ENTREGA 3. EA. GRUPO M3 (19-20).
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

Fecha límite: 22-XI-2019 antes de las 20:00 horas.

Entregar en la hora de problemas en mano o enviar por correo: andonide@ucm.es.

Problema 1. Se definen las dos nociones siguientes:

Definición 1. Sea G un conjunto no vacío con una operación binaria interna dada por

$$\begin{array}{rccc} \cdot: & G\times G & \longrightarrow & G \\ & (a,b) & \mapsto & a\cdot b \end{array}.$$

Decimos que un par $(G,\cdot)$ satisfaciendo que la **operación** $\cdot$ es **asociativa**; a saber, que

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c,\quad \forall\ a,b,c\in G,$$

es

- un *grupo por la izquierda* si además satisface los axiomas siguientes:
  (i) Existe un elemento $1\in G$ tal que $g\cdot 1=g$ para todo $g\in G$.
  (ii) Existe un elemento $g^{-1}\in G$ tal que $g\cdot g^{-1}=1$ para todo $g\in G$.
- un *grupo por la derecha* si además satisface los axiomas siguientes:
  (i) Existe un elemento $1\in G$ tal que $1\cdot g=g$ para todo $g\in G$.
  (ii) Existe un elemento $g^{-1}\in G$ tal que $g^{-1}\cdot g=1$ para todo $g\in G$.

(1) Probar que $(G,\cdot)$ es un grupo por la izquierda si, y sólo si, lo es por la derecha. Deducir que los elementos neutro e inverso para cada $g\in G$ son únicos. Decimos, en cualquiera de los dos casos, que $G\equiv(G,\cdot)$ es un grupo.

Solución: Veámoslo por doble implicación[1]:

- $\boxed{\Rightarrow)}$ Sea $g\in G$ arbitrario. Existen $h_g=g^{-1}, k_g=\left(g^{-1}\right)^{-1}, 1\in G$ tales que
$$g\cdot h_g=1=h_g\cdot k_g.$$
Luego, por la asociatividad y debido a la existencia del neutro, es
$$h_g\cdot g=h_g\cdot(g\cdot h_g)\cdot k_g=(h_g\cdot 1)\cdot k_g=h_g\cdot k_g=1\Longrightarrow \boxed{g^{-1}\cdot g=1\left(=g\cdot g^{-1}\right)}.$$
Así, en virtud de lo que se ha probado, es
$$g=g\cdot 1=(g\cdot h_g)\cdot g=1\cdot g\Longrightarrow \boxed{g\cdot 1=1=1\cdot g}.$$
- $\boxed{\Leftarrow)}$ Sea $g\in G$ arbitrario. Existen $h_g=g^{-1}, k_g=\left(g^{-1}\right)^{-1}, 1\in G$ tales que
$$h_g\cdot g=1=k_g\cdot h_g.$$
Luego, por la asociatividad y debido a la existencia del neutro, es
$$g\cdot h_g=k_g\cdot(h_g\cdot g)\cdot h_g=k_g\cdot(1\cdot h_g)=k_g\cdot h_g=1\Longrightarrow \boxed{g\cdot g^{-1}=1\left(=g^{-1}\cdot g\right)}.$$
Así, en virtud de lo que se ha probado, es
$$g=1\cdot g=g\cdot(h_g\cdot g)=g\cdot 1\Longrightarrow \boxed{g\cdot 1=1=1\cdot g}.$$

[1]De hecho, se puede probar que podemos cruzar estas dos nociones y exigir la existencia del neutro a derecha/izquierda junto, ahora, con la correspondiente existencia del inverso a izquierda/derecha.

Además, una vez se tiene esto, la **unicidad de los elementos neutro e inverso** para cada $g \in G$ fijo es **inmediata**. En efecto, si $h_g, h'_g \in G$ son inversos de $g \in G$ arbitrarios, entonces $g \cdot h_g = 1 = g \cdot h'_g$ por definición; y, multiplicando por uno de estos inversos a izquierda, se sigue inmediatamente $h_g = h'_g$. Análogamente, si $h, h' \in G$ son neutros del grupo, entonces $g \cdot h = g = g \cdot h'$ para todo $g \in G$ arbitrario; y, multiplicando por el inverso a izquierda, se sigue que $h = h'$ sin mucho esfuerzo.

