ENTREGA 4. EEAA. GRUPO M3 (19-20).
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

Fecha límite: 11-XII-2019 (antes de las 13:30 horas[1]).

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

Problema 1. Se considera el 4-*grupo de Klein* definido por

$$V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq \mathcal{S}_4.$$

(1) Considérese la acción natural de V sobre el conjunto $X = \{1,2,3,4\}$[2]. Escribir las órbitas de dicha acción, y encontrar los estabilizadores de cada punto dado en X.

Solución: Recordemos que por definición las *órbitas* y los *estabilizadores* en V para cada $\alpha \in X$ vienen dados, respectivamente, por

$$\mathrm{Orb}_V(\alpha) := \{\alpha \cdot g \mid g \in V\} \subseteq X \quad \text{y} \quad \mathrm{Stab}_V(\alpha) := \{g \in V \mid \alpha \cdot g = g\} \subseteq V.$$

Por como viene definido el 4-grupo de Klein, es obvio que

$$\mathrm{Orb}_V(1) = \mathrm{Orb}_V(2) = \mathrm{Orb}_V(3) = \mathrm{Orb}_V(4) = X.$$

Así, se tiene que $|\mathrm{Orb}_V(\alpha)| = 4$ para todo $\alpha \in X$. De esta manera, por la fórmula que relaciona los cardinales de órbitas y estabilizadores[3], se tiene que $|\mathrm{Stab}_V(\alpha)| = 1$ en todos los casos; y, al ser este un subgrupo de G como bien sabemos, necesariamente

$$\mathrm{Stab}_V(1) = \mathrm{Stab}_V(2) = \mathrm{Stab}_V(3) = \mathrm{Stab}_V(4) = \{1\}.$$

Cabe observar que todos los puntos de X pertenecen a la misma clase de equivalencia por la acción natural de V dado que todas estas son iguales.

(2) Demostrar que este es subgrupo normal de $\mathcal{A}_4$ y $\mathcal{S}_4$ (en particular, hemos probado así que estos dos no pueden ser grupos simples). Hallar los subgrupos normales propios de V y demostrar que, de hecho, estos no pueden ser subgrupos normales en $\mathcal{A}_4$ y $\mathcal{S}_4$.

Solución: Es obvio que $V \leq \mathcal{A}_4$ (pues $V \cap \mathcal{A}_4 = V$ por tener los elementos de V signatura par trivialmente). Dicho esto, basta probar que $V \lhd \mathcal{S}_4$ y habremos terminado. En efecto, dado $\sigma \in \mathcal{A}_4 \subseteq \mathcal{S}_4$ arbitrario, en tal caso $\sigma^{-1}V\sigma \subseteq V$ por definición de normalidad. Sean $\sigma \in \mathcal{S}_4$ y $\tau \equiv (x,y)(z,w) \in V$ (esta última no trivial, ya que de serlo el resultado es inmediato) cualesquiera, donde descomponemos σ en producto de ciclos disjuntos por $\sigma = \sigma_1 \cdots \sigma_n$ donde $n \leq 4$. Si $n = 4$ el resultado es inmediato (sólo tenemos la permutación trivial). Vamos por tanto a estudiar por separado los tres casos restantes[4]:

---

[1] Este límite es **para aquellos que quieran recibir las correcciones de esta entrega antes de Navidades**, a lo más tardar, en la última clase de problemas que será la próxima semana. Para el resto, la entrega puede ampliarse en una semana (en principio, **hasta el miércoles 18-XII-2019 a la misma hora**).

[2] A saber, la acción definida por $\begin{array}{rccc} \cdot : & V \times X & \longrightarrow & X \\ & (\sigma, i) & \mapsto & (i)\sigma \end{array}$.

[3] Pues recordemos que $|V : \mathrm{Stab}_V(\alpha)| = |\mathrm{Orb}_V(\alpha)|$ para cada $\alpha \in X$ dado.

[4] Otra manera de hacer esta prueba, más rápida, es usar el **Ejercicio** 4 visto en la **Hoja de Ejercicios** 5 gracias al cual sabemos que $\mathcal{S}_4$ está generado por ciertas permutaciones (se dan hasta tres sistemas de generadores), de tal forma que basta comprobar la condición de normalidad para V sobre estos generadores;

