Ejercicio 1. *(3,5 puntos)*

1. ¿Hay algún elemento de orden 8 en S_6? ¿y de orden 60 en S_{12}?
2. Dados dos grupos G, G' y dos subgrupos normales $H \triangleleft G, H' \triangleleft G'$, pruebe que $H \times H'$ es un subgrupo normal de $G \times G'$ y que existe un isomorfismo natural
$$\frac{G \times G'}{H \times H'} \simeq \frac{G}{H} \times \frac{G'}{H'}.$$
3. ¿Puede ser finito el grupo de automorfismos de un grupo infinito?
4. Describa todos los automorfismos de $C_2 \times C_2$ indicando las imágenes de unos generadores. Pruebe que $S_3 \simeq \mathrm{Aut}(C_2 \times C_2)$ a través de la tabla del grupo.

Solución del Ejercicio 1.-
1) Sabemos que toda permutación σ (distinta de la identidad) se escribe de forma única como composición (conmutativa) de ciclos disjuntos, y que además el orden de σ es el m.c.m. de los órdenes de dichos ciclos. En S_6 hay ciclos de orden $2, 3, 4, 5$ o 6, y por tanto las posibles longitudes, de menor a mayor, de los ciclos disjuntos τ_i que aparezcan en la descomposición $\sigma = \tau_1 \cdots \tau_m$ sólo pueden ser las siguientes (su suma ha de ser menor o igual que 6):
$m = 1$: $2, 3, 4, 5, 6$
$m = 2$: $(2, 2), (2, 3), (2, 4), (3, 3)$
$m = 3$: $(2, 2, 2)$

En todos estos casos el m.c.m. resultante nunca es 8 y por tanto no hay permutaciones en S_6 que tengan orden 8.

También podemos llegar al mismo resultado de la siguiente forma: para que $\sigma = \tau_1 \cdots \tau_m$ tenga orden 8, el m.c.m. de los órdenes de los τ_i ha de ser 8, pero para ello alguno de los τ_i ha de tener orden 8, lo cual es imposible en S_6.

En el caso de S_{12} existen permutaciones σ que sean composición de tres ciclos disjuntos de órdenes $3, 4, 5$ (nótese que $3 + 4 + 5 = 12 \leq 12$) y todas ellas tendrán como orden m.c.m.$\{3, 4, 5\} = 60$. Por ejemplo
$$\sigma = (123)(4567)(89ABC),$$
donde para evitar confusiones A, B, C representan a $10, 11, 12$ respectivamente.

2) La prueba de que $H \times H'$ es un sugbgrupo normal de $G \times G'$ es muy fácil a partir de las definiciones y de la operación de grupo en $G \times G'$.

Sea $f : G \times G' \to \frac{G}{H} \times \frac{G'}{H'}$ la aplicación definida por $f(x, x') = (xH, x'H')$ (no es necesario analizar si está bien definida o no, pues para dar la imagen de cada elemento no hemos tenido que hacer ninguna elección).

Se prueba muy fácilmente que f es un homomorfismo de grupos. Además, f es sobreyectivo, pues todo elemento de $\frac{G}{H}$ (resp. de $\frac{G'}{H'}$) es de la forma xH (resp. $x'H'$), para algún elemento $x \in G$ (resp. $x' \in G'$).

Claramente el núcleo de f es $H \times H'$, y por tanto, por el primer teorema de isomorfía, el homomorfismo f induce un isomorfismo
$$\overline{f} = \frac{G \times G'}{\ker f} = \frac{G \times G'}{H \times H'} \xrightarrow{\simeq} \mathrm{Im} f = \frac{G}{H} \times \frac{G'}{H'}.$$

También podemos definir directamente la aplicación $\overline{f} : \frac{G \times G'}{H \times H'} \to \frac{G}{H} \times \frac{G'}{H'}$ mediante la expresión
$$\overline{f}((g, g')(H \times H')) = (gH, g'H'),$$
pero hemos de comenzar por probar que $\overline{f}$ está bien definida y después que es un isomorfismo.

3) El grupo aditivo de los enteros $\mathbf{Z}$ es infinito y tan sólo tiene dos elementos que son, cada uno de ellos, generadores: el 1 y el -1. Como consecuencia todo automorfismo de $\mathbf{Z}$ debe de llevar 1 en 1 (la identidad) o 1 en -1 (el dado por $x \in \mathbf{Z} \mapsto -x \in \mathbf{Z}$), es decir $\mathbf{Z}$ sólo tiene dos automorfirmos.

4) El grupos cíclico C_2 está generado por un elemento a de orden 2: $C_2 = \{1, a\}$, $a \neq 1, a^2 = 1$.

