

SOLUCIONES DEL SEGUNDO PARCIAL.

**Ejercicio 1.**

- A) Si  $G$  es un grupo finito y  $H < G$  entonces  $|H| \mid |G|$ .
- B)  $o(g) = |\langle g \rangle| \mid |G| \quad \forall g \in G$  (Lagrange).
- C) Como  $\#U(29) = 28$ , por Lagrange, los posibles órdenes de  $\bar{2}$  en  $U(29)$  son 1, 2, 4, 7, 14 ó 28.  
Como  $2^4 = 16 \not\equiv 1 \pmod{29}$  descartamos al 1 al 2 y al 4.  
Por otra parte  $2^5 = 32 \equiv 3 \pmod{29} \Rightarrow 2^{15} \equiv 3^3 = 27 \equiv -2 \pmod{29} \rightarrow 2^{14} \equiv -1 \not\equiv 1 \pmod{29}$  así que descartamos al 14 y también al 7 como órdenes.  
Por lo tanto  $o(\bar{2}) = 28$  en  $U(29)$  y por lo tanto 2 es raíz primitiva módulo 29. Observamos que  $2^5 = 32 \equiv 3 \pmod{29} \Rightarrow 2^{10} \equiv 9 \pmod{29} \Rightarrow \boxed{s=10}$ .
- D) Como  $x$  tiene que ser coprimo con 29 y 2 es raíz primitiva módulo 29, tenemos que  $x = 2^\alpha \pmod{29}$  para algún  $\alpha \in \{0, 1, \dots, 27\}$ . Entonces  $x^{18} \equiv 2^{18\alpha} \equiv 2^{10} \pmod{29} \Rightarrow 18\alpha \equiv 10 \pmod{28}$  (pues 2 es raíz primitiva), así que  $9\alpha \equiv 5 \pmod{14} \Rightarrow \alpha \equiv -1 \pmod{14} \Rightarrow \alpha \equiv -1$  ó  $13 \pmod{28}$ . Así que  $x \equiv 2^{-1}$  ó  $2^{13} \pmod{29}$ , nos queda:

$$x \equiv 2^{-1} \equiv 15 \pmod{29} \quad (\text{pues } 2 \cdot 15 = 30 \equiv 1 \pmod{29})$$

$$x \equiv 2^{13} = 2^{10} \cdot 2^3 \equiv 9 \cdot 8 = 36 \cdot 2 \equiv 7 \cdot 2 = 14 \pmod{29}$$

Por lo tanto las soluciones son los  $x \in \mathbb{Z}$  tales que  $x \equiv 14 \pmod{29}$  ó  $x \equiv 15 \pmod{29}$ .

**Ejercicio 2.**

- A) Si  $\varphi : G_1 \rightarrow G_2$  morfismo de grupos  $\Rightarrow G_1 / \text{Ker} \varphi \simeq \text{Im}(\varphi)$ .
- B) Consideramos la función  $\varphi : \mathbb{R}^* \rightarrow \mathbb{R} / \varphi(x) = \log(|x|)$ , que resulta un morfismo (con las operaciones correspondientes) pues  $\varphi(xy) = \log(|xy|) = \log(|x| \cdot |y|) = \log(|x|) + \log(|y|) = \varphi(x) + \varphi(y)$ , así que en virtud del Primer Teorema de Isomorfismos:

$$\mathbb{R}^* / \text{Ker} \varphi \simeq \text{Im}(\varphi)$$

Vemos que  $x \in \text{Ker}(\varphi) \Leftrightarrow \log(|x|) = 0 \Leftrightarrow |x| = 1 \Leftrightarrow x = \pm 1$ , por lo tanto  $\text{Ker}(\varphi) = \{1, -1\}$ .

Vemos también que si  $y \in \mathbb{R} \Rightarrow y = \varphi(e^y)$  por lo tanto  $\text{Im}(\varphi) = \mathbb{R}$ .

- C) i) Si  $o(\bar{z}) = p \Rightarrow pz \equiv 0 \pmod{p^2} \Rightarrow z \equiv 0 \pmod{p} \Rightarrow z = kp$  para algún  $k \in \mathbb{Z}$ .
- ii) Como  $o(\bar{p}) = p$  entonces  $H = \langle \bar{p} \rangle$  es un subgrupo de  $\mathbb{Z}_{p^2}$  de orden  $p$ . Si  $H'$  fuese otro subgrupo de orden  $p$  de  $\mathbb{Z}_{p^2}$  entonces  $H' = \langle \bar{z} \rangle$  (subgrupo de cíclico es cíclico) donde  $\bar{z}$  es un elemento de orden  $p$  de  $\mathbb{Z}_{p^2}$ . Por la parte anterior  $\bar{z} = k\bar{p} \in \langle \bar{p} \rangle \Rightarrow H' = \langle \bar{z} \rangle \subset \langle \bar{p} \rangle$  así que por cardinalidad  $H' = \langle \bar{p} \rangle = H$ .
- iii) Por el Primer Teorema de Isomorfismo  $\mathbb{Z}_{p^2} / \text{ker}(\psi) \simeq \text{Im}(\psi)$  de donde resulta tomando cardinales que:

$$p^2 = |\mathbb{Z}_{p^2}| = |\text{ker}(\psi)| \cdot |\text{Im}(\psi)| \quad (1)$$

de donde  $|\text{Im}(\psi)| \mid p^2$ . Por otra parte  $|\text{Im}(\psi)| \mid pq$  (por Lagrange), así que  $|\text{Im}(\psi)| = 1$  ó  $p$ . Como  $|\text{Im}(\psi)| \neq 1$  pues  $\psi$  es no trivial se tiene que  $|\text{Im}(\psi)| = p$ . De (??) se tiene que también  $|\text{Ker}(\psi)| = p$  así que en virtud de la parte anterior  $\text{Ker}(\psi) = \langle \bar{p} \rangle$  (el único subgrupo de orden  $p$  de  $\mathbb{Z}_{p^2}$ ).