- Si $n = 3$ tenemos que σ es producto de un 2-ciclo con otros dos 1-ciclos. Es decir, la única opción es que $\sigma = (a)(b)(c,d) \in \mathcal{S}_4$. En particular σ coincide con su inversa, y hay un total de $\binom{4}{2} = 6$ elementos bajo este caso. Entonces,
  - si (c,d) es parte de la descomposición de τ en ciclos disjuntos (por ejemplo, sin pérdida de generalidad es $(a,b,c,d) = (x,y,z,w)$), entonces
  $$\sigma\tau\sigma^{-1} = (c,d) \circ (a,b)(c,d) \circ (c,d) = (a,b)(c,d) = \tau \in V.$$
  - si (c,d) no es parte de la descomposición de τ en ciclos disjuntos (por ejemplo, sin pérdida de generalidad es $(a,b,c,d) = (x,z,y,w)$), entonces
  $$\sigma\tau\sigma^{-1} = (c,d) \circ (a,c)(b,d) \circ (c,d) = (a,d)(c,b) \in V.$$
- Si $n = 2$ tenemos que σ es, o bien producto de 2-ciclos, o sino se descompone como un 1-ciclo y otro 3-ciclo. Vamos a estudiar cada caso por separado.
  - En el primero de los casos, supongamos que $\sigma = (a,b)(c,d) \in \mathcal{S}_4$. Se tienen un total de 3 elementos que, en particular, son todas las permutaciones no triviales de V. Por consiguiente, el resultado es trivial por ser V subgrupo.
  - En el otro caso, supongamos que $\sigma = (a)(b,c,d) \in \mathcal{S}_4$. En particular, se tiene que $\sigma^{-1} = (a)(b,d,c) \in \mathcal{S}_4$ y hay un total de $\binom{4}{1} \cdot 2 = 8$ elementos bajo este caso. Se tiene entonces, suponiendo sin pérdida de generalidad que $a = x$ por ejemplo, que
    - si $(z,w) = (b,c)$ (y por tanto $y = d$), entonces
    $$\sigma\tau\sigma^{-1} = (b,c,d) \circ (a,d)(b,c) \circ (b,d,c) = (a,c)(b,d) \in V.$$
    - si $(z,w) = (b,d)$ (y por tanto $y = c$), entonces
    $$\sigma\tau\sigma^{-1} = (b,c,d) \circ (a,c)(b,d) \circ (b,d,c) = (a,b)(c,d) \in V.$$
- Si $n = 1$ es σ un 4-ciclo. A saber, se tiene que $\sigma = (a,b,c,d) \in \mathcal{S}_4$. En este caso, hay un total de $3 \cdot 2 = 6$ elementos y $\sigma^{-1} = (a,d,c,b) \in \mathcal{S}_4$. Entonces, suponiendo sin pérdida de generalidad que $a = x$ por ejemplo, se tiene que
  - si $y = b$ podemos suponer sin pérdida de generalidad que $(z,w) = (c,d)$ y
  $$\sigma\tau\sigma^{-1} = (a,b,c,d) \circ (a,b)(c,d) \circ (a,d,c,b) = (a,d)(b,c) \in V.$$
  - si $y = c$ podemos suponer sin pérdida de generalidad que $(z,w) = (b,d)$ y
  $$\sigma\tau\sigma^{-1} = (a,b,c,d) \circ (a,c)(b,d) \circ (a,d,c,b) = (a,c)(b,d) \in V.$$
  - si $y = d$ podemos suponer sin pérdida de generalidad que $(z,w) = (b,c)$ y
  $$\sigma\tau\sigma^{-1} = (a,b,c,d) \circ (a,d)(b,c) \circ (a,d,c,b) = (a,b)(c,d) \in V.$$

Luego, en cualquier caso, se tiene que $\sigma^{-1}\tau\sigma \in V$. Finalmente, como V es abeliano (todo elemento no trivial tiene orden 2 y aplicamos el **Ejercicio** 7 dado en la **Hoja de Ejercicios** 4; o también se vio con el **Ejercicio** 30 de esa misma hoja que todos los grupos de orden 4 son abelianos), sus subgrupos son todos normales. Más aún, como los no triviales han de tener orden 2 necesariamente por el **Teorema de Lagrange**, al tener que los subgrupos de orden 2 se caracterizan por estar generados a través de elementos con dicho orden, se tiene que **hay tres subgrupos normales no triviales** en V que son **los generados por cada elemento de V no trivial**. Ninguno de estos puede ser normal en los grupos alternado y simétrico que nos tocan.

---

o, más sencillo aún, utilizar que V es unión entre clases de conjugación para $\mathcal{A}_4 \lhd \mathcal{S}_4$ (incluida la del neutro), ya que esto es equivalente a que $V \lhd \mathcal{S}_4$ y $V \lhd \mathcal{A}_4$. Más aún, la clase de conjugación formada por los elementos de V no triviales es especial, pues son las permutaciones que se factorizan en dos trasposiciones disjuntas (que son todos los elementos de orden 2 en $\mathcal{S}_4$ que no son trasposiciones), y se puede demostrar que si $\tau \in \mathcal{S}_4$ es una trasposición, entonces $\sigma\tau\sigma^{-1} \in \mathcal{S}_4$ vuelve a serlo para todo $\sigma \in \mathcal{S}_4$.

En efecto, veamos un **contraejemplo para cada caso**. Sea $\sigma = (1,2,3) \in \mathcal{A}_4 \leq \mathcal{S}_4$.

- Para el subgrupo generado por $(1,2)(3,4)$ se tiene que
$$\sigma(1,2)(3,4)\sigma^{-1} = (1,2,3) \circ (1,2)(3,4) \circ (3,2,1) = (1,3)(2,4) \notin \langle (1,2)(3,4) \rangle .$$
- Para el subgrupo generado por $(1,3)(2,4)$ se tiene que
$$\sigma(1,3)(2,4)\sigma^{-1} = (1,2,3) \circ (1,3)(2,4) \circ (3,2,1) = (1,4)(2,3) \notin \langle (1,3)(2,4) \rangle .$$
- Para el subgrupo generado por $(1,4)(2,3)$ se tiene que
$$\sigma(1,4)(2,3)\sigma^{-1} = (1,2,3) \circ (1,4)(2,3) \circ (3,2,1) = (1,2)(3,4) \notin \langle (1,4)(2,3) \rangle .$$

En particular, esto demuestra que **la propiedad de ser normal no es transitiva**.

(3) Concluir a partir de lo anterior que $\mathcal{A}_4$ es resoluble (luego, también lo es $\mathcal{S}_4$).

Solución: Dado que $\mathcal{A}_4 \lhd \mathcal{S}_4$ trivialmente (pues el alternado es un subgrupo de índice 2 en el simétrico), no hay más que cosiderar la cadena de subgrupos normales
$$\{1\} \lhd V \lhd \mathcal{A}_4 \lhd \mathcal{S}_4;$$
donde cada cociente es abeliano, pues
$$\frac{V}{\{1\}} \cong V \cong \mathbb{Z}_2 \times \mathbb{Z}_2; \quad \frac{\mathcal{A}_4}{V} \cong \mathbb{Z}_3; \quad \text{y} \quad \frac{\mathcal{S}_4}{\mathcal{A}_4} \cong \mathbb{Z}_2.$$
En efecto, no olvidemos que todo grupo cíclico es abeliano en particular.

