Ejercicio 1. *(1 punto)* Se pide:

1. Descomponga en ciclos disjuntos la permutación:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 8 & 7 & 1 & 2 & 4 & 5 \end{pmatrix} \in S_8.$$

2. ¿Existe algún $\tau \in S_8$ tal que $\tau\sigma\tau^{-1} = (1234)(56)(78)$? En caso afirmativo, calcule τ.

Solución del Ejercicio 1.-
1) $\sigma = (1385)(26)(47)$.

2) Sabemos que $\tau(a_1a_2\dots a_r)\tau^{-1} = (\tau(a_1)\tau(a_2)\dots\tau(a_r))$, por tanto existe una τ tal que

$$\tau\sigma\tau^{-1} = (\tau(1)\tau(3)\tau(8)\tau(5))(\tau(2)\tau(6))(\tau(4)\tau(7)) = (1234)(56)(78).$$

Por ejemplo

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 2 & 7 & 4 & 6 & 8 & 3 \end{pmatrix}.$$

(Nótese que τ no es único. Basta tener en cuenta que $(1385) = (3851) = (8513)$ o que $\sigma = (1385)(47)(26) = (3851)(74)(62) = \cdots$.)

Ejercicio 2. *(3 puntos)* Sean $C_2 = \{1, x\}, C_3 = \{1, y, y^2\}$ grupos cíclicos de orden 2 y 3 respectivamente y sea $f : C_3 \to C_3$ la aplicación definida por $f(g) = g^2$ para cada $g \in C_3$. Se pide:

1. Pruebe que f es un automorfismo de C_3. Comprobar que f tiene orden 2 en tanto que elemento del grupo $\mathrm{Aut}(C_3)$ de los automorfismos de C_3.

2. Sea $\varphi : C_2 \to \mathrm{Aut}(C_3)$ el homomorfismo de grupos dado por $\varphi(x^i) = f^i$, $i = 0, 1$. Consideremos la siguiente operación interna en $C_3 \times C_2$:

$$(a, b) \star (c, d) := (a \cdot [\varphi(b)(c)], b \cdot d), \quad (a, b), (c, d) \in C_3 \times C_2.$$

   Pruebe que $(C_3 \times C_2, \star)$ es un grupo.

3. Para el grupo anterior, defina un homomorfismo sobreyectivo $h : C_3 \times C_2 \to C_2$ y demuestre que su núcleo es un grupo cíclico de orden 3.

Solución del Ejercicio 2.-
1) Para probar que $f : C_3 \to C_3$ es un automorfismo de grupos hemos de probar que es un homomorfismo de grupos y que es una aplicación biyectiva.

f es homomorfismo de grupos: hay que probar que $f(ab) = f(a)f(b)$ para cualesquiera elementos $a, b \in C_3$.
En efecto:

$$f(ab) = (ab)^2 = abab \overset{\star}{=} aabb = a^2b^2 = f(a)f(b),$$

donde la igualdad $\star$ se da porque C_3 es un grupo cíclico y por tanto abeliano.

f es una aplicación biyectiva: como f va de C_3 en sí mismo y C_3 es un conjunto finito, basta probar que f es inyectiva o que f es sobreyectiva.
a) Veamos que f es inyectiva, o lo que es lo mismo, que $\ker f = \{1\}$. Si $a \in \ker f$ entonces $1 = f(a) = a^2$ de donde a tiene un orden que divide a 2. Por otra parte el orden de a divide al orden de C_3 (teorema de Lagrange) que es 3. Así pues el orden de a debe ser 1 y por tanto $a = 1$.
b) También podemos ver directamente que f es sobreyectiva, o incluso que es biyectiva, pues $C_3 = \{1, y, y^2\}$ y $f(1) = 1, f(y) = y^2, f(y^2) = (y^2)^2 = y^4 = y$ (nótese que $y^3 = 1$).

Una vez que sabemos que f es un automorfismo de C_3, podemos considerarlo como elemento del grupo $\mathrm{Aut}(C_3)$, cuya operación es la composición de aplicaciones. En particular podemos hallar su orden, que es el menor entero $r > 0$ tal que f^r es la aplicación identidad.
Evidentemente f no es la identidad ($f(y) = y^2 \neq y$).
Calculemos la segunda potencia f^2: $f^2(1) = f(f(1)) = f(1) = 1$, $f^2(y) = f(f(y)) = f(y^2) = (y^2)^2 = y^4 = y$, $f^2(y^2) = f(f(y^2)) = f((y^2)^2) = f(y^4) = f(y) = y^2$, luego $f^2(a) = a$ para todo elemento $a \in C_3$ y por tanto f^2 es la identidad. De aquí deducimos que f tiene orden 2 dentro del grupo de los automorfismos de C_3.

