**RELACIÓN DE PROBLEMAS DE ÁLGEBRA.**
**CURSO 2005/2006**

## GRUPOS. SUBGRUPOS. TEOREMA DE LAGRANGE. APLICACIONES.

**Ejercicio 1.**– Sea $G$ un grupo finito de orden par. Pruebe que el número de elementos de $G$ de orden 2 es impar y, por tanto, que $G$ contiene un elemento de orden 2.

**Ejercicio 2.**– Sea $G$ un grupo y $n$ un entero positivo.

(1). Si el orden de todo elemento de $G$ es un divisor de $n$, estudie si el orden de $G$ es forzosamente un divisor de $n$.

(2). Si $G$ es finito y su orden es un múltiplo de $n$, estudie si $G$ contiene necesariamente un elemento de orden $n$.

**Ejercicio 3.**– Sea $G$ un grupo y $H_1, H_2, H_3$ subgrupos de $G$. Pruebe que

$$H_1 \cdot (H_2 \cap H_3) \subset (H_1 \cdot H_2) \cap (H_1 \cdot H_3).$$

**Ejercicio 4.**– Sea $G$ un grupo finito, y sean $H$ y $K$ subgrupos de $G$ con índices (en $G$) primos entre sí. Pruebe que $G = H \cdot K$.

**Ejercicio 5.**– Sean $C_n$ y $C_m$ grupos cíclicos de órdenes $n$ y $m$, respectivamente. Pruebe que $C_n \times C_m$ es un grupo cíclico si y sólo si $\mathrm{mcd}(n, m) = 1$.

**Ejercicio 6.**– Sea $S(P)$ el grupo de simetría de un polígono regular $P$ de $n$ lados, esto es, el conjunto de todos los movimientos del plano que dejan $P$ invariante. Demuestre que podemos hallar dos elementos $\sigma$ y $\tau$ que verifican:

(1). $S(P) = \langle \sigma, \tau \rangle$.

(2). $o(\sigma) = 2$, $o(\tau) = n$.

(3). $\sigma\tau = \tau^{-1}\sigma$.

**Ejercicio 7.**– Sea $G$ un grupo. Pruebe que son equivalentes:

(1). $G$ es abeliano.

(2). $(ab)^2 = a^2b^2$, para cualesquiera $a, b \in G$.

(3). $b^{-1}a^{-1}ba = 1$, para cualesquiera $a, b \in G$.

**Ejercicio 8.**– Pruebe que la unión de dos subgrupos de un grupo $G$ es un subgrupo de $G$ si y sólo si uno de los subgrupos contiene al otro. Pruebe que un grupo nunca es unión de dos subgrupos propios.

**Ejercicio 9.**– Los grupos que aparecen en este ejercicio se entienden como subgrupos de $(\mathbb{Q}, +)$. Sean $a, b, m, n \in \mathbb{Z}$ con $1 = \mathrm{mcd}(a, m) = \mathrm{mcd}(b, n)$, $d = \mathrm{mcd}(a, b)$ y $e = \mathrm{mcm}(m, n)$. Pruebe:

(1). $\langle 1/a, 1/b \rangle = \langle d/(ab) \rangle$.

(2). $\langle a/m, b/n \rangle = \langle d/e \rangle$.

(3). Todo subgrupo de $\mathbb{Q}$ finitamente generado es cíclico.

**Ejercicio 10.**– Sea $G$ un grupo tal que todo elemento tiene orden 2. Entonces $G$ es abeliano.

**Ejercicio 11.**– Pruebe que un grupo es finito si y sólo si contiene un número finito de subgrupos (Idea: Pruébelo primero para grupos cíclicos).

**Ejercicio 12.**– Sean $A, B \in GL(2,\mathbb{R})$ dadas por

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Sea $G = \langle A, B\rangle \subset GL(2,\mathbb{R})$.

(1). Calcule los grupos $\langle A\rangle$ y $\langle B\rangle$.

(2). Calcule todos los posibles productos de la forma $A^n B^m$, con $n, m > 0$.

(3). Pruebe que todo producto de la forma $B^p A^q$, con $p, q > 0$ se puede escribir de la forma $A^n B^m$.

(4). Pruebe que todo producto de la forma $A^{n_1} B^{m_1} ... A^{n_p} B^{m_p}$ se puede escribir de la forma $A^n B^m$.

(5). Pruebe (no es necesario hacer cálculos) que

$$G = \left\{I, A, A^2, A^3, A^4, A^5, B, AB, A^2B, A^3B, A^4B, A^5B\right\}.$$

(6). Halle los órdenes de los elementos de $G$. Pruebe que $G$ no contiene subgrupos cíclicos de orden 4.

(7). Halle todos los subgrupos de $G$ de orden primo.

(8). Pruebe que todo subgrupo de $G$ de orden 4 contiene a $A^3$.

**Ejercicio 13.**– Escriba la tabla de una operación binaria en el conjunto $A = \{a, b, c, d\}$ de manera que no exista ningún subconjunto propio (es decir, distinto de $A$) que sea estable por la operación.

**Ejercicio 14.**– Sabemos que en un grupo, el simétrico de cada elemento es único (para demostrarlo hemos de utilizar la asociatividad de la operación). Escriba la tabla de una operación binaria en el conjunto $A = \{a, b, c, d\}$ de manera que $a$ sea elemento neutro y algún elemento tenga dos simétricos distintos.

**Ejercicio 15.**– Dado un conjunto $A$, consideremos el conjunto $B = \{f : A \longrightarrow A \mid f \text{ es una aplicación}\}$ con la operación binaria dada por la composición de aplicaciones. Sabemos que dicha operación posee como elemento neutro a la aplicación identidad $\mathrm{id}_A$. Pruebe que un elemento $f$ de $B$ posee simétrico si y sólo si $f$ es una aplicación biyectiva.

**Ejercicio 16.**– Sea $G$ un grupo y $H \subset G$ un subgrupo cuyo índice $i(H, G)$ es un número primo $p$. Pruebe que $H$ es un subgrupo propio maximal de $G$, es decir, que el único subgrupo de $G$ distinto de $H$ que contiene a $H$ es el propio $G$.

**Ejercicio 17.**– Escriba las tablas de un grupo cíclico $C_2$ con dos elementos, de un grupo cíclico $C_3$ con tres elementos, así como de los productos cartesianos $C_2 \times C_2$ y $C_2 \times C_3$. ¿Son cíclicos estos dos últimos grupos? Conteste razonadamente.

**Ejercicio 18.**– Sea $G = \langle a\rangle$ un grupo cíclico finito de orden $m$.

(1). Si $H$ es subgrupo de $G$, entonces $H$ es cíclico o $H = \{1\}$. Si $H = \langle a^l\rangle$, con $l = \min\{k | a^k \in H\}$ entonces $l$ divide a $m$ y $|H| = m/l$.

(2). Si $k$ divide a $m$ entonces $K = \langle a^k\rangle$ es de orden $m/k$.

(3). El número de subgrupos distintos de $G$ es el mismo que el número de divisores distintos de $m$.

(4). Existe a lo sumo un subgrupo de $G$ de cualquier orden dado.

**Ejercicio 19.**– Pruebe que todo subgrupo $H$ de un grupo cíclico $G$ es también cíclico. ¿Qué se puede decir de $G/H$?

**Ejercicio 20.**– Calcule el orden del elemento $18+\mathbb{Z}24$ en $\mathbb{Z}/\mathbb{Z}24$. Calcule el orden del elemento $(4+\mathbb{Z}12, 2+\mathbb{Z}8) \in \mathbb{Z}/\mathbb{Z}12 \times \mathbb{Z}/\mathbb{Z}8$. Calcule los elementos de orden finito del grupo $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z} \times \mathbb{Z}/\mathbb{Z}4$.

**Ejercicio 21.**– Sea $G$ un grupo, $g \in G$ y definimos una nueva multiplicación $\cdot$ sobre $G$ por la fórmula $a \cdot b = agb$ para todo $a, b \in G$. Pruebe que $G$ con la operación $\cdot$ es un grupo.

**Ejercicio 22.**– Pruebe que $\mathbb{R}^* \times \mathbb{R}$ es un grupo con la operación definida por

$$(a, b)(c, d) = (ac, ad + b).$$

¿Es abeliano?

**Ejercicio 23.**– Sea $V \subset \mathrm{GL}_2(\mathbb{R})$ el conjunto

$$V = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Pruebe que $V$ es un subgrupo de $\mathrm{GL}_2(\mathbb{R})$.

**Ejercicio 24.**– Sean $b_0, m_0$ y $n_0$ enteros positivos y consideremos el conjunto $S \subset \mathrm{GL}_3(\mathbb{Z})$ definido por

$$S = \left\{ \begin{pmatrix} 1 & m & n \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : m_0|m, n_0|n, b_0|b \right\}.$$

¿Cuándo es $S$ un subgrupo?

**Ejercicio 25.**– Sea $G$ un grupo que tiene ocho elementos, que notaremos por los números $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Supongamos que el producto de $v, w \in G$ lo escribimos como $v * w$ y que se verifica

- $v * w \leq v + w$ para todo $v, w \in G$.
- $v * v = 0$ para todo $v \in G$.

Reconstruya la tabla de multiplicación de $G$.

**Ejercicio 26.**– Sea $c$ una constante real positiva y $v$ un número con $-c < v < c$. Consideremos la matriz

$$A(v) = \lambda(v) \begin{pmatrix} 1 & -v \\ -v/c^2 & 1 \end{pmatrix},$$

donde $\lambda(v) = \left(\sqrt{1 - \frac{v^2}{c^2}}\right)^{-1}$.

(1). Pruebe que

$$A(v_1)A(v_2) = A(v_3)$$

donde

$$v_3 = \frac{v_1 + v_2}{1 + \frac{v_1 v_2}{c^2}}.$$

(2). Use lo anterior para demostrar que la multiplicación de matrices induce una estructura de grupo en el conjunto

$$G = \{A(v) | -c < v < c\}.$$

Este grupo se denomina *grupo de Lorentz*.

**Ejercicio 27.**– En $G = \mathrm{GL}_2(\mathbb{R})$ consideremos las matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Pruebe que $A$ tiene orden 3, $B$ tiene orden 4 y que $AB$ tiene orden infinito.

**Ejercicio 28.**– Pruebe que si $G$ es un grupo no abeliano, entonces tiene al menos orden seis.

**Ejercicio 29.**– Sean $n, m$ números enteros. Pruebe que

(1). $\langle n \rangle = \mathbb{Z}n$.

(2). $\mathbb{Z}n + \mathbb{Z}m = \langle n, m \rangle = \mathbb{Z}d$, donde $d = \text{mcd}(m, n)$.

(3). $\mathbb{Z}n \cap \mathbb{Z}m = \mathbb{Z}k$, donde $k = \text{mcm}(m, n)$.

**Ejercicio 30.**– Sea $G$ un grupo, y $a \in G$.

(1). Si $a$ tiene orden finito, entonces $a^{-1}$ también y $o(a^{-1}) = a$.

(2). Si $a$ tiene orden infinito entonces $a^{-1}$ tiene orden infinito.

(3). Si $o(a) = n$ y $a^m = 1$ entonces $n$ divide a $m$.

## NORMALIDAD. COCIENTES. HOMOMORFISMOS. TEOREMAS DE ISOMORFÍA.

**Ejercicio 31.**– Sea $G$ un grupo. Pruebe que la intersección arbitraria de subgrupos normales de $G$ es un subgrupo normal de $G$.

**Ejercicio 32.**– Sea $G$ un grupo y $d$ un entero positivo. Supongamos que $G$ posee un único subgrupo $H$ de orden $d$. Demuestre que $H$ es normal.

**Ejercicio 33.**– Halle todos los subgrupos del grupo de simetría del cuadrado, indicando cuáles son normales.

**Ejercicio 34.**– Sea $n$ un entero positivo. Denotaremos

$$U_n = \{i + \mathbb{Z}n \mid 0 \leq i \leq n-1, \text{ tales que existe } j \in \mathbb{Z} \text{ con } ij + \mathbb{Z}n = 1 + \mathbb{Z}n\}.$$

Pruebe que $U_n$ es un grupo con el producto (definido de la manera natural en $\mathbb{Z}/\mathbb{Z}n$). Halle todos los subgrupos de $U_{16}$.

**Ejercicio 35.**– Sea $f : \mathbb{R} \longrightarrow \mathbb{C}^*$ la aplicación dada por $f(x) = \cos x + i\text{sen}x$. Pruebe que $f$ es un homomorfismo de grupos y calcule su núcleo e imagen.

**Ejercicio 36.**– Estudie cuántos endomorfismos de $\mathbb{Z}$ existen. Estudie cuántos homomorfismos existen entre $\mathbb{Z}$ y $\mathbb{Z}/\mathbb{Z}2$, así como entre $\mathbb{Z}$ y $\mathbb{Z}/\mathbb{Z}8$.

