) = f(a^{-1}a) = f(a^{-1})f(a)$, muestra que $f(a^{-1}) = (f(a))^{-1}$.
Sea H un subgrupo de G y sean $f(a)$ y $f(b)$ dos elementos cualesquiera en $f(H)$. Entonces, $f(ab) = f(a)f(b)$ de modo que $f(a)f(b) \in f(H)$, esto es, $f(H)$ es cerrado bajo la operación de G'. El hecho de que $f(e) = e'$ y $f(a^{-1}) = (f(a))^{-1}$ completa la demostración de que $f(H)$ es un subgrupo de $f(G)$.
Suponga que H es normal en G y sea $f(g) \in f(G)$. Ahora bien

$$(f(g))^{-1}f(h)f(g) = f(g^{-1})f(h)f(g) = f(g^{-1}hg),$$

como $g^{-1}hg \in H$, tenemos que $f(g^{-1}hg) \in f(H)$. Así, $f(H)$ es normal en $f(G)$. Ahora, en la otra dirección, sea K' un subgrupo de G'. Suponga que a y b están en $f^{-1}(K')$. Entonces, $f(ab) = f(a)f(b)$ y $f(a)f(b) \in K'$; de modo que $ab \in f^{-1}(K')$. Además, K' debe contener la identidad $f(e)$, de modo que $e \in f^{-1}(K')$. Si $a \in f^{-1}(K')$ entonces $f(a) \in K'$, de modo que $(f(a))^{-1} \in K'$. Pero $(f(a))^{-1} = f(a^{-1})$, luego $a^{-1} \in f^{-1}(K)$. Por tanto, $f^{-1}(K')$ es un subgrupo de G. Si K' es un subgrupo normal de $f(G)$ entonces para $b \in f^{-1}(K')$ y $g \in G$ tenemos $f(g^{-1}bg) = (f(g))^{-1}f(b)f(g)$
y $(f(g))^{-1}f(b)f(g)$ está en K'.
De modo que $g^{-1}bg \in f^{-1}(K')$. Por tanto, $f^{-1}(K')$ es normal en G. □

Definición 1.14. El Kernel de un homomorfismo ϕ de un grupo G en un grupo G' es el conjunto de elementos de G cuya imagen, bajo ϕ es el elemento identidad de G'.

Teorema 1.15. *(**Teorema fundamental del homomorfismo**.) Sea f un homomorfismo de un grupo G en un grupo G', con Kernel K. Entonces $f(G)$ es un grupo y existe un isomorfismo de $f(G)$ en G/K.*

Demostración.
En el teorema 1.14 se vio que $f(G)$ es un grupo, pues G es un caso particular de un subgrupo de G.
Sea $aK \in G/K$, tratemos de definir una función

$$\begin{aligned} \phi : G/K &\mapsto f(G) \\ aK &\mapsto f(a) \end{aligned}$$

Definimos, así, la función ϕ en una clase lateral escogiendo un representante a de la clase lateral.

1. Debemos mostrar que ϕ está bien definida, esto es, que es independiente de nuestra selección del representante. Para ello, sea $b \in aK$. Es necesario mostrar que $f(a) = f(b)$. Pero $b \in aK$ significa que $b = ak_1$ para $k_1 \in K$, de modo que, $a^{-1}b = k_1$. Entonces

   $$e' = f(k_1) = f(a^{-1}b) = f(a^{-1})f(b) = (f(a))^{-1}f(b).$$

   De aquí,

   $$f(b) = f(a)e' = f(a).$$

   Así, ϕ está bien definida.

2. Para mostrar que ϕ es inyectiva.
   Supóngase que $\phi(aK) = \phi(bK)$. Entonces $f(a) = f(b)$, de modo que

   $$e' = (f(a))^{-1}f(b) = f(a^{-1})f(b) = f(a^{-1}b).$$

Así por la definición de K, $a^{-1}b \in K$. Pero, $a^{-1}b \in K$ implica que $b \in aK$, de modo que $bK = aK$. Por lo tanto, ϕ es inyectiva.

3. Es obvio que ϕ es sobreyectiva.

4. La ecuación

$$\phi[(aK)(bK)] = \phi(abK) = f(ab) = f(a)f(b) = \phi(aK)\phi(bK)$$

completa la demostración de que ϕ es un isomorfismo.

□

Definición 1.15. Sea G un grupo de orden $p^n m$ con p un primo que no divide a m; todo subgrupo de G de orden p^n se dice que es un **p-subgrupo de Sylow de G**.

Ejemplo 1.7. Sea $\mathbb{Z}_{10} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\}$

$$orden[0] = 1 \qquad orden[5] = 2$$
$$orden[1] = 10 \qquad orden[6] = 5$$
$$orden[2] = 5 \qquad orden[7] = 10$$
$$orden[3] = 10 \qquad orden[8] = 5$$
$$orden[4] = 5 \qquad orden[9] = 10$$

El subgrupo H generado por $[5]$ es un $2-$subgrupo de Sylow de $\mathbb{Z}_{10}$. El subgrupo K generado por $[2]$ es un $5-$subgrupo de Sylow de $\mathbb{Z}_{10}$.

1.5. Teorema fundamental de los grupos abelianos finitos

Existen muchas demostraciones de el teorema fundamental de los grupos abelianos finitos, el cual afirma que cada grupo abeliano finito es un producto de grupos cíclicos. La demostración de este teorema es un poco extensa y utiliza muchos conceptos que no son necesarios para el desarrollo de este trabajo por tal razón sólo se enunciará el teorema y su respectiva demostración la encontramos en ([4], capítulo 20).

A continuación enunciaremos y demostraremos el teorema de Cauchy para grupos abelianos finitos el cual es previo a la demostración del teorema fundamental de los grupos abelianos finitos y cuya demostración es fácil realizar con los conceptos trabajados hasta ahora.

