ESTRUCTURAS ALGEBRAICAS–(Grupo 16)–(24-05-19)

CUESTIONES

1.-Consideramos el grupo $G = \{(a,b) \mid a,b \in \mathbb{R}, a \neq 0\}$ con la operación

$$(a,b) * (c,d) = (ac, ad+b).$$

Determinar, razonadamente, si $H = \{(1,t) \in G \mid t \in \mathbb{R}\}$ es un subgrupo normal de G.

2.- Factorizar el polinomio $p(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1$ sobre los cuerpos $\mathbb{Q}, \mathbb{R}$, y $\mathbb{Z}/2\mathbb{Z}$.

3.-Sea G un grupo finito, $H \leq G$, $N \lhd G$, con $H \leq N$ y N cíclico. Demostrar entonces que $H \lhd G$.

4.-Sea G un grupo abeliano que consta de 8 elementos de orden 3, 18 elementos de orden 9 y el 1_G. Encontrar, justificando la respuesta, la descomposición de G como un producto directo de grupos cíclicos.

PROBLEMAS

1.-(i) Sea G un grupo abeliano de orden n, sea $k \in \mathbb{N}$ y $f : G \longrightarrow G$ el homomorfismo definido por $f(x) = x^k$. Hallar $\mathrm{Ker}(f)$ cuando $(k,n) = 1$. (1,5 ptos)

(ii) Aplicar el apartado anterior a un determinado grupo G (¿cuál?) para resolver la congruencia $x^5 \equiv 2^5 \pmod{29}$. (1,5 ptos)

(iii) Resolver la congruencia: $x^{301} \equiv 1 \pmod{29}$. (2 ptos)

2.

.-Supongamos que H es un grupo abeliano y sea $f : G \longrightarrow H$ un homomorfismo. Definimos una aplicación $\alpha : G \times G \longrightarrow H$ por $\alpha((g_1, g_2)) = f(g_1)f(g_2)^{-1}$

i) Probar que α es homomorfismo.

ii) En el caso de que $G = \Sigma_3$, $H = \{1, -1\}$ y f el homomorfismo signatura, describir ~~enumerar~~ los elementos de $\mathrm{Ker}(\alpha)$ y calcular su orden .

iii) Siguiendo con el caso anterior, ¿$\mathrm{Ker}(\alpha)$ es abeliano? y ¿existen dos subgrupos H_1 y H_2 de G tales que $\mathrm{Ker}(\alpha) = H_1 \times H_2$? (Razona las respuestas).

NOTA: La revisión del examen tendrá lugar el martes 4 de junio de 9h. a 12h.

Examen (24-05-2019)

Cuestiones

1. Consideramos el grupo $G = \{(a,b) \mid a,b \in \mathbb{R},\ a \neq 0\}$ con la operación

$$(a,b) * (c,d) = (ac, ad+b)$$

Determinar, razonadamente, si $H = \{(1,t) \in G \mid t \in \mathbb{R}\}$ es un subgrupo normal de G.

En primer lugar, tenemos que ver que h es subgrupo de G y sabemos por teoría que:

$H \leq G \iff \forall u,v \in H,\ uv^{-1} \in H$

Entonces, tomamos dos elementos cualesquiera de H tal que
$(1,t), (1,u) \in H \Rightarrow H \leq G \iff (1,t)*(1,u)^{-1} \in H$

Tenemos que halla $(1,u)^{-1}$:

$(1,u)*(1,u') = (1,0) \Rightarrow (1, u'+u) = (1,0) \Rightarrow \begin{cases} 1 = 1 \\ u'+u = 0 \Rightarrow u' = -u \end{cases}$

$(1,u)^{-1} = (1,-u)$

Y por lo tanto, $(1,t)*(1,-u) = (1, \underbrace{-u+t}_{\in \mathbb{R} \neq 0}) \Rightarrow (1,t)*(1,-u) \in H$

Con lo cual concluimos que $H \leq G$. Ahora veamos si $H \lhd G$:

$H \lhd G \iff g^{-1}Hg \in H,\ \forall g \in G \iff g^{-1}hg \in H,\ \forall g \in G$

Seguimos el mismo proceso para hallar el simétrico de $g \in G$:

$(a,b)*(a',b') = (1,0) \Rightarrow (aa', ab'+b) = (1,0) \Rightarrow$

$\Rightarrow \left.\begin{cases} aa' = 1 \Rightarrow a' = a^{-1} \\ ab'+b = 0 \Rightarrow b' = -ba^{-1} \end{cases}\right\} \Rightarrow g^{-1} = (a^{-1}, -ba^{-1})$

Por ultimo,

$$(a^{-1}, -ba^{-1}) * (1, t) * (a, b) = (a^{-1}, -ba^{-1}) * (a, b+t) =$$

$$= (1, a^{-1}(b+t) - ba^{-1}) = (1, \underbrace{a^{-1}t}_{\in \mathbb{R}}) \in H \Rightarrow g^{-1}Hg \in H \Rightarrow H \triangleleft G \blacksquare$$

2. Factorizar el polinomio $p(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1$ sobre los cuerpos $\mathbb{Q}$, $\mathbb{R}$, y $\mathbb{Z}/2\mathbb{Z}$.

Tenemos el polinomio $p(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1$ aplicamos Ruffini:

$$\begin{array}{r|rrrrrrr}
 & 1 & 2 & 3 & 4 & 3 & 2 & 1 \\
-1 & & -1 & -1 & -2 & -2 & -1 & -1 \\
\hline
 & 1 & 1 & 2 & 2 & 1 & 1 & \boxed{0} \\
-1 & & -1 & 0 & -2 & 0 & -1 & \\
\hline
 & 1 & 0 & 2 & 0 & 1 & \boxed{0} &
\end{array}$$

$\Rightarrow x^5 + x^4 + 2x^3 + 2x^2 + x + 1$

$\Rightarrow x^4 + 2x^2 + 1$

$$z = x^2 \Rightarrow z^2 + 2z + 1 = 0 \Rightarrow z = \frac{-2 \pm \sqrt{4-4}}{2} \Rightarrow z = -1 \Rightarrow$$

$$\Rightarrow x = \sqrt{-1} = i \in \mathbb{C}$$

Por lo tanto,

- En $\mathbb{Q}$ se descompondría en producto de irreducibles de la siguiente forma:

  $p(x) = (x+1)^2 (x^4 + 2x + 1)$

- En $\mathbb{R}$ se descompondría en producto de irreducibles de la siguiente forma:

  $p(x) = (x+1)^2 (x^4 + 2x + 1)$

· En $\mathbb{Z}/2\mathbb{Z}$ se descompondría en producto de irreducibles de la siguiente forma:

$p(x) = (x + \bar{1})^6$

* Darse cuenta de que $-\bar{1} = \bar{1}$ en $\mathbb{Z}/2\mathbb{Z}$.

3. Sea G un grupo finito, $H \leq G$, $N \trianglelefteq G$, con $H \leq N$ y N cíclico. Demostrar entonces que $H \trianglelefteq G$.

Como N es cíclico, aplicamos el teorema fundamental de los cíclicos, "$H_1 = N$ y $|H| = |H_1| \Rightarrow H = H_1$"

$N \trianglelefteq G \Rightarrow N^g = N, \forall g \in G$

$H \leq N = N^g \Rightarrow H \in g^{-1}Ng \Rightarrow H = g^{-1}Ng \Rightarrow gHg^{-1} = N \Rightarrow H^g \in N \Rightarrow$

$\Rightarrow H^g \leq N$

Por lo tanto, $H^g \leq N$ y $|H^g| = |H| \Rightarrow H = H^g \Rightarrow H^g \in H \Rightarrow H^g \trianglelefteq G$ ■

4. Sea G un grupo abeliano que consta de 8 elementos de orden 3, 18 elementos de orden 9 y el 1_G. Encontrar justificando la respuesta, la descomposición de G como un producto directo de grupos cíclicos.

$|G| = |\text{El. de orden } 3| + |\text{El. de orden } 9| + |1_G| = 8 + 18 + 1 = 27 \Rightarrow$

$\Rightarrow |G| = 27 \Rightarrow G \cong C_{27}$

Posibles estructuras: - $C_3 \times C_3 \times C_3 \Rightarrow$ No podría ser ya que no tiene elementos de orden 9

- $C_3 \times C_9$

Por lo tanto, la única posibilidad sería $G \cong C_3 \times C_9$

- En C_9 hay $\varphi(9) = 6$ elementos de orden 9
- En C_3 hay $\varphi(3) = 2$ elemento de orden 3

$\Rightarrow 6 \cdot 2 = 12$

Luego tendríamos otros 12 elementos de orden 9 al multiplicar los de orden 3 con los de orden 9 $\Rightarrow 12+6 = 18$ elementos en total de orden 9 $\Rightarrow C_{27} \cong C_3 \times C_9 \Rightarrow 27 = 1 + \underbrace{18}_{\text{orden } 9} + \text{orden } 3 \Rightarrow$

$\Rightarrow 8$ = elementos de orden 3 ✓ ∎

Problemas

1. I) Sea G un grupo abeliano de orden n, sea $k \in \mathbb{N}$ y $f: G \to G$ el homomorfismo definido por $f(x) = x^k$. Hallar $Ker(f)$ cuando $(k,n) = 1$.

Tenemos $f: G \to G$, $|G| = n$, $k \in \mathbb{N}$, $(k,n) = 1$.
$x \mapsto f(x) = x^k$

$Ker(f) = \{x \in G \mid f(x) = 1\} = \{x \in G \mid x^k = 1\}$

Tenemos $(k,n) = 1 \underset{\text{Bezout}}{\Rightarrow} \exists\, a,b \in \mathbb{Z}$ tal que $an + bk = 1 \Rightarrow$

$\Rightarrow x^{an+bk} = x \Rightarrow (x^{an})(x^{bk}) = x \Rightarrow (\underbrace{x^n}_{1_G})^a (\underbrace{x^k}_{\in Ker(f)})^b = x \Rightarrow$

$\Rightarrow 1^a \cdot 1^b = x \Rightarrow x = 1$

Por lo tanto, $Ker(f) = \{1_G\}$.

II) Aplicar el apartado anterior a un determinado grupo G (¿cual?) para resolver la congruencia $x^5 \equiv 2^5 \pmod{29}$

Por el apartado anterior, definimos $f: \mathcal{U}(\mathbb{Z}/29\mathbb{Z}) \to \mathcal{U}(\mathbb{Z}/29\mathbb{Z})$
$x \longmapsto x^k$

donde $G = \mathcal{U}(\mathbb{Z}/29\mathbb{Z})$ y como vemos en este caso $(5,29) = 1$.

Entonces, aplicamos el apartado anterior

$f(x) = x^5 = \bar{2}^5 = f(\bar{2}) \Rightarrow x = \bar{2}$

III) Resolver la congruencia: $x^{301} \equiv 1 \pmod{29}$

$\varphi(29) = 28 \Rightarrow 301 = 28 \cdot 10 + 21 \Rightarrow x^{301} = x^{28\cdot 10 + 21} \Rightarrow$

$\Rightarrow (\underbrace{x^{28}}_{1})^{10} \cdot x^{21} \Rightarrow x^{21} \equiv 1 \pmod{29}$

$$\left.\begin{array}{l} o(x) \mid 21 \\ o(x) \mid 28 \end{array}\right\} \Rightarrow o(x) \mid (21, 28) = 7 \Rightarrow o(x) = 1 \text{ ó } 7$$

- Si $o(x) = 1 \Rightarrow x = 1$
- Si $o(x) = 7$, tenemos que buscar elementos de orden 7 en $U(\mathbb{Z}/29\mathbb{Z})$

$$o(x^i) = \frac{o(x)}{(o(x), i)} \Rightarrow (28, i) = 4 \Rightarrow i = \{4, 8, 16, 20, 24\}$$

$o(\bar{2}) = 28$

Y por lo tanto, las posibles soluciones serían:

$\{\bar{1}, \bar{2}^4, \bar{2}^8, \bar{2}^{12}, \bar{2}^{16}, \bar{2}^{20}, \bar{2}^{24}\} = \{\bar{1}, \overline{16}, \overline{24}, \bar{7}, \overline{25}, \overline{23}, \overline{20}\}$

2. Supongamos que H es un grupo abeliano y sea $f: G \to H$ un homomorfismo. Definimos una aplicación $\alpha: G \times G \to H$ por

$\alpha((g_1, g_2)) = f(g_1) f(g_2)^{-1}$

I) Probar que α es homomorfismo.

II) En el caso de $G = \Sigma_3$, $H = \{-1, 1\}$ y f el homomorfismo signatura, describir los elementos de $Ker(\alpha)$ y calcular su orden.

III) Siguiendo en el caso anterior, ¿$Ker(\alpha)$ es abeliano? y ¿existen dos subgrupos H_1 y H_2 de G tales que $Ker(\alpha) = H_1 \times H_2$?

I)

Tenemos que ver si α es homomorfismo de grupos:

Sean $(g_1, g_2), (g_3, g_4) \in G\times G$ tal que $g_1, g_2, g_3, g_4 \in G$

$$\alpha((g_1, g_2)\cdot(g_3, g_4)) = \alpha((g_1 g_3, g_2 g_4)) = f(g_1 g_3)\cdot f(g_2 g_4)^{-1} =$$

$$\underset{\substack{\downarrow \\ f \text{ homomorfismo}}}{=} f(g_1)f(g_3)f(g_2)^{-1}f(g_4)^{-1} \underset{\substack{\downarrow \\ H \text{ abeliano}}}{=} f(g_1)f(g_2)^{-1}f(g_3)f(g_4)^{-1} =$$

$$= \alpha((g_1, g_2))\cdot\alpha((g_3, g_4))$$

Por lo tanto, $\alpha((g_1, g_2)\cdot(g_3, g_4)) = \alpha((g_1, g_2))\cdot\alpha((g_3, g_4)) \Rightarrow$

$\Rightarrow \alpha$ es homomorfismo.