CONCLUSIONES: Salvo erratas en las cuentas o líos a la hora de explicar las cosas (se dan demasiadas vueltas con las que al final no se termina demostrando nada, cuando es mucho más fácil que todo lo que se hace), no ha habido grandes problemas en las resoluciones.

Problema 2. El objetivo ahora pasa por probar que **el menor grupo no abeliano y simple es, salvo isomorfismo, el grupo alternado $\mathcal{A}_5$**. Para probar este resultado, los pasos que se van a seguir son los siguientes[5]:

(1) Dado G un grupo no abeliano arbitrario, demostrar que este no es simple si
(i) $|G| = p^r m$ con p primo tal que $r \geq 1$ y $p > m > 1$.

Solución: Basta aplicar los **Teoremas de Sylow**. En efecto, como $p \neq m$ por hipótesis, obtenemos que $n_p - 1 \in p\mathbb{Z}$ y $n_p | m$. Luego, si $n_p > 1$ (de lo contrario, existe un único p-subgrupo de Sylow normal y habremos terminado), necesariamente es $n_p \geq p+1$ y, como $n_p | m$ según se ha dicho, existe $c \in \mathbb{Z}$ con $c \geq 1$ tal que $m = cn_p \geq n_p \geq p+1 > p$, lo cual es imposible dado que $p > m$ por hipótesis.

(ii) $|G| = 2^p q$ con $q = 2^p - 1$ primo (los llamados *primos de Mersenne*)[6].

[5]Para la redacción de este problema, me he basado en la última parte sobre **aplicaciones a los Teoremas de Sylow** del artículo *The Sylow Theorems and Their Applications* de **Amin Idelhaj**. Puede ojearse por si alguien se pierde en un momento dado, pero **en ningún caso se debe copiar la resolución dada sin entenderla** (de hecho, no se razonan todos los pasos y el ejercicio propuesto no es exactamente igual).

[6]En particular, se tiene que p es primo, pues de lo contrario tampoco podría serlo q. En efecto, de ser así
$$q = 2^p - 1 = (2^a)^b - 1 = (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1\right),$$
siendo $p = ab$ para $a, b > 1$ enteros, por como se descompone el polinomio ciclotómico de grado p cuando este es un número compuesto, entrando en contradicción con el hecho de que q sea primo por hipótesis.

Solución: Aplicamos de nuevo los **Teoremas de Sylow**. Se tiene en tal caso que $n_q - 1 \in q\mathbb{Z}$ y $n_q | 2^p$. Si $n_q = 1$ hemos terminado, luego vamos a suponer que $n_q > 1$ para ver si obtenemos algún subgrupo normal. En virtud de lo visto, la única opción que queda es $n_q = 2^p$. Sean por tanto $H_1, \ldots, H_{q+1}$ los q-subgrupos de Sylow para G. Como estos tienen orden primo, todas las intersecciones de dos entre estos han de ser triviales (**Teorema de Lagrange**). Por consiguiente, el número de elementos que tengan orden q en G es $(q-1) \cdot 2^p = |G| - 2^p$. Esto significa que los 2-subgrupos de Sylow que haya han de contener los 2^p elementos restantes; y, como estos subgrupos tienen, precisamente, orden 2^p por hipótesis, existe un único 2-subgrupo de Sylow H_2 que, por unicidad, debe ser normal en G.

(iii) $|G| = p^2 q$ con p y q primos distintos.

Solución: Vamos a distinguir dos casos:

* Si $p > q$ estamos ante un caso particular del apartado (i) visto ahora mismo. En efecto, basta tomar los valores $r = 2$ y $m = q$ primo.
* Si $q > p$ vamos a aplicar los **Teoremas de Sylow** para el otro primo. A saber, es $n_q - 1 \in q\mathbb{Z}$ y $n_q | p^2$. Luego, si $n_q > 1$ (en caso contrario hemos acabado), necesariamente ha de ser $n_q = p^2$ por ser $q > p$ (no puede ser que $n_q = p < q$ puesto que $p - 1 \notin q\mathbb{Z}$ bajo esta hipótesis). Sin embargo, en estas condiciones, tenemos que $p^2 - 1 = (p+1)(p-1) \in q\mathbb{Z}$ que, bajo la hipótesis de $q > p$ impuesta, sólo nos deja como opción que $p + 1 = q$. A saber, uno de estos dos primos ha de ser par y, como el único primo par es 2 como es bien sabido, necesariamente $p = 2$ y $q = 3$. Esto viene a decirnos que basta descartar el caso $|G| = 12$ que, de hecho, ya está descartado por el apartado anterior ($3 = 2^2 - 1$ es un primo de Mersenne para $p = 2$)[7].

De esta manera, se ha demostrado que G no puede ser simple nunca.

(2) Probar que todo grupo G no abeliano que tenga orden 24 ó 48 no puede ser simple.

Solución: Se trata de probar que G con $|G| = 3 \cdot 2^r$ con $r = 3$ y $r = 4$ no puede ser simple. Por los **Teoremas de Sylow**, se tiene que $n_2 | 3$ y $n_2 - 1 \in 2\mathbb{Z}$. Por tanto, se tiene que $n_2 \in \{1, 3\}$. Supongamos que $n_2 = 3$ (pues, en caso contrario, habremos terminado). Sea H el normalizador en G para un 2-subgrupo de Sylow que tiene índice 3 en G. Vamos a considerar el homomorfismo de grupos $\varphi \colon G \longrightarrow \mathcal{S}_3$ inducido por la acción de G sobre las coclases a izquierda de H[8]. A saber, dado $g \in G$ arbitrario, se tiene que $\varphi(g) \equiv \sigma_g \in \mathcal{S}_3$ es para cada $xH \in \{H, x_1 H, x_2 H\}$ arbitrario $\sigma_g(xH) := (gx)H$ en virtud de como viene dada la acción. Este tiene por núcleo a

$$\ker(\varphi) = \bigcap_{g \in G} gHg^{-1}.$$

[7]Otra manera de argumentar esto sería como en el caso anterior: si $n_q = p^2$ esto significa que el número de q-subgrupos de Sylow es p^2. Sean estos $H_1, \ldots, H_{p^2}$ que, además, tienen orden primo. Es decir, la intersección entre estos es trivial. Por consiguiente, el número de elementos que tengan orden q en G es $(q-1) \cdot p^2 = |G| - p^2$, luego los p-subgrupos de Sylow deben contener los p^2 elementos restantes, y como estos subgrupos tienen, precisamente, orden p^2 por hipótesis, existe un único p-subgrupo de Sylow H_p que es normal en G.

