Examen EA. Junio 2017. Solución.

1º Teoría.

2º ⓐ $p(-1) = (-1)^3 + 1 = 0 \Rightarrow$ $x=-1$ es raíz de $p(x)$

$\Rightarrow$ $x+1$ es factor de $p(x)$.

Dividimos x^3+1 entre $x+1$ con la regla de Ruffini.

$$\begin{array}{r|rrrr} & 1 & 0 & 0 & 1 \\ -1 & & -1 & 1 & -1 \\ \hline & 1 & -1 & 1 & \boxed{0} \end{array}$$

luego $p(x) = (x+1)(x^2-x+1)$.

Veamos si el segundo factor tiene divisores.
Hallemos sus raíces:

$$x = \frac{1 \pm \sqrt{1-4\cdot 1\cdot 1}}{2} = \frac{1 \pm \sqrt{-3}}{2} = \frac{1 \pm \sqrt{3}\cdot i}{2}$$

No tiene raíces en $\mathbb{R}$, por tanto tampoco en $\mathbb{Q}$, como es de grado 2 es irreducible.

Solución: $p(x) = (x+1)(x^2-x+1)$.

ⓑ En el apartado anterior hemos hallado las raíces en $\mathbb{C}$.

Solución: $p(x) = (x+1)\left(x - \frac{1+\sqrt{3}i}{2}\right)\left(x - \frac{1-\sqrt{3}i}{2}\right)$

Todos los factores son irreducibles por ser de grado 1.

(c) Partimos de la factorización de (a)

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

mod 2, estamos en $\mathbb{Z}_2[x]$

Veamos que $q(x) = x^2+x+1$ es irreducible

$q(0) = 0+0+1 = 1 \neq 0$

$q(1) = 1+1+1 = 1 \neq 0$

Como no tiene raíces y es de grado 2, es irreducible.

Solución: $p(x) = (x+1)(x^2+x+1)$.

(d) Veamos que todo polinomio tiene un representante de clase de grado ≤ 2.

(Dado $q(x) \in \mathbb{Z}_2[x]$, denotamos por $[q(x)]$ su clase módulo I.).

Por el teorema de la división, dividiendo entre x^3+1 tenemos

$$q(x) = (x^3+1) \cdot c(x) + r(x)$$

con grado $(r(x)) <$ grado $(x^3+1) = 3$.

Tomando clases temos

$$[q(x)] = \underbrace{[x^3+1]}_{=[0]} [c(x)] + [r(x)]$$

Luego $[q(x)] = [r(x)]$ y grado $(r(x)) \leq 2$.

En $\mathbb{Z}_2[x]$ hay 8 polinomios de grado ≤ 2, luego como mucho hay 8 clases:

$[0]$ $\quad$ $[x^2]$

$[1]$ $\quad$ $[x^2+x]$

$[x]$ $\quad$ $[x^2+1]$

$[x+1]$ $\quad$ $[x^2+x+1]$

Todas estas clases son distintas, ya que si la resta de 2 polinomios de grado ≤ 2 es múltiplo de x^3+1, esos polinomios tienen que ser iguales.

Por tanto las 8 clases anteriores son los elementos de B.

e) $[0]$ no es invertible (nunca lo es)
$[0]$ no es divisor de cero (por definición)

Sabemos que $x^3+1=(x+1)(x^2+x+1)$

Tomando clases.

$$\underset{\displaystyle [0]}{\underset{\shortparallel}{[x^3+1]}} = [x+1][x^2+x+1]$$

luego $[x+1]$ y $[x^2+x+1]$ son divisores de cero.

Sabemos que $[x^3+1]=[0] \Rightarrow$

$[x^3]+[1]=[0] \Rightarrow [x^3] = -[1] \underset{\text{mod } 2}{\Rightarrow}$

$$[x^3]=[1]$$

$$\Rightarrow \quad [x]\cdot[x^2] = [1].$$

Luego $[x]$, $[x^2]$ son invertibles

Además $\begin{cases} [x]^{-1} = [x^2] \\ [x^2]^{-1} = [x] \end{cases}$

Sabemos $[x^2+x] = [x][x+1]$

Multiplicando por $[x^2+x+1]$:

$$[x^2+x+1][x^2+x] = [x]\underbrace{[x+1][x^2+x+1]}_{=[0]} = [0]$$

divisores de cero.

Luego $[x^2+x]$ es divisor de cero.

Sabemos $[x^2+1] = [x+1][x+1]$

Multiplicando por $[x^2+x+1]$:

$$[x^2+x+1][x^2+1] = \underbrace{[x^2+x+1][x+1]}_{=[0]}[x+1] = [0]$$

divisores de cero

Luego $[x^2+1]$ es divisor de cero.

Por último $[1]$ siempre es invertible, ya que.

$$[1]\cdot[1] = [1].$$

Además $[1]^{-1} = [1]$

3º a) No pueden ser isomorfos ya que $\mathbb{Q}$ es cuerpo y $\mathbb{Z}$ no lo es (2 no tiene inverso en $\mathbb{Z}$).

b) En $\mathbb{Z}_2 \times \mathbb{Z}_4$ hay 2 elementos invertibles

$(1,1)$ y $(1,3)$

En $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ hay un único elemento invertible: $(1,1,1)$.

Por tanto no pueden ser isomorfos.

c) Sí son isomorfos. Conocemos, de teoría, un isomorfismo:

$$\begin{aligned} \mathbb{Z}_6 &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \\ [a]_6 &\longmapsto ([a]_2, [a]_3) \end{aligned}$$

d) Sí son isomorfos. Conocemos, de teoría un isomorfismo.