II)

$G = \Sigma_3$

$H = \{1, -1\}$

¿Elementos de Σ_3?

$(1) \to (-1)^{0+0+0} = +1$

$(1\,2) \to (-1)^{1+0} = -1$

$(1\,3) \to (-1)^{1+0} = -1$

$(2\,3) \to (-1)^{1+0} = -1$

$(1\,2\,3) \to (-1)^2 = +1$

$(1\,3\,2) \to (-1)^2 = +1$

$$\mathrm{Ker}(\alpha) = \{(g_1, g_2) \in G\times G \mid \alpha((g_1, g_2)) = 1_H\} =$$

$$= \{(g_1, g_2) \in G\times G \mid f(g_1)f(g_2)^{-1} = 1_H\} =$$

$$= \{(g_1, g_2) \in G\times G \mid f(g_1) = f(g_2)\}$$

Luego el $\mathrm{Ker}(\alpha)$ contiene a los elementos de G que tienen igual signatura

Ahora vamos a calcular el orden de $|\mathrm{Ker}(\alpha)|$, luego aplicando el primer teorema de isomorfía:

$$\frac{|G\times G|}{|\mathrm{Ker}(\alpha)|} \cong |\alpha(G\times G)| = |H|$$

$$\left.\begin{array}{l} |G| = |\Sigma_3| = 3! = 6 \Rightarrow |G\times G| = (3!)^2 = 6^2 = 36 \\ |f(G\times G)| = |H| = 2 \end{array}\right\} \Rightarrow \underline{\mathrm{Ker}(\alpha)} = \frac{36}{2} = \underline{\underline{18}}$$

III)

Tomamos dos elementos de $Ker(\alpha)$, luego sean $g_1, g_2 \in G$ tal que $f(g_1) = f(g_2) \Rightarrow sig(g_1) = sig(g_2) \Rightarrow Ker(\alpha)$ abeliano $\overset{??}{\Longleftrightarrow}$ $sig(g_1)\, sig(g_2) = sig(g_2)\, sig(g_1)$

Supongamos que $g_1, g_2 \in A_8 \Rightarrow sig(g_1) = sig(g_2) = 1 \Rightarrow$

$$\Rightarrow \left.\begin{array}{l} sig(g_1) \cdot sig(g_2) = 1 \cdot 1 = 1 \\ sig(g_2) \cdot sig(g_1) = 1 \cdot 1 = 1 \end{array}\right\} \Rightarrow Ker(\alpha) \text{ es abeliano}$$

Supongamos que es cierto y existen H_1 y $H_2 \in Ker(\alpha)$ tales que $Ker(\alpha) = H_1 \times H_2$

luego, lo prodríamos descomponer como producto de dos subgrupos H_1 y H_2 tal que uno de ellos serían los pares de elementos que tienen misma signatura y positiva y el otro sería los que tienen misma signatura y negativa, respectivamente, con lo cual

$$\left.\begin{array}{l} |H_1| = 3 \cdot 2 = 6 \\ |H_2| = 3 \cdot 2 = 6 \end{array}\right\} \Rightarrow |H_1 \times H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|} = \frac{36}{|H_1 \cap H_2|} = |Ker(\alpha)| \Rightarrow$$

$\Rightarrow |H_1 \cap H_2| = 2$ Absurdo, pues H_1 y H_2 no tienen elementos en común. Por lo tanto $\nexists H_1, H_2$ tales que $Ker(\alpha) = H_1 \times H_2$

Examen (22-01-09)

Cuestiones

1. Consideramos el grupo $G = \{(a,b) \mid a, b \in \mathbb{R}, a \neq 0\}$ con la operación.

$$(a,b) * (c,d) = (ac, ad+b)$$

Determinar razonadamente, si $H = \{(1,t) \in G \mid t \in \mathbb{R}\}$ es un subgrupo normal de G.

En primer lugar, tenemos que ve que H es subgrupo de G, y $H \leq G \Leftrightarrow$ para $x \in H, y^{-1} \in H^{-1}$, luego $xy^{-1} \in H$. Con lo cual debemos calcular el elemento neutro y el simetrico:

$$(1,t) * (e_1, e_2) = (1,t) \Rightarrow (1e_1, 1t + e_2) = (1,t) \Rightarrow$$

$$\Rightarrow (e_1, t+e_2) = (1,t) \Rightarrow \begin{cases} \underline{e_1 = 1} \\ \cancel{t} + e_2 = \cancel{t} \Rightarrow \underline{\underline{e_2 = 0}} \end{cases}$$

Elemento neutro: $(1,0)$

$$(1,t) * (a', b') = (1,0) \Rightarrow (a', b'+t) = (1,0) \Rightarrow \begin{cases} \underline{a' = 1} \\ b'+t = 0 \Rightarrow \underline{\underline{b' = -t}} \end{cases}$$

Elemento simetrico: $(1,-t)$

Por lo tanto

$$(1,t) * (1, -t') = (1, -t'+t) \in H \Rightarrow H \leq G.$$

Ahora por ultimo tenemos que demostrar que $H \triangleleft G$. luego por definición $gHg^{-1} \in H$, $\forall g \in G$.

$$(a,b) * (1,t) * (a^{-1}, -ba^{-1}) = (a, at+b) * (a^{-1}, -ba^{-1}) =$$

$$= (1, \cancel{-b} + at + \cancel{b}) = (1, at) \in H \Rightarrow H \triangleleft G.$$

2. Sea $f: G_1 \to G_2$ un homomorfismo de grupos. Supongamos que $|G_1| = 18$ y $|G_2| = 15$ y que f no es el homomorfismo trivial ¿Cuanto vale entonces $|f(G_1)|$?

$$f(G_1) \leq G_2 \underset{\substack{\text{Teorema} \\ \text{de Cauchy}}}{\Rightarrow} |f(G_1)| \mid |G_2| = 15$$

Por el primer teorema de isomorfía:

$$\frac{|G_1|}{|\text{Ker} f|} = |f(G_1)| \Rightarrow |f(G_1)| \mid |G_1| = 18$$

Luego, $|f(G_1)| \mid (|G_1|, |G_2|) = (18, 15) = 3 \Rightarrow |f(G)| = 1$ ó 3 y como suponemos que f no es un homomorfismo trivial $\Rightarrow$

$\Rightarrow |f(G_1)| = 3$.

3. Sea G un grupo finito, $H \leq G$, $N \trianglelefteq G$, con $H \leq N$ y N cíclico. Demostrar entonces que $H \trianglelefteq G$.

Como N es cíclico, aplicamos el teorema fundamental de los cíclicos, $H_1 \leq N$ y $|H| = |H_1| \Rightarrow H = H_1$

$N \trianglelefteq G \Rightarrow N^g = N, \forall g \in G$

$H^g \leq N^g = N \Rightarrow H^g \leq N$

Entonces como $H^g \leq N$ y $|H^g| = |H| \Rightarrow H = H^g \Rightarrow H \trianglelefteq G$

4. Sea G un grupo abeliano que consta de 8 elementos de orden 3, 18 elementos de orden 9 y el 1_G. Encontrar, justificando la respuesta, la descomposición de G como producto directo de grupos cíclicos

$|G| = 18 + 8 + 1 = 27 \Rightarrow |G| = 27 = 3^3$

Posibles estructuras: - $C_3 \times C_3 \times C_3$ $\Rightarrow$ No puede darse ya que debería tener elementos de orden 9
- $C_9 \times C_3$

Entonces, $G \cong C_9 \times C_3$.

$\left.\begin{array}{l}\text{En } C_9 \text{ hay } \varphi(9) = 6 \text{ elementos de orden } 9 \\ \text{En } C_3 \text{ hay } \varphi(3) = 2 \text{ elementos de orden } 3\end{array}\right\} \Rightarrow$

$\Rightarrow$ Al multiplicar los elementos de orden 9 por los de orden 3 y 1_G obtenemos otros 12 elementos de orden 9 (total: 18 elementos de orden 9). Por lo que $27 = 1 + 18 +$ elementos de orden 3

$\Rightarrow$ Elementos de orden $3 = 8$.

Problemas

1. I) Sea G un grupo abeliano de orden n, sea $k \in \mathbb{N}$ y $f: G \to G$ el homomorfismo definido por $f(x) = x^k$. Hallar $\ker(f)$ cuando $(k,n)=1$

II) Aplicar el apartado anterior a un determinado grupo G (¿cual?) para resolver la congruencia $x^5 \equiv 2^5 \pmod{29}$.

III) Resolver la congruencia $x^{301} \equiv 1 \pmod{29}$

I)

Tenemos $f: G \to G$, $x \mapsto f(x) = x^k$, $|G| = n$, $(k,n)=1$.

El $\ker(f) = \{x \in G \mid f(x) = 1_G\} = \{x \in G \mid x^k = 1_G\} \Rightarrow$

$$o(x^k) = \frac{o(x)}{(o(x),k)} = \frac{n}{(k,n)} = n \Rightarrow o(x^k) = n$$

$$x^k = 1_G \Rightarrow o(x^k) = o(x) = o(1) = 1 \Rightarrow x = 1 \Rightarrow \ker(f) = \{1_G\}$$

II)

$$U(\mathbb{Z}/29\mathbb{Z}),\ \varphi(29) = 28,\ (28,5) = 1 \Rightarrow f: \mathbb{Z}/29\mathbb{Z} \to \mathbb{Z}/29\mathbb{Z},\ x \longmapsto x^5 \Rightarrow$$

$$\Rightarrow f(\bar{x}) = x^5 = \bar{2}^5 = f(\bar{2}) \Rightarrow x = \bar{2}$$

III)

$$301 = 28 \cdot 10 + 21$$

$$x^{301} = x^{28 \cdot 10 + 21} = (\underbrace{x^{28}}_{1})^{10} x^{21} = x^{21}$$

Entonces tenemos que resolve la siguiente congruencia:

$$x^{21} \equiv 1 \pmod{29}$$

$$\left.\begin{array}{l} o(x) \mid 21 \\ o(x) \mid 28 \end{array}\right\} \Rightarrow o(x) \mid (21,28) = 7 \Rightarrow o(x) = 1 \text{ ó } 7$$

• Si $o(x)=1 \Rightarrow x=1$

• Si $o(x)=7$:

$\bar{2}=\{\bar{1},\bar{2},\bar{4},\bar{8},\overline{16},\bar{3},\bar{6},\overline{12},\overline{24},\overline{19},\bar{9},\overline{18},\bar{7},\overline{14},\overline{-1},\ldots\}$

$\Rightarrow o(\bar{2})=28$

$o(x^i)=\dfrac{o(x)}{(o(x),i)} \Rightarrow 7=\dfrac{28}{(28,i)} \Rightarrow (28,i)=4 \Rightarrow$

$\Rightarrow i=\{4,8,12,16,20,24\}$

Posibles soluciones: $\{\bar{1},\bar{2}^4,\bar{2}^8,\bar{2}^{12},\bar{2}^{16},\bar{2}^{20},\bar{2}^{24}\}=$

$=\{\bar{1},\overline{16},\overline{24},\bar{7},\overline{25},\overline{23},\overline{20}\}$

2. Sea G un subgrupo de Σ_7 generado por las permutaciones

$$\alpha=(123)(4567) \quad y \quad \beta=(23)(57)$$

I) Probar que $\langle\alpha\rangle \trianglelefteq G$, $G/\langle\alpha\rangle \cong C_2$, calcular $|G|$ y deducir que $G=\langle\alpha\rangle\langle\beta\rangle$

II) Demostrar que también $G=\langle\alpha\beta,\beta\rangle$ pero que $G\neq\langle\alpha\beta\rangle\langle\beta\rangle$. ¿Cuál es la razón?

III) Determinar todos los subgrupos $N \trianglelefteq G$ tal que $N\leq\langle\alpha\rangle$

I)

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&6&7&4\end{pmatrix}=(123)(4567)$$

$$\beta=\begin{pmatrix}1&2&3&4&5&6&7\\1&3&2&4&7&6&5\end{pmatrix}=(23)(57)$$

$\langle\alpha\rangle \trianglelefteq G \Leftrightarrow \mu^\sigma\in\langle\alpha\rangle,\ \forall\mu\in\langle\alpha\rangle$ y $\forall\sigma\in G$

¿$\alpha^\alpha\in\langle\alpha\rangle$? ¿$\alpha^\beta\in\langle\alpha\rangle$?