El producto cartesiano $C_2 \times C_2$ está generado por los elementos $x = (a, 1), y = (1, a)$, ambos de orden 2, cuyo producto conmuta (en realidad $C_2 \times C_2$ es un grupo abeliano):
$$x^2 = (a^2, 1^2) = (1, 1), y^2 = (1^2, a^2) = (1, 1), xy = (a, a) = yx, x \neq 1 \neq y.$$
Se tiene
$$C_2 \times C_2 = \{(1, 1), x = (a, 1), y = (1, a), z = xy = yx = (a, a)\}.$$
En resumen, el grupo $G = C_2 \times C_2$ es un grupo abeliano con 4 elementos: el elemento neutro y tres elementos más de orden 2. Además $z = xy, x = yz, y = xz$. Dicho de otra forma, $\langle x, y; x^2 = 1, y^2 = 1, xy = yx\rangle$ es una presentación de G, y $G = \langle x, y\rangle = \langle x, z\rangle = \langle y, z\rangle$.

Como x, y son generadores de G, todo endomorfismo estará determinado por sus imágenes. Además, dados dos elementos cualesquiera $c, d \in G$ siempre se tiene $c^2 = d^2 = 1, cd = dc$ y por tanto existe un endomofismo único $f_{c,d} : G \to G$ tal que $f_{c,d}(x) = c, f_{c,d}(y) = d$. Se trata ahora de detectar cuáles de los $f_{c,d}$ son automorfismos, o lo que es lo mismo (puesto que G es finito), cuáles son sobreyectivos. Pero para que $f_{c,d}$ sea sobreyectivo es necesario y suficiente que c, d sean generadores de G. Así pues, podemos excluir los casos en que c o d son el elemento neutro o cuando $c = d$.

Los automorfismos de G son pues $f_{x,y}$ (que es la identidad), $f_{x,z}$, $f_{y,x}$, $f_{y,z}$, $f_{z,x}$, $f_{z,y}$. Por tanto el grupo de automorfismos de G tiene 6 elementos.

Calculemos como ejemplo la composición $f_{x,z} \circ f_{y,x}$:

$$(f_{x,z} \circ f_{y,x})(x) = f_{x,z}(f_{y,z}(x)) = f_{x,z}(y) = z,$$

$$(f_{x,z} \circ f_{y,x})(y) = f_{x,z}(f_{y,z}(y)) = f_{x,z}(z) = f_{x,z}(xy) = f_{x,z}(x)f_{x,z}(y) = xz = y,$$

de donde $f_{x,z} \circ f_{y,x} = f_{z,y}$.

Las demás composiciones se calculan del mismo modo y llegamos a que la tabla del grupo $\mathrm{Aut}(G)$ es:

$\circ$	Id	$f_{x,z}$	$f_{y,x}$	$f_{y,z}$	$f_{z,x}$	$f_{z,y}$
Id	Id	$f_{x,z}$	$f_{y,x}$	$f_{y,z}$	$f_{z,x}$	$f_{z,y}$
$f_{x,z}$	$f_{x,z}$	Id	$f_{z,x}$	$f_{z,y}$	$f_{y,x}$	$f_{y,z}$
$f_{y,x}$	$f_{y,x}$	$f_{y,z}$	Id	$f_{x,z}$	$f_{z,y}$	$f_{z,x}$
$f_{y,z}$	$f_{y,z}$	$f_{y,x}$	$f_{z,y}$	$f_{z,x}$	Id	$f_{x,z}$
$f_{z,x}$	$f_{z,x}$	$f_{z,y}$	$f_{x,z}$	Id	$f_{y,z}$	$f_{y,x}$
$f_{z,y}$	$f_{z,y}$	$f_{z,x}$	$f_{y,z}$	$f_{y,x}$	$f_{x,z}$	Id

(Nótese que de la tabla anterior deducimos que $\mathrm{Aut}(G) \simeq S_6$).

Ejercicio 2. *(1 punto)*

1. Sea R un dominio, $a \in R$ un elemento irreducible y $b \in R$. Pruebe que
   (a) Si $b \in \langle a \rangle$ entonces $\mathrm{mcd}(a, b) = a$.
   (b) Si $b \notin \langle a \rangle$ entonces $\mathrm{mcd}(a, b) = 1$.
2. Dé un ejemplo de un dominio R y un elemento $a \in R$ irreducible tal que $R/\langle a \rangle$ no sea dominio de integridad.

Solución del Ejercicio 2.