## Ejercicio 2.

- A. Sea  $n = o(g)$ , entonces  $g^n = e_{G_1}$ . Por ser  $\psi$  homomorfismo se tiene que  $\psi(g^n) = \psi(\underbrace{g * \cdots * g}_{n \text{ veces}}) = \underbrace{\psi(g) *' \cdots *' \psi(g)}_{n \text{ veces}} = \psi(g)^n$ . Así que  $\psi(g)^n = \psi(g^n) = \psi(e_{G_1}) = e_{G_2}$  (la última igualdad vale pues  $\psi$  es homomorfismo). Así que, por propiedades del orden se tiene que  $o(\psi(g)) | n$ . ( $*$  denota la operación de  $G_1$  y  $*'$  la de  $G_2$ ).
- B. Dada  $\sigma \in S_n$ , existen trasposiciones  $\tau_1, \dots, \tau_k$  tal que  $\sigma = \tau_1 \tau_2 \cdots \tau_k$  (pues toda permutación es producto de trasposiciones). Así que  $\psi(\sigma) = \psi(\tau_1 \tau_2 \cdots \tau_k) = \psi(\tau_1) \psi(\tau_2) \cdots \psi(\tau_k) = e_G * e_G \cdots * e_G = e_G$  (la segunda igualdad vale pues  $\psi$  es homomorfismo y la tercer igualdad es por hipótesis).
- C. Por lo visto en la parte B, basta con probar que si  $\psi : S_n \rightarrow G$  es homomorfismo, entonces  $\psi(\tau) = e_G$  para toda trasposición  $\tau \in S_n$ . Sea  $\tau$  una trasposición; entonces  $o(\tau) = 2$  y por la parte A. se tiene que  $o(\psi(\tau)) | 2$ . Por otro lado, como  $\psi(\tau) \in G$  se tiene que  $o(\psi(\tau)) | |G|$  y  $|G|$  es impar. De estas dos condiciones se deduce que  $o(\psi(\tau)) = 1$  y por lo tanto  $\psi(\tau) = e_G$ .
- D. Sea  $\psi : S_3 \rightarrow \mathbb{Z}_4$  un homomorfismo de grupos. Como los homomorfismos preservan neutros, se tiene que  $\psi(id) = \bar{0}$ . Sea  $\sigma \in \{(123), (132)\}$ ; entonces  $o(\sigma) = 3$  y por la parte A. tenemos que  $o(\psi(\sigma)) | 3$ . Pero  $\psi(\sigma) \in \mathbb{Z}_4$  y en  $\mathbb{Z}_4$  no hay elementos de orden 3; por lo tanto  $o(\psi(\sigma)) = 1$  y entonces  $\psi(\sigma) = \bar{0}$ . Queda ver cuanto vale  $\psi$  en las trasposiciones. Si  $\tau$  es una trasposición,  $o(\tau) = 2$  así que  $o(\psi(\tau)) | 2$ . Así que  $\psi(\tau) \in \{\bar{0}, \bar{2}\}$ .

Sopongamos que por ejemplo  $\psi((12)) = \bar{0}$ ; entonces  $\psi((13)) = \psi((123)(12)) = \psi((123)) + \psi((12)) = \bar{0} + \bar{0} = \bar{0}$ . Análogamente se prueba que  $\psi((13)) = \bar{0}$  y por lo tanto  $\psi$  es el homomorfismo trivial. De igual forma se prueba que si cualquier trasposición está en  $\ker(\psi)$ , entonces están todas y por lo tanto  $\psi$  es el homomorfismo trivial.

Es decir que si  $\psi$  no es el trivial, entonces  $\psi(\tau) = \bar{2}$  para toda  $\tau$  trasposición.

Queda ver que el homomorfismo definido por  $\psi(id) = \psi((123)) = \psi((132)) = \bar{0}$  y  $\psi((12)) = \psi((13)) = \psi((23)) = \bar{2}$  es efectivamente un homomorfismo. Una forma de ver esto es que  $\psi(\sigma) = \bar{0}$  si  $\sigma$  es par y  $\psi(\sigma) = \bar{2}$  si  $\sigma$  es impar.

Así que:

- Si  $\sigma_1$  y  $\sigma_2$  son impares, tenemos que  $\sigma_1 \sigma_2$  es par y por lo tanto  $\psi(\sigma_1) + \psi(\sigma_2) = \bar{2} + \bar{2} = \bar{0} = \psi(\sigma_1 \sigma_2)$ .
- Si  $\sigma_1$  y  $\sigma_2$  son pares,  $\sigma_1 \sigma_2$  es par y por lo tanto  $\psi(\sigma_1) + \psi(\sigma_2) = \bar{0} + \bar{0} = \bar{0} = \psi(\sigma_1 \sigma_2)$ .
- Si  $\sigma_1$  es par y  $\sigma_2$  es impar,  $\sigma_1 \sigma_2$  es impar y por lo tanto  $\psi(\sigma_1) + \psi(\sigma_2) = \bar{0} + \bar{2} = \bar{2} = \psi(\sigma_1 \sigma_2)$ .
- El caso  $\sigma_1$  impar y  $\sigma_2$  par es análogo al último.