$\alpha^\alpha=\alpha^{-1}\alpha\alpha=\alpha\in\langle\alpha\rangle$

$\alpha^\beta=(\beta(1)\ \beta(2)\ \beta(3))(\beta(4)\ \beta(5)\ \beta(6)\ \beta(7))=$

$=(1\ 3\ 2)(4\ 7\ 6\ 5)=\alpha^{-1} \Rightarrow \langle\alpha\rangle \trianglelefteq G.$

$o(\alpha) = 12$

$o(\beta) = 2$

$$G/\langle\alpha\rangle = \langle \alpha\langle\alpha\rangle, \beta\langle\alpha\rangle \rangle = \langle \underset{1_{G/\langle\alpha\rangle}}{\langle\alpha\rangle}, \beta\langle\alpha\rangle \rangle =$$

$$= \langle \beta\langle\alpha\rangle \rangle \cong C_2$$

$$\beta\langle\alpha\rangle = \bar{\beta}, \; \bar{\beta}^2 = \langle\alpha\rangle = 1_{G/\langle\alpha\rangle}$$

$$|G| = |\langle\alpha\rangle| \cdot \underbrace{\left|\frac{G}{\langle\alpha\rangle}\right|}_{\cong C_2} = 12 \cdot 2 = 24$$

$$|\langle\alpha\rangle\langle\beta\rangle| = \frac{|\alpha||\beta|}{|\langle\alpha\rangle \cap \langle\beta\rangle|}$$

$$|\langle\alpha\rangle \cap \langle\beta\rangle| = 1 \text{ ó } 2$$

- Si $|\langle\alpha\rangle \cap \langle\beta\rangle| = 2 \Rightarrow 2 = \frac{12}{(12,i)} \Rightarrow (12,i) = 6$

$$\left.\begin{array}{l} 2 = \frac{12}{(12,i)} \Rightarrow (12,i) = 6 \\ 2 = \frac{2}{(12,i)} \Rightarrow (12,i) = 1 \end{array}\right\} \Rightarrow \alpha^6 = \beta$$

$$\alpha^6 = \beta \Rightarrow \alpha^6 = (5\,7)(6\,2) \neq (2\,3)(5\,7) = \beta \Rightarrow \alpha^6 \neq \beta$$

- Si $|\langle\alpha\rangle \cap \langle\beta\rangle| = 1 \Rightarrow$

$$\left.\begin{array}{l} 1 = \frac{12}{(12,i)} \Rightarrow (12,i) = 12 \\ 1 = \frac{2}{(12,i)} \Rightarrow (12,i) = 2 \end{array}\right\} \Rightarrow \alpha^{12} = \beta^2$$

$$\alpha^{12} = 1 = \beta^2$$

Y por lo tanto, $|\langle\alpha\rangle \cap \langle\beta\rangle| = 1 \Rightarrow \underline{|\langle\alpha\rangle\langle\beta\rangle|} = \frac{12 \cdot 2}{1} = \underline{24}$

$$\Rightarrow G = \langle \alpha, \beta \rangle = \langle\alpha\rangle\langle\beta\rangle$$

Examen (07-09-2010)

1. Calcular el resto de la división de $2^{15}+12^{13}$ entre 13.

$\varphi(13)=12$

Luego

$$(2^{12+3})+(12^{12+1}) = \underbrace{2^{12}}_{1}\cdot 2^3 + \underbrace{12^{12}}_{1}\cdot 12 = \overline{2^3+12} = \overline{8}+\overline{12}=\overline{20}$$

Luego el resto de dividir $2^{15}+12^{13}$ entre 13 es 20.

2. Calcular $(\overline{13})^{-1}$ en el grupo multiplicativo $U(\mathbb{Z}/216\mathbb{Z})$.

Aplicamos el algoritmo de Euclides para hallar $(216,13)$:

$216 = 13\cdot 16 + 8 \Rightarrow 8 = 216\cdot 1 + 13\cdot(-16)$

$13 = 8\cdot 1 + 5 \Rightarrow 5 = 13\cdot 1 + 8\cdot(-1)$

$8 = 5\cdot 1 + 3 \Rightarrow 3 = 8\cdot 1 + 5\cdot(-1)$

$5 = 3\cdot 1 + 2 \Rightarrow 2 = 5\cdot 1 + 3\cdot(-1)$

$3 = 2\cdot 1 + 1 \Rightarrow 1 = 3\cdot 1 + 2\cdot(-1)$

$2 = 1\cdot 2 + 0$

$1 = 3\cdot 1 + 2\cdot(-1) = 3\cdot 2 + 5\cdot(-1) = 8\cdot 2 + 5\cdot(-3) = 8\cdot 5 + 13\cdot(-3) =$

$$\boxed{1 = 216\cdot 5 + 13\cdot(-83)}$$

Luego, $\overline{1} = \underbrace{\overline{216}}_{\overline{0}}\cdot\overline{5} + \overline{13}\cdot\underbrace{\overline{(-83)}}_{\overline{133}} \Rightarrow \overline{1} = \overline{13}\cdot\overline{133}$, luego $(\overline{13})^{-1} = \overline{133}$

3. Determinar la descomposición del grupo $\mathcal{U}(\mathbb{Z}/60\mathbb{Z})$ en producto directo de cíclicos.

$$|\mathcal{U}(\mathbb{Z}/60\mathbb{Z})| = \varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5) = 2 \cdot 2 \cdot 4 =$$
$$= 2^4 = 16$$

$$\mathcal{U}(\mathbb{Z}/60\mathbb{Z}) \cong \mathcal{U}(\mathbb{Z}/4\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/3\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/5\mathbb{Z}) \cong C_2 \times C_2 \times C_4$$

Ahora buscamos 2 elementos de orden 2 y otro de orden 4 en $\mathcal{U}(\mathbb{Z}/60\mathbb{Z})$.

$$\mathcal{U}(\mathbb{Z}/60\mathbb{Z}) = \{\overline{1}, \ , \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}, \overline{31}, \overline{37}, \overline{41}, \overline{43}, \overline{47}, \overline{49},$$
$$\overline{53}, \overline{59}\}$$

Sabemos que $\overline{(-1)}$ tiene orden 2, luego $o(\overline{-1}) = o(\overline{59}) = 2$

$$\overline{7} = \{\overline{1}, \overline{7}, \overline{49}, \overline{343} = \overline{43}, \overline{2401} = \overline{1}\}$$

$$\overline{11} = \{\overline{1}, \overline{11}, \overline{121} = \overline{1}\}$$

Luego $\langle\overline{7}\rangle$ tiene orden 4 y $\langle\overline{11}\rangle$ tiene orden 2. Y por lo tanto

$$\mathcal{U}(\mathbb{Z}/60\mathbb{Z}) \cong \underset{\substack{\cong \\ C_2}}{\langle\overline{11}\rangle} \times \underset{\substack{\cong \\ C_2}}{\langle\overline{59}\rangle} \times \underset{\substack{\cong \\ C_4}}{\langle\overline{7}\rangle}$$

4. Resolver la congruencia

$$x^{51} \equiv 1 \pmod{18}$$

$$\left.\begin{array}{l} \varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = 6 \\ 51 = 6 \cdot 8 + 3 \end{array}\right\} \Rightarrow x^{6 \cdot 8 + 3} \equiv 1 \pmod{18} \Rightarrow$$

$$\Rightarrow \underbrace{(x^6)}_{1}{}^8 \cdot x^3 \equiv 1 \pmod{18} \Rightarrow x^3 \equiv 1 \pmod{18}$$

$$\left.\begin{array}{l} o(x) \mid 3 \\ o(x) \mid 6 \end{array}\right\} \Rightarrow o(x) \mid (6,3) = 3 \Rightarrow o(x) = 1 \text{ ó } 3$$

- Si $o(x)=1 \Rightarrow x=1$
- Si $o(x)=3 \Rightarrow$ existe algun elemento en $U(\mathbb{Z}/18\mathbb{Z})$ tal que tiene orden 3, luego $U(\mathbb{Z}/18\mathbb{Z})=\{\bar{1},\bar{5},\bar{7},\overline{11},\overline{13},\overline{17}\}$

$\langle\bar{7}\rangle=\{\bar{1},\bar{7},\overline{49}=\overline{13},\overline{343}=\bar{1}\} \Rightarrow o(\bar{7})=3$

$\langle\bar{5}\rangle=\{\bar{1},\bar{5},\bar{7},\underset{-\bar{1}}{\overset{\parallel}{\overline{17}}},\overline{13},\overline{11},\bar{1}\} \Rightarrow o(\bar{5})=6$

$\langle\overline{11}\rangle=\{\bar{1},\overline{11},\overline{13},\underset{-\bar{1}}{\overset{\parallel}{\overline{17}}},\bar{7},\bar{5},\bar{1}\} \Rightarrow o(\overline{11})=6$

$\langle\overline{13}\rangle=\{\bar{1},\overline{13},7,\bar{1}\} \Rightarrow o(\overline{13})=3$

$\langle\overline{17}\rangle=\{\bar{1},\overline{17},\bar{1}\} \Rightarrow o(\overline{17})=2$

Entonces las posible soluciónes a la congruencia $x^{51}\equiv 1 \pmod{18}$ serían $\bar{1},\bar{7},\overline{13}$.

5. Responder, razonadamente, a las siguientes preguntas:

I) ¿Cuantas clases de conjugación de elementos de orden 10 existen en Σ_{10}?

II) ¿Cuantos elementos de orden 10 posee A_{10}?

I)

Posibles estructuras de orden 10 en Σ_{10}:

1)(5-ciclo)(2-ciclo)(2-ciclo)(1-ciclo)

2)(5-ciclo)(2-ciclo)(1-ciclo)(1-ciclo)(1-ciclo)

3)(10-ciclo)

1) $|Cl_{\Sigma_{10}}(5\text{-c})(2\text{-c})(2\text{-c})(1\text{-c})|=\dfrac{|G|}{|C_{\Sigma_{10}}()|}=\dfrac{10!}{5\cdot2\cdot2\cdot2!}=90720$

2) $|Cl_{\Sigma_{10}}(5\text{-c})(2\text{-c})(1\text{-c})(1\text{-c})(1\text{-c})|=\dfrac{|G|}{|C_{\Sigma_{10}}()|}=\dfrac{10!}{5\cdot2\cdot3!}=\dfrac{9!}{3!}=9\cdot8\cdot7\cdot6\cdot5\cdot4$
$=60480$

3) $|Cl_{\Sigma_{10}}(10\text{-c})|=\dfrac{|G|}{|C_{\Sigma_{10}}()|}=\dfrac{10!}{10}=362880$

El total sería la suma de los 3, luego en total sería 514080

II)

De los calculados anteriormente, en A_{10} solo estarán las clases de conjugación que tienen signatura positiva:

$(10-c) \to sig(10-c) = (-1)^9 = -1 \Rightarrow (10-c) \notin A_{10}$

$(5-c)(2-c)(2-c)(1-c) = (-1)^{4+1+1} = +1 \Rightarrow (5-c)(2-c)(2-c)(1-c) \in A_{10}$

$(5-c)(2-c)(1-c)(1-c)(1-c) = (-1)^{4+1} = -1 \Rightarrow (5-c)(2-c)(1-c)(1-c)(1-c) \notin A_{10}$

Por lo tanto, en A_{10} habrá 90720 elementos de orden 10.

Problemas

1. I) Determinar todos los subgrupos de $G = \langle g \rangle$ de orden 48 y su relación de contenido entre ellos

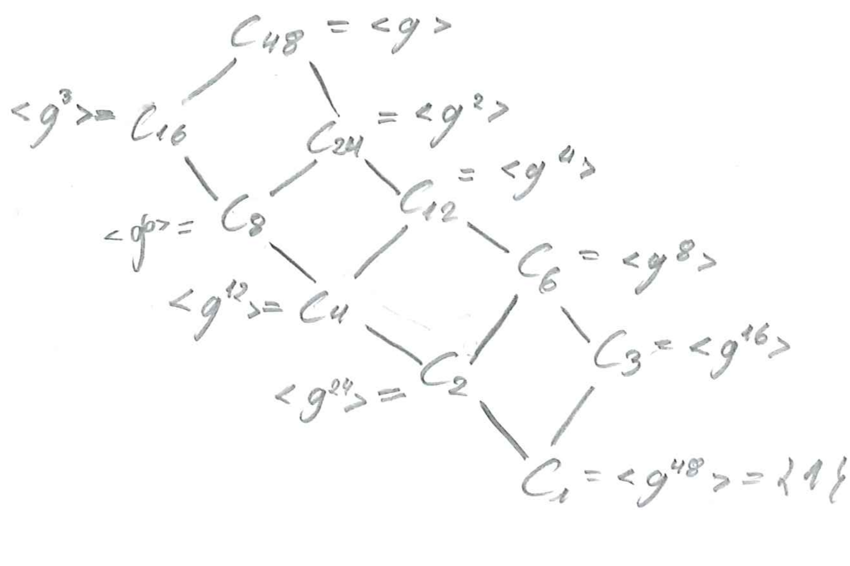
II) Dado el endomorfismo $f: G \to G$ mediante $f(g) = g^{30}$. Enumerar todos los elementos de los subgrupos $Ker(f)$ y $f(G)$, y dar la estructura de los subgrupos.

$48 = 2^4 \cdot 3 \Rightarrow G \cong C_{48}$

Por la propiedad fundamental de los cíclicos $\forall m \in \mathbb{N}$ tal que $m \mid |G|$, $\exists! \, C_m \leq C_{48}$. Y tenemos los siguientes divisores:

$1, 2, 3, 4, 6, 8, 12, 16, 24, 48$

Además, sabemos que $C_m = \langle g^{48/m} \rangle$, luego tendríamos el siguiente retículo:



II)

$$|f(G)| = o(g^{30}) = \frac{o(g)}{(o(g),30)} = \frac{48}{(48,30)} = \frac{48}{6} = 8 \Rightarrow |f(G)| = 8 \Rightarrow$$

$\Rightarrow f(G) \cong C_8$

Aplicamos el 1er teorema de isomorfía:

$$\frac{|G|}{|Ker(f)|} = |f(G)| \Rightarrow |Ker(f)| = \frac{|G|}{|f(G)|} = \frac{48}{8} = 6 \Rightarrow |Ker(f)| = 6 \Rightarrow$$

$\Rightarrow Ker(f) \cong C_6$

$f(G) = \langle g^6 \rangle = \{1, g^6, g^{12}, g^{18}, g^{24}, g^{30}, g^{36}, g^{42}\}$

$Ker(f) = \langle g^8 \rangle = \{1, g^8, g^{16}, g^{24}, g^{32}, g^{40}\}$

2. Sea A el subgrupo de Σ_9 generado por las permutaciones:

$\alpha = (27)(39)(68)(145) \qquad \beta = (514)(238796)$

I) Probar que A es abeliano, hallar $\langle\alpha\rangle \cap \langle\beta\rangle$ y calcular $|A|$.

II) Expresar A como producto directo de grupos cíclicos, dando sus respectivos generadores.