1. Hagamos notar que en un dominio no siempre existe el máximo común divisor de dos números.
   (a) Si $b \in \langle a \rangle$ entonces b es múltiplo de a, por lo que a es divisor común de a y b. Si d divide a a y b, en particular divide a a. Por tanto, existe el máximo común divisor y es igual a a.
   (b) Sea $b \notin \langle a \rangle$. Si d divide a a y a b, por ser a irreducible, solamente puede ocurrir que $d = u$, u unidad de R o bien d es asociado de a. En este último caso tendríamos que $\langle d \rangle = \langle a \rangle$, y como $b \in \langle d \rangle$, llegaríamos a que $b \in \langle a \rangle$. Por tanto, la única posibilidad es que d sea unidad, que es lo que queríamos probar.
2. Sabemos que una condición equivalente a que $R/\langle a \rangle$ sea dominio de integridad es que $\langle a \rangle$ sea un ideal primo, o lo que es lo mismo, que a sea primo en R. Por tanto, buscamos un dominio donde existan elementos irreducibles no primos. Por ejemplo, sea $R = \mathbf{Z}[\sqrt{-3}]$, y consideremos $a = 2$. Veamos que es irreducible. La aplicación norma está definida como $N(\alpha+\beta\sqrt{-3}) = \alpha^2+3\beta^2$. Es claro entonces que $N(\alpha+\beta\sqrt{-3}) = 1$ implica que $\beta = 0, \alpha^2 = 1$, por lo que las unidades de R son 1 y -1. Si $a = a_1 \cdot a_2$, $a_1, a_2 \in R$ no unidades, entonces $4 = N(a_1)N(a_2)$ con $N(a_1) \neq 1$ y $N(a_2) \neq 1$. Únicamente queda $N(a_1) = 2, N(a_2) = 2$. Si $a_1 = \alpha_1 + \beta_1\sqrt{-3}, \alpha_1, \beta_1 \in \mathbf{Z}$, entonces $2 = N(a_1) = \alpha_1^2 + 3\beta_1^2$, de donde $\beta_1^2 = 0$. Pero entonces $\alpha_1^2 = 2$, lo que es imposible. Por tanto, a no admite una factorización y es irreducible.
   Veamos ahora que no es primo. Tenemos que $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Sin embargo, vamos a probar que 2 no divide a $1 + \sqrt{-3}$ ni a $1 - \sqrt{-3}$. Si $1 + \sqrt{-3} = 2(\alpha + \beta\sqrt{-3})$, con $\alpha, \beta \in \mathbf{Z}$, entonces

$$1 = 2\alpha,$$
$$1 = 2\beta$$

   lo que es imposible con coeficientes enteros. Análogo para $1 - \sqrt{-3}$.

Ejercicio 3. *(2,5 puntos)* Sea k un cuerpo y R el conjunto de polinomios de $k[X]$ que no tienen el término de grado 1, es decir, polinomios de la forma $a_0 + a_2X^2 + a_3X^3 + \ldots + a_nX^n$.

1. Pruebe que R es un subanillo de $k[X]$.
2. Pruebe que X^2 y X^3 son irreducibles en R, pero no son primos. ¿Es R un dominio euclídeo?

3. Sea A un DFU y F el cuerpo de fracciones de A. Pruebe que $d \in A$ es un cuadrado en A si y solamente si d es un cuadrado en F.

4. Dé un contraejemplo de lo anterior para el anillo R.

Solución del Ejercicio 3. Los elementos de R son los polinomios $a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ con $a_1 = 0$.

1. La estructura de anillo de $k[X]$ viene determinada por la suma y el producto de polinomios. Veamos que estas operaciones son internas en R. En efecto, sean $p(X), q(X) \in R$. Entonces $p(X) - q(X) \in R$ pues ninguno aporta término de grado 1. En consecuencia, R es un subgrupo de $k[X]$. Por otro lado, si $a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n, b(X) = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m$ son elementos de $k[X]$, el término de grado 1 en el producto $a(X)b(X)$ tiene como coeficiente $a_0b_1 + a_1b_0$. Si $p(X), q(X) \in R$ entonces los coeficientes de los términos de grado 1 son nulos y por lo anterior también el del producto. Por último, es claro que $1 \in R$.