**Ejercicio 37.**– Sea $G$ un grupo, $C(G)$ su centro. Pruebe que $C(G)$ es un subgrupo normal de $G$. Si $H$ es un subgrupo de $C(G)$, pruebe que $H$ es normal en $G$. De manera más general, estudie si un subgrupo normal de un subgrupo normal es normal en el total.

**Ejercicio 38.**– Sea $G$ un grupo generado por la familia $\{a_i \mid i \in I\}$. Sea $f : G \longrightarrow G'$ un homomorfismo de grupos y $H = \langle h_j \mid j \in J \rangle$ un subgrupo de $G$. Pruebe que:

(1). El homomorfismo $f$ está completamente determinado por su acción sobre los $a_i$.

(2). Supongamos que las familias $\{a_i\}$ y $\{h_j\}$ son cerradas para la inversión de elementos. Entonces el subgrupo $H$ es normal si y sólo si $a_i h_j a_i^{-1} = H$ para todo $i \in I$ y para todo $j \in J$.

**Ejercicio 39.**– Sea el conjunto

$$G = \left\{ f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R} \mid (a, b) \in \mathbb{R}^2, \ a \neq 0 \right\},$$

donde $f_{a,b}(x) = ax + b$. Se pide:

(1). Pruebe que $G$ es un grupo con la composición de aplicaciones.

(2). Pruebe que la aplicación $F : G \longrightarrow G$ dada por $F(f_{a,b}) = f_{a,0}$ es un homomorfismo de grupos. Halle el núcleo y la imagen del homomorfismo $F$.

**Ejercicio 40.**– Sea $G$ un grupo y $H$ un subgrupo normal de orden 2 tal que $G/H$ es cíclico. Pruebe que $G$ es abeliano. Si $G = S_3$ y $H = (12)$, ¿cuáles de las condiciones anteriores se verifican?

**Ejercicio 41.**– Si $H$ es un subgrupo de $G$ de índice 2, entonces $H$ es normal en $G$.

**Ejercicio 42.**– Sea $G$ un grupo y $L$ un subgrupo normal de $G$. Si $L$ y $G/L$ son abelianos, ¿podemos concluir que $G$ es abeliano?

**Ejercicio 43.**– Sea $f : G \to G'$ un epimorfismo de grupos y pongamos $N = \ker(f)$. La correspondencia $H \mapsto f(H)$ define una biyección entre el conjunto de subgrupos de $G$ que contienen a $N$ y el conjunto de subgrupos de $G'$, que conserva la normalidad.

**Ejercicio 44.**– Sea $G$ un grupo y $H$ un subgrupo abeliano de $G$ tal que $H \cdot C(G) = G$, donde $C(G)$ denota el centro de $G$. Demuestre que $G$ es abeliano. Concluya que $G$ es abeliano si y sólo si $G/C(G)$ es cíclico.

**Ejercicio 45.**– Sea $H$ un subgrupo cíclico finito de $G$ y $H \lhd G$. Sea $K = \langle b \rangle$ un subgrupo propio de $H$.

(1). Si $g \in G$ entonces $o(b) = o(g^{-1}bg)$.

(2). Si $g \in G$ entonces $\langle g^{-1}bg \rangle = K$.

(3). Deduzca que $K \lhd G$.

**Ejercicio 46.**– Sea $f : G \to K$ un homomorfismo sobreyectivo, con $K$ grupo cíclico de orden 10. Pruebe que $G$ tiene subgrupos normales de índices $2, 5$ y $10$.

**Ejercicio 47.**– Sea $G$ un grupo y $H$ el subgrupo de $G$ generado por los elementos de la forma $g^2$, con $g \in G$. Pruebe que $H \lhd G$.

**Ejercicio 48.**– Sea $f : G \to K$ un homomorfismo de grupos, con $G$ finito. Entonces $|\operatorname{im}(f)|$ divide a $|G|$.

**Ejercicio 49.**– Sea $G$ un grupo, $H$ un subgrupo y $M, N$ subgrupos normales de $G$ tales que $H \cap M = H \cap N$. Pruebe que $HM/M$ es isomorfo a $HN/N$.

**Ejercicio 50.**– Sean $\{1\} \subset G_1 \subset G$ y $G_1 \lhd G$, con $G/G_1$ y $G_1$ grupos abelianos. Sea $H$ un subgrupo cualquiera de $G$. Demuestre que $H_1 = H \cap G_1$ es normal en $H$ y que $H/H_1$ y $H_1$ son abelianos.

**Ejercicio 51.**– Sea $f : G \to K$ un homomorfismo de grupos, $S$ un subgrupo de $K$ y $H = f^{-1}(S)$. Demuestre que

(1). $H$ es subgrupo de $G$.

(2). $\ker(f) \subset H$.

(3). Si $S \lhd K$ entonces $H \lhd G$.

(4). Si $H_1$ es un subgrupo de $G$ tal que $\ker(f) \subset H_1$ y $f(H_1) = S$ entonces $H_1 = H$.

**Ejercicio 52.**– Sea $G$ un grupo finito de orden impar y $x \in G$. Demuestre que existe $y \in G$ tal que $x = y^2$.

**Ejercicio 53.**– Sea $H$ un subgrupo normal de orden dos de un grupo $G$. Pruebe que $H \subset C(G)$.

**Ejercicio 54.**– Sea $H \lhd G$ y supongamos que $G/H$ es abeliano. Pruebe que todo subgrupo $K \subset G$ que contiene a $H$ es normal.

**Ejercicio 55.**– Encuentre todos los subgrupos de $(\mathbb{Z}/\mathbb{Z}2)^3$, indicando los que son normales y hallando los cocientes, en esos casos.

**Ejercicio 56.**– Encuentre todos los subgrupos de orden 4 del grupo $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}4$.

**Ejercicio 57.**– Sea $G$ un grupo finito y $K \subset H \subset G$ subgrupos. Pruebe que $i(H:G)i(K:H) = i(K:G)$.

**Ejercicio 58.**–

(1). Sea $H = \langle (0+\mathbb{Z}4, 1+\mathbb{Z}6) \rangle \subset G = \mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}6$. Establezca, si es posible, un isomorfismo entre $G/H$ y $\mathbb{Z}/\mathbb{Z}4$.

(2). Sea $H = \langle (0+\mathbb{Z}4, 2+\mathbb{Z}6) \rangle \subset G = \mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}6$. Establezca, si es posible, un isomorfismo entre $G/H$ y $\mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}2$.

(3). Sea $H = \langle (2+\mathbb{Z}4, 3+\mathbb{Z}6) \rangle \subset G = \mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}6$. Establezca, si es posible, un isomorfismo entre $G/H$ y $\mathbb{Z}/\mathbb{Z}12$.

**Ejercicio 59.**– Recordemos que

$$U_n = \{ i + \mathbb{Z}n \mid 0 \leq i \leq n-1, \text{ tales que existe } j \in \mathbb{Z} \text{ con } ij + \mathbb{Z}n = 1 + \mathbb{Z}n \}.$$

Calcule todos los subgrupos de $U_{15}$, indicando cuáles son normales.

**Ejercicio 60.**– Halle el grupo de simetría de la figura formada por los ejes coordenados del plano euclídeo. Obtenga todos los subgrupos, indicando los que son normales.

**Ejercicio 61.**– Sea $G$ un grupo, $H$ y $K$ subgrupos de $G$. Se dice que $G$ es producto directo interno de $H$ y $K$ si $\Phi : H \times K \to G$ dada por $\Phi(h,k) = hk$ es un isomorfismo de grupos. Pruebe que $G$ es producto directo interno de $H$ y $K$ si y sólo si:

(1). $G = HK$

(2). $hk = kh$ para todo $h \in H$ y $k \in K$.

(3). $H \cap K = \{1\}$.

**Ejercicio 62.**– Usando el ejercicio anterior pruebe que $S_3$ no es producto directo interno de 2 de sus subgrupos.

**Ejercicio 63.**– Sea $G$ un grupo y $f : G \to G$ un homomorfismo de grupos tal que $f \circ f = f$. Sean $H = \ker(f)$ y $K = \mathrm{im}(f)$. Pruebe que:

(1). Para todo $x \in G$, $xf(x)^{-1} \in H$. Deduzca que $G = H \cdot K$.

(2). $H \cap K = \{1\}$.

(3). Si $K \lhd G$, entonces la aplicación $f : H \times K \to H \cdot K$ definida por $f(h,k) = hk$ es un isomorfismo de grupos.

**Ejercicio 64.**– Sea $n = rs$, donde $r$ y $s$ son primos entre sí. Pruebe que $\mathbb{Z}/\mathbb{Z}n$ es producto directo interno de sus subgrupos cíclicos $\langle r + \mathbb{Z}n \rangle$ y $\langle s + \mathbb{Z}n \rangle$.

**Ejercicio 65.**– Pruebe que $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}/\mathbb{Z}2$.

**Ejercicio 66.**– Calcule todos los homomorfismos de grupos de $\mathbb{Z}$ en $\mathbb{Z}/\mathbb{Z}n$. Calcule todos los homomorfismos de grupos de $\mathbb{Z}/\mathbb{Z}7$ en $\mathbb{Z}/\mathbb{Z}16$.

**Ejercicio 67.**– En $D_{12} = \langle \sigma, \tau |\ \tau^6 = \mathrm{id}, \sigma^2 = \mathrm{id}, \tau^{-1}\sigma = \sigma\tau \rangle$, consideremos los subgrupos $H = \langle \tau^2, \sigma \rangle, K = \langle \tau^3 \rangle$. Pruebe que $H$ y $K$ son normales en $D_{12}$, que $H \cap K = \{\mathrm{id}\}$ y $D_{12} \simeq H \times K$.

**Ejercicio 68.**– Sea

$$G = \{ \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} | n \in \mathbb{Z} \}.$$

Pruebe que $G$ es subgrupo de $\mathrm{GL}_2(\mathbb{R})$. ¿Es isomorfo a $\mathbb{Z}$?

**Ejercicio 69.**– Sea $D_8 = \{\sigma, \tau | \sigma^2 = 1, \tau^4 = 1, \tau^{-1}\sigma = \sigma\tau\} = \{1, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\}$, y $Q_8 = \{a, b | a^2 = b^2, a^4 = 1, ab = ba^3\} = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$. Pruebe que $D_8 \not\simeq Q_8$.

**Ejercicio 70.**– Sea $G$ un grupo. Pruebe que las aplicaciones definidas por

$$\begin{array}{ccc} G & \to & G \\ g & \mapsto & g^{-1} \end{array}, \quad \begin{array}{ccc} G & \to & G \\ g & \mapsto & g^2 \end{array}$$

son homomorfismos de grupos si y solamente si $G$ es abeliano.

**Ejercicio 71.**– Sea $C_n$ el grupo cíclico de orden $n$. Para cada $a \in \mathbb{Z}$ definimos

$$\begin{array}{rcl} \sigma_a : C_n & \to & C_n \\ x & \mapsto & \sigma_a(x) = x^a \end{array}$$

(1). Pruebe que $\sigma_a \in \mathrm{Aut}(C_n)$ si y solamente si $\mathrm{mcd}(a, n) = 1$.

(2). $\sigma_a = \sigma_b$ si y solamente si $n$ divide a $a - b$.

(3). Pruebe que $\sigma_a \circ \sigma_b = \sigma_{ab}$ para todo $a, b \in \mathbb{Z}$.

**Ejercicio 72.**– Sea $G = \mathbb{Z}/\mathbb{Z}24$ y $\tilde{G} = G/\langle\overline{12}\rangle$. Para cada entero $a$ simplificamos la notación $\tilde{\bar{a}}$ como $\tilde{a}$.

(1). Pruebe que $\tilde{G} = \{\tilde{0}, \tilde{1}, \ldots, \tilde{11}\}$.

(2). Calcule el orden de cada elemento de $\tilde{G}$.

(3). Pruebe que $\tilde{G} \simeq \mathbb{Z}/\mathbb{Z}12$.

**Ejercicio 73.**– En $D_8 = \{\mathrm{id}, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\}$, con $\sigma\tau = \tau^{-1}\sigma$, consideremos los subgrupos $H = \langle\sigma\rangle, K = \langle\sigma, \tau^2\rangle$.

(1). Pruebe que $K \lhd D_8, H \lhd K$ pero que $H$ no es normal en $D_8$.

(2). Calcule todos los subgrupos de $D_8$, e indique cuáles son normales.

**Ejercicio 74.**– Pruebe que un subgrupo $H \subset G$ es normal si y sólo si para cada $x \in G$ y para cada $h \in H$ se verifica que $[x, h] = xhx^{-1}h^{-1} \in H$.

**Ejercicio 75.**–

(1). Sea $S \subset G$ un subconjunto tal que $xSx^{-1} \subset \langle S\rangle$ para todo $x \in G$. Pruebe que $\langle S\rangle \lhd G$.