[8]Este procedimiento funciona siempre que se tenga un grupo G con orden $|G| = p^r n$ siendo $p \nmid n$ primo y $r \geq 1$ para tener al menos un subgrupo de índice $n > 1$ con $n! < |G|$ y proceder como se explica a continuación. En efecto, podemos construir un homomorfismo de grupos $\varphi \colon G \longrightarrow \mathcal{S}_n$ inducido por la acción de G sobre las coclases a izquierda de dicho subgrupo, y llegar a un **absurdo si** $\ker(\varphi)$ es un **subgrupo normal trivial** por ser $n > 1$ y $n! < |G|$. Luego $\ker(\varphi) \lhd G$ es subgrupo normal propio, y G no puede ser simple.

Este es un subgrupo normal de G. **Veamos que es propio**. Si φ es **inyectiva**, entonces $3 \cdot 2^r = |G| \leq |\mathcal{S}_3| = 3! = 6$ que es absurdo en las condiciones dadas. Si φ es el **homomorfismo trivial**, entonces $3 \cdot 2^r = |G| = |\ker(\varphi)| \leq |H| = 2^r$[9] que vuelve a ser absurdo, en este caso siempre (pues $H \leq G$ es un subgrupo de índice mayor que 1 en G). Luego, tenemos un subgrupo de G normal no trivial, lo cual implica que G no es simple en ninguno de los casos dados.

(3) Concluir usando los apartados anteriores, así como algunos de los resultados vistos tanto en teoría como en la **Hoja de Ejercicios** 5 durante las clases de problemas, que todo grupo no abeliano cuyo orden sea menor que 60 es necesariamente no simple.

Solución: Basta hacer una tabla coloreada con los números del 1 al 59. En efecto,

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	**36**	37	38	39	**40**	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59

Paso a aclarar cada caso (que, claramente, no son disjuntos):

- Se han marcado en rojo los números primos (y también el 1), ya que se tratan de grupos cíclicos (el grupo trivial es cíclico) que, en particular, son abelianos.
- Se han marcado en azul todos los p-grupos de orden no primo, pues se vio en el **Ejercicio** 11 resuelto en la **Hoja de Ejercicios** 5 que estos siempre tienen al centro como subgrupo (normal) no trivial cuando son no abelianos.
- Se han marcado en amarillo los grupos de orden p^2q con p y q primos distintos, pues acabamos de ver que estos nunca son simples.
- Se han marcado en gris los grupos de orden $p^r m$ con p primo tal que $r > 1$ y $p > m > 1$, pues acabamos de ver que estos nunca son simples. En particular, se han marcado en verde los grupos de orden pq con p y q primos distintos (caso concreto de los grises), los cuales además se vio en el **Ejercicio** 19 resuelto en la **Hoja de Ejercicios** 5 que nunca son simples (de hecho, muchos son cíclicos).
- Se han marcado en cian los grupos de orden $2^p q$ con $q = 2^p - 1$ primo, pues acabamos de ver que estos nunca son simples.
- Se han marcado de magenta los grupos de orden 24 y 48 ahora estudiados.
- Quedan marcados en **negrita** los grupos de orden $30, 36$ y 40 que vienen recogidos en el **Ejercicio** 15 dado en la **Hoja de Ejercicios** 5 como grupos no simples.

Dicho todo esto, damos por conlcuido el apartado.

(4) Probar que el grupo alternado $\mathcal{A}_5$ es un grupo simple.

Solución: Se sigue del **Teorema de Abel: Simplicidad del Grupo Alternado** (en los apuntes de la asignatura **Teorema 2.2.13**) para $n = 5$. Alternativamente, como se sabe que $H \lhd \mathcal{A}_5$ si, y sólo si, se tiene que H es unión disjunta entre algunas clases de conjugación para $\mathcal{A}_5$ (necesariamente la clase formada por el neutro debe ser parte de esta unión), al tener las distintas clases de $\mathcal{A}_5$ cardinales $1, 12, 12, 15$ y 20 cada una, observamos que ninguna combinación de sumas entre estas que incluya a 1 (salvo las dos triviales 1 y 60) va a dar un divisor del orden de $\mathcal{A}_5$ que es 60. Luego, por el **Teorema de Lagrange**, no pueden existir subgrupos normales no triviales.

[9] Por como viene definido el núcleo para este homomorfismo de grupos, sabemos que $\ker(\varphi) \subseteq gHg^{-1}$ para cada $g \in G$ dado; luego, en particular, para $g = 1 \in G$ se tiene que $\ker(\varphi) \subseteq H$ trivialmente.

(5) Demostrar que todo grupo no abeliano G con orden 60 y simple es isomorfo a $\mathcal{A}_5$. Para probar esto, los pasos que se sugiere seguir son los siguientes:
   (i) Demostrar que todo grupo simple de orden 60 admite un subgrupo que tenga índice 5 (**Sugerencia**: Calcular el número de elementos con órdenes 3 y 5 en el grupo G y llegar, estudiando los posibles elementos de orden 2 que puede haber, a que el normalizador de un 2-subgrupo de Sylow para G tiene índice 5).