(2) Demostrar que el conjunto formado por las 8 matrices complejas

$$\pm \mathrm{Id} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \pm A = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

$$\pm B = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad \pm C = \pm i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

forman un grupo respecto del producto habitual[2]. ¿Es este **cíclico**? ¿Y **abeliano**? Comprobar que este da una **representación del grupo cuaternio**[3] **de orden** 8.

Solución: Para la primera parte, basta recordar que en el **Ejercicio** 1 dado en la **Hoja de Ejercicios** 1 se probó que $\mathbb{I}^* = \{\pm \mathrm{Id}, \pm A, \pm B, \pm C\}$ (las unidades del anillo de los cuaternios enteros es nuestro conjunto). Así, como **las unidades de un anillo unitario tienen siempre estructura de grupo** para el producto[4], este resultado es inmediato. También vimos en ese ejercicio que

$$A \cdot B = -C \neq C = B \cdot A,$$

luego este **grupo no** es **abeliano**; y, en consecuencia, **no puede ser** tampoco **cíclcio**. Finalmente, no resulta complicado comprobar que se tienen las identidades[5]

$$A^4 = \mathrm{Id}, \quad A^2 = -\mathrm{Id} = B^2, \quad A^B = (-B) \cdot A \cdot B = -A.$$

Por tanto, tenemos que estamos ante el grupo cuaternio de orden 8 por definición.

(3) Denotamos por $\mathrm{GL}(2, \mathbb{R})$ al grupo de matrices reales que tienen dimensión 2×2 con el producto habitual. Escribir la tabla del subgrupo de $\mathrm{GL}(2, \mathbb{R})$ generado por las matrices

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

¿Qué grupo conocido presentan estos dos elementos? Comprobar las relaciones. ¿Qué tienen en común este grupo y el ahora estudiado en el apartado anterior?

---

[2]A las matrices

$$\sigma_x := -iA = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := -iB = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{y} \quad \sigma_z := -iC = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

se las conoce por *matrices de Pauli* (importantes en física; entre otros, en teoría conforme de campos). Este grupo coincide con las unidades del anillo de cuaterniones enteros estudiado en el **Ejercicio** 1 **de la Hoja** 1.

[3]A saber, que existen a y b generadores del grupo, tales que $a^4 = \mathrm{Id}, a^2 = b^2, a^b \equiv b^{-1}ab = a^{-1}$.

[4]Dado que yo parece no lo tenía del todo claro, lo pruebo: Sea A un anillo unitario arbitrario, y consideremos el conjunto de sus unidades A^*. La asociatividad es obvia por tener esta en A por definición; y, ahora, sea $u \in A^*$ una unidad arbitraria. Como estamos en un anillo unitario, sabemos que $1 \cdot u = u$. Además, por definición de unidad, existe $v \in A^*$ tal que $u \cdot v = 1$. A saber, existe un inverso $u^{-1} := v \in A^*$.

[5]De hecho, se puede comprobar que, cada dos matrices que se tomen del conjunto $\{A, B, C\}$ cualesquiera, estas son generadoras del grupo cuaternio. En particluar, se comprueba que $\mathrm{ord}\,(A) = \mathrm{ord}\,(B) = \mathrm{ord}\,(C) = 4$.