Teorema 1.16. *(**Teorema de Cauchy para grupos abelianos finitos**.) Si G es un grupo abeliano de orden n y p es un primo que divide a n, G contiene un elemento de orden p, y por tanto un subgrupo con p elementos.*

Demostración.
La demostración se realiza por inducción sobre el orden del grupo. Si $n = 1$ el resultado es cierto. Supongamos que el resultado es cierto para todo grupo G de orden inferior a n, $n > 1$. Como G tiene al menos dos elementos, existe $x \in G$ tal que $x \neq e$. Si $n = p$, x tiene orden p por el teorema de Lagrange, y el resultado queda probado.
Supongamos, por tanto, que $p < n$. Si llamamos s al orden de x y p divide a s, $x^{s/p}$ es de orden p (teorema 1.7) y también en este caso hemos demostrado el resultado.
Supongamos entonces que $n > p$ y que p no divide al orden de x. Sea $N = \langle x \rangle$; como G es abeliano, N es un subgrupo normal de G. Puesto que $N \neq \{e\}$

$$|G/N| = |G|/|N| < |G| = n.$$

Además como p divide a n y no divide a $|N|$, de la igualdad $n = (n/|N|)|N|$. Se deduce que p divide a $n/|N| = |G/N|$, se puede, por tanto, aplicar la hipótesis de inducción a G/N para encontrar un elemento $[y] = yN$ de orden p en G/N. Sea k el orden de y en G. Como yN es de orden p en G/N, $yN \neq N, y^2N \neq N, ..., y^{p-1}N \neq N, y^pN = N$. Se obtiene fácilmente que si $j = 1, 2, 3, ...$, $y^jN = N$ si y sólo si j es múltiplo de p. Como $y^k = e \in N$ se tiene que $y^kN = N$ y, por tanto, k es múltiplo de p. Así pues, $y^{k/p} \in G$ y tiene orden p (teorema 1.7). También en este caso hemos encontrado un elemento de orden p. □

Definición 1.16. Dados los grupos $G_1, G_2, ..., G_k$ se define su **producto directo** como el grupo formado por los elementos de la forma $(g_1, g_2, ..., g_k)$ con $g_j \in G_j$ para todo $j = 1, 2, ..., k$, con la operación

$$(g_1, g_2, ..., g_k)(g'_1, g'_2, ..., g'_k) = (g_1g'_1, g_2g'_2, ..., g_kg'_k).$$

Teorema 1.17. *(**Teorema fundamental de los grupos abelianos finitos**.) Si G es un grupo abeliano finito, entonces G es isomorfo a un producto directo de grupos cíclicos.*

Ejemplo 1.8. Dados los grupos $\mathbb{Z}_6$ y $\mathbb{Z}_3 \times \mathbb{Z}_2$, veamos que estos dos grupos son isomorfos. Sea $\beta : \mathbb{Z}_6 \mapsto \mathbb{Z}_3 \times \mathbb{Z}_2$ donde:

$$\begin{aligned}
\beta([0]) &= ([0],[0]) \\
\beta([1]) &= ([1],[1]) \\
\beta([2]) &= ([2],[0]) \\
\beta([3]) &= ([0],[1]) \\
\beta([4]) &= ([1],[0]) \\
\beta([5]) &= ([2],[1])
\end{aligned}$$

Claramente β es una función biyectiva y además por medio de las siguientes tablas podemos observar que $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

+	([0],[0])	([1],[1])	([2],[0])	([0],[1])	([1],[0])	([2],[1])
([0],[0])	([0],[0])	([1],[1])	([2],[0])	([0],[1])	([1],[0])	([2],[1])
([1],[1])	([1],[1])	([2],[0])	([0],[1])	([1],[0])	([2],[1])	([0],[0])
([2],[0])	([2],[0])	([0],[1])	([1],[0])	([2],[1])	([0],[0])	([1],[1])
([0],[1])	([0],[1])	([1],[0])	([2],[1])	([0],[0])	([1],[1])	([2],[0])
([1],[0])	([1],[0])	([2],[1])	([0],[0])	([1],[1])	([2],[0])	([0],[1])
([2],[1])	([2],[1])	([0],[0])	([1],[1])	([2],[0])	([0],[1])	([1],[0])

1.6. Números de Fermat

Fermat estudió los números de la forma $2^{2^n}+1$ para $n = 0, 1, 2, ...$ y conjeturó que siempre eran primos. La conjetura resulta cierta para los cinco primeros números de Fermat que son $3, 5, 17, 257$ y 65537, sin embargo, Euler demostró en 1732 que el sexto número de Fermat no es primo y se puede factorizar como:

$$2^{2^5}+1 = 2^{32}+1 = (641)(6700417).$$

Como datos importantes para comentar a cerca de los números primos podemos decir que:

1. El mayor primo de Fermat conocido es 65537.

2. Todo primo impar es de la forma $4k+1$ ó $4k+3$ para $k \in \mathbb{Z}_+$. Debido a que todo número entero es de la forma $4k$, $4k+1$, $4k+2$ ó $4k+3$, y los números de la forma $4k$ y $4k+2$ son múltiplos de dos luego no son primos impares, entonces la única posibilidad para este número primo impar es que sea de la forma $4k+1$ o $4k+3$.

Dentro del estudio de los números primos existe una propiedad muy importante que es la que nos brinda la posibilidad de factorizar todo entero $n > 1$ como producto de ellos y esta factorización resulta esencialmente única. El siguiente teorema formaliza este resultado.

Teorema 1.18. ***Teorema fundamental de la aritmética****: Todo entero $n > 1$ ó es primo, ó se puede factorizar como producto de primos. Este producto es único salvo el orden de los factores.*

Demostración.
Sea S el conjunto de todos los números naturales que son primos o que pueden escribirse como producto de primos.
Claramente $S \subseteq \{k \in \mathbb{N} : k \geqslant 2\}$ y además tenemos que:

1. $2 \in S$ porque 2 es un número primo.

2. Supongamos que $n > 2$ y que $k \in S$ para todo k tal que $2 \leqslant k < n$. Veamos que $n \in S$. Si n no es primo existen r y t tales que $n = rt$ con $2 \leqslant r < n$ y $2 \leqslant t < n$ y por hipótesis, ellos o son primos, o producto de primos. En consecuencia, n es producto de primos y así $n \in S$.

Para probar la unicidad usaremos inducción sobre n. Para $n = 2$ claramente la representación es única. Supongamos ahora que para todo entero k con $2 \leqslant k < n$ la representación es única y supongamos que

$$n = p_1 p_2 p_3 ... p_s = q_1 q_2 q_3 ... q_t,$$

donde p_i y q_i son primos con $p_1 \leqslant p_2 \leqslant p_3 \leqslant ... \leqslant p_s$ y $q_1 \leqslant q_2 \leqslant q_3 \leqslant ... \leqslant q_t$.
Así, si p_1 divide a $(q_1 q_2 q_3 ... q_t)$ entonces $p_1 = q_j$ para algún j por lo tanto, $q_1 \leqslant p_1$. Análogamente si q_1 divide a $(p_1 p_2 p_3 ... p_s)$ entonces $q_1 = p_i$ para algún i y por tanto $p_1 \leqslant q_1$. Lo anterior demuestra que $p_1 = q_1$ y cancelando tenemos

$$\tfrac{n}{p_1} = p_2 p_3 ... p_s = q_2 q_3 ... q_t.$$

Como $\frac{n}{p_1} < n$ la hipótesis de inducción garantiza que estas dos representaciones de $\frac{n}{p_1}$ son idénticas (hemos escogido un orden) y en consecuencia $s = t$ y para cada i, $p_i = q_i$. Por el principio de inducción matemática la prueba queda completa. □

1.7. La función ϕ de Euler

Definición 1.17. Para cada entero positivo n, definimos $\phi(n)$ como el número de enteros positivos menores o iguales que n y primos relativos con n.