   Solución: Siguiendo la sugerencia dada, vamos a aplicar los **Teoremas de Sylow** para calcular el número de elementos que tengan órdenes 3 y 5 en G de orden $60 = 2^2 \cdot 3 \cdot 5$. Como G es simple, se tiene que $n_3, n_5 \neq 1$. Así, en primer lugar, se calcula inmediatamente que $n_5 = 6$. Por otro lado, se tiene que $n_3 \in \{4, 10\}$. Sin embargo, si $n_3 = 4$ se tiene que existe un 3-subgrupo de Sylow para G cuyo normalizador en G tiene índice 4. Pero esto es imposible cuando G es simple[10]. En consecuencia, se tiene que $n_3 = 10$. Con todo esto, podemos afirmar que el número de elementos con orden 3 es $(3-1) \cdot 10 = 20$ mientras que el número de elementos con orden 5 es $(5-1) \cdot 6 = 24$. Vamos a estudiar ahora el número de elementos que tengan orden 2. Por los **Teoremas de Sylow**, se tiene que $n_2 \in \{1, 3, 5, 15\}$. Es obvio que $n_2 \neq 1$ por ser G simple. Además, también $n_2 \neq 3$ por la propiedad que se acaba de explicar a pie de página. Si $n_2 = 5$ hemos terminado, pues esto significa que existe un subgrupo que tiene índice 5 para G (que es el normalizador de cualquier 2-subgrupo H_2 de Sylow). Vamos por tanto a descartar el caso $n_2 = 15$ y habremos terminado. De darse esta situación, como los 2-subgrupos de Sylow bajo estas condiciones se intersecan **a lo más** en 2 elementos, se tiene que han de haber como mínimo $(4-1) \cdot 15 - (2-1) \cdot 15 = 30$ elementos de orden 2 **en el caso más favorable** (a saber, cuando menos elementos de orden 2 puede haber porque las intersecciones de dos subgrupos son máximas). Así, tenemos que **el número total de elementos que tienen orden** $1, 2, 3$ **y** 5 **está acotado inferiormente** por $1 + 30 + 20 + 24 = 75 > 60 = |G|$, lo cual es imposible otra vez. En resumen, la única posibilidad es que $n_2 = 5$ y, por tanto, tal y como ya se ha explicado, debe existir $N_G(H_2)$ un subgrupo de índice 5 para G tal y como se pedía probar.

   (ii) Utilizando lo anterior, concluir que todo grupo G no abeliano que tenga orden 60 y simple tiene que ser isomorfo a $\mathcal{A}_5$ (**Sugerencia**: Dado $H \leq G$ con índice 5, considerar la **acción transitiva** de G sobre las coclases a izquierda de H que induce un homomorfismo no trivial $\phi\colon G \longrightarrow \mathcal{S}_5$, y concluir que $\mathrm{Im}(\phi) = \mathcal{A}_5$).

   Solución: Acabamos de ver que si G es simple de orden 60 entonces existe $H \leq G$ con índice 5. Más aún, la acción de G sobre las coclases a izquierda de H induce un monomorfismo de grupos que va de G en $\mathcal{S}_m$ como se ha explicado. En nuestro caso particular, suponiendo que $\phi\colon G \longrightarrow \mathcal{S}_5$ es dicho monomorfismo de grupos, esto significa por aplicación del **Primer Teorema de Isomorfía** que $G \cong \mathrm{Im}(\phi)$. Si se prueba que $\mathrm{Im}(\phi) = \mathcal{A}_5$ habremos terminado la demostración.

[10]En general, **los grupos no abelianos que sean simples no pueden tener subgrupos de índices** $2, 3$ **ó** 4. En efecto, suponiendo que H_n es dicho subgrupo de índice $n \in \{2, 3, 4\}$ arbitrario, si consideramos el homomorfismo de grupos **no trivial** (pues $n > 1$) dado por $\varphi\colon G \longrightarrow \mathcal{S}_n$ e inducido por la acción de G sobre las coclases a izquierda de H_n ya comentado, como este no puede tener núcleo no trivial (por ser simple el grupo G y el núcleo un subgrupo normal), necesariamente debe ser inyectivo. Esto es, por aplicación del **Primer Teorema de Isomorfía** es $G \cong \mathrm{Im}(\varphi)$ (a saber, se ha probado que G es isomorfo a un subgrupo de $\mathcal{S}_n$). Pero esto es imposible, pues $|G| \not| n! = |\mathcal{S}_n|$ salvo si $|G| \in \{1, 2, 3, 4, 6, 12, 24\}$ que, hemos visto, son todos casos de grupos no simples o abelianos. Por tanto, entramos en contradicción con el **Teorema de Lagrange**.

Es obvio que $|\mathrm{Im}(\phi)| = |G| = 60$ según acabamos de probar[11]. Veamos ahora que se da al menos una inclusión; en concreto, que $\mathrm{Im}(\phi) \subseteq \mathcal{A}_5$. Para ello, basta ver que los elementos de $\mathrm{Im}(\phi)$ tienen signatura 1. En otras palabras, si se toma el *homomorfismo de grupos signatura* dado por $\mathrm{sign}\colon \mathcal{S}_5 \longrightarrow \{-1, 1\}$ y se restringe a $\mathrm{Im}(\phi)$ (que vuelve a ser homomorfismo de grupos), es trivial (todo va a parar al 1). Evidentemente esta restricción es no inyectiva (de lo contrario $\mathrm{Im}(\phi)$ tendría orden 2 como máximo); luego, al ser $\mathrm{Im}(\phi)$ simple, necesariamente debe ser el homomorfismo de grupos trivial. Es decir, se tiene que $\mathrm{sign}\,(\mathrm{Im}(\phi)) = \{1\}$ que, por definición del grupo alternado, significa que $\mathrm{Im}(\phi) \subseteq \mathcal{A}_5$.