Solución: Se puede comprobar que el subgrupo generado por estos dos elementos a y b tiene orden 8 (a saber, está formado por un total de 8 elementos), pues

$$a^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -\mathrm{Id} \Longrightarrow a^4 = \mathrm{Id} \quad \text{y} \quad b^2 = \mathrm{Id};$$

donde, además, es evidente que

$$b \cdot a = a^{-1} \cdot b = a^3 \cdot b \quad \text{y} \quad b \cdot a^2 = a^2 \cdot b.$$

Es decir, se tiene que $\langle a, b \rangle = \left\{ \mathrm{Id}, a, b, a^2, a^3, ab, a^2b, a^3b \right\}$. Calculamos la tabla para este. Esta es, donde **se multiplican los elementos de la primera fila por los de la columna puesta bajo la operación**[6], la siguiente:

$\cdot$	Id	a	b	a^2	a^3	ab	a^2b	a^3b
Id	Id	a	b	a^2	a^3	ab	a^2b	a^3b
a	a	a^2	a^3b	a^3	Id	b	ab	a^2b
b	b	ab	Id	a^2b	a^3b	a	a^2	a^3
a^2	a^2	a^3	a^2b	Id	a	a^3b	b	ab
a^3	a^3	Id	ab	a	a^2	a^2b	a^3b	b
ab	ab	a^2b	a^3	a^3b	b	Id	a	a^2
a^2b	a^2b	a^3b	a^2	b	ab	a^3	Id	a
a^3b	a^3b	b	a	ab	a^2b	a^2	a^3	Id

.

Este no es otro que el grupo diedral de orden 8 (a saber, el cuarto grupo diédrico), como ya se ha comprobado antes cuando hemos obtenido, precisamente, las relaciones que definen este. En principio, este grupo y el que se ha visto en el apartado anterior tienen en común que **ambos son grupos de orden** 8 **no abelianos**. Estos son, además, no isomorfos (como se va a ver); y, de hecho, **son los dos únicos grupos de orden** 8 **no abelianos (salvo isomorfismo)**. Demostrar esto termina de resolver el **problema de clasificación para los grupos de orden** 8.

CONCLUSIONES: En general, los problemas más graves están en el primer y último apartado. En el primero, bastantes son los que comenten constantemente un mismo error, y es que utilizan algunos axiomas que, en principio, no se tienen para probar el resultado (o que resuelven un problema totalmente diferente). Por favor, estad atentos a lo que se os pide demostrar, y utilizad aquello que se os da para llegar al resultado. En el último, mucha gente no hace correctamente la tabla del grupo, que no es más que la tabla de multiplicación para todos los elementos con el resto, sin dejarse ni uno.

[6]Es importante darse cuenta de que en cada fila y columna tenemos a todos los elementos de G como cabe esperar por el **Ejercicio** 1 visto en la **Hoja de Ejercicios** 4.

Problema 2. Sean $f\colon G_1 \longrightarrow G_2$ un homomorfismo de grupos.

(1) Dado $g \in G_1$ **elemento de orden finito**, probar que $\operatorname{ord}(f(g)) \,|\operatorname{ord}(g)$ (en particular $f(g) \in G_2$ también tiene orden finito). Si f es inyectivo, entonces $\operatorname{ord}(f(g)) = \operatorname{ord}(g)$.

Solución: Para la primera parte, basta ver que $f(g)^{\operatorname{ord}(g)} = 1$. En efecto, como f es homomorfismo de grupos, es

$$f(g)^{\operatorname{ord}(g)} = f\left(g^{\operatorname{ord}(g)}\right) = f(1) = 1;$$

luego $f(g)$ tiene orden finito, y este verifica que $\operatorname{ord}(f(g)) \,|\operatorname{ord}(g)$. Veamos ahora que $\operatorname{ord}(g)|\operatorname{ord}(f(g))$ cuando f es inyectiva; a saber, si se cumple que $\ker(f) = \{1\}$. En esta situación, al ser f homomorfismo de grupos, se tiene que

$$1 = f(g)^{\operatorname{ord}(f(g))} = f\left(g^{\operatorname{ord}(f(g))}\right) \iff g^{\operatorname{ord}(f(g))} \in \ker(f) \iff g^{\operatorname{ord}(f(g))} = 1.$$

En definitiva, de esto se sigue finalmente la igualdad $\operatorname{ord}(f(g)) = \operatorname{ord}(g)$ deseada.

