12/05

Practico 7: grupos – Conceptos Básicos

Ejercicio 6. Sean H_1 y H_2 dos subgrupos de un grupo G.

a. Probar que $H_1 \cap H_2$ es un subgrupo de G.

b. Probar que si $H_1 \cup H_2$ es un subgrupo de G entonces $\underbrace{H_1 \subseteq H_2}$ o $\underbrace{H_2 \subseteq H_1}$ (en general la unión de subgrupos **no** es un subgrupo).

Def (Subgrupo): $H \subseteq G$ es subgrupo si

(1) $e \in H$

(2) Si $g \in H \Rightarrow g^{-1} \in H$ (cerrado por inversos)

(3) Si $g, h \in H \Rightarrow gh \in H$. (cerrado por la operación)

(a) Queremos ver (1), (2) y (3) para $H = H_1 \cap H_2$.

(1) $e \in H$: $\left\{\begin{array}{l} e \in H_1 \text{ pues } H_1 \text{ es subgrupo} \\ e \in H_2 \text{ pues } H_2 \text{ es subgrupo} \end{array}\right. \Rightarrow e \in H_1 \cap H_2$ ✓

(2) $g \in H \Leftrightarrow \left\{\begin{array}{l} g \in H_1 \\ g \in H_2 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} g^{-1} \in H_1 \\ g^{-1} \in H_2 \end{array}\right. \Leftrightarrow g^{-1} \in H_1 \cap H_2$.

(3) $\begin{array}{l} g \in H \\ h \in H \end{array} \Rightarrow \left\{\begin{array}{l} g, h \in H_1 \Rightarrow gh \in H_1 \\ g, h \in H_2 \Rightarrow gh \in H_2 \end{array}\right\} \Rightarrow gh \in H_1 \cap H_2$.

(b) $2\mathbb{Z}$ son subgrupo de $(\mathbb{Z}, +, 0)$

$3\mathbb{Z}$ es subgrupo de $(\mathbb{Z}, +, 0)$

$2\mathbb{Z} \cup 3\mathbb{Z} = \{ x \in \mathbb{Z} : x = \dot{2} \text{ o } x = \dot{3} \}$

$e \in 2\mathbb{Z} \cup 3\mathbb{Z}$ ✓

Cerrado por inverso

X Cerrado por la suma: $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z} \Rightarrow$ no es subgrupo.

→ Obs: $2\mathbb{Z} \not\subseteq 3\mathbb{Z}$

$3\mathbb{Z} \not\subseteq 2\mathbb{Z}$

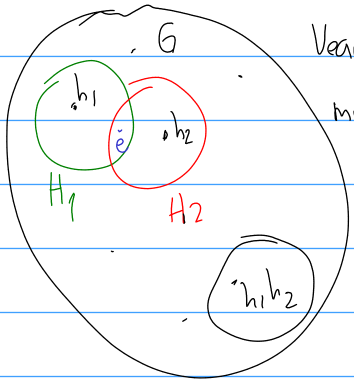
Sin embargo $\begin{array}{l} 2\mathbb{Z} \text{ es subgrupo} \\ 4\mathbb{Z} \text{ es subgrupo} \end{array}$ $4\mathbb{Z} \subseteq 2\mathbb{Z} \Rightarrow 2\mathbb{Z} \cup 4\mathbb{Z} = 2\mathbb{Z}$ es subgrupo.

Suponemos que $H_1 \cup H_2$ es subgrupo pero $H_1 \overset{A}{\nsubseteq} H_2$ y $\overset{B}{\underline{H_2} \nsubseteq H_1}$.

Por A $\exists\ h_1 \in H_1 \setminus H_2$

Por B $\exists\ h_2 \in H_2 \setminus H_1$

Queremos ver que $h_1 \cdot h_2 \notin H_1 \cup H_2$, es decir, $h_1 \cdot h_2 \notin H_1$ y $h_1 h_2 \notin H_2$



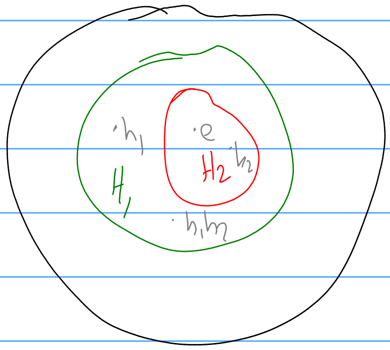
Veamos que $h_1 \cdot h_2 \notin H_1$. Supongamos que $h_1 h_2 \in H_1$, multiplicamos a izq. por $h_1^{-1} \in H_1$: $\underbrace{h_1^{-1} h_1} h_2 \in H_1$

$\Rightarrow e \cdot h_2 = h_2 \in H_1$. ↯

$h_1 h_2 \notin H_2$: multiplicamos por h_2^{-1} a derecha:

Si $h_1 h_2 \in H_2 \Rightarrow h_1 h_2 h_2^{-1} \in H_2$ (pues H_2 subgrupo)

$\Rightarrow h_1 \in H_2$ ↯.