Ejemplo 1.9. Tenemos la siguiente tabla que incluye los cinco primeros valores de ϕ.

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4

Teorema 1.19. *Si p es un número primo y a es un entero positivo entonces*

$$\phi(p^a) = p^a - p^{a-1}.$$

Demostración.
Los enteros positivos menores o iguales que p^a que no son primos relativos con p son precisamente los p^{a-1} múltiplos de p

$$1 \cdot p, 2 \cdot p, 3 \cdot p, ..., p^{a-1} \cdot p$$

Por lo tanto, $\phi(p^a) = p^a - p^{a-1}$. □

CAPÍTULO 2

Subconjuntos de orden perfecto

2.1. Definiciones y propiedades

Antes de iniciar nuestro estudio es importante tener clara la notación que usaremos: G será un grupo abeliano finito, $|G|$ denotará el cardinal, y $(\mathbb{Z}_m)^t$ será usado para indicar $(\mathbb{Z}_m \times \mathbb{Z}_m \times ... \times \mathbb{Z}_m)$ t-factores.

Definición 2.1. Si x es un elemento de G, definimos el **subconjunto orden de G determinado por** x al conjunto de todos los elementos en G con el mismo orden de x.

Definición 2.2. Un grupo G se dice que **tiene subconjuntos de orden perfecto**(SOP) si el número de elementos en cada subconjunto orden de G es un divisor de $|G|$.

Ejemplo 2.1. a. Sea $G = (\mathbb{Z}_2)^2 \times \mathbb{Z}_3$. Es claro que $|G| = 12$.

$$ord([0],[0],[0]) = 1 \qquad ord([1],[0],[0]) = 2$$
$$ord([0],[0],[1]) = 3 \qquad ord([1],[0],[1]) = 6$$
$$ord([0],[0],[2]) = 3 \qquad ord([1],[0],[2]) = 6$$
$$ord([0],[1],[0]) = 2 \qquad ord([1],[1],[0]) = 2$$
$$ord([0],[1],[1]) = 6 \qquad ord([1],[1],[1]) = 6$$
$$ord([0],[1],[2]) = 6 \qquad ord([1],[1],[2]) = 6$$

ORDEN DEL ELEMENTO	CARDINAL DEL SUBCONJUNTO ORDEN
1	1
2	3
3	2
6	6

entonces $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ tiene subconjuntos de orden perfecto.

b. Sea el grupo $\mathbb{Z}_3$, como $\mathbb{Z}_3$ tiene dos elementos de orden 3 y 2 no divide a 3 entonces $\mathbb{Z}_3$ no tiene subconjuntos de orden perfecto.
Observe que $\mathbb{Z}_3 \cong \{[0]\} \times \{[0]\} \times \mathbb{Z}_3$ es subgrupo de G, luego la propiedad de tener subconjuntos de orden perfecto no siempre se cumple para los subgrupos.

c. Sea $G = (\mathbb{Z}_2)^2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$. Es claro que $|G| = 24$.

$ord([0],[0],[0]) = 1$ $ord([1],[0],[0]) = 2$ $ord([0],[0],[1]) = 3$
$ord([1],[0],[1]) = 6$ $ord([0],[0],[2]) = 3$ $ord([1],[2],[0]) = 6$
$ord([0],[1],[0]) = 4$ $ord([1],[1],[0]) = 4$ $ord([0],[1],[1]) = 12$
$ord([1],[1],[1]) = 12$ $ord([0],[1],[2]) = 12$ $ord([1],[1],[2]) = 12$
$ord([0],[2],[0]) = 2$ $ord([1],[2],[0]) = 2$ $ord([0],[2],[1]) = 6$
$ord([1],[2],[1]) = 6$ $ord([0],[2],[2]) = 6$ $ord([1],[2],[2]) = 6$
$ord([0],[3],[0]) = 4$ $ord([1],[3],[0]) = 4$ $ord([0],[3],[1]) = 12$
$ord([1],[3],[1]) = 12$ $ord([0],[3],[2]) = 12$ $ord([1],[3],[2]) = 12$

ORDEN DEL ELEMENTO	CARDINAL DEL SUBCONJUNTO ORDEN
1	1
2	3
3	2
4	4
6	6
12	8

entonces $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ tiene subconjuntos de orden perfecto.

Lema 2.1. *Si p es un número primo entonces cada elemento de $\mathbb{Z}_p$, diferente de la identidad, tiene orden p.*

Demostración.
Sea x un elemento de $\mathbb{Z}_p$ con x diferente de la identidad. Por el teorema de Lagrange el orden de x divide al orden de $\mathbb{Z}_p$; además el orden de $\mathbb{Z}_p$ es p entonces el orden de x divide a p; como p es primo el orden de x es 1 ó el orden de x es p.

El único elemento de $\mathbb{Z}_p$ que tiene orden igual a 1 es el elemento identidad, pero x es diferente de la identidad; por lo tanto, el orden$(x) = p$. □

Lema 2.2. *Si C es un grupo cíclico con $|C|$ una potencia de un primo p entonces C tiene un único subgrupo de orden p.*

Demostración.
Sea $|C| = n$. Como C es un grupo cíclico entonces existe $x \in C$ tal que x es un generador de C. Como p divide a n, $x^{n/p}$ es un elemento de orden p (teorema 1.7) y por tanto el subgrupo H generado por este elemento tiene orden p.
Para ver que H es único, supongamos que existe otro subgrupo K de C de orden p; como C es cíclico, K también lo es y por tanto está generado por un elemento x^m con m el menor entero positivo tal que $x^m \in K$. Además el orden de x^m es p y por teorema 1.7, $p = n/(n, m)$. Por tanto,

$$x^m \in \langle x^m \rangle \text{ pero } x^m = x^{(n,m)\cdot m/(n,m)} \in \langle x^{(n,m)} \rangle \text{ y } \langle x^{(n,m)} \rangle = \langle x^{n/p} \rangle, \text{entonces}$$
$$x^m \in \langle x^{n/p} \rangle.$$

Luego $\langle x^m \rangle$ es un subgrupo de $\langle x^{n/p} \rangle$. Es decir, K es subgrupo de H y además K y H tienen el mismo número de elementos entonces $K = H$. □

Lema 2.3. *Si C es un grupo cíclico con $|C|$ una potencia de un primo p entonces C contiene exactamente $p - 1$ elementos de orden p.*

Demostración.
Del corolario 1.1 el número de elementos de orden p en C es igual al número de generadores del único subgrupo de orden p en C, éste número es $\phi(p) = p-1$ (definición 1.17). Luego C posee $p - 1$ elementos de orden p. □

Proposición 2.1. *Supongamos que G tiene subconjuntos de orden perfecto y p es un divisor primo de $|G|$. Entonces $p - 1$ divide a $|G|$.*