I)

$\alpha = (27)(39)(68)(145) \Rightarrow \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 9 & 5 & 1 & 8 & 2 & 6 & 3 \end{pmatrix}$

$\beta = (514)(238796) \Rightarrow \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 8 & 5 & 1 & 2 & 9 & 7 & 6 \end{pmatrix}$

$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 6 & 1 & 4 & 7 & 3 & 2 & 8 \end{pmatrix} = (154)(298)(367)$

$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 6 & 1 & 4 & 7 & 3 & 2 & 8 \end{pmatrix} = (154)(298)(367)$

$\Rightarrow \alpha\beta = \beta\alpha \Rightarrow$

$\Rightarrow$ A es abeliano

$\underline{\underline{o(\alpha)}} = mcm(2,3) = \underline{\underline{6}}$
$\underline{\underline{o(\beta)}} = mcm(3,6) = \underline{\underline{6}}$ $\Big\} \Rightarrow o(\alpha) = o(\beta) = 6$

$|\langle\alpha\rangle \cap \langle\beta\rangle| \mid (o(\alpha), o(\beta)) = 6$, luego tenenemos 4 posibilidades:

1) $|\langle\alpha\rangle \cap \langle\beta\rangle| = 6 \Rightarrow \alpha = \beta$, no es cierto, luego $|\langle\alpha\rangle \cap \langle\beta\rangle| \neq 6$

2) $|\langle\alpha\rangle \cap \langle\beta\rangle| = 3 \Rightarrow o(g^i) = \dfrac{o(g)}{(o(g), i)} \Rightarrow 3 = \dfrac{6}{(6,i)} \Rightarrow (6,i) = 2 \Rightarrow$

$\Rightarrow i = 2, 4$. Tenemos otras 2 posibilidades:

a) $\alpha^2 = \beta^2$: $\left.\begin{array}{l}\alpha^2 = (1\,5\,4) \\ \beta^2 = (5\,4\,1)(2\,8\,9)(3\,7\,6)\end{array}\right\} \Rightarrow \alpha^2 \neq \beta^2$

b) $\alpha^4 = \beta^4$: $\left.\begin{array}{l}\alpha^4 = (1\,4\,5) \\ \beta^4 = (5\,1\,4)(2\,9\,8)(3\,6\,7)\end{array}\right\} \Rightarrow \alpha^4 \neq \beta^4$

3) $|\langle\alpha\rangle \cap \langle\beta\rangle| = 2 \Rightarrow o(g^i) = \dfrac{o(g)}{(o(g), i)} \Rightarrow 2 = \dfrac{6}{(6,i)} \Rightarrow (6,i) = 3 \Rightarrow$

$\Rightarrow i = 3$

Por lo que, $\alpha^3 = \beta^3$

$\left.\begin{array}{l}\alpha^3 = (7\,2)(3\,9)(6\,8) \\ \beta^3 = (7\,2)(3\,9)(6\,8)\end{array}\right\} \Rightarrow \alpha^3 = \beta^3 \checkmark$

Y por lo tanto, $|\langle\alpha\rangle \cap \langle\beta\rangle| = 2$ y además $\langle\alpha\rangle \cap \langle\beta\rangle =$
$= \langle\alpha^3\rangle = \langle\beta^3\rangle$

Por último, $\underline{|A|} = \dfrac{|\langle\alpha\rangle|\,|\langle\beta\rangle|}{|\langle\alpha\rangle \cap \langle\beta\rangle|} = \dfrac{6 \cdot 6}{2} = \underline{\underline{18}}$

II)

$A \cong C_{18}$. Las posible estructuras son:

$C_{18} \cong C_2 \times C_9$

$C_{18} \cong C_2 \times C_3 \times C_3 \cong C_6 \times C_3$

Como en A no hay elementos de orden 9, ya que $9 \nmid 6 \Rightarrow$

$\Rightarrow A \cong C_2 \times C_3 \times C_3 \cong \langle \alpha^2 \rangle \times \langle \alpha^3 \rangle \times \langle \beta^3 \rangle \cong C_6 \times C_3 \cong \langle \alpha \rangle \times \langle \beta^2 \rangle$

Examen (27-06-2013)

Cuestiones

2. Sea G un grupo, $g \in G$ y $m, n \in \mathbb{N}$ con $(m,n)=1$. Probar que si $g^m = 1 = g^n$, entonces $g=1$. ¿Se puede asegurar lo mismo si $(m,n) \neq 1$?

• Metodo 1 (Bezout): $\exists a,b \in \mathbb{Z} : am+bn=1$

$g = g^{am+bn} = (g^{am}) \cdot (g^{bn}) = (g^m)^a \cdot (g^n)^b = 1^a \cdot 1^b = 1 \Rightarrow \underline{g=1}$

• Metodo 2 (orden de un elemento):

Si $k = o(g)$ y $g^m = 1 = g^n \Rightarrow \left.\begin{matrix} k \mid n \\ k \mid m \end{matrix}\right\} \Rightarrow k \mid (n,m) = 1 \Rightarrow$

$\Rightarrow o(g) = 1 \Rightarrow g = 1.$

- Contraejemplo: En $C_6 = \langle g \rangle$, $\begin{matrix} g^6 = 1 \\ g^{12} = 1 \end{matrix}$ y $(6,12) = 2 \neq 1 \Rightarrow g \neq 1.$

3. ¿Cuantos elementos de orden 4 tiene el grupo simetrico Σ_6? ¿Y el subgrupo alternado A_6?

$(\cdot,\cdot)(\cdot,\cdot)(\cdot)(\cdot) = \dfrac{6!}{2 \cdot 2! \cdot 2!} = 6 \cdot 5 \cdot 3 = 90$

$(\cdot,\cdot,\cdot,\cdot)(\cdot)(\cdot) = \dfrac{6!}{4 \cdot 2!} = 6 \cdot 5 \cdot 3 = 90$

Elementos de orden 4 de $\Sigma_6 = 180$

En el grupo alternado:

(4-ciclo)(1-ciclo)(1-ciclo) $\longrightarrow$ signatura $- \Rightarrow \notin A_6$

(2-ciclo)(2-ciclo)(1-ciclo)(1-ciclo) $\longrightarrow$ signatura $+ \Rightarrow \in A_6$

Elementos de orden 4 en $A_6 = 90$.

4. Sean G, H grupos $|G| = m$, $|H| = n$ y $(n, m) = 1$. ¿Si $f: G \to H$ es un homomorfismo de grupos, entonces debe ser $f(g) = 1$ para todo $g \in G$?

Sabemos que
$$\left.\begin{array}{l} o(f(g)) \mid o(g) \\ o(g) \mid |G| = m \\ o(f(g)) \mid |H| = n \end{array}\right\} \Rightarrow o(f(g)) \mid (m, n) = 1 \Rightarrow f(g) = 1 \blacksquare$$

Problemas

1. Sea $G = \mathcal{U}(\mathbb{Z}/63\mathbb{Z})$.

I) Expresad G como producto directo de subgrupos cíclicos.

II) Determinar todos los subgrupos de G de orden 4 y de orden 9, respectivamente dando la estructura de tales subgrupos.

III) Resolver la congruencia $x^{399} \equiv 1 \pmod{63}$

IV) Sea $f: G \to G$ definida por $f(\bar{n}) = \bar{n}^{10}$. Determinar los subgrupos $\operatorname{Ker} f$ y $f(G)$, expresadlos como producto directo de subgrupos cíclicos.

I)

$$|\mathcal{U}(\mathbb{Z}/63\mathbb{Z})| = \varphi(63) = \varphi(3^2) \cdot \varphi(7) = 6 \cdot 6 = 36$$

$$\mathcal{U}(\mathbb{Z}/63\mathbb{Z}) \cong \underbrace{\mathcal{U}(\mathbb{Z}/9\mathbb{Z})}_{C_6} \times \underbrace{\mathcal{U}(\mathbb{Z}/7\mathbb{Z})}_{C_6}$$

$$G = \mathcal{U}(\mathbb{Z}/63\mathbb{Z}) \cong C_6 \times C_6$$

Buscamos elementos de orden 6:

$\langle \bar{2} \rangle = \{ \bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5, \bar{2}^6 \} = \{ \bar{2}, \bar{4}, \bar{8}, \overline{16}, \overline{32}, \overline{64} = \bar{1} \} \to$ SI

$\langle \bar{3} \rangle = \{ \bar{3}, \bar{9}, \overline{27}, \overline{71} = \bar{8}, \overline{24}, \overline{72} = \bar{9} \} \to$ NO

$\langle \bar{5} \rangle = \{ \bar{5}, \overline{25}, \overline{125} = -\bar{1}, \dots \} \to$ SI

Por tanto, $\boxed{G = \langle \bar{2} \rangle \times \langle \bar{5} \rangle}$

II)

$\varphi(63) = \varphi(3^2)\cdot\varphi(7) = 6\cdot 6 = 2^2\cdot 3^2$

Entonces, existen dos P-Sylow: $> P_{2\text{-sylow}} = <\underset{}{\overset{\overline{8}}{\overset{\shortparallel}{\overline{2}^3}}}> \times <\overset{\overline{-1}}{\overset{\shortparallel}{\overline{5}^3}}> \cong C_2\times C_2$

$> P_{3\text{-sylow}} = <\underset{\overline{4}}{\underset{\shortparallel}{\overline{2}^2}}> \times <\underset{\overline{25}}{\underset{\shortparallel}{\overline{5}^2}}> \cong C_3\times C_3$

III)

$x^{399} \equiv 1 \pmod{63}$

$399 = 36\cdot 11 + 3 \Rightarrow x^{36\cdot 11+3} \equiv 1 \pmod{63} \Rightarrow \underbrace{(x^{36})^{11}}_{1}\cdot x^3 \equiv \overline{1} \pmod{63} \Rightarrow$

$\Rightarrow x^3 \equiv 1 \pmod{63}$

Soluciones: Son $x\in G$, con $o(x)=3$. Posibles soluciones:

$\{\overline{1}, \overline{4}, \overline{4}^2, \overline{25}, \overline{25}^2, \overline{4}\cdot\overline{25}, \overline{4}^2\cdot\overline{25}, \overline{4}\cdot\overline{25}^2, \overline{4}^2\cdot\overline{25}^2\} =$

$=\{\overline{1}, \overline{4}, \overline{16}, \overline{25}, \overline{58}, \overline{37}, \overline{22}, \overline{46}, \overline{43}\}$

IV)

$f: G \to G$
$\overline{r} \mapsto \overline{r}^{10}$ $\Rightarrow f: <\overline{2}>\times<\overline{5}> \longrightarrow <\overline{2}^{10}> \times <\overline{5}^{10}> = <\overline{16}>\times<\overline{58}>$

$$\left.\begin{array}{l} o(\overline{2}^4) = \dfrac{o(\overline{2})}{(o(\overline{2}),4)} = \dfrac{6}{2} = 3 \\[2ex] o(\overline{5}^4) = \dfrac{o(\overline{5})}{(o(\overline{5}),4)} = \dfrac{6}{2} = 3 \end{array}\right\} \Rightarrow f(G) \cong C_3\times C_3$$

Por el 1er Teorema de isomorfía: $\dfrac{|G|}{|\mathrm{Ker} f|} = |f(G)| \Rightarrow$

$\Rightarrow |\mathrm{Ker}(f)| = \dfrac{|G|}{|f(G)|} = \dfrac{C_6\times C_6}{C_3\times C_3} = \dfrac{6\cdot 6}{3\cdot 3} = 2\cdot 2 \Rightarrow$

$\Rightarrow |\mathrm{Ker}(f)| \cong C_2\times C_2 = <\overline{8}> \times <\overline{-1}>$

2.I) En el anillo de polinomio de coeficientes reales $\mathbb{R}[x]$ consideramos los subconjuntos:

a) $A = \{a_n x^n + \dots + a_1 x \mid n \geq 1,\ a_i \in \mathbb{R}\}$

b) $B = \{a_n x^n + \dots + a_1 x + a_0 \mid n \geq 0,\ a_i \in \mathbb{Q}\}$

c) $C = \{a x^n + \dots + a_1 x + a \mid n \geq 0,\ a \in \mathbb{R}\}$

d) $D = \{(x^2+x)p(x) + (x^2-1)q(x) \mid p(x), q(x) \in \mathbb{R}[x]\}$

e) $E = \{f(x) \in \mathbb{R}[x] \mid f(x) = 0$ ó grad $f(x) \leq 5\}$

Explica razonadamente cuales de estos subconjuntos de $\mathbb{R}[x]$ y cuales son ideales. Sobre estos últimos, ¿se trata de ideales principales? En tal caso, dar un generador. ¿Son ideales maximales?

II) Dar un ejemplo de un dominio de integridad R y un ideal I de R de forma que el anillo cociente R/I no sea un dominio de integridad (dar un ejemplo de un elemento no nulo R/I que sea divisor de cero). Encontrar un ideal J, en caso de que exista, tal que $I \subset J \subset R$ y que R/J sea un cuerpo (los contenidos deben ser estrictos).

III) Estudiar si los siguientes polinomios son irreducibles en los anillos de polinomios $\mathbb{K}[x]$ que se indican:

a) $f(x) = x^3 + x + 1 \in \mathbb{F}_5(x)$; b) $f(x) = x^3 + x + 1 \in \mathbb{F}_{11}[x]$;

c) $f(x) = x^5 + x^4 - 6x^2 + 3 \in \mathbb{Q}[x]$.

I)

a) Es un ideal por definición $\Rightarrow$ Subanillo

b) Es un subgrupo y es cerrado para el producto, es decir, es un subanillo, pero no es un ideal.

c) No es subanillo $\Rightarrow$ No es ideal.

d) $D = \mathbb{R}[x](x^2+x) + \mathbb{R}[x](x^2-1) = (x^2+x)(x^2-1) = \text{mcd}\{x^2+x, x^2-1\} =$
$= (x+1) \rightarrow$ ideal pricipal $\Rightarrow$ Ideal $\Rightarrow$ Subanillo.

(a) y (d) son los unicos que tienen ideales principales; (a): x
(d): $x+1$

II)

$R = \mathbb{Z}$, $I = 4\mathbb{Z}$ $\Rightarrow$ $R/I = \mathbb{Z}/4\mathbb{Z}$

$J = 2\mathbb{Z}$

$4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$

III)

a) $f(x) = x^3 + x + 1 \in \mathbb{F}_5[x] = \mathbb{Z}/5\mathbb{Z}$ es irreducible

b) $f(x) = x^3 + x + 1 \in \mathbb{F}_{11}[x] = \mathbb{Z}/11\mathbb{Z}$ es irreducible

c) $f(x) = x^5 + x^4 - 6x^2 + 3 \in \mathbb{Q}[x]$ es irreducible

*En este apartado hemos utilizado lo siguiente:

Los cuerpos tienen inverso si f irreducible $\Rightarrow$ tiene inverso.