2) Hemos de probar que la operación $\star$ definida en $C_3 \times C_2$ tiene elemento neutro (a la izquierda y a la derecha), que todo elemento posee elemento simétrico (a ambos lados) y que la operación es asociativa.

Elemento neutro: tenemos que buscar un elemento $(e_1, e_2) \in C_3 \times C_2$ tal que

$$(e_1, e_2) \star (a, b) = (a, b) \star (e_1, e_2) = (a, b)$$

para todo $(a, b) \in C_3 \times C_2$.

Veámoslo primero a la izquierda. Debemos tener:

$$(a, b) = (e_1, e_2) \star (a, b) = (e_1 \cdot [\varphi(e_2)(a)], e_2 \cdot b),$$

de donde $b = e_2 \cdot b$, y como b puede ser cualquier elemento de C_2 deducimos que $e_2 = 1$ (el elemento neutro de C_2).

Por otra parte, como $\varphi : C_2 \to \mathrm{Aut}(C_3)$ es un homomorfismo de grupos, tenemos que $\varphi(1)$ ha de ser la identidad (el elemento neutro de $\mathrm{Aut}(C_3)$) y por tanto:

$$a = e_1 \cdot [\varphi(e_2)(a)] = e_1 \cdot [\varphi(1)(a)] = e_1 \cdot [\mathrm{Id}(a)] = e_1 \cdot a$$

y de nuevo, como a es un elemento arbitrario de C_3, deducimos que $e_1 = 1$ (el elemento neutro de C_3).

Así pues, de existir un elemento (e_1, e_2) neutro a la izquierda para la operación $\star$, éste ha de ser $(1, 1)$. Comprobemos ahora que $(1, 1)$ es el elemento neutro a ambos lados.

El cálculo anterior muestra que lo es a la izquierda. Veámoslo a la derecha:

$$(a, b) \star (1, 1) = (a \cdot [\varphi(b)(1)], b \cdot 1) \stackrel{*}{=} (a \cdot 1, b \cdot 1) = (a, b),$$

donde la igualdad $*$ proviene del hecho de que para cada $b \in C_2$, $\varphi(b)$ es un automorfismo de C_3 y en particular $\varphi(b)(1) = 1$.

Elemento simétrico: dado $(a, b) \in C_3 \times C_2$ hemos de encontrar $(a', b') \in C_3 \times C_2$ tal que

$$(a, b) \star (a', b') = (a', b') \star (a, b) = (1, 1).$$

Para ello:

$$(1, 1) = (a, b) \star (a', b') = (a \cdot [\varphi(b)(a')], b \cdot b'),$$

de donde $1 = b \cdot b'$ y por tanto $b' = b^{-1}$. Por otra parte $1 = a \cdot [\varphi(b)(a')]$, de donde $\varphi(b)(a') = a^{-1}$. Pero como $\varphi(b)$ es un automorfismo de C_3, deducimos que

$$a' = \varphi(b)^{-1}(a^{-1}) \stackrel{*}{=} \varphi(b^{-1})(a^{-1}),$$

donde la igualdad $*$ proviene de que $\varphi : C_2 \to \mathrm{Aut}(C_3)$ es un homomorfismo de grupos.

Así pues, el candidato a simétrico de (a, b) es $(\varphi(b^{-1})(a^{-1}), b^{-1})$. Demostremos que en efecto lo es. El cálculo anterior muestra que lo es a la derecha. Veámoslo a la izquierda:

$$(\varphi(b)^{-1}(a^{-1}), b^{-1}) \star (a, b) = ([\varphi(b^{-1})(a^{-1})] \cdot [\varphi(b^{-1})(a)], b^{-1} \cdot b) \stackrel{*}{=} (1, 1),$$

donde la igualdad $*$ proviene de que $\varphi(b^{-1})$ es un homomorfismo (incluso un automorfismo) de grupos:

$$[\varphi(b^{-1})(a^{-1})] \cdot [\varphi(b^{-1})(a)] = \varphi(b^{-1})(a^{-1} \cdot a) = \varphi(b^{-1})(1) = 1.$$

3) La aplicación $h : C_3 \times C_2 \to C_2$ dada por la segunda proyección, i.e. $h(a, b) = b$, es claramente un homomorfismo de grupos:

$$h((a, b) \star (c, d)) = h(\cdots, bd) = bd = h(a, b)h(c, d).$$

Obviamente h es sobreyectiva. Por el primer teorema de isomorfía sabemos que

$$(C_3 \times C_2)/\ker h \simeq C_2,$$

de donde deducimos que $\ker h$ ha de ser un subgrupo de $C_3 \times C_2$ con 3 elementos, y por tanto ha de ser cíclico.