Demostración.
Para probar este resultado, contamos el número de elementos en G de orden p. Por el teorema fundamental de los grupos abelianos finitos $G \cong C_1 \times C_2 \times ... \times C_t \times M$, donde cada C_i es un grupo cíclico con $|C_i|$ una potencia positiva de p y M es también un grupo cíclico formado por los grupos cuyo orden no son divisibles por p; cada elemento

de G puede tomarse como una $(t+1)$-upla ordenada. Un elemento cuyo orden es menor o igual a p debe tener la identidad de M como su entrada en la $t+1$ posición. Cada una de las otras entradas debe ser un elemento de orden a lo sumo p en su respectivo grupo. Por el Teorema de Cauchy para grupos abelianos finitos cada C_i tiene un subgrupo de orden p y como $|C_i| = p^\alpha$, no existe un entero $1 < m < p$ tal que m sea el orden de un elemento de C_i. Por lo tanto cada entrada en las t-uplas cuyo orden es menor o igual a p tienen orden 1 ó p. Tales t-uplas deben tener exactamente orden p en G excepto cuando la identidad aparece en cada entrada. Además del lema 2.3 tenemos que cada C_i tiene $p-1$ elementos de orden p, por tanto, el número total de elementos de orden p en G es

$$p^t - 1 = (p-1)(p^{t-1} + p^{t-2} + ... + 1).$$

Como G tiene subconjuntos de orden perfecto entonces $(p-1)(p^{t-1} + p^{t-2} + ... + 1)$ divide a $|G|$, luego $(p-1)$ divide a $|G|$. □

Corolario 2.1. *Si G tiene subconjuntos de orden perfecto y es no trivial entonces $|G|$ es par.*

Demostración.
Si $|G|$ es 2 se cumple. Si $|G| > 2$ por el teorema fundamental de la aritmética $|G|$ es primo o es el producto de números primos. Si $|G| = p$ con p primo, como $p > 2$, p es primo impar. Por el lema 2.1, G tiene $p-1$ elementos de orden p, por lo tanto G no tiene subconjuntos de orden perfecto, lo cual contradice la hipótesis. Si $|G|$ es el producto de números primos, existe un primo p que divide a $|G|$, como G tiene subconjuntos de orden perfecto, por la proposición 2.1 $p-1$ divide a $|G|$, como p es primo impar entonces $p-1$ es par, luego $|G|$ es par. □

Mientras la proposición 2.1 impone severas restricciones sobre el cardinal de un grupo con subconjuntos de orden perfecto. Resulta que tales grupos son muy abundantes. Este hecho es formalizado en el teorema 2.1 pero algunos fundamentos previos son necesarios.

Lema 2.4. *Si a, b y t son enteros positivos con $b \leq a$ y sea $G \cong (\mathbb{Z}_{p^a})^t$ donde p es un número primo, entonces el número de elementos en G de orden p^b es $(p^{b-1})^t(p^t - 1)$.*

Demostración.
De forma análoga a la demostración de la proposición 2.1 pensamos en un elemento arbitrario de G como una t-upla ordenada donde cada entrada es un elemento de $\mathbb{Z}_{p^a}$. Un elemento de G cuyo orden es p^b debe tener un elemento de orden p^b como una entrada en al menos una de sus t-posiciones. Para contar tales elementos sistemáticamente, contamos primero el número de t-uplas con un elemento de orden p^b en la primera posición, seguido por elementos de orden menor o igual a p^b en las siguientes $t-1$ posiciones. El número de elementos de orden p^b en $\mathbb{Z}_{p^a}$ es el número de generadores del único subgrupo cíclico de $\mathbb{Z}_{p^a}$ de orden p^b. Este número es $\phi(p^b) = p^b - p^{b-1}$ donde ϕ es la función de Euler (ver definición 1.17). Ella determina el número de escogencias para la primera posición en la t-upla. Puesto que tenemos algún elemento de $\mathbb{Z}_{p^a}$ con orden menor o igual a p^b en las siguientes $t-1$ posiciones y existe exactamente un subgrupo de orden p^c para cada $c \leq b$ (el cual tiene $\phi(p^c)$ generadores) existen

$$1 + \phi(p) + \phi(p^2) + ... + \phi(p^{b-1}) + \phi(p^b) =$$
$$1 + (p-1) + (p^2 - p) + ... + (p^{b-1} - p^{b-2}) + (p^b - p^{b-1}) = p^b$$

escogencias para cada una de las $t-1$ posiciones. Es decir, $\phi(p^b)$ para la primera posición seguidos por p^b escogencias para las siguientes $t-1$ posiciones. Esto se resume en:

$$\phi(p^b)(p^b)^{t-1}$$

tales elementos en G.
Seguidamente, contamos las t-uplas con un elemento de orden estrictamente menor que p^b en la primera posición, un elemento de orden exactamente p^b en la segunda posición, y un elemento de $\mathbb{Z}_{p^a}$ con orden menor o igual a p^b en las siguientes $t-2$ posiciones. Esto conduce a

$$1 + \phi(p) + \phi(p^2) + ... + \phi(p^{b-1}) =$$
$$1 + (p-1) + (p^2 - p) + ... + (p^{b-1} - p^{b-2}) = p^{b-1}$$

formas de escoger la primera posición, $\phi(p^b)$ escogencias para la segunda posición, seguidos por p^b escogencias para las siguientes $t-2$ posiciones. Esto es, existen:

$$(p^{b-1})\phi(p^b)(p^b)^{t-2}$$

tales elementos en G.

Continuamos este proceso, contando elementos con entradas al inicio de la t-upla que tengan orden menor que p^b, exactamente una entrada de orden p^b, y las siguientes entradas de orden menor o igual a p^b. Sumando los elementos totales se obtiene una expresión para el número total de elementos de orden p^b en G.

Sea

$$T = \phi(p^b)(p^b)^{t-1} + (p^{b-1})\phi(p^b)(p^b)^{t-2} + (p^{b-1})(p^{b-1})\phi(p^b)(p^b)^{t-3} \\ +... + (p^{b-1})^{t-2}\phi(p^b)(p^b) + (p^{b-1})^{t-1}\phi(p^b).$$

Entonces

$$\begin{aligned} T =& \ \phi(p^b)(p^{b-1})^{t-1}[p^{t-1} + p^{t-2} + ... + p + 1] \\ =& \ (p^b - p^{b-1})(p^{b-1})^{t-1}[(p^t - 1)/(p-1)] \\ =& \ p^{b-1}(p-1)(p^{b-1})^{t-1}[(p^t - 1)/(p-1)] \\ =& \ (p^{b-1})(p^{b-1})^{t-1}(p^t - 1)) \\ =& \ (p^{b-1})^t(p^t - 1). \end{aligned}$$

□

Lema 2.5. *Sea $G \cong (\mathbb{Z}_{p^a})^t \times M$ y $\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^t \times M$, donde a y t son enteros positivos y p es un primo que no divide a $|M|$. Suponga que d es el orden de un elemento en $\hat{G}$ y que p^{a+1} no divide a d. Entonces G y $\hat{G}$ contienen el mismo número de elementos de orden d.*

Demostración.