2. Si X^2 factoriza en R, sean $a(X), b(X) \in R$ no constantes tales que $X^2 = a(X)b(X)$. Por cuestiones de grado solamente es posible que tengan grado 1, lo que es imposible. Para X^3, un razonamiento análogo implica que o bien grado$(a(X)) = 1$ o bien grado$(b(X)) = 1$.
   Observemos que X^2 no divide a X^3 en R, pues en otro caso tendríamos $X^3 = X^2a(X)$, y por el grado llegaríamos a grado$(a(X)) = 1$. Es evidente también que X^3 no puede dividir a X^2. Por otro lado, tenemos que $X^6 = X^3 \cdot X^3$ y $X^6 = X^2 \cdot X^2 \cdot X^2$. Sin embargo, X^2 no divide a X^3 ni X^3 divide a X^2, de donde son elementos no primos en R.
   Por lo anterior, existen elementos irreducibles no primos, por lo que R no es dominio de factorización única. Recordemos que un dominio euclídeo es dominio de ideales principales y, en consecuencia, dominio de factorización única. Por tanto, R no es dominio euclídeo (aun siendo subanillo de $k[X]$, que sí lo es).

3. Sea $d \in A$. Es evidente que si d es cuadrado en A lo es también en F, pues $A \subset F$. Supongamos entonces que existen $a_1, a_2 \in A, a_2 \neq 0$ tales que $d = (a_1/a_2)^2$. Podemos tomar a_1, a_2 primos entre sí. Entonces $da_2^2 = a_1^2$ y esto implica que a_2 divide a a_1^2. Pero entonces a_2 divide a a_1, porque los factores primos de a_1^2 son los mismos que los de a_1, pero con exponente doble. Esto es contradictorio con el carácter irreducible de la fracción a_1/a_2.

4. Consideremos $d = X^2$. Es claro que no es cuadrado en R, por cuestiones de grado. Sin embargo, $d = (X^3/X^2)^2$ y X^3/X^2 es un elemento del cuerpo de fracciones de R.

Ejercicio 4. *(3 puntos)* Sea K el cuerpo de descomposición de $X^3 - 2$ sobre $\mathbf{Q}$.

1. Demuestre que $K = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{2})$.
2. Halle $[K : \mathbf{Q}]$.
3. Sea $\alpha = \sqrt{-3} + \sqrt[3]{2}$. Deduzca si $K = \mathbf{Q}(\alpha)$.
4. Describa los elementos del grupo de Galois $G(K|\mathbf{Q})$, simultáneamente,
   (a) en términos de las imágenes de $\sqrt{-3}$ y $\sqrt[3]{2}$,
   (b) en términos de las imágenes de las raíces de $X^3 - 2$.

Solución del Ejercicio 4.

1. Las raíces de $X^3 - 2$ son

$$\begin{aligned} x_1 &= \sqrt[3]{2} \in \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3}), \\ x_2 &= \sqrt[3]{2}(\cos(2\pi/3) + i\,\mathrm{sen}(2\pi/3)) = \sqrt[3]{2}(-1/2 + \sqrt{-3}/2) \in \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3}), \\ x_3 &= \sqrt[3]{2}(\cos(4\pi/3) + i\,\mathrm{sen}(4\pi/3)) = \sqrt[3]{2}(-1/2 - \sqrt{-3}/2) \in \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3}). \end{aligned}$$

   Luego $K = \mathbf{Q}(x_1, x_2, x_3) \subset \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3})$. Recíprocamente, $\sqrt[3]{2} \in K$ y $x_2 - x_3 = \sqrt[3]{2}\sqrt{-3} = x_1\sqrt{-3}$, de donde $\sqrt{-3} = (x_2 - x_3)/x_1 \in K$. Luego $\mathbf{Q}(\sqrt[3]{2}, \sqrt{-3}) \subset K$.

2. Como $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}) \subset K$, por la fórmula del grado tenemos que

$$[K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt[3]{2})][\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}].$$

   Por un lado, $x_1 = \sqrt[3]{2}$ es raíz del polinomio $X^3 - 2$, que es irreducible sobre $\mathbf{Q}$ por el criterio de Eisenstein. Entonces $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$. Por otra parte, $\sqrt{-3}$ es raíz del polinomio $X^2 + 3$ en $\mathbf{Q}(\sqrt[3]{2})[X]$. Si fuera reducible sería producto de dos polinomios de grado 1 con coeficientes en $\mathbf{Q}(\sqrt[3]{2})[X]$. Entonces $\pm\sqrt{-3} \in \mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{R}$, lo que es falso. Luego $X^2 + 3$ es irreducible sobre $\mathbf{Q}(\sqrt[3]{2})[X]$ y tenemos entonces que $[K : \mathbf{Q}(\sqrt[3]{2})] = 3$. Por lo anterior, $[K : \mathbf{Q}] = 6$.