Práctico 8: Grupos (Lagrange, ordenes)

Teorema de Lagrange: *Si G es un grupo finito y H un subgrupo de G entonces $|H|$ divide a $|G|$.*

$g \in G \Rightarrow o(g) = \min\{n \in \mathbb{Z}^+ : g^n = e\}$

Ejemplo: $(\mathbb{Z}_3, +, 0)$ orden del $1 = \min\{n \in \mathbb{Z}^+ : \underbrace{1+1+\dots+1}_{n} = 0\}$
$= 3$

$(GL_3(\mathbb{R}), \cdot, Id)$ $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \Rightarrow o(A) = 2$

Ejercicio 2.

a. Sean $G = \mathrm{GL}(2,\mathbb{R})$ el grupo multiplicativo de las matrices invertibles 2×2 con coeficientes en $\mathbb{R}$, $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ y $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$. Probar que $o(A) = 4$, B orden $o(B) = 3$ y que AB tiene orden infinito.

b. Hallar elementos $a, b \in \mathbb{Z}_2 \times \mathbb{Z}$ de orden infinito tales que $a + b$ tiene orden finito (suma coordenada a coordenada).

(a)

$o(A) = 4$

$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq Id$

$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq Id$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq Id$

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$A^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = Id$ ✓ $\Rightarrow o(A) = 4.$

$o(B) = 3$

$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$\underset{B}{\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}} \underset{B^2}{\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}} \underset{B^3}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}$

$o(AB) = \infty$ $AB = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \overset{AB}{\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}}$

...

Podemos ver por inducción que $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$n = \checkmark$

(b) Queremos $a=(a_1,a_2)\in \mathbb{Z}_2\times\mathbb{Z}$ y $b=(b_1,b_2)$ tales que (a_1+b_1, a_2+b_2) tengan orden finito pero a, b tengan orden ∞.

Ejemplos que no funcionan: $a=(0,1)$ $b=(0,1)$ $\Rightarrow$ $a+b=(0,2)$ tiene orden ∞.

$a=(1,0)$ $b=(1,0)$ $\Rightarrow$ $a+b=(2,0)=(0,0)$ tiene orden finito. Pero $\Rightarrow$ $a=b$ también!

Ejemplo que sirve: $a=(1,k)$ $b=(1,-k)$ con $k\neq 0$

$a+b=(0,0)$ que tiene orden 1. Además

$a^n=(n\cdot 1, n\cdot k)\neq(0,0)$ si $k\neq 0$ $\Rightarrow$ tiene orden ∞.

Lo mismo ocurre con b.

Ejercicio 3. Escriba la tabla de multiplicación de $U(18)$. Hallar los órdenes de los elementos de $U(18)$. ¿Es $U(18)$ cíclico?

$U(18)=\{n<18$ tales que $\text{mcd}(n,18)=1\}$

$|U(18)|=\varphi(18)=\varphi(3^2\cdot 2)=\varphi(2)\cdot\varphi(9)=9-3=6$

$U(18)=\{\bar{1},\bar{5},\bar{7},\bar{11},\bar{13},\bar{17}\}$

·	①	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7					
11	11					
13	13					
17	17					

$o(1)=1$

$5^1\neq 1$

$\boxed{5^2}=7\neq 1$

$\boxed{5^3}=5^2\cdot 5=25\cdot 5\equiv 7\cdot 5\equiv 17\not\equiv 1$

$5^4\equiv 5^3\cdot 5\equiv 17\cdot 5\equiv 13\not\equiv 1$

$5^5\equiv 5^4\cdot 5\equiv 13\cdot 5\equiv 11\not\equiv 1$

$\boxed{5^6}\equiv 5^5\cdot 5\equiv 11\cdot 5\equiv 1$

Simplificar: Cuando G es finito, por Lagrange el orden de un element divide al orden del grupo $\Rightarrow$ no hace falta calcular 5^4 ni 5^5 porque $4\nmid 6$.

$5\nmid 6$.