Un elemento arbitrario de $\hat{G}$ puede ser representado como una pareja ordenada (x, y), donde x es un elemento de$(\mathbb{Z}_{p^{a+1}})^t$ y y es un elemento de M. El orden de (x, y) es el mínimo común múltiplo de los órdenes de x y de y. Como p no divide a $|M|$ esto es simplemente el producto de dos órdenes. Por esto, si d es el orden del elemento (x, y) y p^{a+1} no divide a d, podemos factorizar a d como $p^b m$, donde $0 \leq b \leq a$; donde p^b es el orden de x y m es el orden de y. Seguidamente, contamos el número de elementos de orden $p^b m$ en $\hat{G}$, contamos el número de elementos en $(\mathbb{Z}_{p^{a+1}})^t$ de orden p^b y multiplicamos esta cantidad por el número de elementos de orden m en M. Por el lema 2.1, este total es precisamente $(p^{b-1})^t(p^t - 1)k$ donde k es el número de elementos en M de orden m, siendo este total el mismo número de elementos de orden $p^b m$ en G. □

2.2. Tres teoremas importantes

En esta sección se enunciarán y se demostrarán tres teoremas que serán la base para la demostración del teorema principal.

Teorema 2.1. *Sea* $G \cong (\mathbb{Z}_{p^a})^t \times M$ *y* $\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^t \times M$ *donde* a *y* t *son enteros positivos y* p *es un primo que no divide a* $|M|$*. Si* G *tiene subconjuntos de orden perfecto, entonces* $\hat{G}$ *tiene subconjuntos de orden perfecto.*

Demostración.
Como en la demostración del lema 2.5, sea (x, y) un elemento de $\hat{G}$, donde x es un elemento de $(\mathbb{Z}_{p^{a+1}})^t$ y y un elemento de M. Sea d el orden de (x, y). Asumimos inicialmente que d no es divisible por p^{a+1}. Como G tiene subconjuntos de orden perfecto por el lema 2.5 garantizamos que la cardinalidad del subconjunto orden de $\hat{G}$ determinado por (x, y) es igual a la cardinalidad del subconjunto orden de G determinado por (x, y). Dado que $|\hat{G}| = p^t|G|$ y que d divide $|G|$ ya que G tiene subconjuntos de orden perfecto entonces d divide $|G|p^t$ esto es d divide $|\hat{G}|$ por tanto $\hat{G}$ tiene subconjuntos de orden perfecto.
Supongamos ahora que d es divisible por p^{a+1}. Entonces el orden de x en $(\mathbb{Z}_{p^{a+1}})^t$ es exactamente p^{a+1}, podemos factorizar a d como $p^{a+1}m$, donde m es el orden de y en M. Sea k el número de elementos en M que tienen orden m. Por el lema 2.4, el número total de elementos de orden d es $(p^a)^t(p^t-1)k$. Para completar la demostración debemos mostrar que este número en realidad divide a $|\hat{G}|$.
Aplicando el lema 2.4 para G decimos que el número de elementos en G que tiene orden $p^a m$ es $(p^{a-1})^t(p^t-1)k$, el cual divide $|G|$ porque G tiene subconjuntos de orden perfecto. Puesto que $|\hat{G}| = p^t|G|$ se sigue que

$$p^t(p^{a-1})^t(p^t-1)k = (p^a)^t(p-1)k$$

divide $|\hat{G}|$. □

Damos algunos ejemplos para ilustrar el teorema 2.1

Ejemplo 2.2. Sea el grupo $G = (\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

ORDEN DEL ELEMENTO	CARDINAL DEL SUBCONJUNTO O.
1	1
2	15
3	2
5	4
6	30
10	60
15	8
30	120

El cual tiene subconjuntos de orden perfecto. El teorema 2.1, nos permite incrementar el exponente sobre algunos de los primos que aparecen y suministrar nuevos grupos con subconjuntos de orden perfecto. Por ejemplo, $(\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ y $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ también tienen subconjuntos de orden perfecto. Además aplicando el teorema 2.1 sucesivamente produce grupos tales como $(\mathbb{Z}_{16})^4 \times \mathbb{Z}_9 \times \mathbb{Z}_{125}$ con subconjuntos de orden perfecto.

El hecho importante que aprendimos del teorema 2.1 es que podemos generar nuevos grupos con subconjuntos de orden perfecto de los ya existentes, y por este mecanismo, exhibir un número infinito de tales grupos. Esto conlleva a una pregunta natural: ¿es posible generar nuevos subgrupos SOP por otro camino? Es decir, ¿dado un *"gran"* grupo con subconjuntos de orden perfecto, podemos desarrollar una técnica para hallar unos pequeños subgrupos no triviales con subconjuntos de orden perfecto? La respuesta es sí, y para hacerlo dividimos el proceso en dos etapas para hacer las ideas más transparentes. Los detalles se dan en los siguientes dos teoremas.

Teorema 2.2. *Suponga que G tiene subconjuntos de orden perfecto y que $G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times ... \times \mathbb{Z}_{p^{a_{s-1}}} \times (\mathbb{Z}_{p^{a_s}})^t \times M$, donde p es un primo que no divide a $|M|$ y $a_1 \leqslant a_2 \leqslant ... \leqslant a_{s-1} < a_s$ son enteros positivos. Entonces $\hat{G} \cong (\mathbb{Z}_{p^{a_s}})^t \times M$ también tiene subconjuntos de orden perfecto.*

Demostración.
En esta demostración nuevamente consideramos un elemento en $\hat{G}$ como un par ordenado (x, y), con x un elemento de $(\mathbb{Z}_{p^{a_s}})^t$ y y un elemento de M. Como en la demostración del lema 2.5, el orden de (x, y) puede ser factorizado como $p^b m$ con $b \leqslant a_s$, donde p^b

es el orden de x y m es el orden de y. Adicionalmente, supongamos que $p^c k$, donde p no divide a k, es el número de elementos en M que tienen orden m. Entonces por el lema 2.4, el número de elementos de $\hat{G}$ que tienen orden $p^b m$ es

$$(p^{b-1})^t(p^t-1)p^c k.$$

Procedemos a probar que este número es un divisor de $|\hat{G}|$. Además utilizando las técnicas de conteo desarrolladas en la demostración del lema 2.4 y el lema 2.5, se prueba que el número de elementos en G que tienen orden $p^{a_s} m$ es:

$$p^a(p^{a_s-1})^t(p^t-1)p^c k,$$

donde $a = \sum_{i=1}^{s-1} a_i$. Este número divide $|G|$ por G tener subconjuntos de orden perfecto, dado que $|G| = p^a|\hat{G}|$ con $a = \sum_{i=1}^{s-1} a_i$ concluimos que $p^a(p^{a_s-1})^t(p^t-1)p^c k$ divide a $p^a|\hat{G}|$ además sabemos que $b \leqslant a_s$ entonces (p^{b-1})divide a (p^{a_s-1}). Así, $(p^{b-1})^t(p^t-1)p^c k$ divide $|\hat{G}|$ por lo tanto $\hat{G}$ tiene subconjuntos de orden perfecto. □