(2) Deducir de lo anterior que, si f es un isomorfismo de grupos, entonces G_1 y G_2 tienen el mismo número de elementos con el mismo orden.

Solución: Como f es un isomorfismo de grupos, por ser en particular **sobreyectiva**, tenemos que $G_2 = \{f(g) \mid g \in G_1\}$. Más aún, como estamos ante un **monomorfismo de grupos**, hemos probado que $\operatorname{ord}(g) = \operatorname{ord}(f(g))$ para todo $g \in G_1$ con orden finito. De hecho, en caso de que g tenga orden infinito, la igualdad que se ha probado en el apartado anterior sigue siendo cierta, y tenemos que $f(g)$ tiene orden infinito. En resumen, por como viene dado G_2 en estas condiciones, se tiene que G_1 y G_2 tienen el mismo número de elementos con el mismo orden.

(3) Aplicar este último apartado a los dos grupos estudiados en el **Problema** 1 anterior para concluir que estos NO pueden ser grupos isomorfos.

Solución: Basta estudiar **los órdenes** de $\mathcal{D}_8$ y el grupo cuaternio de orden 8:

- En $\mathcal{D}_8 = \langle a, b \mid a^4 = 1 = b^2, a^b = a^{-1}\rangle$ tenemos que $\operatorname{ord}(a) = 4$ y $\operatorname{ord}(b) = 2$ según hemos visto en el problema anterior. Además, por la fórmula del orden de una potencia dada en el **Ejercicio** 2 que se encuentra en la **Hoja de Ejercicios** 4 ya vista, se tiene que

$$\operatorname{ord}\left(a^2\right) = 2 \quad \text{y} \quad \operatorname{ord}\left(a^3\right) = 4.$$

  Por otro lado, se comprueba fácilmente que

$$\operatorname{ord}(ab) = \operatorname{ord}\left(a^2b\right) = \operatorname{ord}\left(a^3b\right) = 2.$$

  A saber, en $\mathcal{D}_8$ hay (además del neutro, que viene caracterizado por tener orden 1) 5 elementos de orden 2 y, por otro lado, se tienen 2 elementos de orden 4.
- En el grupo cuaternio de orden 8 hemos visto que

$$\operatorname{ord}(A) = \operatorname{ord}(B) = \operatorname{ord}(C) = 4.$$

  Luego, todos los elementos, salvo $\pm\mathrm{Id}$ (que tienen orden 1 para el caso positivo, mientras que orden 2 para el caso negativo como bien sabemos), tienen orden 4.

En definitiva, **estos dos grupos no pueden ser isomorfos** porque el número de elementos con órdenes 2 y 4 en el grupo cuaternio de orden 8 y en $\mathcal{D}_4$ no coinciden.

CONCLUSIONES: En general, este ejercicio está bastante bien salvo ciertas explicaciones que no se dan correctamente (o que, y esto es tal vez más una opinión personal, se emplean unas resoluciones bastante retorcidas cuando estas son inmediatas prácticamente).

Problema 3. Sea G un grupo. Para cada $x, y \in G$ arbitrarios, definimos el *conmutador* de x e y como $[x,y] := xyx^{-1}y^{-1} \in G$. En estas condiciones, sea $\Gamma_G \equiv \{[x,y] : x, y \in G\} \subseteq G$. Se define el *subgrupo derivado* de G como $G' \equiv [G,G] := \langle \Gamma_G \rangle \leq G$.

(1) Probar que $[G,G]$ es el menor subgrupo normal de G que contiene a Γ_G.