3. Sabemos que $\{1, \sqrt{-3}\}$ es una base del $\mathbf{Q}$-e.v. $Q(\sqrt{-3})$, y que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una base del $\mathbf{Q}$-e.v. $Q(\sqrt[3]{2}$. Entonces $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{-3}, \sqrt{-3}\sqrt[3]{2}, \sqrt{-3}\sqrt[3]{4}\}$ es una base de K como $\mathbf{Q}$-e.v. Por una parte , $\alpha = \sqrt{-3} + \sqrt[3]{2} \in K$, luego $\mathbf{Q}(\alpha) \subset K$. Entonces $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ es un divisor de 6. Expresamos α^n en términos de la base anterior, para cada n. Obtenemos

	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$	$\sqrt{-3}$	$\sqrt{-3}\sqrt[3]{2}$	$\sqrt{-3}\sqrt[3]{4}$
1	1	0	0	0	0	0
α	0	1	0	1	0	0
α^2	-3	0	1	0	2	0
α^3	2	-9	0	-3	0	3

pues $\alpha^2 = -3 + \sqrt[3]{4} + 2\sqrt{-3}\sqrt[3]{2}, \alpha^3 = 2 - 9\sqrt[3]{2} - 3\sqrt{-3} + 3\sqrt{-3}\sqrt[3]{4}$. Como $\{1, \alpha, \alpha^2, \alpha^3\}$ son linealmente independientes sobre $\mathbf{Q}$ (rango de la matriz de coordenadas igual a 4), concluímos que $[\mathbf{Q}(\alpha) : \mathbf{Q}] > 3$. La única posibilidad es entonces $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6$, de donde $\mathbf{Q}(\alpha) = K$.

4. Por el teorema de Artin, $|G(K|k)| = [K : k]$, ya que $F(G(K|k)) = k$. Sea $G = G(K|\mathbf{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$. Si $K = \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3})$, como $\sigma_i(\sqrt[3]{2})^3 - 2 = 0$, se tiene que $\sigma_i(\sqrt[3]{2}) = \{x_1, x_2, x_3\}$. Análogamente, $\sigma_i(\sqrt{-3}) = \pm\sqrt{-3}$.

   (a) Como hay 6 posibilidades distintas y 6 elementos distintos en G, debe ser, por ejemplo,

$$\begin{aligned}
&\sigma_1(\sqrt[3]{2}) = x_1, \sigma_1(\sqrt{-3}) = \sqrt{-3},\\
&\sigma_2(\sqrt[3]{2}) = x_1, \sigma_2(\sqrt{-3}) = -\sqrt{-3},\\
&\sigma_3(\sqrt[3]{2}) = x_2, \sigma_3(\sqrt{-3}) = \sqrt{-3},\\
&\sigma_4(\sqrt[3]{2}) = x_2, \sigma_4(\sqrt{-3}) = -\sqrt{-3},\\
&\sigma_5(\sqrt[3]{2}) = x_3, \sigma_5(\sqrt{-3}) = \sqrt{-3},\\
&\sigma_6(\sqrt[3]{2}) = x_3, \sigma_1(\sqrt{-3}) = -\sqrt{-3}
\end{aligned}$$

   (b) Si $K = \mathbf{Q}(x_1, x_2, x_3)$, entonces $\sigma(x_i) = x_j$ para todo $\sigma \in G$. Es fácil ver que

$$\begin{aligned}
&\sigma_1(x_1) = x_1, \sigma_1(x_2) = x_2, \sigma_1(x_3) = x_3,\\
&\sigma_2(x_1) = x_1, \sigma_2(x_2) = x_3, \sigma_2(x_3) = x_2,\\
&\sigma_3(x_1) = x_2
\end{aligned}$$

   De la expresión de x_2 en función de $\sqrt[3]{2}$ y $\sqrt{-3}$ se tiene que $\sigma_3(x_2) = \sigma_3(x_1)(-1/2 + \sigma_3(\sqrt{-3})/2) = x_2(-1/2 + \sqrt{-3}/2) = x_1(-1/2 + \sqrt{-3}/2)^2 = x_3$, y entonces $\sigma_3(x_3) = x_1$. Análogamente, $\sigma_4(x_1) = x_2$ y $\sigma_4(x_2) = x_2(-1/2 - \sqrt{-3}/2) = x_1, \sigma_4(x_3) = x_3$. Sin más que hacer los cálculos se obtiene

$$\begin{aligned}
&\sigma_5(x_1) = x_3, \sigma_5(x_2) = x_3, \sigma_5(x_3) = x_2,\\
&\sigma_6(x_1) = x_3, \sigma_6(x_2) = x_2, \sigma_6(x_3) = x_1
\end{aligned}$$