Teorema 2.3. *Suponga que G tiene subconjuntos de orden perfecto y que $G \cong (\mathbb{Z}_{p^a})^t \times M$, donde p es un primo no divisor de $|M|$. Entonces $\hat{G} \cong (\mathbb{Z}_p)^t \times M$ también tiene subconjuntos de orden perfecto.*

Demostración.
Consideramos un elemento en $\hat{G}$ como una pareja ordenada (x, y) con x un elemento de $(\mathbb{Z}_p)^t$ y y un elemento de M. Como p no divide a $|M|$, podemos factorizar el orden de (x, y) como pm donde p es el orden de x y m el orden de y. Además, supongamos que k es el número de elementos en M que tienen orden m. Entonces por el lema 2.4, el número de elementos en $\hat{G}$ que tienen orden pm es

$$(p^t-1)k.$$

Debemos probar que este número divide $|\hat{G}|$. Por el lema 2.4 el número de elementos en G que tienen orden $p^a m$ es

$$(p^{a-1})^t(p^t-1)k.$$

Este número divide a $|G|$, por G tener subconjuntos de orden perfecto.Puesto que $|G| = (p^{a-1})^t|\hat{G}|$ tenemos que

$$(p^{a-1})^t(p^t-1)k \text{ divide } (p^{a-1})^t|\hat{G}|.$$

Por lo tanto,

$$(p^t - 1)k \text{ divide } |\hat{G}|.$$

□

Aquí está una ilustración del uso de estos dos teoremas.

Ejemplo 2.3. En el ejemplo 2.1, vimos que $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ tiene subconjuntos de orden perfecto. De acuerdo a los teoremas 2.2 y 2.3, $\mathbb{Z}_2 \times \mathbb{Z}_3$ y $\mathbb{Z}_2$ también tienen subconjuntos de orden perfecto.

De los teoremas 2.2 y 2.3, podemos ver que dado un grupo G con subconjuntos de orden perfecto, podemos limitar nuestra búsqueda a los subgrupos más pequeños no triviales de G con esta propiedad, a subgrupos H cuyos p-subgrupos de Sylow son abelianos elementales para cada primo p. Es decir, cada p-subgrupo de Sylow de H es isomorfo a $(\mathbb{Z}_p)^t$ para algún entero positivo t. En particular, puesto que un grupo G no trivial con subconjuntos de orden perfecto tiene orden par (corolario 2.1) allí existe un subgrupo H de G con subconjuntos de orden perfecto cuyos 2-subgrupos de Sylow es abeliano elemental. Sobre la base de estas observaciones, formalizamos la noción relevante de más pequeño en la siguiente definición.

Definición 2.3. Suponga que $G \cong (\mathbb{Z}_2)^t \times M$, donde $|M|$ es impar. Llamamos a G **un grupo minimal SOP**, si G tiene subconjuntos de orden perfecto y no existe un subgrupo propio $\hat{M}$ de M tal que $(\mathbb{Z}_2)^t \times \hat{M}$ tiene subconjuntos de orden perfecto.

Es decir, G es **un grupo minimal SOP** si no existe en G un subgrupo propio con la propiedad de tener subconjuntos de orden perfecto.

Ejemplo 2.4. Los dos grupos $\mathbb{Z}_2 \times \mathbb{Z}_3$ y $\mathbb{Z}_2$ tienen subconjuntos de orden perfecto.
$\mathbb{Z}_2$ es un grupo minimal SOP ya que no existe en él un subgrupo propio con subconjuntos de orden perfecto.
$\mathbb{Z}_2 \times \mathbb{Z}_3$ no es grupo minimal SOP ya que el subgrupo $\mathbb{Z}_2 \times \{[0]\}$ tiene subconjuntos de orden perfecto.

CAPÍTULO 3

Los números de Fermat y los grupos finitos

Cuando $G \cong (\mathbb{Z}_2)^t \times M$ es un grupo minimal SOP con $|M|$ libre de cuadrados, el factor M está determinado únicamente por el valor de t. Este es el contenido del teorema 3.1 para el cual algunas observaciones preliminares pueden resultar de utilidad en su demostración.

Si tratamos de construir un grupo $G \cong (\mathbb{Z}_2)^t$ con las condiciones dadas anteriormente tenemos que: Como $(\mathbb{Z}_2)^t$ es un factor de G, hay exactamente $2^t - 1$ elementos de orden 2 (lema 2.4), y como G tiene subconjuntos de orden perfecto por la definición de grupo minimal SOP $2^t - 1$ debe dividir a $|G|$. Así pues, G (por lo tanto M) debe contener un p-subgrupo de Sylow para cada primo p divisor de $2^t - 1$.

Empezamos con un valor particular de t e intentamos construir un grupo minimal SOP $''agregando''$ factores cíclicos a $(\mathbb{Z}_2)^t$ para cada uno de los primos divisores de $2^t - 1$ esto garantiza que G es un grupo abeliano. Debido a que un grupo cíclico cuyo orden es una potencia de p, tiene exactamente $p - 1$ elementos de orden p, este proceso es un tanto complicado por la siguiente razón, cuando agregamos un factor cíclico correspondiente a un primo p particular divisor de $2^t - 1$, debemos entonces asegurar que los primos

divisores de $p-1$ también dividen a $|G|$; de otra forma G no tendría subconjuntos de orden perfecto.
Tendríamos entonces que agregar aún más factores cíclicos los cuales podrían producir un factor M cuyo orden no es libre de cuadrados. Además, no hay una razón obvia que nos asegure que este proceso de agregar factores debiera terminarse eventualmente en el grupo minimal SOP deseado. De aquí se desprende que existen valores t con los cuales podemos construir grupos minimales SOP, pero que hay solamente un número finito de tales valores.
Por otro lado, los factores de 2^t-1 que como previamente indicamos juega un papel en la construcción de M, son ocasionalmente números de Fermat. Como t crece podemos continuar construyendo grupos minimales SOP en la medida que esos números de Fermat sean primos. Una vez encontremos un número de Fermat compuesto, el proceso para.