Solución: Como G' es el subgrupo generado por Γ_G según como lo hemos definido, se tiene que es el **menor subgrupo de G que contiene a Γ_G** por definición. Sin embargo, más aún, **este es normal**. Para ello, dado $g \in G$ un elemento cualquiera, basta ver que $gG'g^{-1} = G'$. En efecto, suponiendo que tenemos $h \in G'$ arbitrario, que es por definición un producto finito de conmutadores del tipo $[x_i, y_i]$ donde $x_i, y_i \in G$ con $i \in \{1, \dots, l\}$ para l finito, se tiene que

$$gh = g\,[x_1,y_1]\cdots[x_l,y_l] :=$$
$$= \left(gx_1g^{-1}gy_1g^{-1}gx_1^{-1}g^{-1}gy_1^{-1}g^{-1}\right) g \cdots g^{-1} \left(gx_lg^{-1}gy_lg^{-1}gx_l^{-1}g^{-1}gy_l^{-1}g^{-1}\right) g =$$
$$= \left[gx_1g^{-1}, gy_1g^{-1}\right] \cdots \left[gx_lg^{-1}, gy_lg^{-1}\right] g \in G'g \iff ghg^{-1} \in G'.$$

Sólo falta ver que este es el **menor subgrupo normal que contiene a Γ_G**. Pero esto se tiene gratis, pues este es el menor subgrupo que contiene a Γ_G por definición; y, además, todo subgrupo normal es, en particular, como bien se sabe, un subgrupo.

(2) Demostrar que G es abeliano si, y sólo si, se tiene que $\Gamma_G = \{1_G\}$. Concluir que el grupo cociente $G/[G,G]$ es abeliano siempre.

Solución: Sean $x, y \in G$ arbitrarios. Es obvio que $xy = yx$ si, y sólo si, se tiene que $[x,y] = xyx^{-1}y^{-1} = 1$ (de hecho, esta es la razón de existencia del conmutador). Luego G es abeliano si, y sólo si, es $\Gamma_G = \{1_G\}$. Como consecuencia, dado que

$$\left[xG', yG'\right] := [x,y]\,G' = 1_GG' = 1_{G/G'}, \quad \forall\, x, y \in G$$

trivialmente, se tiene que el grupo cociente G/G' es abeliano siempre.

(3) ¿Es todo subgrupo de G que contiene a $[G,G]$ normal? Probar el recíproco (a saber, todo subgrupo H normal de G contiene al derivado) si el cociente G/H es abeliano.

Solución: Sea H un subgrupo de G que contiene a G'. Dados $h \in H$ y $g \in G$ dos elementos cualesquiera, debemos ver si $x \equiv ghg^{-1} \in H$. Pero esto es cierto, pues

$$x = ghg^{-1} = \left(ghg^{-1}h^{-1}\right) h = [g,h]\,h \in \Gamma_G H \subseteq G'H \subseteq HH = H.$$

Ahora bien, si H es un subgrupo de G tal que G/H es abeliano, se tiene que, para cualesquiera elementos $x, y \in G$ dados, se cumple que

$$(Hx)\,(Hy) := H\,(xy) = H\,(yx) =: (Hy)\,(Hx) \iff H = H\left(xyx^{-1}y^{-1}\right) = H\,[x,y]\,.$$

Luego $[x,y] \in H$. A saber, se tiene que $\Gamma \subseteq H$ y, por ser G' el menor subgrupo normal que contiene a Γ_G como ya hemos probado, concluimos que $G' \subseteq H$.

CONCLUSIONES: Sin incidencias reseñables que comentar en general, salvo lo típico de dar más vueltas de las necesarias para llegar a la solución en bastantes casos.

Problema 4. El objetivo de este ejercicio es demostrar que las unidades de $\mathbb{Z}_p$, con p un número primo, forman un grupo cíclico de orden $p-1$ (que no es un número primo).

(1) Dado G un **grupo abeliano** arbitrario, sean g y h dos elementos de órdenes n y m respectivamente. Demostrar que existe un elemento en G de orden $\mathrm{mcm}(n,m)$.

