Teoría de Grupos

Cristo Daniel Alvarado

28 de enero de 2024

Índice general

Capítulo 7

Grupos de Sylow

7.1. Los p-grupos

Cuando tenemos un grupo finito G, para analizar su estructura surgen problemas ya que, mientras más complicada sea su descomposición en primos, más complicado es entender su estructura (casi por norma general). Por ello, se estudiará en caso particular en que el orden de G es una potencia de un número primo.

Proposición 7.1.1
Sean p un número primo, G un grupo de orden p^n, con $n \in \mathbb{N}$, actuando G sobre un conjunto no vacío. Entonces,

$$|X| \equiv |X^G| \mod p$$

Demostración:
Sea R un conjunto completo de representantes bajo la relación de acción de G sobre X. Claro que $X^G \subseteq R$, y por ende, la ecuación de clase generalizada está dada por:

$$|X| = |X^G| + \sum_{x \in R \backslash X^G} |G \cdot x|$$

donde p divide a $|G \cdot x|$, para cada $x \in R \backslash X^G$. Por tanto, se sigue que $|X| \equiv |X^G| \mod p$. □

A continuación, analizaremos un ejemplo que nos servirá para entender la teoría de más adelante.

Ejemplo 7.1.1
Sean G un grupo finito, p un número primo, y H un subgrupo de G tal que $|H| = p^m$, donde $m \in \mathbb{Z}_{\geq 0}$. Sea X el conjunto

$$X = \{gH | g \in G\}$$

es decir, X es el conjunto de clases laterales izquierdas de H en G. Tenemos que H actúa sobre X por traslación izquierda, dada la acción:

$$h \cdot gH = hgH$$

para todo $h \in H$. Por definición, es inmediato que $[G : H] = |X|$, y además:

$$X^H = \{gH | g \in N_G(H)\}$$

ya que, si $g \in N_G(H)$, entonces $gh = hg$, para todo $h \in H$. Luego:

$$h \cdot gH = hgH = ghH = gH, \quad \forall h \in H$$

por tanto, $gH \in X^H$. De esta forma $|X^H| = [N_G(H) : H]$. Por la proposición 7.1.1, se tiene que

$$[G : H] \equiv [N_G(H) : H] \quad \text{mód } p$$

en particular, si $p|[G : H]$, entonces $p|[N_G(H) : H]$ lo cual implica que la contención de H en $N_G(H)$ es propia.

Teorema 7.1.1 (**Teorema de Cauchy**)
Sean p un número primo y G un grupo finito tal que p divide a $|G|$. Enotnces existe un elemento de orden p en G.

Demostración:
Sea

$$X = \{(x_1, \ldots, x_p) | x_i \in G, \forall i \in [|1, p|] \ \& \ x_1 \cdots x_p = e\}$$

X es no vacío, pues $(e, \ldots, e) \in X$. Definamos la función

$$\begin{aligned} f : X &\to \overbrace{G \times \cdots \times G}^{p\text{-veces}} \\ (x_1, \ldots, x_p) &\mapsto (x_1, \ldots, x_{p-1}) \end{aligned}$$

Afirmamos que f es biyectiva. En efecto, veamos que

1. f **es suprayectiva**. Sea $(x_1, \ldots, x_{p-1}) \in G^{p-1}$. Tomemos $x_p = (x_1 \cdots x_{p-1})^{-1} = x_{p-1}^{-1} \cdots x_1^{-1}$. Se tiene que:

   $$\begin{aligned} x_1 \cdots x_{p-1} \cdot x_p &= x_1 \cdots x_{p-1} \cdot (x_{p-1}^{-1} \cdots x_1^{-1}) \\ &= e \end{aligned}$$

   por lo cual, $(x_1, \ldots, x_{p-1}, x_p) \in X$. Y,

   $$f(x_1, \ldots, x_{p-1}, x_p) = (x_1, \ldots, x_{p-1})$$

   Así, f es suprayectiva.

2. f **es inyectiva**. Sean $Z = (z_1, \ldots, z_p), Y = (y_1, \ldots, y_p) \in X$ tales que $f(z_1, \ldots, z_p) = f(y_1, \ldots, y_p)$, es decir

   $$(z_1, \ldots, z_{p-1}) = (y_1, \ldots, y_{p-1})$$

   Pero, como $Z, Y \in X$, debe de suceder que

   $$\begin{aligned} z_1 \cdots z_p &= e \\ y_1 \cdots y_p &= e \end{aligned}$$

   por lo cual

   $$\begin{aligned} z_p &= z_{p-1}^{-1} \cdots z_1^{-1} \\ y_p &= y_{p-1}^{-1} \cdots y_1^{-1} \end{aligned}$$

   pero, como $(z_1, \ldots, z_{p-1}) = (y_1, \ldots, y_{p-1})$ entonces $z_p = y_p$. Por tanto, $Z = Y$. Así, f es inyectiva.

por (1) y (2), f es biyectiva, luego $|X| = |G|^{p-1}$. Como $p \mid |G|$, entonces $p \mid |X|$, es decir

$$|X| \equiv 0 \mod p$$

Ahora hacemos actuar al grupo cíclico $\mathbb{Z}/p\mathbb{Z}$ en el conjunto X a través de la acción cíclica. Si $(x_1, \ldots, x_p) \in X$, su órbita está dada por el conjunto:

$$\mathbb{Z}/p\mathbb{Z} \cdot (x_1, \ldots, x_p) = \{(x_1, \ldots, x_p), (x_2, \ldots, x_p, x_1), \ldots (x_p, x_1, \ldots, x_{p-1})\}$$

Luego, dado $(x_1, \ldots, x_p) \in X$, se tiene que $(x_1, \ldots, x_p) \in X^{\mathbb{Z}/p\mathbb{Z}}$ si, y solo si $x_1 = x_2 = \cdots = x_p$. Ahora bien, por la proposición 7.1.1,

$$|G|^{p-|} = |X| \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \mod p$$

donde $\mathbb{Z}/p\mathbb{Z} \neq \emptyset$, pues $(e, \ldots, e) \in X$. Por tanto, $p \mid |X^{\mathbb{Z}/p\mathbb{Z}}|$, es decir $|X^{\mathbb{Z}/p\mathbb{Z}}| = pr > 1$, donde $r \in \mathbb{N}$. Por lo cual, existe un elemento $a \in G \setminus \{e\}$ tal que $a^p = e$. □

Este teorema se usa para probar el teorema que sigue de esta definición.

Definición 7.1.1
Sea p un número primo. Todo grupo G se dice que es **p-grupo**, si todo elemento de G es del orden p^t, donde $t \in \mathbb{Z}_{\geq 0}$.

Notemos que la identidad e de un grupo G es de orden $1 = p^0$ para cada $p \in \mathbb{N}$ número primo. Si H es un subgrupo de G tal que H es p-grupo, diremos que H **es p-subgrupo de** G. Por lo cual, $\langle e \rangle$ es un p-subgrupo de G.

Proposición 7.1.2
Sea p un número primo. Un grupo finito G es p-grupo si, y solo si G es del orden una potencia de p.

Teorema 7.1.2 (Nombre)
Teorema

Proposición 7.1.3 (Nombre)
Proposición

Corolario 7.1.1 (Nombre)
Corolario

Lema 7.1.1 (Nombre)
Lema

Definición 7.1.2 (Nombre)
Definición

Observación 7.1.1 (Nombre)
Observación

Ejemplo 7.1.2 (Nombre)
Ejemplo

Ejercicio 7.1.1 (Nombre)
Ejercicio