Ejercicios de Álgebra Básica. Curso 2010/11

Ejercicio 1.– Construir las tablas de verdad de las siguientes proposiciones:

(1). $\neg p \to \neg q$

(2). $[(p \vee q) \wedge \neg q] \to p$

(3). $[(p \wedge q) \to r] \wedge p \to (q \to r)$

(4). $[(p \vee q) \wedge \neg q] \to p$

(5). $[(p \to q) \wedge p] \to q$

Ejercicio 2.– Construir las tablas de verdad de las siguientes proposiciones $(p \to q) \wedge (q \to p)$ y $p \leftrightarrow q$ y probar que son lógicamente equivalentes.

Ejercicio 3.– Probar que la proposición $(p \wedge q) \vee (\neg p \vee \neg q)$ es una tautología y $(\neg p \vee \neg q) \wedge (p \wedge q)$ es una contradicción.

Ejercicio 4.– Usando los cuantificadores universales y existenciales, formalizar las siguientes proposiciones:

(1). Existen elementos del conjunto A que son menores que todos los elementos del conjunto B.

(2). Todo elemento del conjunto A se puede escribir como suma de dos cuadrados de enteros.

Ejercicio 5.– Dar una prueba directa de la siguiente proposición: Todo entero acabado en cero es un número par.

Ejercicio 6.– Probar, usando el método de inducción, la fórmula de la suma de n términos de una progresión geométrica de razón r,

$$S_n = \frac{ra_n - a_1}{r-1}.$$

Ejercicio 7.– Probar que, para todo $n \in \mathbb{N}$, se verifica que

$$1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6.$$

Ejercicio 8.– Probar que $2^n > n^2, \forall n \geq 5$.

Ejercicio 9.– (•) Sean m, n enteros no negativos. Recordamos que el número combinatorio $\binom{m}{n}$ está definido de la forma siguiente:

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}$$

Probar que $\binom{m}{n} = \binom{m}{m-n}$ y que $\binom{m}{n-1} + \binom{m}{n} = \binom{m+1}{n}$.

Ejercicio 10.– (•) Probar por inducción que

$$(a+b)^m = \sum_{n=0}^{m} \binom{m}{n} a^{m-n} b^n.$$

Ejercicio 11.– Probar que todo número natural mayor que 1 es divisible por un número primo.

Ejercicio 12.– Probar que $\forall n \geq 30$, existen enteros no negativos k, j tales que $n = k6 + j7$. (Ver primero los casos $n = 30, 31, 32, 33, 34$ y 35).

Ejercicio 13.– Efectuar las siguientes operaciones:

$$\begin{array}{lll} (1+2i)^6 & 1/(3+i) & (2-i)/3i \\ ((1-i)^5-1)/((1+i)^5+1) & (1+i)^5/(1-i)^5 & (1+i)^n/(1-i)^{n-2},\ n \geq 3. \end{array}$$

Ejercicio 14.– Calcular i^n, $n \in \mathbb{Z}$.

Ejercicio 15.– Probar que la raíz cuadrada de $x + iy$, $x, y \geq 0$, es

$$\pm\left(\sqrt{\frac{1}{2}\left(x+\sqrt{x^2+y^2}\right)}+i\sqrt{\frac{1}{2}\left(-x+\sqrt{x^2+y^2}\right)}\right).$$

Ejercicio 16.– Escribir en la forma $a + ib$:

$$\sqrt{2i},\ \sqrt{3-4i},\ \sqrt{-3-4i},\ \sqrt{1-i\sqrt{3}},\ \sqrt[4]{-1},\ \sqrt[4]{2-i\sqrt{12}}.$$

Ejercicio 17.– Expresar los siguientes números complejos es forma trigonométrica:

$$1, -1, i, -i, 1+i, -1+i, -1-i, 1-i, 1+i\sqrt{3}, -1+i\sqrt{3}, -1-i\sqrt{3}, 1-i\sqrt{3}, \sqrt{3}+i, \sqrt{3}-i.$$

Ejercicio 18.– Sea $z = r(\cos(\alpha) + i\mathrm{sen}(\alpha))$. Dar una fórmula (en forma trigonométrica) para $\sqrt{z}$. Usarla para calcular la raíz cuadrada de los números del ejercicio anterior.