(2). Sea $n \in \mathbb{N}$, $H_n = \langle\{x^n : x \in G\}\rangle$. Pruebe que $H_n \lhd G$.

(3). Si $n \in \mathbb{N}$, pruebe que $\{x^n : x \in D_8\}$ es un subgrupo normal de $D_8$. ¿Ocurre lo mismo con $D_6$?

**Ejercicio 76.**– Sea $G = \langle A, B\rangle \subset \mathrm{GL}_2(\mathbb{Z}/\mathbb{Z}3)$, con

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Deduzca razonadamente si $G$ es isomorfo a $D_8$ o a $Q_8$.

## PERMUTACIONES. EL GRUPO ALTERNADO.

**Ejercicio 77.**– Dadas las siguientes permutaciones de $S_7$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 2 & 1 \end{pmatrix}, \ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 3 & 2 & 4 & 6 \end{pmatrix},$$

se pide:

(1). Halle todos los posibles productos de dos, tres y cuatro $\sigma_i$ (distintas entre sí).

(2). Descomponga las permutaciones $\sigma_i$ y las halladas en (1) como producto de ciclos disjuntos.

(3). Halle las inversas de las permutaciones $\sigma_i$ y de las halladas en (1).

(4). Descomponga las permutaciones $\sigma_i$ y las halladas en (1) como producto de trasposiciones.

(5). Halle los índices de las permutaciones $\sigma_i$ y de las halladas en (1).

**Ejercicio 78.**– Calcule los subgrupos normales de $A_3, S_3, A_4, S_4$.

**Ejercicio 79.**– Halle el centro de $S_n$.

**Ejercicio 80.**– Sean, en $S_n$, una permutación $\sigma$ y un ciclo $(i_1...i_k)$. Determine el conjugado del ciclo por $\sigma$, esto es, $\sigma(i_1...i_k)\sigma^{-1}$.

**Ejercicio 81.**– Se denomina un partición de un número $n$ a un sucesión de enteros $n_1, ..., n_k$ verificando

$$1 \leq n_i \leq n_{i+1} \leq n,\ \forall i = 1, ..., k,\ \text{y}\ \sum n_i = n.$$

(1). Demuestre que toda permutación de $S_n$ induce de manera natural un partición de $n$.

(2). Dos permutaciones $\sigma, \sigma' \in S_n$ se dicen conjugadas si existe $\tau \in S_n$ tal que $\tau\sigma\tau^{-1} = \sigma'$. Pruebe que dos permutaciones son conjugadas si y sólo si inducen la misma partición de $n$.

**Ejercicio 82.**– Sea $n \geq 2$ un entero y definimos la aplicación $\varphi : S_n \longmapsto S_{n+2}$ que lleva $\sigma$ en $\varphi(\sigma)$, donde

$$\begin{array}{lll} \varphi(\sigma)(i) = \sigma(i), & \text{cuando} & 1 \leq i \leq n \\ \varphi(\sigma)(n+1) = n+1, \varphi(\sigma)(n+2) = n+2 & \text{cuando} & \epsilon(\sigma) = 1 \\ \varphi(\sigma)(n+1) = n+2, \varphi(\sigma)(n+2) = n+1 & \text{cuando} & \epsilon(\sigma) = -1 \end{array}$$

(1). Halle $\varphi(5\,3\,8\,6\,7\,4\,1\,2) \in S_{10}$ y calcule su descomposición en ciclos disjuntos.

(2). Pruebe que $\varphi$ es un monomorfismo de grupos.

(3). Pruebe que la imagen de $\varphi$ está contenida en $A_{n+2}$.

**Ejercicio 83.**– Pruebe que todo grupo finito es isomorfo a un subgrupo de un grupo alternado.

**Ejercicio 84.**– Estudie los subgrupos normales que puede haber en $S_n$.

**Ejercicio 85.**– Una permutación se dice regular si todos los ciclos que aparecen en su descomposición tienen la misma longitud. Pruebe que una permutación es regular si y sólo si es potencia de un ciclo.

**Ejercicio 86.**– Pruebe que existe un monomorfismo $i : S_n \times S_m \hookrightarrow S_{m+n}$.

**Ejercicio 87.**– Sean los subconjuntos de $S_4$ dados por

$$H = \langle (1\,2\,4\,3), (2\,3) \rangle,$$

$$K = \{1, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (2\,4), (1\,4)(2\,3), (1\,3), (1\,2)(4\,3)\}.$$

(1). Pruebe que $K$ es un subgrupo de $S_4$.

(2). Construir los subgrupos de $K$, señalando cuáles son normales.

(3). Dé, razonadamente, todos los elementos de $H$.

(4). Pruebe que $H \cap K$ es un subgrupo normal de $K$.

**Ejercicio 88.**– Razone por qué no se puede dar un monomorfismo de $C_2 \times C_2$ en $S_3$.

**Ejercicio 89.**– Construya un monomorfismo de $C_6$ en $S_5$.

**Ejercicio 90.**– Halle el número de ciclos de longitud 3 y 5 que hay en $S_5$. Pruebe que un subgrupo de $A_5$ que no contenga ciclos (distintos de 1) no puede tener más de quince elementos.

**Ejercicio 91.**– Denominaremos soporte de $\tau \in S_n$ a los $i \in \{1, ..., n\}$ tales que $\tau(i) \neq i$. Sea $t$ una trasposición. Pruebe que la aplicación $\varphi : S_n \longrightarrow S_n$ definido por $\varphi(\sigma) = t\sigma t^{-1}$ es un automorfismo que deja invariante $A_n$. Determine el conjunto de ciclos que quedan invariantes por $\varphi$ en función de los soportes del ciclo y de $t$.

**Ejercicio 92.**– Describa, explícitamente, $D_{10}$ como subgrupo de $S_5$.

**Ejercicio 93.**– Sea $n \geq 3$

(1). Calcule $(1\ i)(1\ j)(1\ i)$; $(i-1\ i)(1\ i-1)(i-1\ i)$; $(1\ 2\ \ldots n)(i-1\ i)(1\ 2\ \ldots n)^{-1}$, siendo $2 \leq i, j \leq n$ distintos.

(2). Demuestre que $S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n)\rangle = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n)\rangle = \langle (1\ 2\ \ldots n), (1\ 2)\rangle$.

**Ejercicio 94.**– Sea $G$ un grupo de orden 6.

(1). Si $G$ es no abeliano entonces $G$ es isomorfo a $S_3$.

(2). Si $G$ es abeliano entonces $G$ es isomorfo a $C_6$.

**Ejercicio 95.**– Consideremos en $S_7$ la permutación

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

Calcule la descomposición en ciclos disjuntos de $\sigma, \sigma^2, \sigma^{-1}$. Calcule el orden de $\sigma, \sigma^2, \sigma^{-1}$.

**Ejercicio 96.**– En $S_{11}$, ¿cual es el mayor orden que puede tener un elemento?

**Ejercicio 97.**– Sea $\sigma$ el $m$-ciclo $(12\ldots m)$. Pruebe que $\sigma^i$ es un $m$-ciclo si y solamente si $\text{mcd}(i, m) = 1$.

**Ejercicio 98.**–

(1). Si $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$, determine si existe un $n$-ciclo $\sigma (n \geq 10)$ tal que $\tau = \sigma^k$ para algún entero $k$.

(2). Si $\tau = (1\ 2)(3\ 4\ 5)$, determine si existe un $n$-ciclo $\sigma (n \geq 5)$ tal que $\tau = \sigma^k$ para algún entero $k$.

**Ejercicio 99.**– Sea $n \geq 3$.

(1). Compruebe que $(i\ j)(j\ k) = (i\ j\ k)$, $(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l)$, $(i\ j\ k) = (1\ i\ j)(1\ j\ k)$, $(1\ i\ j) = (1\ 2\ j)(1\ 2\ i)^2$, siendo todos los índices distintos.

(2). Pruebe que $A_n$ está generado por los 3-ciclos.

(3). Pruebe que $A_n = \langle (1\ 2\ i), i = 3, \ldots, n\rangle$.

**Ejercicio 100.**–

(1). Si $n \geq 4$, $3 < j \leq n$, calcule $(3\ 2\ j)(1\ 2\ 3)^2(3\ 2\ j)^{-1}$.

(2). Sea $N \lhd A_n$ para $n \geq 3$. Con el ejercicio anterior, pruebe que si $N$ contiene un 3-ciclo entonces $N = A_n$.

**Ejercicio 101.**– Pruebe que $A_4$ no tiene subgrupos de orden 6, usando ejercicios anteriores.

**Ejercicio 102.**–

(1). Sean $\sigma = (1\ 2\ \ldots r)\sigma'$, $r \geq 4$, $\sigma'$ producto de ciclos disjuntos que no tienen elementos en $\{1, 2, \ldots, r\}$, y $\tau = (1\ 2\ 3)$. Calcule $[\tau, \sigma]$.

(2). Sean $\sigma = (1\ 2\ 3)(4\ 5\ 6)\sigma'$, $\sigma'$ producto de ciclos disjuntos que no tienen elementos en $\{1, 2, \ldots, 6\}$, y $\tau = (2\ 3\ 4)$. Calcule $[\tau, \sigma]$.

(3). Sean $\sigma = (1\ 2\ 3)\sigma'$, $\sigma'$ producto de trasposiciones disjuntas que no tienen elementos en $\{1, 2, 3\}$. Calcule $\sigma^2$.

(4). Sean $\sigma = (1\ 2)(3\ 4)\sigma'$, $\sigma'$ producto de trasposiciones disjuntas que no tienen elementos en $\{1, 2, 3, 4\}$, y $\tau = (2\ 3\ 4)$, $\rho = (1\ 4\ 5)$. Calcule $[\rho, [\tau, \sigma]]$.

(5). Si $n \geq 5$, demuestre que $A_n$ es simple, es decir, no tiene subgrupos normales propios.

**Ejercicio 103.**–

(1). Pruebe que un $r$-ciclo es par (impar) si y solamente si $r$ es par (impar).

(2). Pruebe que una permutación $\sigma$ es par si y solamente si existe un número para de ciclos de orden par en la descomposición de $\sigma$ en ciclos disjuntos.

(3). Pruebe que si un subgrupo $G$ de $S_n$ contiene una permutación impar entonces $G$ contiene un subgrupo normal $H$ tal que $i(H : G) = 2$.

**Ejercicio 104.**– Aplique la demostración dada del teorema de Cayley para encontrar un subgrupo de $S_n$ isomorfo al grupo cíclico $C_n$, para cada $n \geq 3$.

**Ejercicio 105.**– Aplique la demostración dada del teorema de Cayley para encontrar un subgrupo de $S_6$ isomorfo al grupo $S_3$.

**Ejercicio 106.**– Sea $H \subset S_n$ definido por $H = \{f \in S_n : f(1) = 1\}$. Pruebe que $H$ es un subgrupo de $S_n$ isomorfo a $S_{n-1}$. ¿Es $H$ normal en $S_n$?

**Ejercicio 107.**– Sea $H$ el subgrupo de $S_4$ generado por $\sigma = (1234)$ y $\tau = (12)(34)$, y $K$ el subgrupo de $H$ generado por $\sigma$. Pruebe que $K$ es un subgrupo normal de $H$. ¿Cuántos elementos tienen $K$ y $H/K$?

**Ejercicio 108.**– Sea $s > 2$ un número impar. Consideremos el conjunto

$$G = \{-1, 1\} \times \{0, 1, \ldots, s-1\},$$

con la operación

$$(e, x) * (f, y) = (ef, ey + x),$$

donde los productos y sumas internas se toman en $\mathbb{Z}/\mathbb{Z}s$.

(1). Pruebe que $(G, *)$ es un grupo.

(2). Calcule un isomorfismo de $G$ en $D_{2s}$, el grupo diédrico de orden $2s$.

(3). Sean $a, b \in \mathbb{Z}/\mathbb{Z}s$, con $a \neq 0$. Definimos la aplicación $\tau : D_{2s} \to D_{2s}$ como

$$\tau(e, x) = (e, e(a - x) + b).$$

Pruebe que $\tau$ es una aplicación biyectiva y que si $u, v \in D_{2s}$, con $u \neq v$ entonces $\tau(u) * v \neq \tau(v) * u$.

**Ejercicio 109.**– Pruebe que $S_3 \simeq \langle a, b : a^2 = 1, b^3 = 1, a^{-1}bab^{-2} = 1\rangle$.

**Ejercicio 110.**– En una máquina tenemos un panel con $n$ celdas, donde se muestra una permutación de $S_n$. Esta máquina cuenta con $n-1$ botones. El primer botón permite el intercambio del contenido de las celdas 1 y 2. El segundo botón realiza el intercambio del contenido de las celdas 2 y 3, y así hasta el botón $n-1$, que realiza el intercambio de las celdas $n-1$ y $n$. Queremos reordenar la permutación de partida de

tal forma que la celda con el número 1 se coloque en la primera posición, la celda con el número 2 en la segunda posición, y así con todas, con el uso de los botones que tiene el dispositivo. ¿Es posible conseguirlo?