El que $\ker h$ es cíclico puede verse directamente pues:

$$\ker h = \{(1, 1), (y, 1), (y^2, 1)\}$$

y es fácil comprobar que

$$(y, 1)^2 = (y^2, 1), (y, 1)^3 = (1, 1).$$

Ejercicio 3. *(1 punto)*

1. Sea G el grupo de Galois de una extensión normal (de Galois) $K|k$. Si $|G| = 6$ y es cíclico, razone cuántos cuerpos intermedios hay entre k y K.

2. Responda 'verdadera' o 'falsa' a las siguientes afirmaciones:

   (a) Hay cuerpos finitos con 64 elementos.

   (b) Hay cuerpos finitos con 36 elementos.

   (c) Dos cuerpos finitos con el mismo número de elementos son isomorfos.

Solución del Ejercicio 3.-

1) Por el teorema de Galois hay una correspondencia biunívoca entre los subgrupos de G y los cuerpos intermedios entre k y K.

Como G es un grupo cíclico, $G =< \sigma >$, con $\sigma^6 = 1$, sus subgrupos son también cíclicos, tantos como divisores de 6:

$$\begin{array}{l} H_1 = \{1\} =< 1 > \\ H_2 = \{1, \sigma^3\} =< \sigma^3 > \\ H_3 = \{1, \sigma^2, \sigma^4\} =< \sigma^2 >=< \sigma^4 > \\ H_4 = G =< \sigma >=< \sigma^5 > \end{array}$$

Así, hay dos subgrupos propios de G: H_2 y H_3. Por lo tanto, hay dos cuerpos intermedios propios: $F(H_2)$ y $F(H_3)$ (o K^{H_2} y K^{H_3}).

2) (a) $64 = 2^6 = p^n$, con p primo. 'Verdadero'.

(b) $36 = 6^2 \neq p^n$, con p primo. 'Falso'.

(c) Así formulado es un teorema demostrado en las clases teóricas. 'Verdadero'.

Ejercicio 4. *(3 puntos)* El anillo $\mathbf{Z}[\sqrt{2}]$ tiene estructura de dominio euclídeo con la norma $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$. Sea $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}/\mathbf{Z}14$ definida por $\varphi(a + b\sqrt{2}) = (a + 4b) + \mathbf{Z}14$.

1. Pruebe que φ es un homomorfismo de anillos sobreyectivo.
2. Sea $r \in \mathbf{Z}[\sqrt{2}]$ tal que $\delta(r) < 14$ y $\varphi(r) = 0 + \mathbf{Z}14$. Pruebe que $r = 0$.
3. Pruebe que $\ker \varphi = \langle 8 + 5\sqrt{2} \rangle$.
4. Razone si $\mathbf{Z}[\sqrt{2}]$ es un dominio de ideales principales. ¿Son primos los elementos $\sqrt{2}$ y $1 - 2\sqrt{2}$?
5. Se tiene que $8 + 5\sqrt{2} = \sqrt{2}(5 + 4\sqrt{2}) = (4 + 3\sqrt{2})(-1 + 2\sqrt{2})$. Explique por qué lo anterior no contradice la factorización única en $\mathbf{Z}[\sqrt{2}]$.

Solución del Ejercicio 4.-

1) Debemos probar que para cualesquiera $z_1, z_2 \in \mathbf{Z}[\sqrt{2}]$ se verifica que

1. $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$.
2. $\varphi(z_1 \cdot z_2) = \varphi(z_1) \cdot \varphi(z_2)$.
3. $\varphi(1) = 1 + \mathbf{Z}14$.

La tercera es inmediata por la definición de la aplicación. Sean $z_1 = a_1 + b_1\sqrt{2}, z_2 = a_2 + b_2\sqrt{2}$, con $a_1, a_2, b_1, b_2 \in \mathbf{Z}$. Entonces

$\varphi(z_1) + \varphi(z_2) = ((a_1 + 4b_1) + \mathbf{Z}14) + ((a_2 + 4b_2) + \mathbf{Z}14) = (a_1 + a_2) + 4(b_1 + b_2) + \mathbf{Z}14 = \varphi(z_1 + z_2)$.