Ejercicio 19.– Describir las relaciones de inclusión o pertenencia entre los siguientes conjuntos:

$$A = \emptyset,\ B = \{\emptyset\},\ C = \{a, b\},\ D = \{\{a\}, b\},\ E = \{a\},\ F = \{\{a\}\}.$$

Ejercicio 20.– (•) Probar:

(1). $A \cap \overline{A} = \emptyset$.

(2). Si $A \subset B$ entonces $\overline{B} \subset \overline{A}$

(3). Si $A \subset C$ y $B \subset C$ entonces $A \cup B \subset C$

(4). Si $C \subset A$ y $C \subset B$ entonces $C \subset A \cap B$

(5). Si $A \subset B$ y $C \subset D$ entonces $A \cap C \subset B \cap D$ y $A \cup C \subset B \cup D$

Ejercicio 21.– Sea X un conjunto. Denotaremos por $\mathcal{P}(X)$ al conjunto formado por todos los subconjuntos de X. A $\mathcal{P}(X)$ lo denominaremos el conjunto de las partes de X. Calcular $\mathcal{P}(X)$ cuando X es:

(1). $X = \{1, 2\}$

(2). $X = \{a, b, c\}$

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

Ejercicio 22.– Probar que $\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$ si y sólo si $a = a', b = b'$.

Ejercicio 23.– (•) Sean A, B conjuntos finitos, $\sharp A = n = \sharp B$ y $f : A \to B$ una aplicación. Probar que f es inyectiva si y sólo si f es sobreyectiva. Probar, con un ejemplo, que el resultado es falso si los conjuntos no son finitos.

Ejercicio 24.– Sean $A = \{1,2,3,4,5\}, B = \{a,b,c,d,e,f,g\}$.

(1). Dar ejemplos de correspondencias (no aplicaciones) entre A y B y entre B y A.

(2). Dar ejemplos de aplicaciones entre A y B y entre B y A.

(3). Si es posible, dar ejemplos de aplicaciones inyectivas entre A y B y entre B y A.

(4). Si es posible, dar ejemplos de aplicaciones sobreyectivas entre A y B y entre B y A.

Ejercicio 25.– (•) Sean A, B conjuntos finitos, $\sharp A = n, \sharp B = m$ y $f : A \to B$ una aplicación. Probar que:

(1). Si f es inyectiva, entonces $n \leq m$.

(2). Si f es sobreyectiva, entonces $n \geq m$.

(3). Si f es biyectiva, entonces $n = m$.

Ejercicio 26.– Decir cuales de las siguientes correspondencias son aplicaciones:

(1). $f : \mathbb{R}^+ \to \mathbb{R}$, definida por $f(x) = y$ con $y^2 = x$.

(2). $f : \mathbb{Q}^* \to \mathbb{Z}$, definida por $f(p/q) = p$, para todo $p/q \in \mathbb{Q}$, con p y q primos entre sí.

(3). $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2 - 1$.

(4). $f : \mathbb{Z} \to \mathbb{Z}$, definida por $f(x) = 3x + 1$.

Estudiar la inyectividad y sobreyectividad de las aplicaciones anteriores.

Ejercicio 27.– Sean las aplicaciones

$$\begin{array}{rcl} f : \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & (x+1)^2 \end{array} \qquad \begin{array}{rcl} g : \mathbb{R} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & +\sqrt{x} \end{array} \qquad \begin{array}{rcl} h : \mathbb{Z} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 1 - x \end{array}$$

Calcular todas las composiciones posibles de las aplicaciones anteriores.

Ejercicio 28.– (•) Sean $f\colon X \to Y$ y $g\colon Y \to Z$ dos aplicaciones.

(1). Probar que si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

(2). Probar que si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.