Examen (26-01-2006)

Cuestiones

1. Sea G un grupo abeliano finito de orden n, $g \in G$ y m un entero positivo tal que $(m,n)=1$. Demostrar que existe un único $x \in G$ tal que $g = x^m$ (Ayuda: Considerar la aplicación $f: G \to G$ dada por $f(x) = x^m$).

Consideramos $f: G \to G$ tal que $f(x) = x^m$. Tenemos que probar que es un automorfismo:

- f homomorfismo: Sean $x_1, x_2 \in G$ tal que $f(x_1 x_2) = (x_1 x_2)^m = x_1^m x_2^m =$
  $= f(x_1) f(x_2)$ ✓
- f inyectiva $\iff Ker\, f = \{1_G\}$
  $Ker(f) = \{x \in G \mid f(x) = 1\} = \{x \in G \mid x^m = 1\} \Rightarrow x^m = 1 \Rightarrow$
  $$\Rightarrow \left.\begin{array}{l} o(x) \mid m \\ o(x) \mid n \end{array}\right\} \Rightarrow o(x) \mid (m,n) = 1 \Rightarrow o(x) = 1 \Rightarrow x = 1_G \Rightarrow Ker(f) = \{1_G\}.$$
- f sobreyectiva: Aplicamos el 1er teorema de isomorfía
  $$Ker(f) \cong \frac{G}{f(G)} \Rightarrow |Ker(f)| = \frac{|G|}{|f(G)|} \Rightarrow |f(G)| = \frac{|G|}{|Ker(f)|} = |G| \Rightarrow$$
  $\Rightarrow |f(G)| = |G| \Rightarrow f(G) = G \Rightarrow f$ es sobreyectiva

Por lo que f es automorfismo $\Rightarrow \exists!\, x \in G : g = x^m,\ \forall x \in G.$

2. Sea $f: G \to C_n$ un homomorfismo de grupos, donde C_n denota un grupo cíclico de orden n. Probar que si $g \in G$ verifica que $(o(g), n) = 1$, entonces $g \in Ker(f)$

$Ker(f) = \{ g \in G \mid f(g) = 1 \}$

$\underset{\text{Bezout}}{(o(g), n) = 1} \Rightarrow \exists a, b \in \mathbb{Z} : a \cdot o(g) + b \cdot n = 1 \Rightarrow g = g^{a o(g) + bn} = (g^{o(g)})^a (g^{bn}) =$

$= g^{bn}$.

$\Rightarrow f(g) = f(g^{bn}) = (f(g))^{bn} = (\underbrace{f(g^n)}_{n = |C_n|})^b = 1 \Rightarrow g \in Ker f.$

3. Razonar si el grupo alternado A_8 posee elementos de orden 8 y de orden 6. En caso afirmativo, determinar el número de elementos de tal orden.

Sea $\sigma = (8\text{-ciclo})$ tiene signatura negativa $\Rightarrow \sigma \notin A_8 \Rightarrow \nexists \sigma$, con $o(\sigma) = 8$ tal que $\sigma \in A_8$.

$\alpha = (6\text{-ciclo})(2\text{-ciclo}) \to sig(\alpha) = 1 \Rightarrow \alpha \in A_8$

$\alpha = (6\text{-ciclo})(1\text{-ciclo})(1\text{-ciclo}) \to sig(\alpha) = -1 \Rightarrow \alpha \notin A_8$

$\alpha = (3\text{-ciclo})(2\text{-ciclo})(2\text{-ciclo})(1\text{-ciclo}) \to sig(\alpha) = 1 \Rightarrow \alpha \in A_8$

$\alpha = (3\text{-ciclo})(2\text{-ciclo})(1\text{-ciclo})(1\text{-ciclo})(1\text{-ciclo}) \to sig(\alpha) = -1 \Rightarrow \alpha \notin A_8$

$\alpha = (3\text{-ciclo})(2\text{-ciclo})(1\text{-ciclo})(1\text{-ciclo})(1\text{-ciclo})$

Por lo que los únicos de orden 6 que hay en A_8 son:

1) (6-ciclo) (2-ciclo)

2) (3-ciclo) (2-ciclo) (2-ciclo) (1-ciclo)

Entonces,

$$\left.\begin{aligned} &1)\ \frac{8!}{6 \cdot 2} = 3360 \\ &2)\ \frac{8!}{3 \cdot 2 \cdot 2 \cdot 2!} = 1680 \end{aligned}\right\} \Rightarrow x \in A_8 : o(x) = 6 \Rightarrow 3360 + 1680 = 5040 \text{ elementos}$$

Problemas

1. Consideramos el siguiente subconjunto del grupo $GL_3(\mathbb{R})$

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a, b, c \in \mathbb{R} \right\}$$

I) Demostrar que G es un subgrupo de $GL_3(\mathbb{R})$.

II) Probar que $Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \ b \in \mathbb{R} \right\}$.

III) Sea $N = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \ x, y \in \mathbb{R} \right\}$. Definir un homomorfismo $f: G \to \mathbb{R}$

tal que $\ker(f) = N$

IV) ¿$N \trianglelefteq G$? ¿G/N es abeliano?

I)

Sean $A, B \in G$. Tenemos que ver que $A^{-1}B \in G$, luego tenemos que calcular A^{-1}:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Rightarrow$$

$$\Rightarrow \begin{cases} a+a' = 0 \Rightarrow a' = -a \\ b'+ac'+b = 0 \Rightarrow b' = +ac-b \\ c+c' = 0 \Rightarrow c' = -c \end{cases}$$

Por lo tanto,

$$A^{-1} = \begin{pmatrix} 1 & -a & +ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

$$A^{-1}B = \begin{pmatrix} 1 & -a & +ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x-a & y a z + acb \\ 0 & 1 & z-c \\ 0 & 0 & 1 \end{pmatrix} \in G \Rightarrow$$

$$\Rightarrow G \leq GL_3(\mathbb{R})$$

II)

Sabemos que $Z(G) = \{ A \in G \mid AB = BA,\ B \in G \}$.

Sea $B = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$, entonces

$$AB = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix}$$

$$BA = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & y+xc+b \\ & 1 & z+c \\ & & 1 \end{pmatrix}$$

$$\begin{cases} x + a = a + x \Rightarrow a = 0 \\ y + az + b = b + xc + y \Rightarrow y + b = b + y \Rightarrow b = b \\ z + c = c + \cancel{z} \Rightarrow c = 0 \end{cases}$$

Por lo que $Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{R} \right\}$

III)

Definimos $f : (G, +) \longrightarrow (\mathbb{R}, +)$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \longmapsto c$$

- f es homomorfismo: $f(AB) = f\begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} = f + c =$

$= f(A) + f(B)$. ✓

Calculamos $\operatorname{Ker} f = \{ A \in G \mid f(A) = 0 \} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x, y \in \mathbb{R} \right\} \Rightarrow$

$\Rightarrow \operatorname{Ker} f = N$

IV)

Probamos ahora $N \triangleleft G$. $N \triangleleft G \Leftrightarrow A^{-1}BA \in N$, $\forall A \in G$, $\forall B \in N$

$$A^{-1}BA = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & x & cx+y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in N \Rightarrow N \triangleleft G$$

G/N abeliano $\Leftrightarrow g_1 N g_2 N = g_2 N g_1 N$, $\forall g_1, g_2 \in G$, luego sean

$A, B \in G$

$$AN = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & y+b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

$$BN = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+d & y+e \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

$$ANBN = \begin{pmatrix} 1 & 2x+a+d & 2y+e+d \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$$BN \cdot AN = \begin{pmatrix} 1 & x+d & y+e \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x+a & y+b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2x+a+d & 2y+b+xc+cd+e \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$ANBN \neq BNAN \Rightarrow G/N$ no es abeliano.

2. Consideramos el grupo $G = \mathcal{U}(\mathbb{Z}/45\mathbb{Z})$

I) Calcular el elemento $(\overline{17})^{-1}$, sin usar calculadora

II) Determinar las posibles estructuras de los grupos abelianos de orden 24. Descomponer G como producto directo de dos subgrupos y deducir, de su estructura, que G no tiene elementos de orden 8.

III) Resolver la congruencia $x^{34} \equiv 1 \pmod{45}$.

IV) Localizar dos subgrupos de G, N_1 y N_2, tales que $G/N_1 \cong C_2 \times C_2$ y $G/N_2 \cong C_4$

I) Aplicamos el algoritmo de euclides:

$45 = 17 \cdot 2 + 11 \Rightarrow 11 = 45 \cdot 1 + 17 \cdot (-2)$

$17 = 11 \cdot 1 + 6 \Rightarrow 6 = 17 \cdot 1 + 11 \cdot (-1)$

$11 = 6 \cdot 1 + 5 \Rightarrow 5 = 11 \cdot 1 + 6 \cdot (-1)$

$6 = 5 \cdot 1 + 1 \Rightarrow 1 = 6 \cdot 1 + 5 \cdot (-1)$

$5 = 1 \cdot 5 + 0$

Luego $(45, 17) = 1 \underset{(\text{Bezout})}{\Longrightarrow} \exists\, a, b \in \mathbb{Z}$ tales que $a45 + b17 = 1$

$$1 = 6 \cdot 1 + 5 \cdot (-1) = 6 \cdot 1 + 11 \cdot (-1) + 6 \cdot 1 = 11 \cdot (-1) + 6 \cdot 2 =$$
$$= 11 \cdot (-1) + 17 \cdot 2 + 11 \cdot (-2) = 17 \cdot 2 + 11 \cdot (-3) =$$
$$= 17 \cdot 2 + 45 \cdot (-3) + 17 \cdot 6 = 45(-3) + 17 \cdot 8$$

Luego, $1 = 17 \cdot 8 + \underbrace{45}_{\overline{0}} \cdot \underbrace{(-3)}_{\overline{42}} \Rightarrow (\overline{17})^{-1} = \overline{8}$ en $\mathbb{Z}/45\mathbb{Z}$

II)

$24 = 3 \cdot 2^3$, sus posibles estructuras serían:

- $C_3 \times C_8 \cong C_{24}$
- $C_3 \times C_4 \times C_2 \cong C_6 \times C_4 \cong C_{12} \times C_2$
- $C_3 \times C_2 \times C_2 \times C_2 \cong C_6 \times C_2 \times C_2$

Vemos que $o(\overline{2})=12$ y $o(\overline{44})=2$. Por lo que $G \cong C_2 \times C_{12} \cong \langle\overline{2}\rangle \times \langle\overline{44}\rangle$ entonces no existe $x \in G$ tal que $o(x)=8$ porque $8 \nmid 12$ y $8 \nmid 2$

$\langle\overline{44}\rangle = \{\overline{1}, \overline{44}\}$

$\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{32}, \overline{19}, \overline{38}, \overline{31}, \overline{17}, \overline{34}, \overline{23}\}$

III)

$x^{34} \equiv 1 \pmod{45}$

$\varphi(45) = \varphi(9)\cdot\varphi(5) = \varphi(3^2)\cdot 4 = 6\cdot 4 = 24$

$x^{34} = x^{24\cdot 1+10} \Rightarrow x^{34} = x^{24}\cdot x^{10} \Rightarrow \overline{x}^{24}\cdot\overline{x}^{10} \equiv 1 \pmod{45} \Rightarrow$

$\Rightarrow \overline{x}^{10} \equiv 1 \pmod{45}$

$\left.\begin{array}{l} o(x) \mid 10 \\ o(x) \mid 24 \end{array}\right\} \Rightarrow o(x) \mid (10, 24) = 2 \Rightarrow o(x) = 1$ ó 2

- Si $o(x)=1 \Rightarrow x=1$
- Si $o(x)=2$, tenemos que ver en $C_2 \times C_{12}$ que hay un elemento de orden 2 en C_2 y otro elemento de orden 2 por lo que hay 3 en total

$o(y^i) = \dfrac{o(y)}{(o(y), i)} \Rightarrow 2 = \dfrac{12}{(12, i)} \Rightarrow (12, i) = 6 \Rightarrow i = 6$

Por lo que los elementos de orden 2 son:

$\overline{44}$ y $\overline{2}^6 = \overline{19} \Rightarrow \overline{44}\cdot\overline{19} = \overline{26}$

Entonces los posibles soluciones son $x = \{\overline{1}, \overline{44}, \overline{19}, \overline{26}\}$.

IV)

$G/N_2 \cong C_4 \Rightarrow N_2 \cong C_2 \times C_3$

$<\overline{44}> \cong C_2$, ahora necesitamos uno de orden 3

$o(g) = \frac{12}{(12,i)} \Rightarrow 3 = \frac{12}{(12,i)} \Rightarrow (12,i) = 4 \Rightarrow i = 4 \Rightarrow$

$\Rightarrow \bar{2}^4 = \overline{16}$, $o(\overline{16}) = 3 \Rightarrow <\overline{16}> \cong C_3$

$<\overline{44}> = \{\bar{1}, \overline{44}\}$, $<\overline{16}> = \{\bar{1}, \overline{16}, \overline{34}\}$

$<\overline{44}> \cap <\overline{16}> = \{\bar{1}\}$ por lo que $N_2 = <\overline{44}> \times <\overline{16}>$

Ahora $G/N_1 \cong C_2 \times C_2 \Rightarrow N_1 \cong C_6$. Ahora buscamos un elemento de orden 6 :

$6 = \frac{12}{(12,i)} \Rightarrow (12,i) = 2 \Rightarrow i = 2$

$\bar{2}^2 = \bar{4}$, $o(\bar{4}) = 6 \Rightarrow <\bar{4}> \cong C_6$. Y por lo tanto, $N_1 = <\bar{4}>$.

