Repaso Teórico: · T. Lagrange: G grupo finito y $H \leq G \Rightarrow |H| \mid |G|$.
En particular $o(g) = k_g > 1$ divide a $|G|$.

· Homomorfismo: $\varphi: G \to K$ $(G,*)$, $(K,\cdot)$ grupos t.q. $\varphi(g * g') = \varphi(g) \cdot \varphi(g')$.

· Ppdes. de morfismos: $\varphi: G \to K$ morfismo $\Rightarrow$
$\Rightarrow \varphi(e_G) = e_K$
$\Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$
$\Rightarrow \varphi(g^n) = \varphi(g)^n$

· $\ker(\varphi) = \{g \in G : \varphi(g) = e_K\} < G$

· $\mathrm{Im}(\varphi) = \{k \in K : \exists g \in G \ \ f(g) = k\} = \{f(g) : g \in G\} < K$

Ejercicio 12. Sea G un grupo con 4 elementos.

a. Probar que G es abeliano.

b. Probar que o bien $G \simeq \mathbb{Z}_4$ o bien $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

$G = \{e, a, b, c\}$ (1) $ab = ba$ $\qquad \mathbb{Z}_2 = \{0, 1\}$
(2) $ac = ca$
(3) $bc = cb$

(1) $ab = ba$:

$a^{-1} \neq b \rightsquigarrow$ ab: $a \Rightarrow b$ neutro ↯; $b \Rightarrow a$ neutro ↯; $e \Rightarrow a^{-1} = b$ ↯; c ✓ (única opción)

De la misma manera $ba = c$

$a^{-1} = b \rightsquigarrow ab = e = ba$

(2) $ac = ca$: ac — $a \to c$ sería neutro ↯
b Si $ac = b \Rightarrow ca = b$ (la otra opción es $ca = e \to c = a^{-1}$)
$c \to a$ sería neutro ↯
e Si $ac = e \Rightarrow c = a^{-1}$ y conmutan ✓

Idem $bc = cb$.

Obs: $G = \{e, a, b, c\}$ $\Rightarrow$ Al menos un elemento entre $\{a, b, c\}$ debe ser su propio inverso.

Hay dos casos: Un elemento de orden 2 o Tres elementos de orden 2.

Ej: Si a no es su propio inverso $\Rightarrow$ $ab = e$ ($c = c^{-1}$) o $ac = e$ ($b = b^{-1}$)

$\mathbb{Z}_2 \times \mathbb{Z}_2 \rightsquigarrow o((\bar{0}, \bar{0})) = 1$

$o((\bar{1}, \bar{0})) = o((\bar{0}, \bar{1})) = o((\bar{1}, \bar{1})) = 2$

$\mathbb{Z}_4 \longrightarrow o(\bar{0}) = 1$

$o(\bar{1}) = 4$

$o(\bar{2}) = 2$

$o(\bar{3}) = 4$.

obs: Si hay un elemento de orden 4 $\Rightarrow$ va a ser isomorfo a $\mathbb{Z}_4$

Si no hay un elemento de orden 4 $\Rightarrow$ va a ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$

Caso 1: $G = \{e, a, a^{-1}, b\}$. $a^{-1} \neq a$ $\Rightarrow$ tienen orden > 2 $\Rightarrow$ Tienen orden 4 (Lagrange)

($b = b^{-1}$)

Isomorfismo: $\varphi: G \to \mathbb{Z}_4$

$\varphi(e) = e$, $\varphi(a) = \bar{1}$, $\varphi(a^{-1}) = \bar{3}$, $\varphi(b) = 2$

Chequear: $\varphi(a * b) = \varphi(a) + \varphi(b)$

Caso 2 $G = \{e, a, b, c\}$ (a^{-1}, b^{-1}, c^{-1})

Isomorfismo: $\varphi: G \to \mathbb{Z}_2 \times \mathbb{Z}_2$

Queremos φ que respete la operación, que está dada en la tabla.

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b		e	a
c	c			e

Abeliano $\Rightarrow$ simétrica

Completar de la única forma posible.

$\varphi(e) = e$

$\varphi(a) = (1, 0)$

$\varphi(b) = (0, 1)$

$\varphi(c) = (1, 1)$

$\varphi(a * b) = \varphi(c) = (1, 1)$.

$\varphi(a) + \varphi(b) = (1, 0) + (0, 1) = (1, 1)$ ✓

$\varphi(b * c) = \varphi(a) = (1, 0)$

$\varphi(b) + \varphi(c) = (0, 1) + (1, 1) = (1, 0)$

$\varphi(a * c) = \varphi(b) = (0, 1)$

$\varphi(a) + \varphi(c) = (1, 0) + (1, 1) = (0, 1)$

Ejercicio 13. (Examen Julio 2012)

a. Probar que si $\phi : G_1 \to G_2$ es un homomorfismo de grupos finitos y $g \in G_1$, entonces $o(\phi(g)) \mid mcd(|G_1|, |G_2|)$.

b. Hallar todos los homomorfismos $\phi : \mathbb{Z}_2 \to U(8)$.

c. Hallar p sabiendo que p es primo, y existe un homomorfismo no trivial $\phi : \mathbb{Z}_{51} \to \mathbb{Z}_p$ tal que $\phi(\overline{17}) = \overline{0}$.

$3 \cdot 17$

(a) Vimos que $o(\phi(g)) \mid |G_1|$ } Ej 10 parte a.

$o(\phi(g)) \mid |Im \varphi|$

$|Im \varphi|$ por Lagrange divide a $|G_2|$

Por transitividad $o(\phi(g)) \mid |G_2|$

(b) $\phi : \mathbb{Z}_2 \to U(8)$ $\qquad U(8) = \{1, 3, 5, 7\}$

$\phi(0) = 1 \qquad \phi(1) = 3 \qquad \phi(0) \cdot \phi(1) = 1 \cdot 3 = 3$

$\phi(0 + 1) = \phi(1) = 3$

(c) $|\mathbb{Z}_{51}| = 51 = |Ker\, \phi| \cdot |Im\, \phi|$

Por la fórmula (1) $|Ker\, \phi| = 3$ e $|Im\, \phi| = 17$

(2) $|Ker\, \phi| = 17$ e $|Im\, \phi| = 3$ ✗

(3) $|Ker\, \phi| = 1$ e $|Im\, \phi| = 51$ ✗

(4) $|Ker\, \phi| = 51$ e $|Im\, \phi| = 1$ ✗

Pero $Im\, \phi$ es subgrupo de $\mathbb{Z}_p$ con p primo $\Rightarrow$ por Lagrange $|Im\, \phi| = 1$ o $|Im\, \phi| = p$; descartamos (3) pues 51 no es primo.

Descartamos (4) porque ϕ es no trivial por hipótesis.

Queremos por último descartar (1) o (3).

$17 \in Ker\, \phi \Rightarrow o(17) \mid |Ker|$ $\Rightarrow$ estamos en el caso (1).

$o(17) = 3$

Luego $p = 17$.