(3). Si $g \circ f$ es sobreyectiva, probar que g es sobreyectiva.

(4). Si $g \circ f$ es inyectiva, probar que f es inyectiva.

Ejercicio 29.– (•) Sea $f\colon X \to Y$ una aplicación. Demostrar que

(1). f es inyectiva si y sólo si existe una aplicación $g\colon \mathrm{Im(f)} \to X$ tal que $g \circ f = \mathrm{id}_X$. (Esto se conoce como una inversa a izquierda.)

(2). f es sobreyectiva si y sólo si existe una aplicación $h\colon Y \to X$ tal que $f \circ h = \mathrm{id}_Y$. (Esto se conoce como una inversa a derecha.)

Ejercicio 30.– (•) Sean $f : A \to B$ una aplicación, $A_1 \subset A_2 \subset A, B_1 \subset B_2 \subset B$. Probar que:

(1). $f(A_1) \subset f(A_2)$.

(2). $f^{-1}(B_1) \subset f^{-1}(B_2)$.

Ejercicio 31.– Sea $f : \mathbb{R} \to \mathbb{R}$, la aplicación definida por $f(x) = x^2 + x - 2$. Consideremos los conjuntos $A = \{1, -1, 0, 2\}, B = \{0, -2\}$. Calcular $f(A)$ y $f^{-1}(B)$.

Ejercicio 32.– Sea $f : \mathbb{Z} \to \mathbb{Z}$ la aplicación

$$f(n) = \begin{cases} n & \text{si } n \text{ es par} \\ 0 & \text{si } n \text{ es impar} \end{cases}$$

Calcular las restricciones de f a los números pares y a los números impares.

Ejercicio 33.– (•) Sea $f \colon X \to Y$ una aplicación, y sean $A \subseteq X$ y $B \subseteq Y$.

(1). Si f es inyectiva, probar que $A = f^{-1}\big(f(A)\big)$.

(2). Si f es sobreyectiva, probar que $f\big(f^{-1}(B)\big) = B$.

Ejercicio 34.– ¿Son las siguientes relaciones de equivalencia?

(1). En $\mathbb{R}$, $x\,R\,y \iff xy > 0$.

(2). En $\mathbb{Z}$, $x\,R\,y \iff xy \geq 0$.

(3). En $\mathbb{R}^2$, $(x, y)\,R\,(x'y') \iff$ existe un $\lambda \in \mathbb{R}^*$ tal que $x = \lambda x'$ e $y = \lambda y'$

(4). En $\mathbb{Z}$, $x\,R\,y \iff x - y$ es múltiplo de 6.

(5). En $\mathcal{P}(X)$, $A \mathcal{R} B \iff A \cap B \neq \emptyset$, siendo X un conjunto dado.

(6). En $\mathbb{R}^2$, $(x, y)\,R\,(x'y') \iff y' - y = 2(x' - x)$.

En los casos afirmativos dar el conjunto cociente.

Ejercicio 35.– Sea $n \geq 3$.

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

(2). Demostrar que toda permutación de S_n se puede poner como producto de las permutaciones $(1\ i)$, con $i = 2, ..., n$.

(3). Probar que toda permutación de S_n es producto de las permutaciones $(i-1\ i)$, con $i = 2, ..., n$.

(4). Demostrar que toda permutación de S_n se puede poner como producto de las dos permutaciones $(1\,2\ \ldots n)$ y $(1\,2)$.

Ejercicio 36.– 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 37.– (•) Sean, en S_n, una permutación σ y un ciclo $(a_1\ a_2 \ldots a_r)$. Probar que

$$\sigma(a_1\ a_2 \ldots a_r)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \ldots \sigma(a_r)).$$

Ejercicio 38.– 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 σ_i (distintas entre sí).

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

(3). Halle las inversas de las permutaciones σ_i y de las halladas en (1).

(4). Descomponga las permutaciones σ_i y las halladas en (1) como producto de trasposiciones.

(5). Halle los índices de las permutaciones σ_i y de las halladas en (1).

Ejercicio 39.– Sea $n \geq 3$.