Examen (Febrero 2002)

Problemas

1. Supongamos que H es un grupo abeliano y sea $f: G \longrightarrow H$ un homomorfismo. Definimos una aplicación $\alpha: G\times G \longrightarrow H$ por $\alpha((g_1, g_2)) = f(g_1) f(g_2)^{-1}$

I) Probar que α es un homomorfismo.

II) En el caso de que $G = \Sigma_3$, $H = \{-1, 1\}$ y f el homomorfismo signatura, enunciar los elementos de $Ker(\alpha)$ y calcular sus ordenes.

III) Siguiendo con el caso anterior, ¿$Ker(\alpha)$ es abeliano? ¿Y existen dos subgrupos H_1 y H_2 de G tales que $Ker(\alpha) = H_1 \times H_2$?

I) $\alpha((g_1, g_2), (g_3, g_4)) = \alpha((g_1 g_3), (g_2 g_4)) = f(g_1 g_3) \cdot f^{-1}(g_2 g_4) =$

$= \alpha(g_1 g_2) \cdot \alpha(g_3 g_4) = f(g_1) \cdot f^{-1}(g_2) f(g_3) \cdot f(g_4)^{-1} =$

$= f(g_1) \cdot f(g_3) \cdot f(g_2)^{-1} \cdot f(g_4)^{-1} = f(g_1 g_2) \cdot f(g_3 g_4)^{-1}$ con H abeliano

Luego, α es un homomorfismo.

II) $Ker(\alpha) = \{(\sigma_1, \sigma_2) \in \Sigma_3 \times \Sigma_3 \mid \alpha(\sigma_1, \sigma_2) = 1\} =$

$= \{(\sigma_1, \sigma_2) \in \Sigma_3 \times \Sigma_3 \mid f(\sigma_1) f(\sigma_2)^{-1} = 1\} =$

$= \{(\sigma_1, \sigma_2) \in \Sigma_3 \times \Sigma_3 \mid f(\sigma_1) = f(\sigma_2)\}$

$\Sigma_3 = \{1, (12), (13), (23), (123), (132)\}$

$Ker(\alpha) = \{1, (123), (132), (12)(23), (12)(13), (23)(12), (23)(13),$
$(23)(13), (123)(132)\} \Rightarrow$

$\Rightarrow Ker(\alpha) = \{1, (123), (132)\}$

$o(1) = 1$

$o(123) = o(132) = 3$

2. Demostrar que un grupo G con 105 elementos, o tiene un 5-subgrupo de Sylow normal, o tiene un 7-subgrupo de Sylow. Deducir que G tiene un subgrupo normal cíclico N con $|G:N|=3$

Supongamos $\partial_7 \neq 1$ y $\partial_5 \neq 1 \Rightarrow \partial_7 = 15$ y $\partial_5 = 21$ y G tendría:

$15(7-1) = 90$ elementos de orden 7.

$21(5-1) = 84$ elementos de orden 5.

En total $= 84+90 = 174 > 105 = |G|$ Absurdo, por lo que $\partial_7 = 1$ y $\partial_5 = 21$ ó $\partial_7 = 15$ y $\partial_5 = 1$ ó $\partial_7 = 1$ y $\partial_5 = 1$

$$\left.\begin{array}{l} G \\ \left.\begin{array}{l} N_G(N) \\ N \end{array}\right] 3 \\ \\ 1 \end{array}\right] 105 \Rightarrow |N| = 35 \Rightarrow N \cong C_{35} \cong C_7 \times C_5$$

Por tanto, $P \cong C_7$ y $Q \cong C_5$, con P-7 Sylow y Q-5 Sylow de G,

$P \trianglelefteq G$, $Q \trianglelefteq G \Rightarrow N = P \times Q \trianglelefteq G$.

Cuestiones

1. I) Resolver la congruencia: $x^{40} \equiv 1 \pmod{42}$

II) Si es un grupo semidirecto de un subgrupo normal $N = \langle a \rangle$ de orden 42 y un subgrupo $H = \langle b \rangle$ de orden 5, ¿Se puede asegurar que G es abeliano

I)

$$\left.\begin{array}{l} \varphi(42) = \varphi(2)\varphi(3)\varphi(7) = 12 \\ 42 = 12 \cdot 3 + 4 \end{array}\right\} \Rightarrow x^{12 \cdot 3 + 4} \equiv 1 \pmod{42} \Rightarrow$$

$\Rightarrow x^4 \equiv 1 \pmod{42}$

$$\left.\begin{array}{l} o(x) \mid 42 \\ o(x) \mid 4 \end{array}\right\} \Rightarrow o(x) \mid (42,4) = 2 \Rightarrow \left\{\begin{array}{l} x = 1 \Rightarrow 1 \equiv 1 \pmod{42} \\ \text{ó} \\ x = 2 \Rightarrow 16 \not\equiv 1 \pmod{42} \end{array}\right.$$

II)

$N = \langle a \rangle \cong C_{42}$ Si G es abeliano necesitamos que $(42,5)=1$
$H = \langle b \rangle \cong C_5$ y lo es, por tanto G es abeliano.

2. Determinar:
I) ¿Cuantos elementos de orden p hay en C_{p^2} y en $C_p \times C_{p^2}$?
II) ¿Cuantos elementos de orden p^2 hay en C_{p^2} y en $C_p \times C_p$?
III) ¿Cuantos subgrupos de orden p^2 hay en $C_p \times C_{p^2}$? ¿Son todos ellos isomorfos?

I)
• En C_{p^2} como $p \mid p^2 \Rightarrow$ que hay $\varphi(p) = p-1$ elementos de orden p en C_{p^2}
• En $C_p \times C_{p^2}$ como $p \mid p \Rightarrow$ hay $\varphi(p) = p-1$ elementos de orde p.
En C_{p^2} como $p \mid p^2 \Rightarrow$ Hay $\varphi(p) = p-1$ elementos de orden p en C_{p^2}

Pero tambien dos elementos de orden p generan otro de orden p, entonces hay $(p-1)(p-1) = p(p-1)^2$ elementos de orden p.
Por lo tanto, hay $(p-1)+(p+1)+(p-1)^2 = p+p-2+p^2-2p+1 = p^2-1$ elementos de orden p en $C_p \times C_{p^2}$

II)
En C_p, como $p^2 \nmid p \Rightarrow$ no hay elementos p^2 en C_p
En C_{p^2}, como $p^2 \mid p^2 \Rightarrow$ hay $\varphi(p^2) = p(p-1)$ elementos de orden p^2
En C_p hay $\varphi(p) = p-1$ elementos de orden p que junto con los elementos de p^2 de C_{p^2}, generan elementos de orden p^2
$(p-1)(p^2-1)p$.
Entonces, hay $p(p-1)+(p-1)(p^2-1)p$ elementos de orden p en $C_p \times C_{p^2}$

III)

$$|Syl_{p^2}| = \frac{\text{elementos de orden } p^2 \text{ en } C_p \times C_{p^2}}{\varphi(p^2)} = \frac{p^3 - p^2}{p(p-1)} = \underline{\underline{p}}$$

3. Demostrar que el grupo A_7 posee un subgrupo de orden 6 y no posee un subgrupo de índice 6 (subgrupo abeliano y no abeliano

$$A_7 = \frac{7!}{2} = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$$

Sea $|S| = 6$, con $S \leq A_7 \underset{\text{Cauchy}}{\Rightarrow} |S| \mid |A_7| \Rightarrow \underline{\underline{|A_7 : S|}} = 7 \cdot 5 \cdot 4 \cdot 3 = \underline{\underline{420}}$

Examen (21-01-03)

Cuestiones

1. De las siguientes afirmaciones, decir si son verdaderas o falsas, justificando la respuesta en cada caso:

I) Si $G = \langle a \rangle \times \langle b \rangle$ y $N = \langle ab \rangle$, entonces G/N es un grupo cíclico.

II) De $G = \langle a \rangle \cong C_6$ en $H = \langle b \rangle \cong C_{25}$ existen homomorfismos no triviales.

Examen (24-01-2008)

Cuestiones

1. Decidir si son verdaderas o falsas cada una de las tres afirmaciones siguientes, dando una demostración, en el caso verdadero, y un contraejemplo, en el falso:

I) Si a, b son elementos de un grupo G con $o(a)=2$ y $o(b)=3$, entonces $o(ab)=6$

II) Los siguientes dos elementos son conjugados en Σ_7

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$$

III) Sea $G = \langle g \rangle$ un grupo cíclico de orden 63 y sea $f: G \to G$ dado por $f(g) = g^{14}$. Entonces se verifica $G \cong Ker(f) \times f(G)$.

I) Falso. Contraejemplo

Sean $(12), (123) \in \Sigma_3$, luego

$(12)(12) = id \Rightarrow o(12) = 2$

$(123)(123) = (132) \Rightarrow (132)(123) = (132) = id \Rightarrow o(123) = 3$

$(12)(123) = (13)$

$(13)(13) = id \Rightarrow o(13) = 2 \neq 6$

II) Verdadero.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} = (1357)(246)$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = (123)(4567)$$

Son conjugados porque tienen el mismo tipo, es decir, (4-ciclo)(3-ciclo).

III) Verdadero.

$f(G) = \langle g^{14} \rangle \Rightarrow |f(G)| = o(g^{14}) = \dfrac{o(g)}{(o(g), 14)} = \dfrac{63}{(63,14)} = \dfrac{63}{7} = 9$

Por lo tanto, $f(G) \cong C_3 \times C_3$ ó $f(G) \cong C_9$.

Ahora por el 1^er^ teorema de isomorfía de grupos:

$|Ker(f)| = \dfrac{|G|}{|f(G)|} = \dfrac{63}{9} = 7 \Rightarrow |Ker(f)| = 7 \Rightarrow Ker f \cong C_7$

Luego, tenemos dos opciones: $- G \cong C_3 \times C_3 \times C_7 \rightarrow$ no es cíclico
(No es posible, ya que G es cíclico)

$- G \cong C_9 \times C_7$ es cíclico $\Rightarrow$
$\Rightarrow G \cong f(G) \times Ker f$.

2. I) Sea $\sigma = (1\,2\,3\,4\,5\,6) \in \Sigma_6$. Demostar que $C_{\Sigma_6} = \langle \sigma \rangle$.

II) Encontar otra permutación $\tau \in \Sigma_6$ tal que $C_{\Sigma_6}(\sigma) \cap C_{\Sigma_6}(\tau) = \{1\}$.

III) Demostrar que en cualquier grupo G se verifica $Z(G) = \bigcap_{g \in G} C(g)$.

IV) Deducir de los apartados anteriores $Z(\Sigma_6) = \{1\}$.

Problemas

1. Consideramos el siguiente subgrupo de Σ_8

$$G = <\alpha, \beta>$$

donde $\alpha = (1234)(5678)$, $\beta = (1537)(2846)$. Se pide:

I) Demostrar que $<\alpha>$ y $<\beta>$ son normales en G y $G/<\alpha> \cong C_2 \cong G/<\beta>$.
Analizar si G es, o no es abeliano.

II) Calcular $|G|$ y demostrar que $G = <\alpha><\beta>$ y enumerar sus distintos elementos, junto con sus respectivos ordenes.

III) Determinar todos los subgrupos de G y decir cuales de ellos son normales en G.

I)

$o(\alpha) = 4$

$o(\beta) = 4$

Veamos si G es abeliano, es decir, $\alpha\beta = \beta\alpha$

$$\left.\begin{array}{l} \alpha\beta = (1836)(2745) \\ \beta\alpha = (1638)(2547) \end{array}\right\} \Rightarrow \alpha\beta \neq \beta\alpha \Rightarrow G \text{ no es abeliano}$$

¿$<\alpha> \triangleleft G$?

$<\alpha> \triangleleft G \Leftrightarrow \forall \sigma \in <\alpha>, \forall \mu \in G, \sigma^{\mu} \in <\alpha>$

Lo probaremos para los generadores:

$\alpha^{\alpha} = \alpha^{-1}\alpha\alpha = \alpha \in <\alpha>$

$\alpha^{\beta} = (\beta(1)\,\beta(2)\,\beta(3)\,\beta(4))(\beta(5)\,\beta(6)\,\beta(7)\,\beta(8)) = (5876)(3214) =$

$= \alpha^{-1} \in <\alpha>$

Por lo tanto, $<\alpha> \triangleleft G$

¿$<\beta> \triangleleft G$?