CONCLUSIONES: La mayoría de los errores que cabe destacar a lo largo de esta entrega se han producido en este problema. Para empezar, el más importante de todos, se da a la hora de estudiar la simplicidad de grupos que tengan orden 24 ó 48. Varios han sido los que se han puesto a contar elementos dando por sentado que dos 2-subgrupos de Sylow distintos tienen intersección trivial. Esto no es cierto en general (sólo sucede cuando los p-subgrupos de Sylow tienen orden p primo), como bien se ve a la hora de resolver el apartado $5(ii)$. Puede ser que los 2-subgrupos de Sylow se intersequen en $2, 4$ ó, incluso, 8 elementos en el caso de grupos con orden 48. También es considerable el número de personas que no terminan de resolver el apartado (3) olvidando comprobar los casos (recordad que, al haber redactado yo el problema, no es totalmente seguro que queden cerrados todos los casos). En concreto, no se justifican los p-grupos que, cuando no son abelianos, resultan ser no simples porque vimos en el **Ejercicio** 11 dado en la **Hoja de Ejercicios** 5 que tenían centro no trivial (subgrupo normal siempre). Por lo demás, creo que no hay más fallos generales que deba comentar (cada uno verá lo que tiene en concreto al recibir sus correcciones).

Problema 3. Resolver los siguientes **problemas de examen**:

(1) (**Examen** 16 **de Febrero** 2018) Enumerar los distintos grupos abelianos de orden 240 (salvo isomorfismo), señalando sus factores invariantes. Identificar cuál de todos estos se corresponde, en su caso, con el grupo de las unidades del anillo cociente $\mathbb{Z}_{385}$. Decidir, además, cuántos elementos de orden 2 tiene dicho grupo y listarlos.

Solución: Aplicación inmediata del **Teorema de Clasificación para grupos abelianos finitamente generados**. Se tiene que $240 = 2^4 \cdot 3 \cdot 5$. Luego, el mayor coeficiente de torsión siempre es múltiplo de $2 \cdot 3 \cdot 5 = 30$. A partir de aquí es rutinario calcular todos los grupos (salvo isomorfismo) y sus factores invariantes. En efecto,

$$\begin{array}{lll} \mathbb{Z}_{30} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{factores invariantes} & (30, 2, 2, 2); \\ \mathbb{Z}_{60} \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{factores invariantes} & (60, 2, 2); \\ \mathbb{Z}_{60} \times \mathbb{Z}_4 & \text{factores invariantes} & (60, 4); \\ \mathbb{Z}_{120} \times \mathbb{Z}_2 & \text{factores invariantes} & (120, 2); \\ \mathbb{Z}_{240} & \text{factores invariantes} & (240). \end{array}$$

Aplicando directamente el **Teorema Chino de los Restos** para las unidades de los anillos del tipo $\mathbb{Z}_{mn}$ con m y n enteros coprimos, este induce el isomorfismo de grupos

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}_{mn}^* & \longrightarrow & \mathbb{Z}_m^* \times \mathbb{Z}_n^* \\ & r + mn\mathbb{Z} & \mapsto & (r + m\mathbb{Z}, r + n\mathbb{Z}) \end{array}.$$

[11]Llegados aquí, dado que esto es equivalente a decir que **el índice de Im**(ϕ) **en** G **es** 2 por definición, podemos asegurar que este va a ser un subgrupo normal en G. Y, al ser $\mathcal{A}_5$ el único subgrupo normal no trivial de $\mathcal{S}_5$ (no sé si lo habéis probado), necesariamente ha de darse la igualdad $\mathrm{Im}(\phi) = \mathcal{A}_5$ deseada.

Así pues, se tiene que

$$\mathbb{Z}_{385}^* \cong \mathbb{Z}_{11}^* \times \mathbb{Z}_7^* \times \mathbb{Z}_5^* \cong \mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z}_4 \cong \mathbb{Z}_{60} \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Además, como todo grupo cíclico con orden par tiene, en virtud de la caracterización estudiada en el **Ejercicio** 20 dado en la **Hoja de Ejercicios** 5, un único subgrupo de orden 2 (generado por un único elemento de dicho orden), tenemos que hay un único subgrupo $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ en el que se encuentran todos los elementos de orden 2. En definitiva, este subgrupo tiene un total de 7 elementos con orden 2 (todos los de este subgrupo, salvo el neutro), que son todos los que tiene el grupo $\mathbb{Z}_{385}^*$[12].

(2) (**Examen** 15 **de Septiembre** 2007) Se considera el grupo abeliano G generado por $a, b, c, d \in G$ bajo las relaciones

$$12a + 6b + 6c - 6d = 0 \quad \text{y} \quad 2b - 4c - 12d = 0.$$

(i) Calcular los coeficientes de torsión y el rango de G.

Solución: Sea $\varphi\colon \mathbb{Z}^4 \longrightarrow G; (e_1, e_2, e_3, e_4) \mapsto (a, b, c, d)$. Por construcción se tiene $\ker(\varphi) = \langle (12, 6, 6, -6), (0, 2, -4 - 12)\rangle$. Luego el grupo $G \cong \mathbb{Z}^4/\ker(\varphi)$ está determinado por la matriz con coeficientes enteros

$$M = \begin{pmatrix} 12 & 6 & 6 & -6 \\ 0 & 2 & -4 & -12 \end{pmatrix}.$$

Para determinar el grupo abeliano, se realizan **transformaciones elementales por filas y columnas** (intercambiar, cambiar signo y sumar otra multiplicada por escalar entero no nulo) en esta matriz hasta obtener una en la que todas las entradas sean 0 salvo las de posición $(1, 1)$ y $(2, 2)$ donde se van a tener elementos $d_1 = \text{mcd}(\pm 12, \pm 6, \pm 4, \pm 2) = 2$ y d_2 respectivamente tal que $d_1 | d_2$ si $d_2 \neq 0$ (que lo va a ser). En efecto, por ejemplo, se hacen los pasos siguientes:

$$M \overset{c_1 \leftrightarrow c_2}{\sim} \begin{pmatrix} 6 & 12 & 6 & -6 \\ 2 & 0 & -4 & -12 \end{pmatrix} \overset{f_1 \leftrightarrow f_2}{\sim} \begin{pmatrix} 2 & 0 & -4 & -12 \\ 6 & 12 & 6 & -6 \end{pmatrix} \overset{f_2 \leftarrow f_2 - 3f_1}{\sim}$$

$$\overset{f_2 \leftarrow f_2 - 3f_1}{\sim} \begin{pmatrix} 2 & 0 & -4 & -12 \\ 0 & 12 & 18 & 30 \end{pmatrix} \overset{\substack{c_3 \leftarrow c_3 + 2c_1 \\ c_4 \leftarrow c_4 + 6c_1}}{\sim} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 12 & 18 & 30 \end{pmatrix} \overset{\substack{c_3 \leftarrow c_3 - c_2 \\ c_4 \leftarrow c_4 - 2c_2}}{\sim}$$

$$\overset{\substack{c_3 \leftarrow c_3 - c_2 \\ c_4 \leftarrow c_4 - 2c_2}}{\sim} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 12 & 6 & 6 \end{pmatrix} \overset{c_2 \leftrightarrow c_4}{\sim} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 6 & 12 \end{pmatrix} \overset{\substack{c_3 \leftarrow c_3 - c_2 \\ c_4 \leftarrow c_4 - 2c_2}}{\sim} \left(\begin{array}{cc|cc} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \end{array}\right).$$

[12]Otra manera de proceder para este caso particular que, además, nos permite listar estos elementos de orden 2 es la siguiente: el orden del grupo es $240 = 2^4 \cdot 5 \cdot 3$. Luego, como vamos a tener un $\mathbb{Z}_3$ y $\mathbb{Z}_5$ en la descomposición evidentemente, basta estudiar los elementos de orden 2 (**Teorema de Lagrange**), pues estos nos van a fijar como se termina descomponiendo la parte correspondiente a 2^4. Por definición, los elementos de orden 2 son aquellos tales que $x^2 \equiv 1 \bmod 385 = 5 \cdot 7 \cdot 11$. Dicho de otra forma, tienen que cumplir por el **Teorema Chino de los Restos** (aplicado de manera inversa) que $x^2 - 1 = (x + 1)(x - 1)$ sea congruente con 0 módulo 5, 7 y 11. Como todos estos son primos, significa que $5, 7, 11 | (x + 1)$ ó $5, 7, 11 | (x - 1)$. Una vez se tiene esto, vamos a empezar suponiendo que $11 | (x \pm 1)$ (tomamos el primo más grande). Entonces $x = 10 + 11k$ ó $x = 12 + 11k$ para $k \in \mathbb{Z}$. Vamos dando valores a k hasta que x llegue a 385 (cuando hay que pararse), y estudiamos aquellos valores tales que $x \pm 1$ sea mltiplo de 5. Sólo queda estudiar qué pasa con el 7 (es decir, si el número que tenemos $x \pm 1$ es congruente con 0 módulo 7). Haciendo esto, se obtienen todos los elementos de orden 2 en $\mathbb{Z}_{385}^*$ que son los siguientes: $\{34, 76, 111, 274, 309, 351, 384\}$. Hay exactamente **siete elementos de orden** 2. Por el orden que tiene el grupo, sabemos que este admite un subgrupo del tipo $\mathbb{Z}_2^r \times \mathbb{Z}_2^l \times \mathbb{Z}_2^s$ con $r, s, t \in \mathbb{N}$ (cada cíclico tiene **un solo elemento** de orden 2 y, por tanto, nos dan un total de 3 y, después, están los posibles productos entre estos que suman 4 más), y este subgrupo contiene a todos los de orden 2 del grupo (no puede haber más). Sólo falta sacar los valores enteros de r, s y t que han de sumar 4 (la máxima potencia de 2 es 4). Finalmente, se obtiene que $r = s = 1$ y $t = 2$.

Luego, se tiene que

$$G \cong \frac{\mathbb{Z}^4}{\ker(\varphi)} = \frac{\langle e_1\rangle \times \langle e_2\rangle \times \langle e_3\rangle \times \langle e_4\rangle}{\langle (2,0,0,0),(0,6,0,0)\rangle} \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}^2.$$

En definitiva, los coeficientes de torsión del grupo G son $(2,6)$ (correspondiente a la parte de torsión), mientras que el rango de este es 2 (viene de la parte libre).

(ii) Encontrar, si existe, un elemento de orden k para $k \in \{2,4,6,12\}$ en algún grupo que sea isomorfo a G.

Solución: Acabamos de ver que G es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}^2$. Vamos a buscar elementos de los órdenes pedidos en este. Distinguimos casos:
- Si $k = 2$ basta tomar $g = (1,0,0,0) \in \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}^2$.
- Si $k = 4$ no existen elementos de este orden, pues $4 \not| 2,6$ y $\text{mcd}(6,2) = 2$.
- Si $k = 6$ basta tomar $g = (0,1,0,0) \in \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}^2$.
- Si $k = 12$ no existen elementos de este orden, pues $12 \not| 2,6$ y $\text{mcd}(6,2) = 2$.

CONCLUSIONES: En general, no ha habido grandes problemas con estos apartados. Los únicos comentarios, algunas erratas en ciertas cuentas o falta de explicaciones consistentes.

Problema 4[13]**.** Decidir si las **afirmaciones siguientes** son **verdaderas o falsas**, dando una **prueba completa** o un **contraejemplo** cuando corresponda.

(1) Dado G un grupo de orden par, el número de elementos con orden 2 es impar.