**Ejercicio 111.**– Sea $G$ el subgrupo multiplicativo de $\mathrm{GL}_2(\mathbb{C})$ generado por

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(1). Pruebe que $A$ y $B$ satisfacen las relaciones $A^4 = I, A^2 = B^2, B^{-1}AB = A^{-1}$.

(2). Pruebe que $G \simeq Q_8$.

(3). Pruebe que todo subgrupo de $Q_8$ es normal.

**Ejercicio 112.**– Sea $G_n$ el subgrupo multiplicativo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

donde $\zeta = \exp(2\pi i/n)$. Verifique que $G_n$ es isomorfo a $D_{2n}$.

## GRUPOS RESOLUBLES.

**Ejercicio 113.**– Halle el grupo derivado del grupo alternado $A_4$.

**Ejercicio 114.**– Halle el grupo derivado del grupo $Q_8$ de los cuaternios.

**Ejercicio 115.**– Considere el grupo definido por

$$QD_{16} = \langle \sigma, \tau |\ \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle.$$

(1). Pruebe que $QD_{16}$ tiene 16 elementos.

(2). Pruebe que tiene tres subgrupos de orden 8, que son

$$H_1 = \langle \tau, \sigma^2 \rangle, H_2 = \langle \sigma \rangle, H_3 = \langle \sigma^2, \sigma\tau \rangle.$$

(3). Pruebe que $H_1 \simeq D_8, H_2 \simeq C_8, H_3 \simeq Q_8$.

(4). Pruebe que $QD_{16}$ es resoluble.

**Ejercicio 116.**– Sean $G_1$ y $G_2$ grupos resolubles. ¿Es $G_1 \times G_2$ un grupo resoluble?

**Ejercicio 117.**– Sea $G$ un grupo y $G' = [G, G]$ su subgrupo derivado. Llamamos abelianizado de $G$ al cociente $G^{ab} = G/G'$. Pruebe que, para cada grupo abeliano $H$ y para cada homomorfismo $f : G \to H$, existe un único homomorfismo $g : G^{ab} \to H$ tal que $f = g \circ \pi$, donde $\pi$ es el homomorfismo natural de $G$ sobre $G^{ab}$.

**Ejercicio 118.**– Sea $n \geq 3$.

(1). Calcule $[(i\ j), (i\ k)]$.

(2). Deduzca que $S_n' \supset A_n$.

(3). Compruebe que $[\sigma, \tau] \in A_n$ para todo $\sigma, \tau \in S_n$. Concluir que $S_n' = A_n$.

**Ejercicio 119.**– Calcule los subgrupos derivados $D_8'$ y $Q_8'$.

**Ejercicio 120.**– Sea $G$ un grupo, $H \lhd G$, tales que $H$ es resoluble y $G/H$ resoluble. Demuestre que $G$ es resoluble.

**Ejercicio 121.**– Sea $G$ un grupo abeliano finito de orden $n$ y $m$ un entero positivo. Sea $\varphi : G \longrightarrow G$ el endomorfismo de $G$ definido por $\varphi(x) = x^m$, para todo $x \in G$. Pruebe que $\varphi$ es un automorfismo de $G$ si y sólo si $\text{mcd}(n, m) = 1$. (Indicación: aplique el teorema de Cauchy).

## ANILLOS, CUERPOS.

**Ejercicio 122.**– Sean $I_1 = (S_1), I_2 = (S_2)$ ideales de un anillo $A$. Se definen las siguientes operaciones:

$$I_1 + I_2 = (I_1 \cup I_2), \;\; I_1 I_2 = (a_1 a_2 \mid a_j \in I_j), \;\; I_1 : I_2 = \{a \in A \mid \forall x \in I_2, \; ax \in I_1\}.$$

Se pide probar que

(A) $I_1 + I_2 = \{a_1 + a_2 \mid a_j \in I_j\}$.

(B) $I_1 I_2 = (S_1 S_2)$.

(C) $I_1 : I_2$ es un ideal.

(D) $I_1 \cap I_2$ es un ideal. Estudie si se puede generalizar este resultado a la intersección arbitraria de ideales.

**Ejercicio 123.**– Sean $n, m \in \mathbb{Z}_+$. Definimos $d = \text{mcd}(n, m)$, $l = \text{mcm}(m, n)$. Pruebe

$$\mathbb{Z}n + \mathbb{Z}m = \mathbb{Z}d, \;\; \mathbb{Z}n \cap \mathbb{Z}m = \mathbb{Z}l, \;\; (\mathbb{Z}n)(\mathbb{Z}m) = \mathbb{Z}nm, \;\; (\mathbb{Z}n) : (\mathbb{Z}m) = \mathbb{Z}(n/d).$$

**Ejercicio 124.**– Sea $f : R \longrightarrow S$ un homomorfismo de anillos.

(A) Si $I \subset R$ es un ideal, $f(I)$ no es necesariamente un ideal de $S$. Sí lo es cuando $f$ es sobreyectivo.

(B) Si $J \subset S$ es un ideal, $f^{-1}(J) \subset R$ es un ideal.

**Ejercicio 125.**– Se define el radical de un ideal $I$ como

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} \text{ con } x^n \in I\}.$$

Pruebe que

(1). $\sqrt{I}$ es un ideal.

(2). $\sqrt{I} \supset I$ .

(3). $\sqrt{\sqrt{I}} = \sqrt{I}$.

(4). El radical del ideal (0) se conoce como nilradical y se denota por $\text{Nil}(A)$. Estudie el nilradical de un dominio de integridad.

**Ejercicio 126.**– Sea $n \in \mathbb{Z}$, $q|n$. Pruebe que $(\mathbb{Z}/\mathbb{Z}n)/(q + \mathbb{Z}n) \simeq \mathbb{Z}/\mathbb{Z}q$.

**Ejercicio 127.**– Sean $A$ y $B$ dos anillos. Pruebe que el conjunto $A \times B$ admite una estructura natural de anillo. Si $U_A$ y $U_B$ son los respectivos conjuntos de unidades, pruebe que $U_A \times U_B$ es el conjunto de unidades de $A \times B$.

**Ejercicio 128.**– Dados dos anillos $A$ y $B$, pruebe que todos los ideales de $A \times B$ son de la forma $I \times J$ con $I \subset A$, $J \subset B$ ideales. Encuentre todos los ideales de $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}4$.

**Ejercicio 129.**– Sea $p \in \mathbb{Z}$ un número primo. Demuestre que $\langle p, X \rangle$ es un ideal no principal de $\mathbb{Z}[X]$.

**Ejercicio 130.**– Sea $A$ un anillo, $\alpha \in A^*$ y $\beta \in \text{Nil}(A)$. Pruebe que $\alpha + \beta \in A^*$.

**Ejercicio 131.**– Sea $A[X]$ un anillo de polinomios, $f \in A[X]$. Pruebe que $f$ es divisor de 0 si y sólo si existe $0 \neq a \in A$ tal que $af = 0$.

**Ejercicio 132.**– Pruebe que un dominio de integridad con una cantidad finita de elementos es un cuerpo.

**Ejercicio 133.**– Sea $k$ un cuerpo, $\alpha \in k$. Pruebe que el conjunto de polinomios de $k[X]$ que tienen a $\alpha$ como raíz es un ideal $I_\alpha$ generado por $X - \alpha$. Pruebe que $k[X]/I_\alpha$ es un cuerpo, isomorfo a $k$.

**Ejercicio 134.**– Sea $R = \mathbb{Z}/\mathbb{Z}n$. Pruebe que el conjunto de elementos de $R$

$$I = \left\{x + \mathbb{Z}n \mid (x + \mathbb{Z}n)^2 = 0 + \mathbb{Z}n\right\}$$

es un ideal de $R$.

**Ejercicio 135.**– Sean $n, m \in \mathbb{Z}$. Pruebe que la correspondencia

$$\begin{array}{rcl} f : \mathbb{Z}/\mathbb{Z}n & \longrightarrow & \mathbb{Z}/\mathbb{Z}m \\ a + \mathbb{Z}n & \longmapsto & a + \mathbb{Z}m \end{array}$$

está bien definida y es un homomorfismo de anillos si y sólo si $m|n$. En este caso hallar su núcleo y su imagen (hay que dar explícitamente un sistema de generadores de ambos como ideales de sus respectivos anillos).

**Ejercicio 136.**– Se define el conjunto de los cuaterniones de Hamilton como

$$Q = \{a + bi + cj + dk \mid, a, b, c, d \in \mathbb{R}\}$$

con la suma y el producto definidos del modo natural, con los convenios siguientes: $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$. Pruebe que $Q$ es un anillo no conmutativo, en el que todo elemento no nulo tiene inverso.

**Ejercicio 137.**– Sean $n \in \mathbb{Z}$, con $n = p_1^{e_1} \cdots p_r^{e_r}$, y $p_i$ primos distintos. Pruebe que $\sqrt{\mathbb{Z}n} = \mathbb{Z}(p_1 \cdots p_r)$.

**Ejercicio 138.**– Pruebe que son equivalentes:

(1). $\mathbb{Z}/\mathbb{Z}p$ es un cuerpo.

(2). $\mathbb{Z}/\mathbb{Z}p$ es un dominio de integridad.

(3). $p$ es primo.

**Ejercicio 139.**– Sea $f : A \to B$ un homomorfismo de anillos. Pruebe que $A/\ker f$ es isomorfo a $f(A)$ (*Primer teorema de isomorfía*).

**Ejercicio 140.**– Sea $A$ un anillo, $I \subset A$ un ideal, $B \subset A$ un subanillo. Pruebe que:

(1). $B + I := \{b + a \mid b \in B, a \in I\}$ es un subanillo de $A$.

(2). $I$ es un ideal de $B + I$ y $B \cap I$ es un ideal de $B$.

(3). $(B + I)/I \simeq B/(B \cap I)$ (*segundo teorema de isomorfía).*

**Ejercicio 141.**– Sea $A$ un anillo, $I, J$ ideales de $A$, con $I \subset J$. Pruebe que:

(1). $J/I$ es un ideal de $A/I$.

(2). $A/J \simeq (A/I)/(J/I)$ (*tercer teorema de isomorfía*).

**Ejercicio 142.**– Un ideal $I$ de un anillo $A$ se dice primo si, $I \neq A$ y

$$\forall a, b \in A, ab \in I \implies a \in I \quad \text{ó} \quad b \in I$$

(1). Si $I \neq A$, pruebe que $I$ es primo si y sólo si $A/I$ es un dominio de integridad.

(2). Halle todos los ideales de $\mathbb{Z}/\mathbb{Z}24$, comprobando los que son primos.

**Ejercicio 143.**– Sea $D$ un número racional que no sea un cuadrado perfecto en $\mathbb{Q}$, y definimos

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\}$$

como un subconjunto de $\mathbb{C}$.

(1). Pruebe que la suma y el producto son operaciones internas.

(2). Deduzca que $\mathbb{Q}(\sqrt{D})$ es un subanillo de $\mathbb{C}$.

(3). Pruebe que todo elemento no nulo $a+b\sqrt{D}$ tiene un inverso igual a

$$\frac{a-b\sqrt{D}}{a^2-Db^2}.$$

Concluya que $\mathbb{Q}(\sqrt{D})$ es un cuerpo.

(4). Pruebe que $D$ se puede escribir como $D=f^2D'$, donde $f\in\mathbb{Q}$ y $D'\in\mathbb{Z}$, con $D'$ no divisible por el cuadrado de ningún entero mayor que 1. Por ejemplo, $8/5=(2/5)^2\cdot 10$. A $D'$ se le llama parte libre de cuadrados de $D$.

(5). Con la notación anterior, pruebe que $\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{D'})$.

**Ejercicio 144.**– Sea $D$ un entero libre de cuadrados. Pruebe que

$$\mathbb{Z}[\sqrt{D}]=\{a+b\sqrt{D}|a,b\in\mathbb{Z}\}$$

es un subanillo de $\mathbb{Q}(\sqrt{D})$.

Si $D\equiv 1$ mód 4 entonces

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}]=\{a+b\frac{1+\sqrt{D}}{2}|a,b\in\mathbb{Z}\}$$

es un subanillo de $\mathbb{Q}(\sqrt{D})$.

**Ejercicio 145.**– Un elemento $x$ de un anillo $R$ se dice nilpotente si existe $m\geq 0$ tal que $x^m=0$.

(1). Pruebe que si $n=a^kb$ para enteros $a,b$, entonces la clase $(ab)+\mathbb{Z}n$ es un elemento nilpotente en $\mathbb{Z}/\mathbb{Z}n$.

(2). Si $a\in\mathbb{Z}$, pruebe que la clase $a+\mathbb{Z}n$ es nilpotente en $\mathbb{Z}/\mathbb{Z}n$ si y solamente si todo divisor primo de $n$ es también divisor primo de $a$.

