Consulta Segundo Parcial.

Ejercicio 4

Determinar si existen homomorfismos no triviales $f : G \to K$ para cada grupo G y K. En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

(a) $G = \mathbb{Z}_p$ con p primo y $K = S_{p-1}$.
(b) $G = U(p)$ con $p > 2$ primo, y $K = S_{p-2}$.
(c) $G = U(12)$ y $K = \mathbb{Z}_4$.

(a) G tiene orden p (grupo aditivo)

K tiene orden $(p-1)!$

$f: G \to K$ homomorfismo no trivial

$g \mapsto f(g)$ El orden de $f(g)$ divide a $(p-1)! = 1 \dots p-1$.

Pero también divide a $o(g) \in \{1, p\}$.

Entonces $o(f(g)) = 1 \ \forall g$ y f es trivial

$S_{p-1} = \{f : \{1, \dots, p-1\} \to \{1, \dots, p-1\}\}$ biyecciones

(b) $G = U(p) \Rightarrow |G| = \varphi(p) = p-1$.

$K = S_{p-2} \Rightarrow |S_{p-2}| = (p-2)!$

Queremos $f: G \to K$ homomorfismo no trivial.

Sea g r.p. mod p $\to$ g tiene orden $p-1$ $\Rightarrow$ $g^{\frac{p-1}{2}}$ tiene orden 2.

Si mandamos g en algún elem de orden 2 por ej $\Rightarrow$ tenemos un h. no trivial.

Esto lo podemos hacer para $p > 3$. (de forma que S_{p-2} tenga más de un elemento)

(c) $|U(12)| = \varphi(12) = \varphi(2^2 \cdot 3) = 4$

$|\mathbb{Z}_4| = 4$

en $\mathbb{Z}_4$: $o(\bar{1}) = 4$ $o(\bar{2}) = 2$ $o(\bar{3}) = 4$ $o(\bar{0}) = 1$

Queremos ver si $\exists$ $f: U(12) \to \mathbb{Z}_4$ no trivial. Nuevamente $o(f(g)) \mid o(g)$

En $U(12)=\{1,5,7,11\}$

$o(1)=1$ $\quad o(5)=2$ $\quad o(7)=2$ $\quad o(11)=2$.

$\Rightarrow U(12)\cong \mathbb{Z}_2\times\mathbb{Z}_2$

f tendría que tener la siguiente forma: $1\mapsto 0$ y alguno al 2 (sino es trivial)

$o(f(g)) \mid o(g)=2$ $\quad$ si $g\neq 1 \Rightarrow f(g)=2$ o 0

Para que f sea no trivial debe ser $f(g)=2$ para algún g. Supongamos $g=5$

Queremos ver si existe una función con $1\mapsto 0$, $5\mapsto 2$ que respete las operaciones.

	opción 1	opción 2	opción 3	opción 4
$1\mapsto 0$	$1\mapsto 0$	$1\mapsto 0$	$1\mapsto 0$	$1\to 0$
$5\mapsto 0$ o 2	$5\mapsto 2$	$5\mapsto 2$	$5\mapsto 2$	$5\to 2$
$7\mapsto 0$ o 2	$7\mapsto 2$	$7\mapsto 0$	$7\mapsto 2$	$7\to 0$
$11\mapsto 0$ o 2.	$11\mapsto 0$	$11\mapsto 2$	$11\mapsto 2$ ✗	$11\to 0$ ✗

Opción 2: $f(7\cdot 11)=f(5)=2$, $f(7)+f(11)=2$; $f(5\cdot 11)=f(7)=0$, $f(5)+f(11)=0$ ✓

Opción 3: $f(5\cdot 7)=f(11)=2$, $f(5)+f(7)=2+2=0$

Opción 4: $f(5\cdot 7)=f(11)=0$, $f(5)+f(7)=2$

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$U(12)$ — no cíclico.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$ — cíclico

G es cíclico si existe $g\in G$ tal que $\langle g\rangle = G$.
(Recordar que $\langle g\rangle=\{g^n : n\in\mathbb{Z}\}$)

Mult.