$\varphi(z_1)\varphi(z_2) = (a_1 + 4b_1) \cdot (a_2 + 4b_2) + \mathbf{Z}14 = a_1a_2 + 4a_1b_2 + 4a_2b_1 + 16b_1b_2 + \mathbf{Z}14 = a_1a_2 + 4a_1b_2 + 4a_2b_1 + 2b_1b_2 + \mathbf{Z}14$.

porque $16 + \mathbf{Z}14 = 2 + \mathbf{Z}14$.

$\varphi(z_1 \cdot z_2) = \varphi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = \varphi(a_1a_2 + 2b_1b_2 + \sqrt{2}(a_1b_2 + a_2b_1)) = a_1a_2 + 2b_1b_2 + 4(a_1b_2 + a_2b_1) + \mathbf{Z}14$.

2) Sea $r = r_1 + r_2\sqrt{2}, r_1, r_2 \in \mathbf{Z}$ y llamemos $k = r_1^2 - 2r_2^2$. Si $0 + \mathbf{Z}14 = \varphi(r) = r_1 + 4r_2 + \mathbf{Z}14$, se tiene que $r_1 + \mathbf{Z}14 = -4r_2 + \mathbf{Z}14$, entonces $k + \mathbf{Z}14 = (-4r_2)^2 - 2r_2^2 + \mathbf{Z}14 = 14r_2^2 + \mathbf{Z}14 = 0 + \mathbf{Z}14$. Luego k es múltiplo de 14. Como es un número entero comprendido entre -13 y 13, la única posibilidad es que $k = 0$, de donde $r_1^2 = 2r_2^2$. Como $\sqrt{2} \notin \mathbf{Q}$, la única solución es $r_1 = r_2 = 0$.

3) Por un lado tenemos que $\varphi(8 + 5\sqrt{2}) = 8 + 4 \cdot 5 + \mathbf{Z}14 = 0 + \mathbf{Z}14$, por lo que $\langle 8 + 5\sqrt{2} \rangle \subset \ker \varphi$. Para probar la inclusión contraria, sea $z \in \ker \varphi$. Como $\mathbf{Z}[\sqrt{2}]$ es dominio euclídeo, existen $q, r \in \mathbf{Z}[\sqrt{2}]$ tales que $z = q(8 + 5\sqrt{2}) + r$, con $\delta(r) < \delta(8 + 5\sqrt{2}) = 14$. Como $\varphi(z) = 0$ se deduce que $\varphi(r) = 0$. Por el apartado anterior, $r = 0$, por lo que z es múltiplo de $8 + 5\sqrt{2}$.

4) Como $\mathbf{Z}[\sqrt{2}]$ es un dominio euclídeo, es un dominio de ideales principales (resultado de teoría). Además, es un dominio de factorización única, por lo que los elementos irreducibles y primos coinciden. Observemos que $\delta(\sqrt{2}) = 2, \delta(1 - 2\sqrt{2}) = 7$, son números primos, por lo que son elementos irreducibles de de $\mathbf{Z}[\sqrt{2}]$ y por tanto primos.

5) En un DFU la factorización es única salvo producto por unidades y cambio del orden en los factores. Tenemos que

$$\frac{4+3\sqrt{2}}{\sqrt{2}} = 3+2\sqrt{2} = u_1, \; \frac{-1+2\sqrt{2}}{5+4\sqrt{2}} = 3-2\sqrt{2} = u_2.$$

Como $\delta(u_1) = \delta(u_2) = 1$, son unidades, por lo que $4+3\sqrt{2}$ es asociado de $\sqrt{2}$, y por el apartado anterior, irreducible. Lo mismo con respecto a $-1+2\sqrt{2}$ y $5+4\sqrt{2}$. Además $u_1u_2 = 1$, por lo que el cambio en la factorización es por producto por unidades.

Ejercicio 5. *(2 puntos)* Sea $K = \mathbf{Q}(\sqrt{2}, \sqrt{6})$.

1. Halle $[K : \mathbf{Q}]$.
2. Sea $\alpha = \sqrt{2} + \sqrt{3}$. Deduzca si $K = \mathbf{Q}(\alpha)$.
3. Demuestre que $K|\mathbf{Q}$ es una extensión normal (de Galois).
4. Describa los elementos del grupo de Galois $G(K|\mathbf{Q})$, en términos de las imágenes de $\sqrt{2}$ y $\sqrt{6}$.

