G grupo cíclico de orden n

g un generador de G $\rightsquigarrow$ $o(g) = n$

$$G = \langle g \rangle = \{\underset{\substack{\shortparallel \\ g^n}}{e}, g, g^2, g^3, \dots, g^{n-1}\}$$

$$g^m \text{ es un generador de } G \iff mcd(m, \underset{\substack{\shortparallel \\ o(g)}}{n}) = 1$$

Ejercicio 2

generadores de $U(18)$?

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

$$|U(18)| = \varphi(18) = 18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6$$

$$18 = 2 \cdot 3^2$$

* $\overline{5}$ es generador?

$$\overline{5}^2 = \overline{5} \times \overline{5} = \overline{25} = \overline{7}$$
$$\overline{5}^3 = \overline{7} \times \overline{5} = \overline{17}$$
$$\overline{5}^4 = \overline{17} \times \overline{5} = \overline{13}$$
$$\overline{5}^5 = \overline{13} \times \overline{5} = \overline{11}$$
$$\overline{5}^6 = \overline{11} \times \overline{5} = \overline{1}$$

$$o(\overline{5}) = 6 = |U(18)|$$

$\Rightarrow$ $\overline{5}$ es un generador de $U(18)$

* otros generadores?

$$U(18) = \langle \overline{5} \rangle = \{\overline{1}, \overline{5}, \underset{\times}{\overline{5}^2}, \underset{\times}{\overline{5}^3}, \underset{\times}{\overline{5}^4}, \underset{\checkmark}{\overline{5}^5}\}$$

$$\overline{5}^m \text{ es generador de } U(18) \iff mcd(m, \underbrace{o(\overline{5})}_{=6}) = 1$$

los generadores de $U(18)$ son $\overline{5}$ y $\overline{5}^5 = \overline{11}$

Teorema de Lagrange

$$\left.\begin{array}{l} G \text{ un grupo finito} \\ H \text{ un subgrupo de } G \end{array}\right\} \Rightarrow |H| \text{ divide a } |G|$$

$|G|$ = cantidad de elementos de G = orden de G

Ejercicio 6. Sea G un grupo con neutro e. Sean H y K subgrupos finitos de G.

a. Probar que $|H \cap K|$ divide a $\mathrm{mcd}(|H|, |K|)$.

b. Usando lo anterior, probar que si $|H|$ y $|K|$ son coprimos, entonces $H \cap K = \{e\}$.

c. Hallar los posibles valores de $|H|$ si $K \subsetneq H \subsetneq G$, $|G| = 660$ y $|K| = 66$.

a) H y K subgrupos finitos de G

$\Rightarrow H \cap K$ es un subgrupo de G

queremos probar que $|H \cap K| \mid \mathrm{mcd}(|H|, |K|)$

$$\left.\begin{array}{l} H \cap K \text{ es subgrupo de } H \\ H \text{ es un grupo finito} \end{array}\right\} \underset{\text{Lagrange}}{\Rightarrow} |H \cap K| \text{ divide a } |H|$$

$$\left.\begin{array}{l} H \cap K \text{ es subgrupo de } K \\ K \text{ es un grupo finito} \end{array}\right\} \underset{\text{Lagrange}}{\Rightarrow} |H \cap K| \text{ divide a } |K|$$

$$\left.\begin{array}{l} |H \cap K| \text{ divide a } |H| \\ |H \cap K| \text{ divide a } |K| \end{array}\right\} \Rightarrow |H \cap K| \text{ divide a } \mathrm{mcd}(|H|, |K|)$$

b) $|H|$ y $|K|$ coprimos $\Rightarrow H \cap K = \{e\}$

$|H|$ y $|K|$ son coprimos $\Rightarrow \mathrm{mcd}(|H|, |K|) = 1$

$|H \cap K|$ divide a $\mathrm{mcd}(|H|, |K|) = 1 \Rightarrow |H \cap K| = 1$

$\Rightarrow H \cap K = \{e\}$

c) $\overline{K \subsetneq H \subsetneq G}$

$|G| = 660$

$|K| = 66$

posibles valores de $|H|$?

$\left.\begin{array}{l} * \ K \text{ es subgrupo de } H \\ \quad H \text{ grupo finito} \end{array}\right\} \Rightarrow |K| \mid |H| \Rightarrow 66 \mid |H| \Rightarrow |H| = 66q$ para algún $q \in \mathbb{Z}$

$\left.\begin{array}{l} * \ H \text{ es subgrupo de } G \\ \quad G \text{ grupo finito} \end{array}\right\} \Rightarrow |H| \mid |G| \Rightarrow 66q \mid 660$

$\Rightarrow 660 = 66qq'$ para algún $q' \in \mathbb{Z}$

$\Rightarrow 66 \cdot 10 = 66qq'$

$\Rightarrow 10 = qq'$

$\Rightarrow q \mid 10$

posibilidades para q: $\overset{\times}{1}, 2, 5, \overset{\times}{10}$

$q = 1$: $|H| = 66 = |K|$ y esto no puede ser porque $K \subsetneq H$

$q = 2$: $|H| = 66 \cdot 2 = 132$ ✓

$q = 5$: $|H| = 66 \cdot 5 = 330$ ✓

$q = 10$: $|H| = 66 \cdot 10 = 660 = |G|$ y esto no puede ser porque $H \subsetneq G$