(3). Determine los elementos nilpotentes de $\mathbb{Z}/\mathbb{Z}72$.

**Ejercicio 146.**– Queremos resolver la ecuación

$$x^2+y^2=3z^2$$

para valores de $x,y,z\in\mathbb{Z}$.

(1). Pruebe que si existen $x_0,y_0,z_0\in\mathbb{Z}$ verificando la ecuación entonces existen $x_0',y_0',z_0'\in\mathbb{Z}$ que verifican la ecuación y no tienen factores comunes.

(2). Calcule las soluciones de la ecuación para $x,y,z\in\mathbb{Z}/\mathbb{Z}4$.

(3). Deduzca que la única solución de la ecuación original es $x=y=z=0$.

**Ejercicio 147.**– Calcule todos los homomorfismos de anillo de $\mathbb{Z}$ a $\mathbb{Z}/\mathbb{Z}30$. En cada caso describa el núcleo y la imagen.

**Ejercicio 148.**– Sea $F=\{0,1,a,b\}$, donde definimos las operaciones de suma y multiplicación como sigue:

| $+$ | 0 | 1 | $a$ | $b$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $a$ | $b$ |
| 1 | 1 | 0 | $b$ | $a$ |
| $a$ | $a$ | $b$ | 0 | 1 |
| $b$ | $b$ | $a$ | 1 | 0 |

| $\cdot$ | 0 | 1 | $a$ | $b$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $a$ | $b$ |
| $a$ | 0 | $a$ | $b$ | 1 |
| $b$ | 0 | $b$ | 1 | $a$ |

(1). Pruebe que $(F,+,\cdot)$ es un cuerpo con 4 elementos.

(2). Pruebe que el grupo aditivo $(F,+)$ es isomorfo a $(\mathbb{Z}/\mathbb{Z}2)^2$.

(3). Pruebe que el grupo multiplicativo $(F^*, \cdot)$ es isomorfo a $\mathbb{Z}/\mathbb{Z}3$.

**Ejercicio 149.**– Sea $A$ un anillo y $M \subset A$ un ideal.

(1). Pruebe que $M$ es maximal si y sólo si $A/M$ es un cuerpo.

(2). Pruebe que si $M$ es maximal, entonces es primo. ¿Es cierto el recíproco?

**Ejercicio 150.**– Sea $A$ un dominio de integridad, y consideremos elementos $a, b, u, \in A$. Pruebe que:

(1). $A = \langle u \rangle$ si y sólo si $u$ es una unidad de $A$.

(2). $\langle a \rangle \subset \langle b \rangle$ si y sólo si $b \mid a$.

(3). $\langle a \rangle = \langle b \rangle$ si y sólo si $a$ y $b$ son asociados.

**Ejercicio 151.**– Sea $A = \{\frac{a}{2^n} \mid a, n \in \mathbb{Z}\}$.

(1). Pruebe que $A$ es un dominio de integridad.

(2). Halle sus unidades.

(3). Halle el cuerpo de fracciones de $A$.

**Ejercicio 152.**– Sea $p \in \mathbb{Z}$ un número primo y $E_p = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$.

(1). Pruebe que $E_p$ es un dominio de integridad.

(2). Demuestre que $I = \langle p \rangle$ es un ideal maximal de $E_p$.

(3). Halle el cuerpo de fracciones de $E_p$.

**Ejercicio 153.**– Calcule las unidades de $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ y $\mathbb{Z}[\sqrt{-5}]$.

**Ejercicio 154.**–

(1). Demuestre que $1 + \sqrt{2}$ es una unidad de $\mathbb{Z}[\sqrt{2}]$. Deduzca que hay infinitas unidades en $\mathbb{Z}[\sqrt{2}]$.

(2). Demuestre que las ecuaciones de Pell $x^2 - 2y^2 = 1$ y $x^2 - 2y^2 = -1$ tienen infinitas soluciones enteras.

**Ejercicio 155.**–

(1). Sea $\Delta = \{(a, a) \in \mathbb{Z} \mid a \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$. Deduzca si $\Delta$ es un ideal o un subanillo de $\mathbb{Z} \times \mathbb{Z}$.

(2). Estudie si los ideales de $\mathbb{Z} \times \mathbb{Z}$ son todos principales.

(3). Estudie si $\mathbb{Z}2 \times \mathbb{Z}2$ es un ideal primo o maximal de $\mathbb{Z} \times \mathbb{Z}$.

## ANILLOS DE POLINOMIOS.

**Ejercicio 156.**– Sean $p(X) = 2X^3 - 3X^2 + 4X - 5, q(X) = 7X^3 + 33X - 4$. Calcule $p(X) + q(X)$ y $p(X)q(X)$ para los casos en que los coeficientes estén en los anillos

$$\text{a) } \mathbb{Z}, \text{ b) } \mathbb{Z}/\mathbb{Z}2, \text{ c) } \mathbb{Z}/\mathbb{Z}3.$$

**Ejercicio 157.**– Sea $f(X) = X^4 - 16 \in \mathbb{Z}[X]$.

(1). Calcule un polinomio de grado menor o igual que 3 que sea congruente a $7X^{13} - 11X^9 + 5X^5 - 2X^3 + 3$ módulo $f(X)$.

(2). Pruebe que las clases $(X+2)+\langle f(X)\rangle$ y $(X-2)+\langle f(X)\rangle$ son divisores de cero en el anillo cociente $\mathbb{Z}[X]/\langle f(X)\rangle$.

**Ejercicio 158.**– Sea $f(X)=X^3-2X+1\in\mathbb{Z}[X]$, y consideremos $p(X)=2X^7-7X^5+4X^3-9X+1, q(X)=(X-1)^4$. Usaremos notación $\overline{a}$ para indicar elementos del anillo cociente $R=\mathbb{Z}[X]/\langle f(X)\rangle$.

(1). Exprese los siguientes elementos en la forma $\overline{r(X)}$ para algún polinomio $r(X)\in\mathbb{Z}[X]$ de grado menor o igual que 2: $\overline{p(X)}, \overline{q(X)}, \overline{p(X)+q(X)}, \overline{p(X)q(X)}$.

(2). Pruebe que $R$ no es dominio de integridad.

(3). Pruebe que $\overline{X}$ es una unidad en $R$.

**Ejercicio 159.**– Determine los primos $p\in\mathbb{Z}$ tales que $X^2+X+1$ divide a $X^3+2X^2+2X+4$ en $(\mathbb{Z}/\mathbb{Z}p)[X]$. Igual cuestión para $X^2+1$ y $X^3+X^2+22X+15$.

**Ejercicio 160.**– Sea $p\in\mathbb{Z}$ un número primo. Pruebe que la aplicación $f:\mathbb{Z}[X]\to(\mathbb{Z}/\mathbb{Z}p)[X]$ definida por la reducción módulo $p$ de los coeficientes de un polinomio de $\mathbb{Z}[X]$ es un homomorfismo de anillos. Calcule su núcleo e imagen.

**Ejercicio 161.**– Sea $A$ un anillo. Pruebe que $A[X]$ es un anillo con las operaciones suma y producto de polinomios usuales. Si $A$ es dominio encuentre las unidades de $A[X]$. Pruebe que en $\mathbb{Z}/\mathbb{Z}8[X]$, el elemento $1+2X$ es unidad.

**Ejercicio 162.**–

(1). Pruebe la existencia del algoritmo de división entera para dos polinomios $f,g$ de $A[X]$, cuando el coeficiente líder de $g$ es una unidad de $A$.

(2). Encuentre un ejemplo en el que no se da la unicidad del algoritmo de división entera en $A[X]$, si el coeficiente líder del divisor no es una unidad.

(3). Idem con la existencia.

**Ejercicio 163.**– Pruebe que si $k$ es un cuerpo de la forma $\mathbb{Z}/\mathbb{Z}p$, existen polinomios en $k[X]$ que no tienen raíces en $k$.

**Ejercicio 164.**– Pruebe que $p$ es un número primo si y sólo si $(p-1)!+\mathbb{Z}p=-1+\mathbb{Z}p$. (Idea: estudie el polinomio $X^{p-1}-1$ en el anillo $\mathbb{Z}/\mathbb{Z}_p[X]$.

**Ejercicio 165.**– Pruebe la regla de Ruffini: Sea $f(X)=a_nX^n+...+a_1X+a_0\in\mathbb{Z}[X]$, y $p/q\in\mathbb{Q}$ una raíz de $f$ escrita en forma irreducible. Entonces $p|a_0$ y $q|a_n$.

**Ejercicio 166.**– Pruebe el criterio de Eisenstein: Sea $f(X)=a_nX^n+...+a_1X+a_0\in\mathbb{Z}[X]$ tal que existe un primo $p$ verificando:

$$a_n\notin\mathbb{Z}p,\ \ a_i\in\mathbb{Z}p,\ i=0,...,n-1,\ \ a_0\notin\mathbb{Z}p^2.$$

Entonces $f(X)$ es irreducible en $\mathbb{Q}[X]$.

**Ejercicio 167.**– Sea $f(X)=a_nX^n+...+a_1X+a_0\in\mathbb{Z}[X]$, y $p/q\in\mathbb{Q}$ una raíz de $f$ escrita en forma irreducible. Pruebe que, para todo $m\in\mathbb{Z}$, $(p-qm)|f(m)$.

**Ejercicio 168.**– Pruebe que un polinomio $f\in\mathbb{Z}[X]$ no tiene raíces enteras si $f(0)$ y $f(1)$ son impares.

**Ejercicio 169.**– Sea $f(X)\in k[X]$ un polinomio de grado mayor que 0. Pruebe que son equivalentes:

(1). $f(X)$ es irreducible en $k[X]$.

(2). Existe $a\in k$ tal que $f(X-a)$ es irreducible en $k[X]$.

(3). Para todo $a\in k$ $f(X-a)$ es irreducible en $k[X]$.

**Ejercicio 170.**– Dé un ejemplo que pruebe que es posible hallar un cuerpo $k$ y un polinomio $f(X) \in k[X]$ para los cuales no se puede afirmar que la multiplicidad de una raíz $a$ de $f$ es el orden de la última derivada de $f$ que se anula en $a$.

**Ejercicio 171.**– Se dice que un polinomio $f(X_1, ..., X_n) \in k[X_1, ..., X_n]$ es simétrico si, para toda $\sigma \in S_n$, se tiene que

$$f\left(X_{\sigma(1)}, ..., X_{\sigma(n)}\right) = f\left(X_1, ..., X_n\right).$$

Ejemplos de polinomios simétricos son

$$S_1 = X_1 + X_2 + ... + X_n,\ S_2 = \sum_{i<j} X_i X_j, ..., S_k = \sum_{i_1<i_2<...<i_k} X_{i_1} X_{i_2} ... X_{i_k}, ..., S_n = X_1 X_2 ... X_n.$$

Pruebe que todo polinomio simétrico se puede escribir como un polinomio en $S_1, ..., S_n$.

**Ejercicio 172.**– Sea $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in k[X]$, con raíces (no necesariamente en $k$) $\{\alpha_1, ..., \alpha_n\}$. Se define el discriminante de $f$ como el número

$$\mathrm{Disc}(f) = \prod_{i<j} \left(\alpha_i - \alpha_j\right)^2.$$

Pruebe que $\mathrm{Disc}(f) \in k$, independientemente de que las raíces estén o no en $k$. Halle el discriminante de las ecuaciones de segundo, tercer y cuarto grado en función de los coeficientes de las ecuaciones.

**Ejercicio 173.**– Sea $f(X) \in k[X]$ un polinomio con todas sus raíces en $k$, siendo $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Definimos

$$D_0 = \mathrm{mcd}\left(f, f'\right),\ D_1 = \mathrm{mcd}\left(D_0, D_0'\right),\ D_j = \mathrm{mcd}\left(D_{j-1}, D_{j-1}'\right),\ j \geq 2.$$

(1). Pruebe que existe un $n$ tal que $D_n$ es una constante.
Sea $m$ el primer entero tal que $D_{m+1} \in k$. Definimos entonces las familias

$$F_1 = F/D_0,\ F_2 = D_0/D_1, \ldots, F_m = D_{m-2}/D_{m-1}.$$

$$G_1 = F_1/F_2,\ G_2 = F_2/F_3, \ldots, G_m = F_m.$$

(2). Pruebe que los $G_i$ no tienen raíces múltiples.

(3). Pruebe que los $G_i$ son primos entre sí dos a dos.

(4). Pruebe que $f = G_1 G_2^2 \ldots G_m^m$.

(5). Pruebe que $G_i$ tiene como raíces las raíces de $f$ de multiplicidad exactamente $i$.

**Ejercicio 174.**– Se considera el cuerpo $k = \mathbb{Z}/\mathbb{Z}29$.

(1). Pruebe que $k^*$ es un grupo cíclico generado por $2 + \mathbb{Z}29$, *calculando, a lo más, cuatro potencias de 2.*

(2). Utilice el apartado anterior para hallar, razonadamente, las raíces de la ecuación $X^7 - 1 = 0$ en $k$.