$\langle 5\rangle=\{5^1=5,\ 5^2=1\}$

$\langle 7\rangle=\{7^1=7,\ 7^2=1\}$

Aditivo

$\langle 2\rangle=\{2^1=2+0=2,\ 2^2=2+2=0\}$

$\langle 1\rangle=\{1^1=1,\ 1^2=1+1=2,\ 1^3=2+1=3,\ 1^4=3+1=0\}$

Ejercicio 1.

a. Probar que 2 es raiz primitiva módulo 13 y también módulo 27.

b. Hallar todas las raices primitivas módulo 13.

c. Para cada divisor $d \mid 18$, hallar un elemento de $U(27)$ con orden exactamente d.

(c) · 2 es raíz primitiva módulo 27.

· $\varphi(27) = 18$.

· $\bar{2}^{18} = \bar{1}$ y 18 es el mínimo que cumple eso.

· Ej: $d = 9$ $\Rightarrow$ $2^{2 \cdot 18/2} \equiv 1 \ (27)$ $\Rightarrow$ como 18 es el mínimo tq $2^{18} \equiv 1 \ (27)$

$\Rightarrow$ 9 es el min tq $(2^2)^9 \equiv 1 \ (27)$

$\Rightarrow o(4) = 9$.

En gral: Si $d \mid 18$ $\quad 2^{d \cdot 18/d} \equiv 1 \ (27)$ $\Rightarrow$ mismo argumento $o(2^d) = 18/d$.

$o(2^{18/d}) = d$

(b) Para cada $g \in U(13)$ tenemos que ver $o(g)$. g es r.p. si $o(g) = \varphi(13) = 12$. y esto es sii $g^{\varphi(13)/p} \not\equiv 1$ $\forall p \mid 12$ primo. $(p = 2, 3)$.

Si queremos encontrar r.p:

$\langle 2 \rangle = \{2, 2^2, 2^3, \dots\}$ si es todo OK ✓

Si no, tomo el primero que no está en $\langle 2 \rangle$, llamémosle h.

$\langle h \rangle = \{h, \dots\}$ ...

En este caso sabemos que 2 es r.p. $\Rightarrow$ Todo elemento es de la forma $g = 2^k$ $k = 1, \dots, 12$.

Luego: usamos la ppd $o(g^k) = \dfrac{o(g)}{mcd(o(g), k)}$ *

$\Rightarrow$ 2^k es raíz primitiva sii $o(2^k) = \varphi(13) = 12$ sii $mcd(o(2), k) = 1$

sii $mcd(12, k) = 1$.

$\Rightarrow$ Todas las raíces primitivas son 2^k con k coprimo con 12.

$\boxed{2, 2^5, 2^7, 2^{11}}$

Ejercicio 7. Sea p un número primo impar y a una raíz primitiva módulo p^α.

a. Probar que si a es impar entonces la clase de a en $U(2p^\alpha)$ es un generador de dicho grupo.

b. Probar que si a es par entonces la clase de $a + p^\alpha$ en $U(2p^\alpha)$ es un generador de dicho grupo.

c. Concluir que existen raíces primitivas módulo $2p^\alpha$ para p primo impar.

d. Hallar una raíz primitiva módulo 162.

$162 = 2 \cdot 3^4 \Rightarrow p = 3 \quad \alpha = 4$, queremos r.p. módulo $2 \cdot p^\alpha$, como en (a), (b)

Primero necesitamos r r.p. módulo p^α.

Lema 4.1.11. *Sea p un primo impar. Si g es raíz primitiva módulo p entonces g o $g + p$ es raíz primitiva módulo p^2.*

Lema 4.1.12. *Sea p un primo impar. Si g es raíz primitiva módulo p^2, entonces g es raíz primitiva módulo p^k para todo $k \in \mathbb{Z}^+$.*

Por el lema 4.1.12, podemos tomar r una raíz primitiva módulo 9.

Por el lema 4.1.11 2 o 5 va a ser r.p módulo 9.

$$r \text{ r.p. mod } p \Rightarrow \begin{cases} r \text{ es r.p. módulo } p^k \ \forall k \geq 2 \\ \text{ó} \\ r+p \text{ es r.p. módulo } p^k \ \forall k \geq 2. \end{cases}$$

$\overset{5}{2}$ es r.p módulo 9 $\Rightarrow$ $\overset{5}{2}$ es r.p. módulo 81 $\overset{(a)}{\Rightarrow}$ parte (b) 2 es par $\Rightarrow \overset{5}{2} + 81$ es raíz primitiva módulo 162.