Ejercicio 8. Sea $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ una función biyectiva. Probar que el inverso de f es:

$$f^{-1} = \underbrace{f \circ f \circ \ldots \circ f}_{n!-1 \text{ veces}}.$$

$f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ función biyectiva

$f \in S_n$

para probar que $f^{-1} = \underbrace{f \circ f \cdots \circ f}_{n!-1 \text{ veces}}$ vamos a ver que

$$\underbrace{f \circ f \circ \cdots \circ f}_{n!-1 \text{ veces}} \circ f = id$$

entonces queremos probar que $\underbrace{f \circ f \circ f \cdots \circ f}_{n! \text{ veces}} = id$

$\ulcorner$ G grupo finito, $g \in G$

$$g^{|G|} = e$$

$o(g) = |\langle g \rangle|$

$\langle g \rangle$ es un subgrupo de G $\Rightarrow |\langle g \rangle| \mid |G|$

$\Rightarrow o(g) \mid |G|$

$\Rightarrow |G| = o(g)\, q$ para algún $q \in \mathbb{Z}$

$$g^{|G|} = g^{o(g)q} = (\underbrace{g^{o(g)}}_{e})^{q} = e$$

$\llcorner$

$f \in S_n$

queremos probar que $\underbrace{f \circ f \circ f \cdots \circ f}_{n! \text{ veces}} = id$

$$f^{|S_n|} = id$$

$$\underbrace{f \circ f \circ f \cdots \circ f}_{|S_n| \text{ veces}} = id$$

$g \in S_n$ $\quad g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ g(1) & g(2) & g(3) & & g(n) \end{pmatrix} \to$ $n!$ posibilidades para esta fila

$g(1)$: n pos. $\quad g(2)$: $n-1$ pos $\quad g(3)$: $n-2$ pos.

$|S_n| = n!$

entonces: $\underbrace{\overbrace{f \circ f \circ f \cdots \circ}^{\text{es } f^{-1}} f}_{n! \text{ veces}} = id \Rightarrow f^{-1} = \underbrace{f \circ f \circ f \cdots \circ f}_{n! - 1 \text{ veces}}$

Ejercicio 7.

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

b. i) Hallar el resto de dividir 2^{20} entre 253. Sugerencia: $2^8 = 256$.

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

a) Si $a \in U(n) \Rightarrow o(a) \mid \varphi(n)$

$\varphi(n) = |U(n)|$

entonces queremos probar que $o(a) \mid |U(n)|$

$o(a) = |\langle a \rangle|$

$\langle a \rangle$ es un subgrupo de $\underbrace{U(n)}_{\text{grupo finito}} \Rightarrow |\langle a \rangle| \mid |U(n)|$

$\Rightarrow o(a) \mid |U(n)|$

$\Rightarrow o(a) \mid \varphi(n)$

b) Buscamos el orden de $\bar{2}$ en $U(253)$

$\bar{2} \in U(253) \Rightarrow o(\bar{2}) \mid \varphi(253)$

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

$253 = 11 \cdot 23$

$220 = 11 \cdot 10 \cdot 2 = 2^2 \cdot 5 \cdot 11$ $\qquad 2^\alpha 5^\beta 11^\gamma$ $\quad |Div_+(220)| = 3 \cdot 2 \cdot 2 = 12$

$Div_+(220) = \{\underbrace{\cancel{1}, \cancel{2}, \cancel{4}, \cancel{5}, \cancel{10}, \cancel{11}, \cancel{20}, \cancel{22}, \cancel{44}, \cancel{55}, 110, 220}_{\text{posibilidades para } o(\bar{2})}\}$

$2^{55} \equiv -45 \pmod{253} \Rightarrow 2^{55} \equiv 208 \pmod{253}$

$\Rightarrow o(\bar{2}) \neq 55$

$\bar{2}^2 = \bar{4}$ $\qquad 2^2 \equiv 4 \pmod{253}$ $\rightsquigarrow$ descartamos 2

$2^4 \equiv 16 \pmod{253}$ $\rightsquigarrow$ descartamos 4

$2^5 \equiv 16 \cdot 2 \pmod{253}$

$\equiv 32 \pmod{253}$ ⇝ descartamos 5

$2^{10} \equiv 32 \cdot 32 \pmod{253}$

$\equiv 12 \pmod{253}$ ⇝ descartamos 10

$2^{11} \equiv 12 \cdot 2 \pmod{253}$

$\equiv 24 \pmod{253}$ ⇝ descartamos 11

$2^{20} \equiv 12 \cdot 12 \pmod{253}$

$\equiv 144 \pmod{253}$ ⇝ descartamos 20

$2^{22} \equiv 24 \cdot 24 \pmod{253}$

$\equiv 70 \pmod{253}$ ⇝ descartamos 22

$2^{44} \equiv 70 \cdot 70 \pmod{253}$

$\equiv 93 \pmod{253}$ ⇝ descartamos 44

$2^{110} \equiv (-45)(-45) \pmod{253}$

$\equiv 2025 \pmod{253}$

$\equiv 1 \pmod{253}$

$\overline{2}^{110} = \overline{1} \Rightarrow o(\overline{2}) = 110$