(3). Resuelva la ecuación $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = 0$ en $k$.

**Ejercicio 175.**– Sea $R = \mathbb{Z}[2i] = \{a + b2i | a, b \in \mathbb{Z}\}$ y $p(X) = X^2 + 1 \in R[X]$.

(1). Pruebe que el cuerpo de fracciones de $R$ es $K = \mathbb{Q}[i]$.

(2). Pruebe que el polinomio $p(X)$ es reducible en $K[X]$ pero irreducible en $R[X]$.

**Ejercicio 176.**– Determine el carácter reducible o irreducible de los siguientes polinomios:

- $X^3 - 3X - 1$ en $\mathbb{Z}[X]$.

- $X^2 - p$ y $X^3 - p$ en $\mathbb{Q}[X]$, con $p \in \mathbb{Z}$ primo.
- $X^2 + 1$ en $\mathbb{Z}/\mathbb{Z}2[X]$.
- $X^3 + X + 1$ en $\mathbb{Z}/\mathbb{Z}2[X]$.

**Ejercicio 177.**– Sea $I$ un ideal propio de un dominio de integridad $A$, y sea $p(X)$ un polinomio mónico no constante de $A[X]$. Si la imagen de $p(X)$ en $(A/I)[X]$ es irreducible en $(A/I)[X]$ entonces $p(X)$ es irreducible en $A[X]$.

Pruebe que el polinomio $f(X) = X \in \mathbb{Z}/\mathbb{Z}6[X]$ factoriza como $(3X + 4)(4X + 3)$, por lo que no es irreducible. Pruebe que la reducción de $f(X)$ módulo los ideales propios $\langle 2\rangle$ y $\langle 3\rangle$ de $\mathbb{Z}/\mathbb{Z}6$ es un polinomio irreducible.

**Ejercicio 178.**– Pruebe que

- el polinomio $X^4 + 10X + 5$ es irreducible en $\mathbb{Z}[X]$,
- si $a \in \mathbb{Z}$ es divisible por un primo $p$ pero no por $p^2$, entonces $x^n - a$ es irreducible en $\mathbb{Z}[X]$.

Verifique que no se puede aplicar el criterio de Eisenstein a $f(X) = X^4 + 1 \in \mathbb{Z}[X]$. Pruebe mediante Eisenstein que $g(X) = f(X + 1)$ es irreducible en $\mathbb{Z}[X]$. Deduzca que $f(X)$ es irreducible.

**Ejercicio 179.**– Sea $p \in \mathbb{Z}$ un número primo y consideremos el polinomio

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1.$$

Aplique el criterio de Eisenstein a $\Phi_p(X + 1)$ para probar que $\Phi_p(X)$ es irreducible.

**Ejercicio 180.**– Calcule los polinomios mónicos irreducibles de grado menor o igual que 3 en $\mathbb{Z}/\mathbb{Z}2[X]$ y $\mathbb{Z}/\mathbb{Z}3[X]$.

**Ejercicio 181.**– Pruebe que si $X^{n-1} + X^{n-2} + \ldots + X + 1$ es irreducible en $\mathbb{Z}[X]$ entonces $n$ es primo.

**Ejercicio 182.**– Pruebe que $X^3 + nX + 2$ es irreducible en $\mathbb{Z}[X]$ para todos los enteros $n \neq 1, -3, -5$.

## ECUACIONES DE TERCER Y CUARTO GRADO.

**Ejercicio 183.**– Resuelva los siguientes problemas propuestos por Antonio María del Fiore a Tartaglia:

(1). Determine por dónde debe ser cortado un árbol de 12 varas de altura de tal manera que la parte que quede en tierra sea la raíz cúbica de la parte superior cortada.

(2). Encuentre un número que se convierte en 6 cuando se le suma su raíz cúbica.

(3). Un hombre vende un zafiro por 500 ducados, obteniendo así un beneficio de la raíz cúbica del precio que pagó por él. ¿A cuánto asciende el beneficio?

**Ejercicio 184.**– Resuelva la ecuación $x^3 = 15x + 4$ aplicando las fórmulas de Cardano-Tartaglia. Verifique que $4, -2 + \sqrt{3}$ y $-2 - \sqrt{3}$ son las soluciones de la ecuación. Establezca la correspondencia con el resultado obtenido mediante las fórmulas.

## EXTENSIONES DE CUERPOS. GRADO. ELEMENTOS ALGEBRAICOS.

**Ejercicio 185.**– Sea $d \in \mathbb{Z}$ libre de cuadrados y

$$A = \left\{ \begin{pmatrix} a & db \\ b & a \end{pmatrix}, a, b \in \mathbb{Q} \right\}.$$

Pruebe que $A$ es un cuerpo isomorfo a $\mathbb{Q}\left[\sqrt{d}\right]$.

**Ejercicio 186.**– Encuentre el polinomio mínimo de los números complejos $\alpha = \frac{\sqrt{5}+1}{2}$ y $\beta = \frac{\sqrt{5}(i-1)}{2}$.

**Ejercicio 187.**– Calcule $\left[\mathbb{Q}(\sqrt{1+\sqrt{3}}) : \mathbb{Q}\right]$.

**Ejercicio 188.**– Sean $L$ y $K$ subcuerpos de $\mathbb{C}$ con $K \subset L$. Pruebe que si $[L : K]$ es primo, entonces para todo elemento $\alpha \in L \setminus K$ se verifica que $L = K(\alpha)$.

**Ejercicio 189.**– Sea $\alpha \in \mathbb{C}$ un elemento algebraico. Demuestre que si el grado de $\alpha$ es impar, entonces $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$.

**Ejercicio 190.**– Sean $\alpha, \beta$ números algebraicos tales que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$ y $[\mathbb{Q}(\beta) : \mathbb{Q}] = n$. Demuestre que

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = n \iff [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = m,$$

y que estas condiciones se cumplen si $m$ y $n$ son primos entre sí, en cuyo caso $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = mn$. Dé un ejemplo en el que se verifique la condición sin que $m$ y $n$ sean primos entre sí.

**Ejercicio 191.**– Sea $m, n \in \mathbb{Z}$. Pruebe que $\mathbb{Q}\left(\sqrt{m} + \sqrt{n}\right) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Si $m \neq n$ entonces se tiene que $\mathbb{Q}\left(\sqrt{m} - \sqrt{n}\right) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

**Ejercicio 192.**– Dé una base de $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$ como espacio vectorial sobre $\mathbb{Q}$. Exprese en dicha base $1/\left(\sqrt{2} + \sqrt{3} + \sqrt{5}\right)$.

**Ejercicio 193.**– Sean $m$ y $n$ enteros. Dé una condición necesaria y suficiente para que $\mathbb{Q}\left(\sqrt{m}\right)$ y $\mathbb{Q}\left(\sqrt{n}\right)$ sean isomorfos como espacios vectoriales. Idem como cuerpos.

**Ejercicio 194.**– Sea $m$ un entero. Calcule el grupo de automorfismos (como anillo) del cuerpo $\mathbb{Q}\left(\sqrt{m}\right)$ y dé la expresión matricial de cada uno de ellos en función de una base.

**Ejercicio 195.**– Sea $\alpha \in \mathbb{C}$ algebraico. Para cada $\beta \in \mathbb{Q}[\alpha]$, definimos $F(\beta) = \alpha\beta$. Pruebe que $F$ es un endomorfismo de $\mathbb{Q}[\alpha]$ como $\mathbb{Q}$-espacio vectorial. Halle el polinomio característico $\det(\lambda\ \mathrm{id} - F)$ de $F$.

**Ejercicio 196.**– Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $X^3 + 2X^2 + 3X - 2$. Se pide:

(1). Halle $[\mathbb{Q}[\alpha] : \mathbb{Q}]$.

(2). Encuentre el polinomio mínimo de $1 + \alpha$ sobre $\mathbb{Q}$.

(3). Calcule el inverso de $1 - \alpha^2$ como combinación lineal de elementos de una base de $\mathbb{Q}[\alpha]$.

**Ejercicio 197.**– Sean los números complejos $\alpha = \sqrt{1+\sqrt{2}}$ y $\beta = \sqrt{1-\sqrt{2}}$. Se pide:

(1). Halle el polinomio mínimo $f(X)$ de $\beta$ sobre $\mathbb{Q}$, y el valor de $[\mathbb{Q}[\beta] : \mathbb{Q}]$.

(2). Pruebe que el polinomio mínimo de $\alpha$ sobre $\mathbb{Q}$ es también $f(X)$.

(3). Halle $[\mathbb{Q}[\alpha, \beta] : \mathbb{Q}]$.

**Ejercicio 198.**– Consideremos la siguiente extensión de cuerpos: $\mathbb{Q} \subset K = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$. Se pide:

(1). Calcule el grado de la extensión $[K : \mathbb{Q}]$.

(2). Pruebe que $\alpha = \sqrt{2} + \sqrt[3]{2}$ es elemento *primitivo*, esto es, que $K = \mathbb{Q}[\alpha]$.

(3). Dé la lista de todos los subcuerpos $L$ verificando $\mathbb{Q} \subset L \subset K$ con $[L : \mathbb{Q}] = 2$.

**Ejercicio 199.**–

(1). Si sabemos que el polinomio $X^4+4$ es producto de dos polinomios irreducibles de $\mathbb{Q}[X]$, ¿qué grado tienen estos polinomios? Calcule dichos factores irreducibles.

(2). Si $\alpha$ es el número complejo $\sqrt{2i}$ determine $[\mathbb{Q}[\alpha]:\mathbb{Q}]$.

(3). Razone si alguna de las siguientes igualdades es cierta:

*a)* $\mathbb{Q}(\alpha)=\mathbb{Q}(i)$.

*b)* $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2})$.

**Ejercicio 200.**– Sea $\beta\in\mathbb{C}$ una raíz del polinomio $F(X)=X^3-3X+1$ y $K=\mathbb{Q}(\beta)$.

(1). Calcule el grado de la extensión $[K:\mathbb{Q}]$.

(2). Sea $m:K\to K$ la aplicación $\mathbb{Q}$-lineal definida por $m(c)=(1+\beta^2)c$ para cada $c\in K$. Calcule la matriz de $m$ respecto de alguna $\mathbb{Q}$-base de $K$, así como su polinomio característico.

**Ejercicio 201.**– Sea $\mathbb{K}$ un cuerpo y $a\in\mathbb{K}$ un elemento tal que $f(X)=X^n-a$ es un polinomio irreducible. Si $m$ es un divisor de $n$ y $\alpha$ es una raíz de $f(X)$ en alguna extensión de $\mathbb{K}$, calcule el polinomio mínimo de $\alpha^m$ sobre $\mathbb{K}$.

**Ejercicio 202.**– Sea $a=\tan\frac{2\pi}{5}, c=\sec\frac{2\pi}{5}$.

(1). Calcule el polinomio mínimo de $a$ sobre $\mathbb{Q}$.

(2). Calcule el polinomio mínimo de $c$ sobre $\mathbb{Q}$.

(3). Exprese $\cos\frac{2\pi}{5}$ mediante radicales.

**Ejercicio 203.**– Sea $\alpha=\frac{2k\pi}{7}$. Compruebe que $\cos 4\alpha-\cos 3\alpha=0$ y deduzca el polinomio mínimo de $\cos\alpha$ sobre $\mathbb{Q}$.

**Ejercicio 204.**– Sea $p$ un número primo y $a\in\mathbb{Z}/p\mathbb{Z}$. Sea $\alpha$ una raíz del polinomio $f(X)=X^p-X-a$. Exprese las raíces de $f(X)$ en función de $\alpha$ y encuentre un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}/p\mathbb{Z}$.

**Ejercicio 205.**– Construya cuerpos de descomposición de los polinomios $X^3+2X+1$ y $X^3+X^2+X+2$ sobre $\mathbb{Z}/3\mathbb{Z}$. Determine si son isomorfos y, en tal caso, calcule un isomorfismo.

**Ejercicio 206.**– Sea $f(X)\in\mathbb{Q}[X]$ un polinomio irreducible de grado $n$, y $\mathbb{K}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. Demuestre que $[\mathbb{K}:\mathbb{Q}]$ divide a $n!$.

**Ejercicio 207.**– Calcule $\mathbb{K}$ un cuerpo de descomposición de $X^5-2$ sobre $\mathbb{Q}$. Determine $[\mathbb{K}:\mathbb{Q}]$.

**Ejercicio 208.**– Sea $\mathbb{Q}\subset\mathbb{K}$ una extensión de cuerpos tal que $[\mathbb{K}:\mathbb{Q}]=2$. Pruebe que existe $d\in\mathbb{Z}$ libre de cuadrados tal que $\mathbb{K}=\mathbb{Q}[\sqrt{d}]$.

