17-05

Práctico 8

Recordar: • G grupo, $g \in G \Rightarrow o(g) = \min\{n \in \mathbb{Z}^+ : g^n = e\}$ o ∞ si $\nexists$ el mínimo.

$f: \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ tiene orden 4 en $GL_2(\mathbb{R})$

• Lagrange: $H < G$, G finito $\Rightarrow |H| \mid |G|$.

• $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \rightsquigarrow$ Lagrange: si G es finito $o(g) = |\langle g \rangle|$ divide a $|G|$.

Ejercicio 4.

a. Sea G un grupo. Probar que si $a^n = e_G \Rightarrow o(a) | n$.

b. Sea G un grupo. Probar que si $a^n \neq e_G \Rightarrow o(a) \nmid n$

c. Sea G un grupo. Probar que $o(xy) = o(yx)$, $\forall x, y \in G$.

d. Probar que si $a \in U(n) \Rightarrow o(a) | \varphi(n)$.

e. i) Hallar el resto de dividir 2^{20} entre 253.

ii) Sabiendo además que $2^{55} \equiv -45 \pmod{253}$, hallar el orden de 2 en $U(253)$.

(a)

$n = o(a)q + r$ con $0 \leq r < o(a)$

Queremos ver que $r = 0$.

$a^n = e \rightsquigarrow a^{o(a)q + r} = e \Rightarrow \underbrace{\left(a^{o(a)}\right)^q}_{e} \cdot a^r = e$

$\Rightarrow r = 0$ o contradice la minimalidad de $o(a)$

(b) Mismo argumento.

Dividimos n entre $o(a)$. $n = o(a) \cdot q + r$

con $0 \leq r < o(a)$ Queremos $r \neq 0$.

Si $r = 0$ $a^n = a^{o(a) \cdot q} = e^q = e$. ↯

(c)

Tenemos que $(xy)^n = e \iff (yx)^n = e$.

pues si $xyxy\ldots xy = e$
$\Rightarrow x^{-1} = yxy\ldots xy$
y el inverso conmuta con x
$\Rightarrow yxy\ldots xyx = e$,
$(yx)^n$.

$\Rightarrow$ Si $o(xy) = n \rightsquigarrow (yx)^n = e$ pues $(xy)^n = e$.

Si no fuera $n = \min\{n \in \mathbb{Z}^+ : (yx)^n = e\}$

$\Rightarrow \exists\, m < n$ tq $(yx)^m = e$

y por la ppd $\Rightarrow (xy)^m = e$.

(d) Por Lagrange y la ppd: $|\langle g \rangle| = o(g)$, tenemos que si $a \in U(n) \Rightarrow o(a) \mid |U(n)|$

La parte (d) se deduce de $|U(n)| = \varphi(n)$.

(e) i) Euler: si $\text{mcd}(2, 253) = 1$ ✓ $\Rightarrow 2^{\varphi(253)} \equiv 1 \pmod{253}$.

$\varphi(253) = \varphi(23) \cdot \varphi(11) = 22 \cdot 10 = 220$.

. No nos sirve, usemos el Teorema Chino.

Queremos $*$ $\begin{cases} x \equiv 2^{20} \pmod{11} \\ x \equiv 2^{20} \pmod{23} \end{cases}$ sabiendo (Euler) $\begin{cases} 2^{10} \equiv 1 \pmod{11} \\ 2^{22} \equiv 1 \pmod{23} \end{cases}$

$\Rightarrow *$ nos queda: $\leftarrow *$ $\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2^{-2} \equiv (12)^2 \equiv 6 \pmod{23} \end{cases}$

Solución: $x \equiv 86 \pmod{253}$

ii) Por Lagrange $o(2) \mid \varphi(253) = 220$

$\#\text{Div}_+(220) = \#\text{Div}_+(11 \cdot 5 \cdot 2^2) = (2)(2)(3) = 12$.

Tenemos que descartar posibles órdenes.

$\{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, 220\}$

. Por hipótesis descartamos 55, si $2^{11} \equiv 1 \ (253) \Rightarrow 2^{55} \equiv 2^{5 \cdot 11} \equiv 1 \ (253)$ ↯

$\Rightarrow$ descartamos 11

. Por parte previa $2^{20} \neq 1 \Rightarrow$ descartamos divisores de 20: 1, 2, 4, 5, 10, 20

. $2^{110} = 2^{55 \cdot 2} \equiv (-45)^2 \equiv 2025 \equiv 1 \ (253)$, entonces $o(2)$ divide a 110.

. Como $2^{22} \equiv 86 \cdot 2^2 \equiv 91 \ (253)$ debe ser $o(2) = 110$.