Universidad Nacional Autónoma de México
Facultad de Ciencias
Álgebra Moderna I

Primer examen parcial de recuperación

Ángel Iván Gladín García
No. cuenta: 313112470
`angelgladin@ciencias.unam.mx`

3 de junio de 2020

Ejercicio 1. (25 puntos)

Pruebe que si $\alpha = \beta_1\beta_2 \cdots \beta_m$ es un producto de r_i-ciclos disjuntos β_i, entonces el entero positivo s más pequeño con $\alpha^s = 1$ es el mínimo cómun múltiplo de $\{r_1, r_2, \dots, r_m\}$.

Demostración. Como por hipótesis los β_i son disjuntos, podemos usar el hecho de que conmutan para poder hacer lo siguiente,

$$\alpha^n = (\beta_1\beta_2 \cdots \beta_m)^n = \beta_1^n \beta_2^n \cdots \beta_m^n$$

para toda $n \in \mathbb{Z}$. Supongamos que $\alpha^n = 1$ si y sólo si $\beta_i^n = 1$ para $1 \leq i \leq m$. Como α es un n-ciclo y β_i es un r_i-ciclo, se sigue que que todo r_i divide a n, y éso a su vez implica que el $m.c.m.(r_1, r_2, \dots, r_m) \mid n$. Como $\beta_i^n = 1$ para $1 \leq i \leq m$ justo aseguramos que n es el entero más pequeño. Renombrando a $m.c.m.(r_1, r_2, \dots, r_m) = s = n$, se sigue que s es el entero mas pequeño positivo tal que $\alpha^s = 1$. □

Ejercicio 2. (25 puntos)

Sea S un subconjunto no vacío de un grupo G y definimos una relación en G dado por $a \sim b$ si y sólo si $ab^{-1} \in S$. Muestre que $\sim$ es una relación de equivalencia si y sólo si S es un subgrupo de G.

Demostración.

- **Reflexividad:** Como $aa^{-1} = 1 \in S$, por tanto $a \sim a$.
- **Simetría:** Se tiene que $a \sim b$, entonces $ab^{-1} \in S$, entonces $(ab^{-1})^{-1} \in S$, de ahí que $ba^{-1} \in S$. Por tanto $b \sim a$.
- **Transitividad:** Si $a \sim b$ y $b \sim c$, se tiene que $ab^{-1} \in S$ y $bc^{-1} \in S$, pero se tiene que $(ab^{-1})(bc^{-1}) \in S$, lo cual implica que $ac^{-1} \in S$. Por tanto $a \sim c$.

Se asumió que S era un subgrupo de G por un teorema[1] visto en clase. □

Ejercicio 3. (25 puntos)

Demuestra el Teorema de Wilson: Si p es un primo, entonces

$$(p-1)! \equiv -1 \mod p$$

Demostración. Consideremos el grupo G de elementos no cero de $\mathbb{Z}_p$ forma un grupo multiplicativo como $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ donde $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1], [2], \dots, [p-1]\}$ y $(\cdot)$ como el producto en $\mathbb{Z}$, también se tiene que G es abeliano por $\mathbb{Z}$.

[1] **Teorema 2.2** *Un subconjunto S de un grupo G es un subgrupo si y sólo si $1 \in S$ y $s, t \in S$ implica que $st^{-1} \in S$*

Observemos que como p es primo y sea $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tal que $x^2 = 1$ si tiene que:

$$\begin{aligned} & x^2 \equiv 1 \mod p \\ \iff & x^2 - 1 \equiv 0 \mod p \\ \iff & (x+1)(x-1) \equiv 0 \mod p \\ x = & np \pm 1 \end{aligned}$$

Concluyendo así que $x = 1$ ó $x = p - 1$.

Tambien observando que se cumple que $(p-2)! \equiv 1 \mod p$.

Por tanto,

$$(p-1)! \equiv (p-2)! \cdot (p-1) \equiv -1 \mod p$$

□

Ejercicio 4. (25 puntos)

Un grupo G es abeliano si y sólo si la función $\varphi : G \to G$ dada por $\varphi(g) = g^{-1}$ es un automorfismo[2].

Demostración.

($\Longrightarrow$) Supongamos que G es abeliano. Sean $g, h \in G$. Si $\varphi(g) = \varphi(h)$, entonces se tiene que $g^{-1} = h^{-1}$, lo que implica que $g = h$ provando así que φ es inyectiva.

Sea $g \in G$, se tiene que $g^{-1} \in G$ y $\varphi(g^{-1}) = (g^{-1})^{-1} = g$ teniendo así que φ es suprayectiva.

Para concluir, sean $g, h \in G$ se sigue que:

$$\begin{aligned} \varphi(gh) &= (gh)^{-1} = h^{-1}g^{-1} & \\ &= g^{-1}h^{-1} & \text{Por ser } G \text{ abeliano.} \\ &= \varphi(g)\varphi(h) & \end{aligned}$$

Teniendo así que φ es un automorfismo.

($\Longleftarrow$) Supongamos que la función $\varphi : G \to G$ dada por $\varphi(g) = g^{-1}$ es un automorfismo. Sean $g, h \in G$, entonces:

$$\begin{aligned} h^{-1}g^{-1} &= (gh)^{-1} & \\ &= \varphi(gh) & \\ &= \varphi(g)\varphi(h) & \text{Por ser } \varphi \text{ un homomorfismo.} \\ &= g^{-1}h^{-1} & \end{aligned}$$

Lo que implica que $gh = hg$. Como $g, h \in G$ fueron arbitrarios, se concluye que G es abeliano.

□

[2] Un automorfismo de un grupo G es un isomorfismo $\varphi : G \to G$.