**Ejercicio 209.**– Sea $\mathbb{Q}[\alpha]$ una extensión de $\mathbb{Q}$, donde $\alpha$ es raíz del polinomio $X^3+2X^2+3X-2$.

(1). Pruebe que el grado de la extensión es 3.

(2). Calcule el polinomio mínimo de $1+\alpha$ y $1+\alpha+\alpha^2$ sobre $\mathbb{Q}$.

(3). Exprese $\frac{1}{1+5\alpha-7\alpha^2}$ como combinación lineal de los elementos de una base de la extensión.

**Ejercicio 210.**– Sea $\mathbb{K}$ una extensión finita de $k$ de grado $n$ y tomemos un elemento $y\in\mathbb{K}$. Pruebe que el grado del polinomio mínimo de $y$ sobre $k$ es un divisor de $n$. En particular, si $n$ es primo y el elemento $y\notin k$, entonces el grado del polinomio mínimo de $y$ sobre $k$ es $n$. Deduzca que $\mathbb{K}=k[y]$.

**Ejercicio 211.**– Sean $\alpha, \beta$ números algebraicos sobre $\mathbb{Q}$, de grados respectivos $m$ y $n$. Pruebe que $[\mathbb{Q}[\alpha+\beta] : \mathbb{Q}] \leq mn$. Dé un ejemplo en el que se verifique la igualdad.

**Ejercicio 212.**– Encuentre el polinomio mínimo del número complejo $\alpha = \frac{\sqrt{2}+1}{2}$ y calcule $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

**Ejercicio 213.**–

(1). Encuentre el polinomio mínimo del número complejo $\beta = \frac{\sqrt{2}(i-1)}{2}$.

(2). Averigüe si $\mathbb{Q}(i) \subset \mathbb{Q}(\beta)$ y, en caso afirmativo, halle el grado de la extensión.

(3). Halle $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$.

(4). Averigüe si $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\beta)$.

**Ejercicio 214.**– Sea el número complejo $\gamma = \sqrt{1+\sqrt{2}}$. Calcule $[\mathbb{Q}(\gamma) : \mathbb{Q}]$.

**Ejercicio 215.**– Sea $\alpha$ un elemento algebraico sobre $k$, $f(X) \in k[X]$ su polinomio mínimo sobre $k$. Exprese el inverso de $\alpha$ como polinomio en $\alpha$ con coeficientes en $k$.

**Ejercicio 216.**– Sea $\alpha \in \mathbb{C}$ una raíz de $X^3 + 3X + 1 = 0$.

(1). Halle $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

(2). Encuentre el polinomio mínimo de $\alpha^2 + 1$.

(3). Exprese el inverso del número anterior como polinomio en $\alpha$ con coeficientes racionales.

**Ejercicio 217.**– Sean los números complejos $\alpha = \sqrt{1+\sqrt{3}}$ y $\beta = \sqrt{1-\sqrt{3}}$. Se pide:

(1). Halle el polinomio mínimo $f(X)$ de $\beta$ sobre $\mathbb{Q}$, y determine $[\mathbb{Q}[\beta] : \mathbb{Q}]$.

(2). Calcule $[\mathbb{Q}[\alpha, \beta] : \mathbb{Q}]$.

**Ejercicio 218.**–

(1). Demuestre que $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ es irreducible sobre $\mathbb{Q}$.

(2). Si $\alpha = e^{2\pi i/5} \in \mathbb{C}$, halle $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

(3). Halle el polinomio mínimo de $\cos\frac{2\pi}{5} = \frac{\alpha+\alpha^4}{2}$ sobre $\mathbb{Q}$.

(4). Halle un entero $d$ tal que $\mathbb{Q}(\cos\frac{2\pi}{5}) = \mathbb{Q}(\sqrt{d})$.

**Ejercicio 219.**–

(1). Demuestre que $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ es irreducible sobre $\mathbb{Q}$.

(2). Si $\alpha = e^{2\pi i/7} \in \mathbb{C}$, halle $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

(3). Halle el polinomio mínimo de $\cos\frac{2\pi}{7} = \frac{\alpha+\alpha^6}{2}$ sobre $\mathbb{Q}$.

**Ejercicio 220.**– Supongamos que tenemos las extensiones de cuerpos $k \subset \mathbb{L} \subset \mathbb{L}[\alpha]$, y que $[k[\alpha] : k]$ y $[\mathbb{L} : k]$ son primos entre sí. Pruebe que el polinomio mínimo de $\alpha$ sobre $\mathbb{L}$ tiene sus coeficientes en $k$.

**Ejercicio 221.**– Calcule un cuerpo de descomposición de $X^p - 2 \in \mathbb{Q}[X]$, $p$ primo, y su grado sobre $\mathbb{Q}$.

**Ejercicio 222.**– Calcule un cuerpo de descomposición sobre $\mathbb{Q}$ de los siguientes polinomios:

(1). $X^2 - p$, con $p > 0$ y primo.

(2). $X^4 - 8X^2 + 15$.

(3). $X^4 + 1$.

**Ejercicio 223.**– Sea $k$ un cuerpo, $a \in k$ y $p, q$ enteros positivos y primos entre sí.

(1). Pruebe que $z$ es raíz de $X^{pq} - a$ si y sólo si $z^q$ es raíz de $X^p - a$.

(2). Si $X^p - a, X^q - a$ son polinomios irreducibles sobre $k$, entonces $[k[z^p] : k] = q$ y $[k[z^q] : k] = p$.

(3). $X^{pq} - a$ es irreducible sobre $k$ si y sólo si $X^p - a$ y $X^q - a$ son irreducibles sobre $k$.

**Ejercicio 224.**– Sea $a \in \mathbb{Q}$ un número racional que no sea el cubo de ningún número racional.

(1). ¿Cuál es el grado de un cuerpo de descomposición del polinomio $X^3 - a$ sobre $\mathbb{Q}$?

(2). Si $z_1, z_2, z_3$ son las raíces de $X^3 - a$ en $\mathbb{C}$, ¿son iguales $\mathbb{Q}[z_1], \mathbb{Q}[z_2], \mathbb{Q}[z_3]$?

**Ejercicio 225.**– Sea $\mathbb{K}$ una extensión de $k$, con $[\mathbb{K} : k] = p$, y $g(X) \in k[X]$ un polinomio irreducible de grado $q$, primo con $p$. Pruebe que $g(X)$ es irreducible sobre $\mathbb{K}[X]$.

**Ejercicio 226.**– Sea $K|k$ una extensión y $\alpha \in K$. Pruebe que $\alpha$ es algebraico sobre $k$ si y solamente si la extensión $k(\alpha)|k$ es finita.

**Ejercicio 227.**– Sea $\alpha = \sqrt[3]{2}$

(1). Calcule $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ y escriba una base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial.

(2). Escriba la expresión en la misma del elemento $1/\sqrt[3]{2}$

(3). Calcule el polinomio mínimo de $\alpha^2 - 1$ sobre $\mathbb{Q}$.

(4). Exprese el inverso del número anterior como polinomio en $\alpha$ con coeficientes racionales.

(5). Calcule los automorfismos del cuerpo $K$ que dejan fijo a $\mathbb{Q}$.

**Ejercicio 228.**– Sea $p \in \mathbb{Z}$ un número primo, y $\zeta = \exp(2\pi i/p)$ raíz $p$-ésima de la unidad. Pruebe que un cuerpo de descomposición del polinomio $X^p - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}[\zeta]$, y que $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$.

**Ejercicio 229.**– Sea $p \in \mathbb{Z}$ un número primo, y $\zeta = \exp(2\pi i/p)$ raíz $p$-ésima de la unidad. Pruebe que un cuerpo de descomposición del polinomio $X^p - 2$ sobre $\mathbb{Q}$ es $K = \mathbb{Q}[\sqrt[p]{2}, \zeta]$, y que $[K : \mathbb{Q}] = p(p-1)$.

**Ejercicio 230.**– Sea $\rho = \exp(2\pi i/3) = \frac{-1+\sqrt{3}i}{2}$ raíz cúbica de la unidad, y consideremos el cuerpo $K = \mathbb{Q}[\sqrt[3]{2}, \rho]$. Sea $\sigma$ el automorfismo de $K$ definido por

$$\sigma(\sqrt[3]{2}) = \rho\sqrt[3]{2}, \sigma(\rho) = \rho.$$

Pruebe que el conjunto de elementos de $K$ que quedan fijos por la acción de $\sigma$ es $\mathbb{Q}[\rho]$.

**Ejercicio 231.**– Sea $\omega = \exp(2\pi i/7)$ y $\alpha = \omega + \omega^{-1}$.

(1). Pruebe que $\omega$ es raíz del polinomio cuadrático $X^2 - \alpha X + 1$ sobre $\mathbb{Q}[\alpha]$.

(2). A partir del polinomio mínimo de $\omega$ sobre $\mathbb{Q}$, calcule el polinomio mínimo de $\alpha$ sobre $\mathbb{Q}$.

**Ejercicio 232.**– Calcule un elemento primitivo de un cuerpo de descomposición del polinomio $X^5 - 2$ sobre $\mathbb{Q}$.

**Ejercicio 233.**– Deduzca si el polígono regular de 9 lados es constructible con regla y compás. Idem con el polígono regular de 11 lados.

**Ejercicio 234.**– Demuestre que es posible construir con regla y compás el ángulo de $3^o$. Para ello utilice el de $12^o = 72^o - 60^o$.

## TEOREMA FUNDAMENTAL DE LA TEORÍA DE GALOIS. CÁLCULO DE GRUPOS DE GALOIS.

**Ejercicio 235.**– Sea $\mathbb{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Pruebe que $\mathbb{K}$ es de Galois. Calcule $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, sus subgrupos y sus cuerpos fijos correspondientes.

**Ejercicio 236.**– Sea $f(X) \in \mathbb{Q}[X]$ un polinomio irreducible de grado 3, $\Delta$ su discriminante y fijemos $\delta = \sqrt{\Delta}$ una raíz cuadrada. Sea $\mathbb{L}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. Pruebe que

- Si $\delta \in \mathbb{Q}$ entonces $\mathrm{Gal}(\mathbb{L}|\mathbb{Q}) = A_3$.
- Si $\delta \notin \mathbb{Q}$ entonces $\mathrm{Gal}(\mathbb{L}|\mathbb{Q}) = S_3$.

**Ejercicio 237.**– Calcule el grupo de Galois de las siguientes ecuaciones:

- $X^3 - 2 = 0$.
- $X^3 + X^2 + X + 1 = 0$.
- $X^3 - 3X + 4 = 0$.

**Ejercicio 238.**– Sea $f(X) = X^4 + 1$, $\alpha = \sqrt{2}$.

(1). Pruebe que $\mathbb{L} = \mathbb{Q}[\alpha, i]$ es un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.

(2). Calcule $[\mathbb{L} : \mathbb{Q}]$.

(3). Pruebe que $\mathrm{Gal}(\mathbb{L}|\mathbb{Q})$ es isomorfo a $C_2 \times C_2$, donde $C_2$ es el grupo cíclico de 2 elementos.

(4). A partir de los subgrupos de $\mathrm{Gal}(\mathbb{L}|\mathbb{Q})$ determine los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{L}$.

**Ejercicio 239.**– Consideremos las extensiones de cuerpos

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{K} \subset \mathbb{K}[\beta] = \mathbb{L}$$

donde

$$\beta^2 = \frac{1}{\sqrt{2}}\sqrt{3}(\sqrt{2}+1)(\sqrt{3}+1) \in \mathbb{K}.$$

(1). Pruebe que las siguientes ecuaciones definen dos automorfismos $\phi_1, \phi_2$ de $\mathbb{L}$:

$$\phi_1(r) = r, \text{ para todo } r \in \mathbb{Q}, \phi_1(\sqrt{2}) = -\sqrt{2}, \phi_1(\sqrt{3}) = \sqrt{3}, \phi_1(\beta) = \tfrac{1}{1+\sqrt{2}}\beta$$
$$\phi_2(r) = r, \text{ para todo } r \in \mathbb{Q}, \phi_1(\sqrt{2}) = \sqrt{2}, \phi_1(\sqrt{3}) = -\sqrt{3}, \phi_2(\beta) = \beta\tfrac{\sqrt{2}}{\sqrt{3}+1}.$$

(2). Pruebe que el grupo de automorfismos de $\mathbb{L}$ que deja invariante cada elemento de $\mathbb{Q}$ es isomorfo al grupo de los cuaterniones de orden 8

$$Q_8 = \langle x, y | x^2 = y^2, xyx = y, y^4 = 1 \rangle.$$

(3). Pruebe que los subgrupos de $Q_8$ son 1, $Q_8$ y los grupos cíclicos generados por $x^2, x, y$ y $xy$ (sus órdenes respectivos son $2, 4, 4, 4$).

(4). Mediante la aplicación del teorema fundamental de la teoría de Galois, calcule todos los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{L}$.