$<\beta> \triangleleft G \Leftrightarrow \forall \sigma \in <\beta>, \forall \mu \in G, \sigma^{\mu} \in <\beta>$. Razonando de la misma manera:

$\beta^{\beta} = \beta^{-1}\beta\beta = \beta \in <\beta>$

$\beta^{\alpha} = (\alpha(1)\,\alpha(5)\,\alpha(3)\,\alpha(7))(\alpha(2)\,\alpha(8)\,\alpha(4)\,\alpha(6)) = (2648)(3517) = \beta^{-1} \in <\beta>$

Luego $\beta \triangleleft G$

¿ $G/_{<\alpha>} \cong C_2$?

$$G/_{<\alpha>} = \frac{<\alpha,\beta>}{<\alpha>} = <\alpha\cdot<\alpha>, \beta\cdot<\alpha>> = <<\alpha>, \beta<\alpha>> =$$

$$= <\beta<\alpha>> = \underbrace{<\bar{\beta}>}_{\bar{\beta}^2=<\alpha>} \cong C_2$$

¿ $G/_{<\beta>} \cong C_2$?

$$\frac{G}{<\beta>} = \frac{<\alpha,\beta>}{<\beta>} = <\alpha\cdot<\beta>, \beta<\beta>> = <\alpha<\beta>, <\beta>> =$$

$$= <\alpha<\beta>> = \underbrace{<\bar{\alpha}>}_{\bar{\alpha}^2=\beta} \cong C_2$$

II)

$$|G| = \left|\frac{G}{<\alpha>}\right| |<\alpha>| = 2\cdot 4 = 8 \Rightarrow |G| = 8$$

$$|<\alpha><\beta>| = \frac{o(\alpha)\,o(\beta)}{|<\alpha>\cap<\beta>|} = \frac{4\cdot 4}{|<\alpha>\cap<\beta>|}$$

Calculamos $|<\alpha>\cap<\beta>|$:

$$\left.\begin{array}{l} <\alpha>\cap<\beta> \leq <\alpha> \\ <\alpha>\cap<\beta> \leq <\beta> \end{array}\right\} \Rightarrow \left\{\begin{array}{l} |<\alpha>\cap<\beta>| \,\big|\, |<\alpha>| \\ |<\alpha>\cap<\beta>| \,\big|\, |<\beta>| \end{array}\right\} \Rightarrow$$

$$\Rightarrow |<\alpha>\cap<\beta>| \,\big|\, 4 \Rightarrow |<\alpha>\cap<\beta>| = \begin{cases} \cdot 1 \\ \cdot 2 \\ \cdot 4 \end{cases}$$

- $|<\alpha>\cap<\beta>| \neq 4$ ya que $\alpha \neq \beta$
- Si $|<\alpha>\cap<\beta>| = 2 \Rightarrow 2 = \frac{4}{(4,i)} \Rightarrow (4,i) = 2 \Rightarrow i = 2 \Rightarrow$
  $\Rightarrow \alpha^2 = \beta^2$
  Veamos si es cierto, $\alpha^2 = (13)(24)(57)(68) = \beta^2 \Rightarrow$
  $\Rightarrow |<\alpha>\cap<\beta>| = 2$

Por lo tanto, $|<\alpha><\beta>| = \frac{16}{2} = 8 = |G| \Rightarrow G = <\alpha><\beta>$

Los elementos de G serán:

$\{1, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$

$|\langle\alpha\rangle \cap \langle\beta\rangle| = 2 \Rightarrow \langle\alpha\rangle \cap \langle\beta\rangle = \langle\alpha^2\rangle = \langle\beta^2\rangle$

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

$|G| = 8, \ \left|\frac{G}{\langle\alpha\rangle}\right| = \left|\frac{G}{\langle\beta\rangle}\right| = 2$

Calculamos los ordenes de los distintos elementos de G:

- $o(1) = 1, \ o(\alpha) = o(\beta) = 4$
- $o(\alpha^3) = \frac{o(\alpha)}{(3, o(\alpha))} = 4$
- $o(\alpha^2) = \frac{\alpha(\alpha)}{(2, o(\alpha))} = \frac{4}{2} = 2$
- $o(\alpha^2\beta) = \alpha^2\beta = (1735)(2648) \Rightarrow o(\alpha^2\beta) = 4$
- $o(\alpha^3\beta) = (1432)(5876)\beta = (1638)(2547) \Rightarrow o(\alpha^3\beta) = 4$

III)

Veamos cual es la estructura de G. Sabemos que $|G| = 8$ y no abeliano $\Rightarrow G \cong Q_8$ ó $G \cong D_8$

$Q_8 = \langle \alpha, \beta \mid \alpha^4 = 1, \beta^2 = \alpha^2, \alpha^\beta = \alpha^{-1} \rangle$

$D_8 = \langle \alpha, \beta \mid \alpha^4 = 1 = \beta^2, \alpha^\beta = \alpha^{-1} \rangle$

Veamos que

$o(\alpha) = 4 \Rightarrow \alpha^4 = 1$

$|\langle\alpha\rangle \cap \langle\beta\rangle| = 2 \Rightarrow \langle\alpha^2\rangle = \langle\beta^2\rangle \Rightarrow \alpha^2 = \beta^2$

$\alpha^\beta = \beta^{-1}\alpha\beta = \alpha^{-1}$

Por lo que $G \cong Q_8$.

Calculamos los subgrupos

$\forall H \leq G$, $|H| \mid |G| = 8 \Rightarrow |H| = 1, 2, 4, 8$

$|H| = 1 \Rightarrow H = \{1_G\}$

$|H| = 8 \Rightarrow H = G$

Si $|H| = 2 \Rightarrow H = <\alpha^2> \to$ único elemento de orden 2.

Si $|H| = 4 \Rightarrow H = <\mu_1><\mu_2>$ tal que $o(\mu_1) = o(\mu_2) = 2$ no puede ser porque el único elemento de orden 2 es α^2

$H = <\mu>$ tal que $o(\mu) = 4$, entonces son $<\alpha>, <\alpha^2\beta>, <\alpha\beta>$

observamos que

$<\alpha^2\beta> = <\beta^3> = \{1, \beta^3, \beta^6, \beta^9\} = \{1, \beta, \beta^2, \beta^4\} = <\beta>$

$$o(\beta^3) = \frac{o(\beta)}{(o(\beta), 3)} = \frac{4}{(4,3)} = 4$$

$o(\alpha^3\beta) = <\alpha\alpha^2\beta> = <\alpha\beta>$, $<\alpha^3> = <\alpha>$

Por lo que los subgrupos en G son: $<\alpha^2>, <\alpha>, <\beta>, <\alpha,\beta>$.

Veamos si son normales en G:

¿$<\alpha^2> \triangleleft G$?

$(\alpha^2)^\alpha = \alpha^{-1}\alpha^2\alpha = \alpha^2 \in <\alpha^2>$

$(\alpha^2)^\beta = ((18)(24)(57)(68))^\beta = (57)(86)(31)(24) = \alpha^2 \in <\alpha^2>$

Luego $<\alpha^2> \triangleleft G$ y anteriormente hemos visto $<\alpha> \triangleleft G$ y $<\beta> \triangleleft G$.

¿$<\alpha\beta> \triangleleft G$?

$(\alpha\beta)^\alpha = \beta\alpha = (\alpha\beta)^{-1} \in <\alpha\beta>$

$(\alpha\beta)^\beta = (5472)(8163) = (\alpha\beta)^{-1} \in <\alpha\beta>$

Entonces $<\alpha\beta> \triangleleft G$.

2. Sea G un grupo finito cumpliendo la siguiente propiedad:

"Para cualesquiera H y K subgrupos de G, se verifica $H \leq K$ o $K \leq H$"

I) ¿Cuantos p-subgrupos de Sylow tiene G, para p un divisor primo de $|G|$?

II) Deducir que $|G|$ es potencia de un solo primo.

III) Probar que existe un único subgrupo de G para cada divisor de $|G|$.

IV) Deducir que G es cíclico.

Examen (06-09-2006)

Cuestiones

1. Se consideran las permutaciones Σ_7:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$$

I) Calcular α^{18}, β^{-23} y $(\alpha\beta)^{100}$.

II) Decir razonadamente si α y β son conjugados en Σ_7 y, en caso afirmativo, encontrar una permutación δ tal que $\alpha^{\delta} = \beta$.

I)
En primer lugar descomponemos α, β y $\alpha\beta$ en producto de ciclos disjuntos:

$\alpha = (1\,3\,5\,7)(2\,4\,6)$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 6 & 7 & 4 & 3 & 2 \end{pmatrix}$$

$\beta = (1\,2\,3)(4\,5\,6\,7)$

$\alpha\beta = (2\,5\,4\,7)(3\,6)$

$o(\alpha) = 12 \Rightarrow \alpha^{18} = \underbrace{\alpha^{12}}_{1} \cdot \alpha^{6} = \alpha^{6} \Rightarrow \alpha^{18} = (1\,5)(3\,7)$

$\alpha^2 = (1\,5)(3\,7)(2\,6\,4)$

$\alpha^4 = (2\,4\,6)$

$\boxed{\alpha^6 = (1\,5)(3\,7)}$

$\beta^{-23} = \beta^{-24}\beta = (\beta^{12})^{-2}\beta = \beta \Rightarrow \beta^{-23} = (1\,2\,3)(4\,5\,6\,7)$

$(\alpha\beta)^{100}$

$o(\alpha\beta) = 4 \Rightarrow ((\alpha\beta)^4)^{25} = 1$

II)

α y β son conjugados en Σ_7 porque tienen el mismo tipo de factorización en ciclos disjuntos.

$$\gamma = \left(\begin{array}{cccc|ccc} 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ \multicolumn{4}{c|}{(4\text{-ciclo}) \text{ de } \beta} & \multicolumn{3}{c}{(3\text{-ciclo}) \text{ de } \beta} \end{array} \right) =$$

$$= \left(\begin{array}{cccc|ccc} 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \end{array} \right) = (1\,4\,2)(3\,5\,6)$$

2. I) Considerar el grupo multiplicativo $\mathcal{U}(\mathbb{Z}/33\mathbb{Z})$. Calcular el orden de $\bar{2}$ y de $\overline{10}$. Expresar $\mathcal{U}(\mathbb{Z}/33\mathbb{Z})$ como producto directo de subgrupos.

II) Determinar todos los subgrupos de $\mathcal{U}(\mathbb{Z}/33\mathbb{Z})$

I)

$$\left.\begin{array}{l} \{\bar{2}^0, \bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5, \dots, \bar{2}^{10}\} \\ \{\bar{1}, \bar{2}, \bar{4}, \bar{8}, \overline{16}, \overline{32} = -\bar{1}, \dots, \bar{1}\} \end{array}\right\} \Rightarrow o(\bar{2}) = 10$$

$$\left.\begin{array}{l} \{\overline{10}^0, \overline{10}^1, \overline{10}^2\} \\ \{\bar{1}, \overline{10}, \overline{100} = \bar{1}\} \end{array}\right\} \Rightarrow o(\overline{10}) = 2$$

$\varphi(33) = \varphi(3)\cdot\varphi(11) = 2\cdot 10 = 20 = 4\cdot 5$

Posibles estructuras

$G \cong C_2 \times C_2 \times C_5 \cong C_2 \times C_{10}$

$G \cong C_4 \times C_5 \cong C_{20}$

Sabemos que $o(\overline{10}) = 2$ y $o(\overline{32}) = 2$, por lo que $G \cong C_2 \times C_{10}$ porque en $C_4 \times C_5$ no hay elementos de orden 2, y como sabemos $o(\bar{2}) = 10$, $o(\overline{10}) = 2$. Por tanto, $G \cong \langle \bar{2} \rangle \times \langle \overline{10} \rangle$ y $\langle \bar{2} \rangle \cap \langle \overline{10} \rangle = \{\bar{1}\}$

II)

Vemos que los elementos de $\mathcal{U}(\mathbb{Z}/33\mathbb{Z})$ tienen ordenes

1, 2, 5, 10

$\mathcal{U}(\mathbb{Z}/33\mathbb{Z}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}, \overline{10}, \overline{13}, \overline{14}, \overline{16}, \overline{17}, \overline{19}, \overline{20}, \overline{23}, \overline{25}, \overline{26}, \overline{28}, \overline{29}, \overline{31}, \overline{32}\}$

Calculamos los ordenes de los elementos:

- Orden 2 : 3
- Orden 5 : 4
- Orden 1 : 1
- Orden 10 : 12

Elementos de orden 2 : $\overline{10}, \overline{32}, \overline{10 \cdot 32} = \overline{320} = \overline{23}$

Elementos de orden 5 : $5 = \dfrac{10}{(10, i)} \Rightarrow (10, i) = 2 \Rightarrow i = 2$

$\bar{4}^1, \bar{4}^2 = \overline{16}, \bar{4}^3 = \overline{31}, \bar{4}^4 = \overline{25}$

El resto de clases son de orden 10

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

$o(\overline{10}) = o(\overline{32}) = o(\overline{23}) = 2$

$o(\bar{4}) = o(\overline{16}) = o(\overline{31}) = o(\overline{25}) = 5$

$o(\bar{2}) = o(\bar{5}) = o(\bar{7}) = o(\bar{8}) = o(\overline{13}) = o(\overline{14}) = o(\overline{15}) = o(\overline{17}) =$
$= o(\overline{19}) = o(\overline{20}) = o(\overline{26}) = o(\overline{28}) = o(\overline{29}) = 10$

Calculamos los subgrupos:

> Subgrupos de orden 2 : $\langle \overline{10} \rangle, \langle \overline{32} \rangle, \langle \overline{23} \rangle$

> Subgrupos de orden 5 : $\langle \bar{4} \rangle, \langle \overline{16} \rangle, \langle \overline{32} \rangle, \langle \overline{25} \rangle$

> Subgrupos de orden 10 : $\langle \bar{2} \rangle, \langle \bar{5} \rangle, \ldots, \langle \overline{29} \rangle$

> Subgrupos de orden $C_2 \times C_2$: $\langle \overline{10} \rangle \times \langle \overline{32} \rangle, \langle \overline{10} \rangle \times \langle \overline{23} \rangle, \langle \overline{32} \rangle \times \langle \overline{23} \rangle$

Problemas

1. Considerar el siguiente subconjunto del grupo $GL_3(\mathbb{R})$

$$G = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R},\ ad \neq 0 \right\}$$

I) Demostrar que G es un subgrupo no abeliano de $GL_3(\mathbb{R})$.

II) Sea $N = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x, y \in \mathbb{R} \right\}$. Definir un homomorfismo $f : G \to \mathbb{R} \times \mathbb{R}$ tal que $\ker f = N$.

III) ¿$N \trianglelefteq G$? Probar que $N \cong \mathbb{R} \times \mathbb{R}$ y que $G/N \cong \mathbb{R} \times \mathbb{R}$ (multiplicativo).

IV) Encontrar un subgrupo H de G de modo que G sea el producto semidirecto de N y H.

2. Sea G un grupo abeliano de orden $203 = 7 \cdot 29$.

I) Determinar cuantos subgrupos tiene G, distinguiendo aquellos que son normales en G.

II) Determinar el número de elementos de cada orden en G.