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

(2). Probar que toda permutación de A_n se puede expresar como producto de 3-ciclos.

(3). Pruebe que toda permutación de A_n se puede expresar como producto de las permutaciones $(1\ 2\ i)$, con $i = 3, \ldots, n$.

Ejercicio 40.– Probar que todo entero de la forma $\gamma a + \delta b$, con $\gamma, \delta \in \mathbb{Z}$ es un múltiplo del máximo común divisor de a y b.

Ejercicio 41.– Calcular el máximo común divisor, el mínimo común múltiplo y la identidad de Bézout de: 1520 y 23532, 5328 y 245.

Ejercicio 42.– Sean a, b, m, r enteros positivos, d =mcd(r, m). Probar que $ra \equiv rb \bmod m$ entonces $a \equiv b \bmod (m/d)$.

Ejercicio 43.– Responder a las siguientes cuestiones:

(1). Sean $a, b, c \in \mathbb{N}$. Probar que si mcd$(a, b) = 1$ y $ab = c^2$, entonces existen $n, m \in \mathbb{N}$ tales que $a = n^2$, $b = m^2$.

(2). Probar que si mcd$(a, b) = 1$, entonces mcd$(a + b, a - b) = 1$ ó 2.

(3). Al aplicar el algoritmo de Euclides para calcular el mcd(a, b) se obtiene un resto que es un número primo p. Probar que mcd$(a, b) = 1$ o p.

Ejercicio 44.– Demostrar los siguientes resultados:

(1). $c \cdot$ mcd$(a, b) =$ mcd(ac, bc).

(2). Si mcd$(a, b) = d$ y $\alpha a + \beta b = d$, entonces mcd$(\alpha, \beta) = 1$.

(3). Si $a|bc$ y mcd$(a, b)|c$, entonces $a|c^2$.

(4). Si a y b son primos entre sí entonces también lo son $a + b$ y $(a + b)^2 + ab$.

Ejercicio 45.– Demostrar que la fracción $(2n+3)/(4n+5)$ es irreducible para todo n natural.

Ejercicio 46.– Sean $a = n^3 + 3n^2 - 7,\ b = n+1$ dos números enteros con $n > 2$. Demostrar que todo divisor común de a y b divide a 5. ¿Cuál es la condición sobre n para que $\mathrm{mcd}(a,b) = 5$?

Ejercicio 47.– Probar que 6 divide a $a(a+1)(2a+1)$ para todo a natural.

Ejercicio 48.– Dar criterios de divisibilidad para $2, 3, 4, 5, 7, 9, 11$.

Ejercicio 49.– Probar que entre m enteros consecutivos exactamente uno es divisible por m. A partir de esto, dados enteros $m > n > 1$, demostrar que existe t tal que $n \leq t < m$, y tal que $m - n$ divide a t.

Ejercicio 50.– Sea $d = \mathrm{mcd}(a,b)$. Probar que la ecuación $ax + by = c$ admite soluciones enteras si y sólo si c es un múltiplo de d, en cuyo caso existen infinitas soluciones dadas por:

$$x = x_0 + \frac{bn}{d}, \quad y = y_0 - \frac{an}{d}, \qquad n \in \mathbb{Z},$$

donde x_0, y_0 es una solución particular.

Ejercicio 51.– Resolver, si es posible, las siguientes ecuaciones en congruencias:

- $13x \equiv 5 \pmod{11}$
- $8x \equiv 20 \pmod{12}$
- $8x \equiv 5 \pmod{10}$
- $28x \equiv 36 \pmod{24}$