3.1. Teorema principal

Teorema 3.1. *Sea G es un grupo abeliano finito de orden par, cuyo p-subgrupo de Sylow es un grupo cíclico para cada primo impar divisor de $|G|$. Si G es un grupo minimal SOP, entonces G es isomorfo a uno de los siguientes nueve grupos:*

1. $\mathbb{Z}_2$
2. $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$
3. $(\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$
4. $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
5. $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$
6. $(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$
7. $(\mathbb{Z}_2)^{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$
8. $(\mathbb{Z}_2)^{17} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{131071}$
9. $(\mathbb{Z}_2)^{32} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{65537}$.

Antes de la demostración debemos verificar que cada uno de los nueve grupos dados son grupos minimales SOP.
Por el análisis realizado antes de enunciar el teorema 3.1 sabemos que para que un grupo $G \cong (\mathbb{Z}_2)^t \times M$ sea un grupo minimal SOP, el grupo M está determinado por el valor de t, es decir; $|M|$ debe ser libre de cuadrados y cada uno de los factores de M deben ser primos de Fermat.

1. $\mathbb{Z}_2$:
   Del ejemplo 2.4 el grupo es minimal SOP.

2. $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$:
   $t = 2$ entonces $2^t - 1 = 3$. Obteniendo un grupo cuyo cardinal es libre de cuadrados y primo de Fermat. Por tanto,$(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ es un grupo minimal SOP.

3. $(\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$:
   $t = 3$ entonces $2^t - 1 = 7$. Como 7 es un primo de Fermat podemos agregar el grupo $\mathbb{Z}_7$ al anterior de tal forma que los factores del grupo $\mathbb{Z}_3 \times \mathbb{Z}_7$ sean primos de Fermat y el cardinal sea libre de cuadrados. Por tanto, $(\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ es un grupo minimal SOP.

4. $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$:
   $t = 4$ entonces $2^t - 1 = 15$. Como 15 es libre de cuadrados pero no es un número primo, luego lo puedo descomponer en factores de tal forma que cada factor sea un primo de Fermat, obteniendo el grupo $\mathbb{Z}_3 \times \mathbb{Z}_5$. Por lo tanto, $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ es un grupo minimal SOP.

5. $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$:
   $t = 5$ entonces $2^t - 1 = 31$. Como 31 es un primo de Fermat podemos agregar el grupo $\mathbb{Z}_{31}$ de tal forma que los factores del grupo $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$ sean primos de Fermat y el cardinal sea libre de cuadrados. Por lo tanto, $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$ es un grupo minimal SOP.

6. $(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$:
   $t = 8$ entonces $2^t - 1 = 255$. Como 255 es libre de cuadrados pero no es un número primo, luego lo puedo descomponer en factores de tal forma que cada

factor sea un primo de Fermat, obteniendo el grupo $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$. Por lo tanto, $(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$ es un grupo minimal SOP.

7. $(\mathbb{Z}_2)^{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$:
   $t = 16$ entonces $2^t - 1 = 65535$. Como 65535 es libre de cuadrados pero no es un número primo, luego lo puedo descomponer en factores de tal forma que cada factor sea un primo de Fermat, obteniendo el grupo $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$. Por lo tanto, $(\mathbb{Z}_2)^{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$ es un grupo minimal SOP.

8. $(\mathbb{Z}_2)^{17} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{131071}$:
   $t = 17$ entonces $2^t - 1 = 131071$.Como 131071 es un primo de Fermat podemos agregar a el anterior grupo obteniendo un nuevo grupo $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{131071}$ cuyo cardinal es libre de cuadrados. Por lo tanto, $(\mathbb{Z}_2)^{17} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{131071}$ es un grupo minimal SOP.

9. $(\mathbb{Z}_2)^{32} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{65537}$:
   $t = 32$ entonces $2^t - 1 = 65537$.Como 65537 es un primo de Fermat podemos agregar a el grupo $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$ obteniendo un nuevo grupo $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{65537}$ cuyo cardinal es libre de cuadrados. Por lo tanto, $(\mathbb{Z}_2)^{32} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{65537}$ es un grupo minimal SOP.

El siguiente lema será útil en la demostración del teorema 3.1

Lema 3.1. *Si p es un primo, a es un entero positivo y q es un primo divisor de $2^{p^a} - 1$. Entonces p divide a $q - 1$.*

Demostración.
Como 2^{p^a} es congruente a 1 módulo q, 2^{p^a} representa el elemento identidad en el grupo multiplicativo $(\mathbb{Z}_q)^*$ de elementos diferentes de cero de $\mathbb{Z}_q$. Se sigue que el orden de 2 en $(\mathbb{Z}_q)^*$ divide a p^a, dado que los divisores de p^a son de la forma p^n para $0 \leqslant n \leqslant a$ y el orden de 2 es mayor que 1 entonces p divide al orden de 2. Por el teorema de Lagrange el orden de un elemento en un grupo finito divide el orden del grupo, y como el orden de $(\mathbb{Z}_q)^*$ es $q - 1$ concluimos que p divide a $q - 1$. □

DEMOSTRACIÓN DEL TEOREMA 3.1

De forma directa se mostró que cada uno de los nueve grupos indicados son, en realidad un grupo minimal SOP. Debemos verificar que en la lista se encuentran incluidos todos los grupos con las características dadas.
Asumimos que $G \cong (\mathbb{Z}_2)^t \times M$ es un grupo minimal SOP, donde $|M|$ es impar y libre de cuadrados. Existen $2^t - 1$ elementos de orden 2 en G. Debido a que $2^t - 1$ debe dividir $|M|$, $2^t - 1$ es libre de cuadrados.
Sea p un primo impar divisor de t entonces $2^p - 1$ divide a $2^t - 1$ y debe ser también libre de cuadrados. Si q_1 y q_2 son primos distintos divisores de $2^p - 1$ (por lo tanto, dividen a $|M|$), entonces p divide a los dos a $q_1 - 1$ y $q_2 - 1$ (lema 3.1). Así, p^2 divide a $(q_1 - 1)(q_2 - 1)$, el número de elementos de orden $q_1 q_2$ en G, el cual por hipótesis divide $|M|$, luego p^2 divide $|M|$, una contradicción. Por lo tanto, $2^p - 1$ debe ser primo. Además, aplicando la definición y algunas propiedades sobre congruencias tenemos que:

$$\begin{aligned} 2^4 &\equiv 1 \pmod 3, \\ 2^{4n} &\equiv 1 \pmod 3, \\ 2^{4n+1} &\equiv 2 \pmod 3. \end{aligned}$$

Luego 3 divide $2^{4n+1} - 2$. Por otro lado tenemos

$$\begin{aligned} 2^{4n} &\equiv 1 \pmod 3, \\ 2^{4n+3} &\equiv 2^3 \pmod 3, \\ 2^3 &\equiv 2 \pmod 3, \\ 2^{4n+3} &\equiv 2 \pmod 3. \end{aligned}$$