Solución: Esta afirmación es **verdadera**. Los elementos de G pueden dividirse en dos clases disjuntas: $H = \{x \in G \mid x^2 \neq 1\}$ y $G \backslash H$. En H todos los elementos son distintos a su inverso (**Ejercicio** 7 visto en la **Hoja De Ejercicios** 4). Por lo tanto, estos van emparejados cada uno con su inverso(hay un número par de ellos). Como G tiene orden par, en el complementario de H en G ha de haber un número par de elementos. Así, como sólo el neutro tiene orden $1 < 2$ (el resto necesariamente tienen orden 2), tenemos que G contiene un número impar de elementos con orden 2.

(2) Si $H \trianglelefteq G$ y G/H es cíclico, entonces G es necesariamente abeliano.

Solución: Esta afirmación es **falsa**. Basta dar un **contraejemplo**. Si tomamos el **grupo** $G = Q$ **cuaternio** (no abeliano de orden 8 por el **Ejercicio** 3 visto en la **Hoja de Ejercicios** 4), y $H = \langle i\rangle \triangleleft G$ subgrupo normal de índice 2 en el grupo (**Ejercicio** 17 visto en la **Hoja de Ejercicios** 4), se tiene que $G/H \cong \mathbb{Z}_2$ es cíclico.

(3) Los grupos $\mathbb{Z}_3 \times \mathbb{Z}_{120}$ y $\mathbb{Z}_2 \times \mathbb{Z}_{180}$ son isomorfos.

Solución: Esta afirmación es **falsa**. En efecto, los factores invariantes de estos dos grupos abelianos finitos son claramente distintos (**Teorema de Clasificación para grupos abelianos finitamente generados**).

[13]Optativo para aquellos que, a lo largo de las entregas anteriores, hayan ido dejando algún apartado en los problemas propuestos sin hacer, con el fin de darles la oportunidad de aspirar a obtener la nota máxima en dichos casos, o para quienes quieran subir nota (o, simplemente, practicar de cara al examen).

(4) Dados G_1 abeliano y $\varphi\colon G_1 \longrightarrow G_2$ epimorfismo de grupos, entonces G_2 es abeliano.

Solución: Esta afirmación es **verdadera**. Sean $x, y \in G_2$ arbitrarios. Por tener que φ es **sobreyectiva**, existen $a, b \in G_1$ tales que $\varphi(a) = x$ y $\varphi(b) = y$. Como G_1 es un grupo **abeliano**, se tiene por ser φ **homomorfismo de grupos** que

$$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx,$$

demostrándose así la afirmación dada.

(5) Si G es un grupo finito tal que $|G : Z(G)|$ divide a 15, entonces G es abeliano.

Solución: Esta afirmación es **verdadera**. Se tiene que $n \equiv |G : Z(G)| \in \{1, 3, 5, 15\}$. Distinguimos casos:
- Si $n = 1$ se tiene que $G = Z(G)$. Por definición G es abeliano.
- Si $n = 3, 5$ el cociente $G/Z(G)$ es cíclico por ser un grupo de orden primo, y por tanto G es abeliano (**Ejercicio** 21 dado en la **Hoja de Ejercicios** 4).
- Si $n = 15$ el cociente $G/Z(G)$ es cíclico por los **Teoremas de Sylow** (**Ejercicio** 19 dado en la **Hoja de Ejercicios** 5), luego G vuelve a ser abeliano como antes.

Queda por tanto probado el resultado.

(6) En cualquier DFU A se tiene que $(a) + (b) = (\mathrm{mcd}(a, b))$ para todo $a, b \in A$.

Solución: Esta afirmación es **falsa**. Basta tomar $A = \mathbb{R}[x, y]$ que es DFU, junto con (x) e (y) generados por polinomios coprimos; y, sin embargo, su suma no es principal.

(7) Los anillos $\mathbb{Z}_3[x]/\left(x^2 + 1\right)$ y $\mathbb{Z}_3[x]/\left(x^2 + x + 2\right)$ son isomorfos.

Solución: Esta afirmación es **verdadera**. Como los polinomios que se tienen en el cociente son irreducibles sobre los anillos de polinomios con coeficientes en un cuerpo correspondientes, los anillos cociente son **cuerpos con el mismo cardinal**. Por tanto son isomorfos, y se puede construir este isomorfismo sin mucha dificultad[14].

(8) El anillo $\mathbb{Z}\left[x\right]/\left(x^2 - 3\right)$ es un cuerpo.

Solución: Esta afirmación es **falsa**. Aunque el polinomio $x^2 - 3$ resulte ser sobre $\mathbb{Z}$ irreducible, este no genera un ideal maximal ya que $\left(x^2 - 3\right) \subsetneq \left(5, x^2 - 3\right) \subsetneq \mathbb{Z}[x]$[15].

(9) Se tiene que A es DE si, y sólo si, también lo es B cuando $A \cong B$.

Solución: Esta afirmación es **verdadera**. Basta tomar la aplicación $\varphi\colon B \longrightarrow \mathbb{N}\backslash\{0\}$ que dota al anillo con estructura de DE, y definir $\varphi \circ f\colon A \longrightarrow \mathbb{N}\backslash\{0\}$ en A siendo $f\colon A \longrightarrow B$ el isomorfismo que tenemos. Los papeles de A y B son intercambiables por ser la relación de equivalencia "ser isomorfos" simétrica.

(10) La característica de A anillo divide al entero n si $na = 0$ **para algún** $a \in A$ **no nulo**.

Solución: Esta afirmación es **falsa**. Basta tomar $A = \mathbb{Z}_6$ un **anillo que no es DI** de característica 6 donde $2 \cdot [3]_6 = [0]_6$ y, sin embargo, se tiene que $6 \nmid 2$.

[14] En efecto, este es $f\colon \mathbb{Z}_3[x]/\left(x^2 + 1\right) \longrightarrow \mathbb{Z}_3[x]/\left(x^2 + x + 2\right); 1 \mapsto 1; x \mapsto -x + 1$ (o también $x - 1$).

[15] También puede verse que el anillo es isomorfo a $\mathbb{Z}\left[\sqrt{3}\right]$ que sabemos no es cuerpo.