Solución: Podemos suponer sin pérdidad de generalidad que $\mathrm{mcd}(n,m)=1$. En efecto, vamos a probar esto. Para ello, suponiendo que

$$n=\prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{y} \quad m=\prod_{i=1}^{r} p_i^{\beta_i}$$

son las factorizaciones en $\mathbb{Z}$ como producto de primos para n y m respectivamente (donde $\alpha_i,\beta_i\in\mathbb{N}$ para cada $i\in\{1,\dots,n\}$), vamos a considerar

$$\widetilde{n}=\prod_{\substack{i=1\\ \alpha_i\geq\beta_i}}^{r} p_i^{\alpha_i} \quad \text{y} \quad \widetilde{m}=\prod_{\substack{i=1\\ \alpha_i<\beta_i}}^{r} p_i^{\beta_i}.$$

Tenemos que $\widetilde{n}$ **y** $\widetilde{m}$ **son coprimos** con

$$\mathrm{mcm}\left(\widetilde{n},\widetilde{m}\right)=\mathrm{mcm}(n,m)$$

por construcción. Además, es obvio que $\widetilde{n}|n$ y $\widetilde{m}|m$. En estas circunstancias, dados

$$g':=g^{\frac{n}{\widetilde{n}}} \quad \text{y} \quad h':=h^{\frac{m}{\widetilde{m}}},$$

se tiene que estos tienen órdenes $\widetilde{n}$ y $\widetilde{m}$ respectivamente. Esto es inmediato, pues

- por un lado, tenemos que

$$1=\left(g'\right)^{\mathrm{ord}(g')}=g^{\frac{n\mathrm{ord}(g')}{\widetilde{n}}},$$

luego $n|n\mathrm{ord}\left(g'\right)/\widetilde{n}$. A saber, se tiene que $\widetilde{n}|\mathrm{ord}\left(g'\right)$. Más aún, recíprocamente, se tiene que $\mathrm{ord}\left(g'\right)|n'$ ya que

$$\left(g^{\frac{n}{\widetilde{n}}}\right)^{\widetilde{n}}=g^{n}=1$$

por ser $\widetilde{n}$ el orden de g.

- mientras, análogamente, tenemos que

$$1=\left(h'\right)^{\mathrm{ord}(h')}=h^{\frac{m\mathrm{ord}\left(h'\right)}{\widetilde{m}}},$$

luego $m|m\mathrm{ord}\left(h'\right)/\widetilde{m}$. A saber, se tiene que $\widetilde{m}|\mathrm{ord}\left(h'\right)$. Más aún, recíprocamente, se tiene que $\mathrm{ord}\left(h'\right)|\widetilde{m}$ ya que

$$\left(h^{\frac{m}{\widetilde{m}}}\right)^{\widetilde{m}}=g^{m}=1$$

por ser m el orden de h.

En resumen, podemos suponer que m **y** n **son coprimos en este apartado**. De esta manera, basta considerar el producto $gh\in G$. En efecto, veamos que se da la igualdad $\mathrm{ord}(gh)=\mathrm{mcm}(n,m)$. Para ello, es suficiente con ver que estos dos números enteros se dividen mútuamente. En primer lugar, obsérvese que por la hipótesis de ser abeliano tenemos la primera identidad

$$(gh)^{\mathrm{mcm}(n,m)}=\left(g^{\mathrm{mcm}(n,m)}\right)\left(h^{\mathrm{mcm}(n,m)}\right)=1,$$

donde esta última igualdad se debe a que $n,m|\mathrm{mcm}(n,m)$ por definición de mínimo común múltiplo. Así, hemos probado $\mathrm{ord}(gh)|\mathrm{mcm}(n,m)$. Recíprocamente, veamos que $\mathrm{mcm}(n,m)|\mathrm{ord}(gh)$ por unicidad (salvo asociados) del mínimo común múltiplo.

A saber, basta ver que $n, m | \text{ord}(gh)$ y, en consecuencia, habremos terminado por definición. Pero esto es inmediato gracias a la nueva hipótesis que hemos impuesto, ya que así tenemos que $\langle g \rangle \cap \langle h \rangle = \{1\}$ (debido al **Teorema de Lagrange**, pues la intersección de estos dos subgrupos ha de tener orden $\text{mcd}(n, m) = 1$). De esta manera, por estar en un grupo abeliano, se tiene que

$$1 = (gh)^{\text{ord}(gh)} = g^{\text{ord}(gh)} h^{\text{ord}(gh)} \iff g^{\text{ord}(gh)} = \left(h^{-1}\right)^{\text{ord}(gh)}.$$

A saber, necesariamente es $g^{\text{ord}(gh)}, \left(h^{-1}\right)^{\text{ord}(gh)} \in \langle g \rangle \cap \langle h \rangle = \{1\}$ y, por consiguiente, se tiene que $\text{mcm}(n, m) | \text{ord}(gh)$ tal y como andábamos buscando.