**Ejercicio 240.**– Sea $f(X) = X^4 - 2$, $\alpha = \sqrt[4]{2}$.

(1). Pruebe que $\mathbb{L} = \mathbb{Q}[\alpha, i]$ es un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.

(2). Calcule $[\mathbb{L} : \mathbb{Q}]$ y deduzca que el grupo de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ tiene orden 8.

(3). Consideremos los automorfismos de $\mathbb{L}$ definidos por

$$\sigma(r) = r \text{ para todo } r \in \mathbb{Q}, \sigma(\alpha) = \alpha i, \sigma(i) = i,$$
$$\tau(r) = r \text{ para todo } r \in \mathbb{Q}, \tau(\alpha) = \alpha, \tau(i) = -i.$$

Pruebe que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

(4). Demuestre que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ es isomorfo a $D_8$, el grupo diédrico de 8 elementos, definido por $\langle x, y | x^4 = 1, y^2 = 1, xy = yx^3 \rangle$.

(5). Calcule todos los subgrupos de $D_8$ (hay 10 en total).

(6). Calcule todos los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{L}$.

**Ejercicio 241.**– Sea $f(X) = X^3 - 7 \in \mathbb{Q}[X]$. Calcule $\mathbb{K}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ y los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{K}$. ¿Cuáles son cuerpos de descomposición?

**Ejercicio 242.**– Se sabe que $f(X) = X^4 + X^3 + X^2 + X + 1 = \frac{X^5-1}{X-1}$ es un polinomio irreducible sobre $\mathbb{Q}$. Sean $\alpha = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5} \in \mathbb{C}$, $K = \mathbb{Q}(\alpha)$ y $G_f$ el grupo de Galois de $f$ sobre $\mathbb{Q}$ .

(1). Deduzca que $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$ son todas las raíces de $f$. Averigüe si $K$ es un cuerpo de descomposición de $f$ sobre $\mathbb{Q}$.

(2). Calcule $|G_f|$.

(3). Si $\sigma_j \in G_f$ viene dado por $\sigma_j(\alpha) = \alpha^j$, con $j = 1, 2, 3, 4$, deduzca si $G_f = \langle \sigma_j \rangle$ para algún valor de $j$.

(4). Numerando las raíces de $f$ por $x_j = \alpha^j$, con $j = 1, 2, 3, 4$, identifique $G_f$ con un subgrupo de $S_4$. Razone si la conjugación en $\mathbb{C}$ define algún elemento de $G_f$.

(5). Halle todos los subgrupos de $G_f$.

(6). Halle todos los cuerpos intermedios entre $\mathbb{Q}$ y $K$. Deduzca si $\mathbb{Q}(\cos\frac{2\pi}{5})$ y $\mathbb{Q}(\cos\frac{\pi}{5})$ son algunos de estos cuerpos. Halle un valor $d \in \mathbb{Z}$, si existe, tal que $\mathbb{Q}(\cos\frac{2\pi}{5}) = \mathbb{Q}(\sqrt{d})$.

**Ejercicio 243.**– Sea $f(X) = X^8 - 1 \in \mathbb{Q}[X]$ y $\alpha$ una raíz octava primitiva de la unidad, por ejemplo $\alpha = \frac{1}{2}(1+i)\sqrt{2}$. Sea $K$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ y $G$ el grupo de Galois de $f(X)$ sobre $\mathbb{Q}$.

(1). Demuestre que $K = \mathbb{Q}[\alpha]$.

(2). Halle $[K : \mathbb{Q}]$.

(3). Sea $\sigma \in G$. Pruebe que $\sigma(\alpha) = \alpha^k$ si y solamente si $k$ es impar. Verifique si $\sigma^2 = id$.

(4). Si llamamos $x_k = \alpha^k, k = 1, \ldots, 8$ a las raíces de $f(X)$, exprese $G$ como subgrupo de $S_8$.

(5). Halle todos los subgrupos de $G$.

(6). Razone cuáles de los siguientes cuerpos son intermedios entre $\mathbb{Q}$ y $K$ y justifique si hay alguno más:

(a) $\mathbb{Q}[i]$, (b) $\mathbb{Q}[\sqrt{2}]$, (c) $\mathbb{Q}[\sqrt{-2}]$, (d) $\mathbb{Q}[\alpha^2]$, (e) $\mathbb{Q}[\alpha + \alpha^2]$, (f) $\mathbb{Q}[\sqrt{3}]$

**Ejercicio 244.**– Sea $f(X) = X^3 - 7 \in \mathbb{Q}[X]$. Calcule $\mathbb{K}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ y los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{K}$. ¿Cuáles son cuerpos de descomposición?

**Ejercicio 245.**– Sean $f(X) = X^6 + 1 \in \mathbb{Q}[X]$, $\omega \in \mathbb{C}$ una raíz de $X^2 + X + 1$, $K \subset \mathbb{C}$ un cuerpo de descomposición de $f$ sobre $\mathbb{Q}$ y $G = \mathrm{Gal}(K|\mathbb{Q})$.

(1). Demuestre que $K = \mathbb{Q}(\omega, i)$. Para ello demuestre primero que $x_1 = i$, $x_2 = -i$, $x_3 = i\omega$, $x_4 = -i\omega$, $x_5 = i\omega^2$, $x_6 = -i\omega^2$ son todas las raíces de $f$.

(2). Calcule $[K : \mathbb{Q}]$.

(3). Con la notación del apartado 1), exprese $G$ como subgrupo de $S_6$.

(4). Halle todos los subgrupos de $G$.

(5). Razone cuáles de los siguientes cuerpos son intermedios entre $\mathbb{Q}$ y $K$, y justifique si hay alguno más:

$$(a) \quad \mathbb{Q}(i) \quad (b) \quad \mathbb{Q}(\sqrt{2}) \quad (c) \quad \mathbb{Q}(\sqrt{3}) \quad (d) \quad \mathbb{Q}(\sqrt{-3}) \quad (e) \quad \mathbb{Q}(\omega) \quad (f) \quad \mathbb{Q}(i\omega)$$

**Ejercicio 246.**– Sea $f(X) = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$.

(1). Pruebe que $f(X)$ es irreducible en $\mathbb{Q}[X]$ y que tiene 5 raíces distintas.

(2). Deduzca que $G_f$ es isomorfo a un subgrupo de $S_5$.

(3). Pruebe que 5 divide a $|G_f|$.

(4). El teorema de Cauchy para grupos dice: si $G$ es un grupo finito y $p$ es un primo que divide a $|G|$, entonces $G$ tiene un elemento de orden $p$. Con este resultado, pruebe que $G_f$ tiene un elemento que se corresponde con un ciclo de orden 5 en $S_5$.

(5). Compruebe que $f(-2) < 0, f(-1) > 0, f(1) < 0, f(2) > 0$, y deduzca que $f(X)$ tiene exactamente 3 raíces reales.

(6). Pruebe que el automorfismo definido por la conjugación está en $G_f$.

(7). Deduzca que $G_f \simeq S_5$. ¿Es $f(X)$ resoluble por radicales?

**Ejercicio 247.**– Calcule el grupo de Galois de $X^4 - 5$ sobre $\mathbb{Q}[i]$.

**CUERPOS FINITOS.**

**Ejercicio 248.**– Sea $f(X) = X^4 + 1 \in \mathbb{Z}/\mathbb{Z}p[X]$, con $p$ un primo. Pruebe que $f(X)$ es reducible.

**Ejercicio 249.**– Consideremos el polinomio $f(X) = X^4 - 10X^2 + 1 \in \mathbb{Z}[X]$.

(1). Pruebe que $f(X)$ es irreducible en $\mathbb{Z}[X]$.

(2). Sea $p \in \mathbb{Z}$ un número primo y $f \in (\mathbb{Z}/\mathbb{Z}p)[X]$ el polinomio anterior considerando sus coeficientes en $\mathbb{Z}/\mathbb{Z}p$. Pruebe que $f$ es reducible en $(\mathbb{Z}/\mathbb{Z}p)[X]$.

**Ejercicio 250.**– Sea $k$ un cuerpo y $K_1, K_2$ extensiones finitas.

(1). Si $\text{car}(k) = 0$ y $[K_1 : k] = [K_2 : k]$, ¿son $K_1$ y $K_2$ isomorfos como cuerpos? Justifique la respuesta. Indicación: considere, por ejemplo, $\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{3}]$.

(2). Si $k$ es finito y $[K_1 : k] = [K_2 : k]$, ¿son $K_1$ y $K_2$ isomorfos como cuerpos? Justifique la respuesta.

**Ejercicio 251.**– Sea $\mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}2$ el cuerpo finito con dos elementos. Sea $\alpha$ raíz de $X^2 + X + 1$ sobre $\mathbb{F}_2$ y $K_1 = \mathbb{F}_2[\alpha]$. Sea $g(X) = X^2 + \alpha X + 1 \in K_1[X]$.

(1). ¿Cuántos elementos tiene $K_1$? Expréselos en función de $\alpha$.

(2). Pruebe que $g(X)$ es irreducible sobre $K_1[X]$.

(3). Sea $\beta$ raíz de $g(X)$ y $K_2 = K_1[\beta]$. ¿Cuántos elementos tiene $K_2$? Calcule $[K_2 : \mathbb{F}_2]$.

(4). Sea $\varphi : K_2 \to K_2$ definida por $\varphi(x) = x^2$. Pruebe que $\varphi \in \text{Gal}(K_2|\mathbb{F}_2)$, y que el orden de $\varphi$ es 4. Deduzca que $\text{Gal}(K_2|\mathbb{F}_2) = \langle\varphi\rangle$.

(5). Sea $\gamma = \alpha\beta$. Pruebe que $\gamma$ no permanece invariante por ningún elemento de $\mathrm{Gal}(K_2|\mathbb{F}_2)$ distinto de la identidad. Concluya que $K_2 = \mathbb{F}_2[\gamma]$.

**Ejercicio 252.**– (2) Sea $K$ un cuerpo finito,car$(K) \neq 2$, y $\theta$ un generador del grupo multiplicativo $K^*$.

(1). Sea $b \in K^*$ y $k \in \mathbb{N}$ tal que $\theta^k = b$. Pruebe que $b$ es un cuadrado en $K$ si y solamente si $k$ es par.

(2). Pruebe que si $a_1, a_2 \in K$ no son cuadrados entonces $a_1 a_2$ es un cuadrado en $K$.

(3). Sea $a \in K$ no cuadrado y consideremos $K_1 = K[\sqrt{a}]$. Calcule el número de elementos de $K_1$.

(4). Sea $b \in K$. Pruebe que existe $b_1 \in K_1$ tal que $b_1^2 = b$.

(5). Pruebe que si $d_1, d_2 \in K$ no son cuadrados entonces $[K[\sqrt{d_1}, \sqrt{d_2}] : K] = 2$.

(6). Pruebe que el cuerpo de descomposición de $f(X) = X^4 - 10X^2 + 1$ sobre $\mathbb{Q}$ es igual a $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Demuestre que para cualquier primo $p$, $f(X)$ es reducible sobre $\mathbb{F}_p[X]$.

**Ejercicio 253.**– Sea $L|k$ una extensión de cuerpos finitos, con $[L : k] = n$, y $f(X) \in k[X]$ un polinomio irreducible que tiene una raíz $a \in L$. Sea $\Phi$ generador del grupo $\mathrm{Gal}(L|k)$ y

$$g(X) = (X - a)(X - \Phi(a)) \cdots (X - \Phi^{n-1}(a)) \in L[X].$$

(1). Pruebe que

$$g(X) = X^n - a_1 X^{n-1} + \ldots + (-1)^n a_n,$$

donde $a_i = S_i(a, \Phi(a), \ldots, \Phi^{n-1}(a))$, y $S_i$ las funciones simétricas elementales.

(2). Deduzca que $\Phi(a_i) = a_i$ para todo $i = 1, \ldots, n$.

(3). A partir de lo anterior, concluya que $g(X) \in k[X]$ y que $f(X)$ factoriza en $L[X]$ en factores lineales.

**Ejercicio 254.**– Construya un cuerpo finito de 16 elementos y calcule un generador del grupo multiplicativo. ¿Cuántos generadores hay?

**Ejercicio 255.**– Pruebe que $2, 3$ ó $6$ es un cuadrado en $\mathbb{Z}/\mathbb{Z}p$ para todo primo $p$. Concluya que el polinomio $(X^2 - 2)(X^2 - 3)(X^2 - 6)$ tiene una raíz en $\mathbb{Z}/\mathbb{Z}p$ para todo primo $p$ pero no tiene raíces en $\mathbb{Z}$.

**Ejercicio 256.**– Sea $k = \mathbb{Z}/\mathbb{Z}p$ y $a \in k, a \neq 0$. El cuerpo de descomposición del polinomio $f(x) = X^p - X - a$ sobre $k$ es $k[\alpha]$, donde $\alpha$ es una raíz de $f(x)$. Pruebe explícitamente que el grupo de Galois de $k[\alpha]$ sobre $k$ es cíclico.