Solución del Ejercicio 5.-
1) $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{6}) = K$. Por la fórmula del grado:

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

En primer lugar $\sqrt{2}$ es raíz del polinomio $X^2 - 2$, luego $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] \le 2$. Como $\sqrt{2} \notin \mathbf{Q}$, $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] > 1$, luego $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$. Otra manera de razonar hubiera sido utilizar el criterio de Eisenstein para probar que el polinomio anterior es irreducible sobre $\mathbf{Q}$, luego es el polinomio mínimo de $\sqrt{2}$ sobre $\mathbf{Q}$.

$\sqrt{6}$ es raíz del polinomio $X^2 - 6$, luego $[\mathbf{Q}(\sqrt{2}, \sqrt{6}) : \mathbf{Q}(\sqrt{2})] \le 2$. Como $\sqrt{6} \notin \mathbf{Q}(\sqrt{2})$, $[K : \mathbf{Q}(\sqrt{2})] > 1$; en efecto, si $\sqrt{6} = a + b\sqrt{2}$, con $a, b \in \mathbf{Q}$, elevando al cuadrado, $6 = a^2 + 2b^2 + 2ab\sqrt{2}$. por tanto

$$\left\{ \begin{array}{l} 6 = a^2 + 2b^2 \\ 0 = 2ab \end{array} \right. ,$$

que se comprueba fácilmente que no tiene solución en $\mathbf{Q}$. Luego $[K : \mathbf{Q}(\sqrt{2})] = 2$. Atención: es un error muy frecuente afirmar que el polinomio $X^2 - 6$ es irreducible sobre $\mathbf{Q}(\sqrt{2})$ por el criterio de Eisenstein, cuando este criterio sólo lo podemos aplicar sobre $\mathbf{Q}$.

En resumen $[K : \mathbf{Q}] = 4$.

2) Una base de K sobre $\mathbf{Q}$ es $\{1, \sqrt{2}, \sqrt{6}, \sqrt{12} = 2\sqrt{3}\}$, por lo que es evidente que $\alpha \in K$, luego $\mathbf{Q}(\alpha) \subset K$. Expresamos las sucesivas potencias de α en términos de esta base:

	1	$\sqrt{2}$	$\sqrt{6}$	$2\sqrt{3}$
$\alpha^0 = 1$	1	0	0	0
$\alpha = \sqrt{2} + \sqrt{3}$	0	1	0	$\frac{1}{2}$
$\alpha^2 = 5 + 2\sqrt{6}$	5	0	2	0

Como

$$\text{rango} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{2} \\ 5 & 0 & 2 & 0 \end{pmatrix} = 3,$$

las tres potencias $\{1, \alpha, \alpha^2\}$ son linealmente independientes sobre $\mathbf{Q}$, luego no hay una combinación lineal no trivial, con coeficientes en $\mathbf{Q}$, igual a 0. Por tanto $[\mathbf{Q}(\alpha) : \mathbf{Q}] > 2$. Pero por la fórmula del grado, $[\mathbf{Q}(\alpha) : \mathbf{Q}]|4$, luego $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4 = [K : \mathbf{Q}]$, y por tanto $K = \mathbf{Q}(\alpha)$. Atención: el ejercicio no pide calcular el polinomio mínimo de α sobre $\mathbf{Q}$.

3) Para ver que $K|\mathbf{Q}$ es una extensión normal, basta ver que K es el cuerpo de descomposición de $f(X) = (X^2 - 2)(X^2 - 6)$ sobre $\mathbf{Q}$, (porque K contiene a todas las raíces de f, siendo el mínimo de entre los que las contienen) y, además, f es separable, porque $X^2 - 2$ y $X^2 - 6$ tienen todas sus raíces distintas.

4) Para cada $\sigma \in G(K|\mathbf{Q})$ se tiene que $\sigma(\sqrt{2}) = \pm\sqrt{2}$ y $\sigma(\sqrt{6}) = \pm\sqrt{6}$. Por el apartado 1), $|G(K|\mathbf{Q})| = [K : \mathbf{Q}] = 4$. Por tanto, si $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, se tienen las cuatro posibilidades:

$$\begin{array}{ll} \sigma_1(\sqrt{2}) = \sqrt{2}, & \sigma_1(\sqrt{6}) = \sqrt{6} \\ \sigma_2(\sqrt{2}) = -\sqrt{2}, & \sigma_2(\sqrt{6}) = \sqrt{6} \\ \sigma_3(\sqrt{2}) = \sqrt{2}, & \sigma_3(\sqrt{6}) = -\sqrt{6} \\ \sigma_4(\sqrt{2}) = -\sqrt{2}, & \sigma_4(\sqrt{6}) = -\sqrt{6} \end{array} .$$