Ejercicio 52.– Resolver los siguientes sistemas

$$\left\{\begin{array}{lcll} x & \equiv & 5 & \mathrm{mod}\ 2 \\ x & \equiv & 6 & \mathrm{mod}\ 3 \\ x & \equiv & 7 & \mathrm{mod}\ 5 \\ x & \equiv & 8 & \mathrm{mod}\ 7 \end{array}\right. \qquad \left\{\begin{array}{lcll} x & \equiv & 33 & \mathrm{mod}\ 63 \\ x & \equiv & 32 & \mathrm{mod}\ 64 \\ x & \equiv & 34 & \mathrm{mod}\ 65 \end{array}\right. \qquad \left\{\begin{array}{lcll} x & \equiv & 18 & \mathrm{mod}\ 11 \\ x & \equiv & 3 & \mathrm{mod}\ 18 \\ x & \equiv & 7 & \mathrm{mod}\ 25 \\ x & \equiv & 11 & \mathrm{mod}\ 7 \end{array}\right.$$

Ejercicio 53.– Resolver, en $\mathbb{Z}/\mathbb{Z}5$ el sistema

$$\left\{\begin{array}{ccccccc} 2x & + & y & + & z & = & 1 \\ x & + & y & + & 2z & = & 2 \end{array}\right.$$

Ejercicio 54.– Resolver, en $\mathbb{Z}/\mathbb{Z}7$ el sistema

$$\left\{\begin{array}{ccccccc} x & + & y & + & z & = & 3 \\ 2x & + & y & + & 3z & = & 1 \\ x & & & + & 3z & = & 0 \end{array}\right.$$

Ejercicio 55.– Resolver, en $\mathbb{Z}/\mathbb{Z}3$ el sistema (no lineal)

$$\left\{\begin{array}{ccccccc} & & a & + & c & = & 1 \\ b & + & d & + & ac & = & 1 \\ & & ad & + & bc & = & 0 \\ & & & & bd & = & 2 \end{array}\right.$$

Ejercicio 56.– Resolver, en $\mathbb{Z}/\mathbb{Z}5$ el sistema (no lineal)

$$\left\{\begin{array}{ccccccc} & & a & + & c & = & 0 \\ b & + & d & + & ac & = & 0 \\ & & ad & + & bc & = & 0 \\ & & & & bd & = & 4 \end{array}\right.$$

Ejercicio 57.– Demostrar los siguientes resultados:

(1). Si a es primo con 2 y 3, $(a^2 - 1)$ es divisible por 24.

(2). $n^{13} - n$ es divisible entre $2, 3, 5, 7, 13$ para cualquier entero n.

(3). Los enteros a y a^5 tienen igual el último dígito en base 10.

(4). Si $n > 2$ es impar y el orden de 2 en $\mathbb{Z}/\mathbb{Z}n$ es $n - 1$, entonces n es primo.

Ejercicio 58.– Calcular las unidades de $\mathbb{Z}/\mathbb{Z}11$ y $\mathbb{Z}/\mathbb{Z}16$.

Ejercicio 59.– Calcular, en $\mathbb{Z}/\mathbb{Z}26$, $(3 + \mathbb{Z}26)^{11}$ y $(11 + \mathbb{Z}26)^{11}$.

Ejercicio 60.– Sea p un número primo distinto de 2 y 5. Probar que p divide a uno de elementos del conjunto $\{1, 11, 111, 1111, ...\}$.

Ejercicio 61.– Los números de Fermat $F(n)$ están definidos por

$$F(n) = 2^{2^n} + 1.$$

Probar que si $n \neq m$, entonces $F(n)$ y $F(m)$ son primos entre sí[1].

Ejercicio 62.– Hallar el cociente y el resto, en $\mathbb{Q}[x]$, al dividir los polinomios:

(1). $x^3 - 7x - 1,\ x - 2$.

(2). $x^4 - 2x^2 - 1,\ x^2 + 3x - 1$.

(3). $x^4 + x^3 - 1,\ 2x^2 + 1$.

Ejercicio 63.– Calcular los valores de $a \in \mathbb{Q}$ para que $x^3 - ax^2 - 2x + a + 3$ sea divisible por $x - a$.

Ejercicio 64.– Sea $f(x) \in \mathbb{Q}[x]$ un polinomio que al dividirlo por $(x^2 - 3)(x + 1)$, el resto es $x^2 + 2x + 5$. ¿Cuál es el resto de dividir $f(x)$ entre $x^2 - 3$?