I)

G puede tener subgrupos de orden 7 o de orden 29. Veamos cuantos

$$\left.\begin{array}{l} \partial_{29}(G) \mid 7 \\ \partial_{29}(G) \equiv 1 \pmod{29} \end{array}\right\} \Rightarrow \partial_{29}(G) = 1 \Rightarrow \exists Q \trianglelefteq G \text{ tal que } |Q| = 29$$

$$\left.\begin{array}{l} \partial_{7}(G) \mid 29 \\ \partial_{7}(G) \equiv 1 \pmod{7} \end{array}\right\} \Rightarrow \partial_{7}(G) = 1 \text{ ó } 29$$

Supongamos $\partial_7(G) = 1 \Rightarrow \exists P \trianglelefteq G$ tal que $|P| = 7 \Rightarrow$

$\Rightarrow G \cong P \times Q \cong C_7 \times C_{25} \cong C_{203} \Rightarrow G$ abeliano (contradicción)

Por lo que $\partial_7(G) = 29$. Entonces G tiene 29 subgrupos de orden 7 y 1 subgrupo de orden 29.

II)

$$\left.\begin{array}{l} \cdot \text{ N}^{\text{o}} \text{ de elementos de orden } 29 : \varphi(29) = 28 \\ \cdot \text{ N}^{\text{o}} \text{ de elementos de orden } 7 : 29 \cdot \varphi(7) = 29 \cdot 6 = 174 \\ \cdot \text{ N}^{\text{o}} \text{ de elementos de orden } 203 \text{ (neutro)} : 1 \end{array}\right\} \Rightarrow$$

$\Rightarrow 28 + 174 + 1 = 203 = |G|$

Examen (13-12-2005)

1. Resolver la congruencia (sin usar la calculadora)

$$x^{63} \equiv 1 \pmod{18}$$

$\varphi(18) = \varphi(3^2)\cdot\varphi(2) = 6$, $63 = 6\cdot 10 + 3$

Por lo tanto, $x^{63} = x^{6\cdot 10+3} = (x^6)^{10}\cdot x^3 \Rightarrow \underbrace{(x^6)}_{1}{}^{10} x^3 \equiv 1 \pmod{18} \Rightarrow$

$\Rightarrow x^3 \equiv 1 \pmod{18}$

$\left.\begin{matrix} o(x) \mid 3 \\ o(x) \mid 6 \end{matrix}\right\} \Rightarrow o(x) \mid (3,6) = 3 \Rightarrow o(x) = 1$ ó 3

- Si $o(x) = 1 \Rightarrow x = 1$.
- Si $o(x) = 3 \Rightarrow o(x^i) = \dfrac{o(x)}{(o(x), i)} \Rightarrow 3 = \dfrac{6}{(6,i)} \Rightarrow (6,i) = 2 \Rightarrow i = 2$

Entonces, buscamos ahora los elementos de orden 3:

$\bar{5} = \{\underset{\bar{1}}{\bar{5}^0}, \bar{5}, \bar{5}^2 = \overline{25} = \bar{7}, \bar{5}^3 = \overline{17}\}$

$\bar{7} = \{\underset{\bar{1}}{\bar{7}^0}, \bar{7}, \bar{7}^2 = \overline{49} = \overline{13}, \bar{7}^3 = \bar{1}\} \to o(\bar{7}) = 3$

$\overline{11} = \{\bar{1}, \overline{11}, \overline{13}, \overline{17}\}$ -

$\overline{13} = \{\bar{1}, \overline{13}, \bar{7}, \bar{1}\} \to o(\overline{13}) = 3$

$\overline{17} = \{\bar{1}, \overline{17}, \bar{1}\} \to o(\overline{17}) = 2$

Luego las posible soluciones serían $\overline{13}$, $\bar{7}$ y $\bar{1}$

2. I) Si G es un grupo abeliano de orden 36 ¿Que estructura puede tener G?, es decir, ¿Cuales son los distintos tipos de isomorfía?

$36 = 2^2 \cdot 3^2$

$G \cong C_2 \times C_2 \times C_3 \times C_3 \cong C_6 \times C_6$

$G \cong C_4 \times C_3 \times C_3 \cong C_{12} \times C_3$

$G \cong C_9 \times C_2 \times C_2 \cong C_{18} \times C_2$

$G \cong C_4 \times C_9 \cong C_{36}$

II) Si $G = \langle a \rangle \times \langle b \rangle \cong C_8 \times C_6$. Determinar todos los elementos de orden 2, de orden 3 y de orden 6 en G.

- Elementos de orden 2: En C_8 hay un elemento de orden 2 y en C_6 otro también de orden 2 y entre dichos elementos generan otro, luego:

$2 = \frac{8}{(8,i)} \Rightarrow (8,i) = 4 \Rightarrow i = 4$

$2 = \frac{6}{(6,i)} \Rightarrow (6,i) = 3 \Rightarrow i = 3$

Por lo que los elementos de orden 2: $\{a^4, b^3, a^4b^3\}$

- Elementos de orden 3; Solo hay 2 elementos de orden 3 en C_6, $\varphi(3) = 2$

$3 = \frac{6}{(6,i)} \Rightarrow (6,i) = 2 \Rightarrow i = 2 \Rightarrow \{b^2, b^4\}$

- Elementos de orden 6: En C_6 hay $\varphi(6) = 2$ elementos de orden 6, que con el elemento de orden 2 en C_8 generan otros 2 de orden 6 y los 2 elementos de orden 3 con el elemento de orden 2 de C_8 se generan otros 2 de orden 6, en total hay 6 elementos de orden 6.

$6 = \frac{6}{(6,i)} \Rightarrow (6,i) = 1 \Rightarrow i = 1$ ó 5

Entonces, $\{b, b^5, a^4b, a^4b^5, b^2a^4, b^4a^4\}$

III) En el caso anterior, determinar todos los subgrupos de G de orden 6.

Son los siguientes subgrupos los que tenemos:

$\langle b\rangle, \langle b^5\rangle, \langle a^4\rangle\times\langle b\rangle, \langle a^4\rangle\times\langle b^2\rangle, \langle a^4\rangle\times\langle b^5\rangle, \langle b^4\rangle\times\langle a^4\rangle$

Pero podemos ver que: - $\langle b\rangle = \langle b^5\rangle$

- $\langle a^4\rangle\times\langle b\rangle = \langle a^4\rangle\times\langle b^5\rangle$
- $\langle a^4\rangle\times\langle b^2\rangle = \langle a^4\rangle\times\langle b^4\rangle$

Por tanto, hay 3 subgrupos de orden 6.

Problema

1. Considerar los siguientes subconjuntos del grupo $GL_2(\mathbb{K})$, donde $\mathbb{K}$ es un cuerpo

$$G=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix} \mid a,b,c\in\mathbb{K},\ ac\neq 0\right\},\quad N=\left\{\begin{pmatrix} 1 & k\\ 0 & 1\end{pmatrix} \mid k\in\mathbb{K}\right\}$$

Demostrar que

I) G es un subgrupo de $GL_2(\mathbb{K})$. (Ayuda: Si $A=\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}$; calcular en primer lugar la matriz A^{-1}) ¿G es abeliano?

II) Definir un epimorfismo $f: G\longrightarrow(\mathbb{K}^*\times\mathbb{K}^*,\cdot)$ tal que $\operatorname{Ker} f = N$

III) ¿$N\trianglelefteq G$? ¿G/N es abeliano? Encontrar un subgrupo H de G tal que $G=NH$ y $N\cap H=\{1_G\}$.

IV) Definir un isomorfismo $g: N\longrightarrow(\mathbb{K},+)$. ¿$N$ es abeliano?

V) Si $|\mathbb{K}|=p$, con p primo, hallar $|G|$ y $|N|$.

VI) Hallar $Z(G)$

I)

$G \leq GL_2(\mathbb{K}) \Longleftrightarrow A, B \in G, A^{-1}B \in G$

Calculamos entonces A^{-1}:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{l} aa' = 1 \Rightarrow a' = a^{-1} \\ ab'+bc' = 0 \Rightarrow b' = -bc^{-1}a^{-1} \\ cc' = 1 \Rightarrow c' = c^{-1} \end{array}\right\} \Rightarrow A^{-1} = \begin{pmatrix} a^{-1} & -bc^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix}$$

$$\begin{pmatrix} a^{-1} & -bc^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} a^{-1}d & a^{-1}e - fbc^{-1}a^{-1} \\ 0 & c^{-1}f \end{pmatrix} \in G \Rightarrow$$

$\Rightarrow G$ es subgrupo de $GL_2(\mathbb{K})$.

Ahora veamos si G es abeliano:

$BA = AB \Rightarrow G$ abeliano, $\forall A, B \in G$

$$BA = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} ad & db+ec \\ 0 & fc \end{pmatrix}$$

$$AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & fc \end{pmatrix}$$

$BA \neq AB \Rightarrow G$ no es abeliano.

II)

Definimos $f: G \longrightarrow (\mathbb{K}^* \times \mathbb{K}^*, \cdot)$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a,c)$$

Probamos que es ~~homorfismo~~: $\forall A, B \in G$

$$f(AB) = f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right) = f\begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} = (ax, cz) = (a,c)\cdot(x,z) =$$

$$= f(A)\cdot f(B) \Rightarrow f(AB) = f(A)f(B)$$

Probamos que f es sobreyectiva: $\forall (a,c) \in \mathbb{K}^* \times \mathbb{K}^*$, $\exists A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$ tal que $f(A) = (a,c)$

Calculamos $Ker(f)$:

$$Ker f = \{A \in G \mid f(A) = (1,1)\} = \left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G \mid a \in \mathbb{K}\right\} = N$$

III)

Veamos que $N \trianglelefteq G$

$N \trianglelefteq G \Leftrightarrow A^{-1}BA \in N$, $A \in G$, $B \in N$

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad B = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} a^{-1} & -bc^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix}$$

$$A^{-1}BA = \begin{pmatrix} a^{-1} & -bc^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} =$$

$$= \begin{pmatrix} a^{-1} & a^{-1}k - bc^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & a^{-1}b + a^{-1}c^{-1}(k - bc^{-1}) \\ 0 & 1 \end{pmatrix} \in N$$

Luego, $N \trianglelefteq G$

¿ G/N abeliano?

Tomamos nuevamente las matrices A y B, y además una matriz N tal que sea $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, entonces se debe verificar $AN \cdot BN = BNAN$

$$AN \cdot BN = \left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \right] \left[\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \right] =$$

$$= \begin{pmatrix} a & ak+b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} x & xk+y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & a(xk+y)+z(ak+b) \\ 0 & cz \end{pmatrix}$$

$$BN \cdot AN = \begin{pmatrix} x & xk+y \\ 0 & z \end{pmatrix} \cdot \begin{pmatrix} a & ak+b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & x(ak+b)+c(xk+y) \\ 0 & cz \end{pmatrix}$$

Por lo tanto G/N no es abeliano.

Ahora buscamos $H \leq G$ tal que $G = NH$, $N \cap H = \{1_G\}$

$$H \leq G \Rightarrow H = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$$

$$G = NH \Rightarrow \underline{\underline{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}}} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \underline{\underline{\begin{pmatrix} x & y+kz \\ 0 & z \end{pmatrix}}} \Rightarrow$$

$$\Rightarrow \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} x & y+kz \\ 0 & z \end{pmatrix} \Rightarrow \begin{cases} a = x \Rightarrow \underline{x = a} \\ b = y + kz \Rightarrow \underline{\underline{y = b - kc}} \\ c = z \Rightarrow \underline{\underline{z = c}} \end{cases}$$

Para que $k = \frac{b}{c} \Rightarrow y = b - \frac{b}{c} c \Rightarrow y = 0$. Por lo que:

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \middle| \, a, c \in \mathbb{R} \right\}$$

Veamos si $N \cap H = \{1_G\} \Rightarrow N \cap H \Rightarrow \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \Rightarrow \begin{Bmatrix} a = 1 \\ k = 0 \\ c = 1 \end{Bmatrix} \Rightarrow$

$$\Rightarrow N \cap H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_G \right\}$$

III)

Definimos $g: N \longrightarrow (\mathbb{K}, +)$ tal que $g\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = k$

- g es homomorfismo: Sean $N_1, N_2 \in N$

$$f(N_1 + N_2) = f\left(\begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix}\right) = k_1 + k_2 = f(N_1) + f(N_2) \Rightarrow$$

$$\Rightarrow f(N_1 + N_2) = f(N_1) + f(N_2)$$

- g es sobreyectiva: Sea $k_1 \in \mathbb{K}$, entonces $\exists N_1 = \begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} \in N$ tal que $f\begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} = k_1$

- g es inyectiva: Veamos que $\operatorname{Ker} f = \{1_G\}$

$$\operatorname{Ker} f = \{ n \in N \mid f(n) = 0 \} = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in N \,\middle|\, f\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = 0 \right\} =$$

$$= \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in N \,\middle|\, k = 0 \right\} \Rightarrow \operatorname{Ker}(f) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = \{1_G\}$$

Luego, g es un isomorfismo.

Ahora nos falta ver si N es abeliano:

$$\left.\begin{aligned} & N_1 + N_2 = N_2 + N_1 \\ & N_1 + N_2 = \begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & k_1 + k_2 \\ 0 & 2 \end{pmatrix} \\ & N_2 + N_1 = \begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & k_1 + k_2 \\ 0 & 2 \end{pmatrix} \end{aligned}\right\} \Rightarrow N \text{ es abeliano}$$

IV)

V)

$$Z(G) = \{ A, B \in G \mid AB = BA \}, \quad A = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}, \quad B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

$$\left.\begin{aligned} AB &= \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & xc+by \\ 0 & zc \end{pmatrix} \\ BA &= \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & ay+bz \\ 0 & cz \end{pmatrix} \end{aligned}\right\} \Rightarrow$$

$$\Rightarrow \begin{cases} xa = ax \Rightarrow \underline{x = 1} \\ zc = cz \Rightarrow \underline{z = 1} \\ xc + by = ay + bz \Rightarrow c + by = ay + b \Rightarrow c - b = y(a-b) \Rightarrow \end{cases}$$

$$\Rightarrow \underline{y = \frac{c-b}{a-b}}$$

Por lo tanto, $Z(G) = \left\{ \begin{pmatrix} 1 & \frac{c-b}{a-b} \\ 0 & 1 \end{pmatrix} \middle| \; a, b, c \in \mathbb{K} \right\}$