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} &\longrightarrow \mathbb{Z}_6 \\ [a]_{6\mathbb{Z}} &\longmapsto [a]_6 \end{aligned}$$

Obs: Se puede justificar que esta función es isomorfismo mediante el primer teorema de isomorfía o directamente como hicimos en teoría.

4º Teoría.

5º a) $|S_{20}| = 20!$ y $|A_{20}| = 20!/2$

Por tanto $[S_{20} : A_{20}] = 2$.

sabemos por teoría que todo subgrupo de índice 2 es normal, luego

$A_{20} \triangleleft S_{20}$. <u>VERDADERO</u>

b) <u>FALSO</u>. Vamos a construir un contraejemplo:

$G = D_4 = \{id, \sigma, \sigma^2, \sigma^3, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\}$

donde σ giro de 90° en sentido +

y τ es una simetría.

$H = \{id, \sigma^2, \tau, \tau\sigma^2\}$ es subgrupo de H

(visto en ~~[illegible]~~ clase y fácil de comprobar).

$K = \{id, \tau\}$ es subgrupo de H. (obvio)

$H \triangleleft G$ por tener índice 2.

$K \triangleleft H$ por tener índice 2.

Sin embargo $K \ntriangleleft G$: Veámoslo.

$\sigma\tau\sigma^{-1} = \tau\sigma^3\sigma^{-1} = \tau\sigma^2 \notin K$.

c) $|D_{20}| = 2 \cdot 20 = 40$

$|H| = |\langle \sigma \rangle| = 20$ (porque σ tiene orden 20).

luego $[D_{20} : H] = 2 \Rightarrow H \triangleleft D_{20}$

VERDADERO

d) FALSO. Encontremos $a \in H$, $b \in G$ tales que

$b \cdot a \cdot b^{-1} \notin H$.

Tomamos $a = \sigma$; $b = (1\ 3)$.

$b \cdot a \cdot b^{-1} = (1\ 3)(1\ 2\ \ldots\ 20)(1\ 3) =$

$= (1\ 4\ 5\ 6 \ldots 19\ 20\ 3\ 2) \underset{\text{NOT.}}{=} \alpha$

Esta permutación no puede ser un elemento de H ya que no es una potencia de σ:

La única potencia de σ que lleva $1 \mapsto 4$ es σ^3. Pero σ^3 lleva $4 \mapsto 7$, y

α lleva $4 \mapsto 5$

luego α no puede ser potencia de σ.

6º a) Los elementos de A_4 son:

* id, que es par porque $id = (12)(12)$
* Productos de dos permutaciones disjuntas:

$\alpha_1 = (12)(34)$

$\alpha_2 = (13)(24)$

$\alpha_3 = (14)(23)$

que obviamente son pares.

* Ciclos de longitud 3, que son pares porque todo ciclo de longitud n se puede escribir como producto de n-1 transposiciones:

$\beta_1 = (2\,3\,4)$ $\quad\quad$ $\beta_2 = (1\,3\,4)$

$\gamma_1 = (2\,4\,3)$ $\quad\quad$ $\gamma_2 = (1\,4\,3)$

$\beta_3 = (1\,2\,4)$ $\quad\quad$ $\beta_4 = (1\,2\,3)$

$\gamma_4 = (1\,4\,2)$ $\quad\quad$ $\gamma_4 = (1\,3\,2)$

b) Todos los α_i son elementos de orden 2. Por tanto hay 3 subgrupos cíclicos de orden 2:

$H_1 = \langle \alpha_1 \rangle = \{id, \alpha_1\}$

$H_2 = \langle \alpha_2 \rangle = \{id, \alpha_2\}$

$H_3 = \langle \alpha_3 \rangle = \{id, \alpha_3\}$

Todos los β_i, γ_i tienen orden 3.

Además $\beta_i^2 = \gamma_i$. Por tanto hay 4 subgrupos cíclicos de orden 3:

$K_1 = \langle \beta_1 \rangle = \langle \gamma_1 \rangle = \{id, \beta_1, \gamma_1\}$

$K_2 = \langle \beta_2 \rangle = \langle \gamma_2 \rangle = \{id, \beta_2, \gamma_2\}$

$K_3 = \langle \beta_3 \rangle = \langle \gamma_3 \rangle = \{id, \beta_3, \gamma_3\}$

$K_4 = \langle \beta_4 \rangle = \langle \gamma_4 \rangle = \{id, \beta_4, \gamma_4\}$.

Por último $\{id\} = \langle id \rangle$ es un subgrupo cíclico de orden 1.

No hay más subgrupos cíclicos ya que hemos considerado los generados por todos los elementos.

(c) $L = \{id, \alpha_1, \alpha_2, \alpha_3\}$ es subgrupo de A_4, ya que se puede comprobar que $\alpha_i^2 = id \ \forall i = 1,2,3.$ y que $\alpha_i \circ \alpha_j = \alpha_k$ cuando (i,j,k) son índices distintos.

Como L tiene 4 elementos, y los 3 que no son la identidad tienen orden 2, L no es cíclico.

(d) Sea $j \in \{1,2,3,4\}$

Las 3 permutaciones que dejan j fijo son id, β_j, γ_j

Luego $Stab(j) = \{id, \beta_j, \gamma_j\}$

Por el teorema de la órbita-estabilizador

$$|orb(j)| = \frac{|G|}{|stab(j)|} = \frac{12}{3} = 4.$$

Luego $orb(j) = B = \{1,2,3,4\}$