Ejercicio 65.– Sean $f(x) = x^2 - 3x + 2,\ g(x) = x^2 + x + 1$ polinomios con coeficientes en $\mathbb{Q}$. Calcular el máximo común divisor y la identidad de Bèzout.

Ejercicio 66.– Calcular, en $\mathbb{Z}/\mathbb{Z}5[x]$, el máximo común divisor de $3x^3 + 4x^2 + 3$ y $3x^3 + 4x^2 + 3x + 4$.

Ejercicio 67.– Calcular, en $\mathbb{Z}/\mathbb{Z}3[x]$, el máximo común divisor, la identidad de Bèzout y el mínimo común múltiplo de $x^5 + 2x^3 + x^2 + x + 1$ y $x^4 + 2x^3 + x + 1$.

Ejercicio 68.– Calcular, en $\mathbb{Z}/\mathbb{Z}2[x]$, el máximo común divisor, la identidad de Bèzout y el mínimo común múltiplo de $x^6 + x^5 + x^3 + x$ y $x^8 + x^7 + x^6 + x^4 + x^3 + x + 1$.

Ejercicio 69.– Hallar el resto, en $\mathbb{Q}[x]$, al dividir

[1] Fermat conjeturó (1630) que los números $F(n)$ eran primos $\forall n$. Euler, en 1732, probó que $F(5) = 2^{32} + 1 = 4294967297 = 641 \times 6700417$.

(1). $x^3 - 7x - 1,\ x - 2.$

(2). $x^{14} - 2x^2 - 1,\ x - 1.$

(3). $x^{40} + x^{30} - 1,\ x + 1.$

Ejercicio 70.– Sea $f(x) = x^4 - 3x^3 + x^2 + 3x - 2 \in \mathbb{Q}[x]$. Calcular el máximo común divisor de $f(x)$ y $f'(x)$. ¿Tiene $f(x)$ factores múltiples?

Ejercicio 71.– Escribir todos los polinomios de $\mathbb{Z}/\mathbb{Z}2[x]$ de grado menor o igual que tres. Decir cuáles de ellos son irreducibles.

Ejercicio 72.– Calcular las raíces en $\mathbb{C}$ de:

$$\Phi_3(x) = x^3 - 1, \qquad \Phi_8(x) = x^8 - 1, \qquad \Phi_{12}(x) = x^{12} - 1.$$

Ejercicio 73.– Sabiendo que $f(x) = x^4 - 4x^3 + 3x^2 + 14x + 26$ tiene a $3 + 2i$ como raíz, factorizar el polinomio $f(x)$ en factores irreducibles en $\mathbb{R}[x]$.

Ejercicio 74.– Demostrar las siguientes cuestiones:

(1). $\forall z_1, z_2 \in \mathbb{C}$ se verifica que $z_1\overline{z}_2 + \overline{z}_1 z_2 \in \mathbb{R}$.

(2). Si

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 \in \mathbb{C}[x],$$

y consideramos los polinomios

$$\overline{f}(x) = x^n + \overline{a}_{n-1}x^{n-1} + \ldots \overline{a}_1 x + \overline{a}_0,$$

entonces $g(x) = f(x)\overline{f}(x) \in \mathbb{R}[x]$.

(3). Si α es una raíz de $g(x)$, entonces α o $\overline{\alpha}$ es raíz de $f(x)$.

Ejercicio 75.– Calcular las raíces racionales de:

(1). $x^3 - x^2 - 3x + 6$

(2). $6x^3 + x^2 - 5x - 2$

(3). $3x^3 + 7x^2 - 7x - 3.$

Ejercicio 76.– Sea $f(x) \in \mathbb{Z}[x]$ un polinomio mónico.

(1). Probar que todas las posibles raíces racionales son enteras.

(2). Probar que si $b \in \mathbb{Z}$ es una raíz de $f(x)$, entonces $n - b$ divide a $f(n)$ para todo $n \in \mathbb{Z}$.