Luego 3 divide $2^{4n+3} - 2$ puesto que p es primo impar y todo primo impar es de la forma $4n + 1$ o $4n + 3$ observamos que $2^p - 2$ es divisible por 3. Si p_1 y p_2 son primos distintos que dividen a t, entonces 9 divide a $(2^{p_1} - 2)(2^{p_2} - 2)$ con este el número de elementos de orden $(2^{p_1} - 1)(2^{p_2} - 1)$ en G, ya que $2^p - 1$ es primo. Se sigue entonces que 9 divide $|M|$, otra contradicción. Por lo tanto, a lo más un primo impar p divide a t. Similarmente, si $2p$ divide a t, donde p es un primo impar, entonces

$$2^p \equiv 2(mod\,3),$$
$$2^{2p} \equiv 2^2(mod\,3),$$
$$2^2 \equiv 1(mod\,3),$$
$$2^{2p} \equiv 1(mod\,3).$$

Luego 3 divide a $2^{2p}-1$ y este a su vez divide a 2^t-1 teniéndose así que 3 divide a 2^t-1, entonces 9 divide a $(2^t-1)(2^p-2)$ el número de elementos en G de orden $2(2^p-1)$. La característica de libre de cuadrados de $|M|$ excluye también esta posibilidad. Inferimos entonces que t es necesariamente una potencia de un primo.

Suponga ahora que $t = p^a$ donde p es un primo impar y $a \geqslant 2$. De la discusión anterior sabemos que 2^p-1 es un primo divisor de $2^{p^a}-1$. Como $2^{p^a}-1$ es libre de cuadrados se sigue que existe algún primo $q \neq 2^p-1$ que divide a $2^{p^a}-1$. Del lema 2.4, concluimos que p^2 divide a $(q-1)(2^p-2)$, el número de elementos de orden $q(2^p-1)$ en G, de nuevo una contradicción. Por lo tanto, $t = p^a$ con $a \leqslant 1$.

Si $a = 0$ entonces $t = 1$ y $G \cong \mathbb{Z}_2$, el primer grupo de nuestra lista (recordar: G es un grupo minimal SOP). Proseguimos asumiendo que $a = 1$ y por esto $t = p$. Como $2(2^p-1)$, el número de elementos de orden 2^p-1, divide $|G|$, podemos aplicar el mismo análisis para el exponente $p-1$ que originalmente aplicamos a t y concluimos que $p-1$ es una potencia de 2. Esto hace a p un primo de Fermat.

Para resumir: los argumentos precedentes muestran que, excepto para el caso trivial en el que $t = 1$ y $G \cong \mathbb{Z}_2$, $t = p$ un primo de Fermat para el cual $2^{p-1}-1$ divide a $|G|$, ó $t = 2^a$ con $a \geqslant 1$. En ambos casos estamos guiando una situación donde $|G|$ tiene un factor $2^{2^a}-1$ con $a \geqslant 1$. Además dado que

$$\begin{aligned}\prod_{n=0}^{a-1}(2^{2^n}+1) &= (2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)...(2^{2^{a-1}}+1)\\ &= (1+2^1+2^2+2^3+2^4+2^5+2^6+2^7)...(2^{2a-2}+1)\\ &= 1+\sum_{i=1}^{2^a-1}2^i\\ &= 1+[2(2^{2^a-1}-1)]\\ &= 1+2^{2^a}-2\\ &= 2^{2^a}-1.\end{aligned}$$

Podemos observar que

$$2^{2^a}-1 = \prod_{n=0}^{a-1}(2^{2^n}+1) = \prod_{n=0}^{a-1}F_n.$$

De donde queda bien claro que F_5 divide $2^{2^a}-1$ para $a \geqslant 6$. Sin embargo, como 3 divide $2^{2^a}-1$ y 6700417 es un factor primo de F_5, vemos que 9 divide $(2^{2^a}-1)(6700416)$, el número de elementos de orden $2(6700417)$ en G. Así, 9 divide $|M|$, una vez más contradiciendo el hecho que $|M|$ es libre de cuadrados, obsérvese que es aquí donde se hace evidente la conexión entre los números de Fermat y los grupos finitos. Como un resultado, $a \leqslant 5$ y t toma cualquiera de los siguientes valores $\{2,3,4,5,8,16,17,32\}$. Por los comentarios hechos antes de enunciar el teorema 2.3.1, cualquier grupo G minimal SOP asociado con un t dado del conjunto indicado tiene un p-subgrupo de Sylow para cada primo p que divide a 2^t-1. Además, $p-1$ divide a $|G|$. Junto con el requerimiento que $|M|$ es libre de cuadrados, estas condiciones asignan uno y sólo un grupo G para cada uno de tales t. Esto prueba que el número de grupos del tipo especificado es finito y, que todo grupo de este tipo debe aparecer en la lista dada. □
Para terminar queremos mostrar dos ejemplos importantes:

1. Aunque aquí solo trabajamos con grupos abelianos finitos, queremos dar a conocer que S_3, el grupo de simetrías de tres letras, aunque no es abeliano tiene subconjuntos de orden perfecto. Observando la tabla nos será más fácil verificar lo dicho anteriormente.

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

Luego,

$$orden\rho_0 = 1 \qquad orden\mu_1 = 2$$
$$orden\rho_1 = 3 \qquad orden\mu_2 = 2$$
$$orden\rho_2 = 3 \qquad orden\mu_3 = 2$$

Resumiendo la información en la siguiente tabla tenemos que:

ORDEN DEL ELEMENTO	CARDINAL DEL SUBCONJUNTO O.
1	1
2	3
3	2

Por tanto S_3 tiene subconjuntos de orden perfecto.

2. Por otro lado, el único ejemplo conocido de un grupo minimal SOP que contiene un p-subgrupo de Sylow de orden impar no cíclico es

$$(\mathbb{Z}_2)^{11} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times (\mathbb{Z}_{11})^2 \times \mathbb{Z}_{23} \times \mathbb{Z}_{89}.$$

Bibliografía

[1] BAUMSLAG, Benjamín,y BRUCE, Chandler. *Teoría y problemas de teoría de grupos*. México: Mc Graw-Hill, 1972.

[2] DORRONSORO, José,y HERNÁNDEZ, Eugenio. *Números, grupos y anillos*. España: Addison-Wesley/Universidad Autónoma de Madrid, 1996.

[3] FINCH, Carrie,y JONES, Lenny. *A curious connection between Fermat numbers and finite groups*. En: The American Mathematical Monthly. Vol. 109, No. 6.(jun-jul.2002); p 517-524.

[4] FRALEIGH, John B. *Algebra abstracta.Primer curso*. Estados Unidos: Addison-Wesley Iberoamericana, 1982.

[5] JIMENEZ, Rafael, GORDILLO, Enrique, y RUBIANO, Gustavo. *Teoría de números para principiantes*. Bogotá: Unibiblos Sección Imprenta. Universidad Nacional de Colombia, 1999.