(2) Si $\mathbb{K}$ es cuerpo, probar que todo $f \in \mathbb{K}[x]$ de grado n tiene **a lo más** n raíces distintas.

Solución: Sea $f(x) \in \mathbb{K}[x]$ un polinomio de grado n arbitrario. Sea m el **número total** de raíces en $\mathbb{K}$ para f. A saber, sean $\lambda_1, \ldots, \lambda_m \in \mathbb{K}$ tales que $f(\lambda_i) = 0$ para todo $i \in \{1, \ldots, n\}$ (donde puede haber raíces repetidas; pero hay exactamente $r \in \mathbb{N}$ distintas, con $r \leq m$). Como $\mathbb{K}$ es un cuerpo, sabemos que $\mathbb{K}[x]$ es DE (**Ejercicio** 21 visto en la **Hoja de Ejercicios** 2) y, por tanto, el polinomio se factoriza como sigue

$$f(x) = q(x) \cdot \prod_{i=1}^{m} (x - \lambda_i),$$

donde $q(x)$ es un polinomio irreducible (en particular, no nulo) en $\mathbb{K}[x]$ verificando que $0 \leq \deg(q) < \deg(f) = n$. Se tiene entonces que

$$0 \leq \deg(q(x)) < \deg(f(x)) = n = \deg(q(x)) + \deg\left(\prod_{i=1}^{m} (x - \lambda_i)\right) = \deg(q(x)) + m;$$

a saber, es $n - m = \deg(q(x)) \geq 0$ claramente, lo cual equivale a $n \geq m \geq r$. En resumen, se ha probado que n es cota superior del número de raíces distintas de f.

(3) Concluir de todo lo anterior que existe $g \in \mathbb{Z}_p^*$ de orden $p - 1$.

Solución: Esto es equivalente a probar que $\mathbb{Z}_p^*$ es un grupo cíclico. Sea

$$l = \text{mcm}\left(\text{ord}\left([1]_p\right), \text{ord}\left([2]_p\right), \ldots, \text{ord}\left([p-1]_p\right)\right).$$

Tenemos entonces que $[k]_p^l = [1]_p$ para todo $[k]_p \in \mathbb{Z}_p^*$ dado que $\text{ord}\left([k]_p\right) | l$ para todo $k \in \mathbb{Z}$ (por definición de mínimo común múltiplo). Esto significa que el polinomio

$$x^l - [1]_p \in \mathbb{Z}_p^*[x],$$

que es de grado l y viene dado sobre el cuerpo $\mathbb{Z}_p^*$ por construcción, tiene $p-1$ raíces. Por el **apartado** (2) que acabamos de resolver, necesariamente es $l \geq p-1$. Además, como por el **apartado** (1) también probado, cada dos elementos $a, b \in \mathbb{Z}_p^*$ arbitrarios, existe uno que tiene orden $\text{mcm}\left(\text{ord}(a), \text{ord}(b)\right)$. Sea $g \in \mathbb{Z}_p^*$ un elemento concreto, aquel que tiene orden l antes definido, el cual se obtiene aplicando inductivamente este razonamiento[7]. Por tanto, se tiene que $l \leq p - 1$. Es decir, hemos probado la existencia de un elemento $g \in \mathbb{Z}_p^*$ tal que tiene orden $l = p - 1$.

[7]Aquí se está utilizando implícitamente que

$$\text{mcm}(n_1, n_2, \ldots, n_m) = \text{mcm}(n_1, \text{mcm}(n_2, \ldots, n_m)),$$

para todo $n_1, n_2, \ldots, n_m \in \mathbb{Z}$ con m entero positivo.

(4) [8] ¿Se te ocurre o conoces alguna otra manera de demostrar este resultado?[9]

Solución: Según lo que he leído, parece que a nadie se le ha ocurrido ninguna otra forma esencialmente diferente a la propuesta de obtener este resultado. Sí que hay un pequeño grupo que ha dado una solución alternativa a la indicada para este resultado, pero siempre empleando la misma estrategia que se ha dictado (a saber; se trata de la misma prueba que se pide, pero generalizada a cualquier subgrupo para las unidades de un cuerpo arbitrario, o empleando otras propiedades intermedias que no se enuncian en la entrega). Mi idea con este apartado era que se dieran o propusiesen estrategias distintas, como por ejemplo la que sí comenta alguien que se sigue de utilizar el **Teorema de Clasificación para grupos abelianos finitos**, aunque luego no termine de rematar el resultado. Otra forma de proceder es utilizando la llamada **fórmula de inversión** que aparece en los apuntes (**Lema 1.5.20.**), aplicada a la función φ de Euler. De esta manera, de hecho, también se puede probar el resultado general que se ha mencionado. Hay otro par de personas que dan un argumento parecido al que se sigue de esta fórmula, pero que no terminan tampoco de rematarlo correctamente y queda a medias.

CONCLUSIONES: Este parece ser el problema de la entrega en donde, valga la redundancia, más problemas parece que ha habido. En el primer apartado, son bastantes los que se hacen un lío a la hora de realizar la prueba dividiéndola en varios subapartados y razonando por **reducción al absurdo** (lo cual termina en una demostración muy poco elegante y liosa de entender para quien está leyendo). Basta pensar una estrategia un poco ordenada antes de pasarse a escribir nada, como sí que hacen otros muchos. El segundo apartado en general está bastante bien, salvo que algunos parecen no tener claro donde están utilizando el que $\mathbb{K}$ sea un cuerpo (aprovecho para lanzar una pregunta al aire: en caso de tener simplemente un anillo A arbitrario, ¿se sigue cumpliendo el resultado? En caso afirmativo, ¿cómo lo razonaríais?). El último apartado también está bastante bien en general, salvo líos típicos o grupos que razonan sin utilizar lo que han ido demostrando (para algo se habrá pedido hacer).

COMENTARIOS IMPORTANTES: Empiezo con los **asuntos no matemáticos**: por favor, las fechas límites que se dan están para respetarlas escrupulosamente; así como el método de entrega (si no recibo **un único pdf con la resolución de cada uno**, no voy a molestarme en realizar la corrección). Por otro lado, la idea de estos ejercicios es que os enfrentéis a los problemas aplicando estos conocimientos que habéis ido adquiriendo para que veamos donde tenéis problemas e insistir en ello. Si dejáis las cosas en blanco, además de penalizaros (cosa que no voy a hacer por preguntar o resolver mal los ejercicios), no cometéis fallos que podéis hacer en el examen (y ahí ya si que no hay salvación posible). **En cuanto a lo matemático**, un problema bastante general está en la redacción de las soluciones (es algo que nos pasa a todos). No sólo tenéis que intentar hacer bien los ejercicios, sino que debéis lograr que quien os lea pueda seguirlos sin perderse para que pueda entenderos. Por tanto, después de redactar las soluciones, conviene que las leáis (o incluso que las intercambiéis entre vosotros para ver si otros las entienden) y os aseguréis de que alguien mínimamente familiarizado con la materia pueda entenderos y ver que entendéis lo que estáis haciendo (sin dejar argumentos a medias y explicando, a ser posible, todos los pasos no elementales). Expresiones del tipo: esto es trivial, esto se sigue inmediatamente, etc conviene evitarlas.

[8] Este apartado del problema es optativo para quienes quieran trabajarlo.

[9] Por ejemplo, más en general, se puede probar que cualquier subgrupo finito del grupo multiplicativo de un cuerpo es cíclico, y así obtener el resultado deseado en particular.