(3). Usar lo anterior para calcular las raíces racionales de $f(x) = x^4 + 5x^3 - 9x^2 - 14x + 24.$

Ejercicio 77.– Sea $f(x) = x^4 + 15x^3 + 72x^2 + 137x + 174$. Sabiendo que $f(-7) = -1$, calcular las raíces de $f(x)$.

Ejercicio 78.– Estudiar la irreducibilidad y la descomposición en irreducibles de los siguientes polinomios de $\mathbb{Q}[X]$:

(1). $x^5 + x^4 - 2x^3 - 2x^2 - 2x + 4.$

(2). $x^4 + 4x^3 + 6x^2 + 4x - 24$.

(3). $x^5 - 6x^4 + 14x^3 - 16x^2 - 16x + 48$.

(4). $x^4 + 4x^3 + 8x^2 + 10x + 7$ (Indicación: Hacer el cambio $x \longmapsto x - 1$).

(5). $x^4 + 8x^3 + 22x^2 + 24x + 9$.

(6). $x^4 + 2x^3 + 5x^2 + 4x + 4$ (Indicación: Estudiar $f'(x)$).

Ejercicio 79.– Estudiar la irreducibilidad y la descomposición en irreducibles del polinomio $x^4 + 2x - 1$ en $\mathbb{Z}/\mathbb{Z}2[x]$, $\mathbb{Z}/\mathbb{Z}3[x]$ y $\mathbb{Q}[x]$.

Ejercicio 80.– Sea $m(x) = x^2 + x \in \mathbb{Z}/\mathbb{Z}3[x]$. Calcular un representante, módulo $m(x)$, de $f(x)$ de grado menor o igual que el grado de $m(x)$ siendo

(1). $f(x) = x^3 + 2$

(2). $f(x) = x^4 + 2x^2 + 1$

(3). $f(x) = x^n$ con $n = 6, 7, 8, \ldots$.

Ejercicio 81.– Sea $m(x) = x^4 - 2 \in \mathbb{Z}/\mathbb{Z}5[x]$. Calcular un representante, módulo $m(x)$, de $f(x)$ de grado menor o igual que el grado de $m(x)$ siendo

(1). $f(x) = x^5$

(2). $f(x) = x^4 + 2x^2 + 1$

(3). $f(x) = x^n$ con $n = 4, 5, 6, \ldots$.

Ejercicio 82.– En $\mathbb{Z}/\mathbb{Z}2[x]$ módulo $x^4 + x + 1$ calcular el inverso de: $x^3 + x$, $x^2 + x + 1$, $x^2 + x$.

Ejercicio 83.– Resolver en $\mathbb{Z}/\mathbb{Z}2[x]$

$$\begin{array}{rcll} f(x) & \equiv & x & (\text{mod } x^2 + x) \\ f(x) & \equiv & 1 & (\text{mod } x^2 + x + 1) \end{array}$$

Ejercicio 84.– Probar que $\mathbb{Z}$ con la operación $a \star b = a + b + 1$ es un grupo.

Ejercicio 85.– Probar que $\mathbb{R}$ con la operación $a \star b = a + b - ab$ es un grupo.

Ejercicio 86.– Sea G un grupo multiplicativo, $g \in G$ y definimos una nueva operación $\star$ sobre G por la fórmula $a \star b = agb$ para todo $a, b \in G$. Pruebe que G con la operación $\star$ es un grupo.

Ejercicio 87.– 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 88.– Sean n un entero positivo y sea $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ el conjunto de la raíces n–ésimas de la unidad. Probar que U_n es un grupo con el producto de los números complejos.

Ejercicio 89.– Sea X un conjunto, $G = \mathcal{P}(X)$. Decir cuándo $(G, \circ)$ es un grupo, siendo:

(1). $A \circ B = A \cup B$

(2). $A \circ B = A \cap B$

(3). $A \circ B = A - B$ (diferencia)

(4). $A \circ B = A \triangle B$ (diferencia simétrica)

Ejercicio 90.– Sea el conjunto G de las matrices cuadradas de orden 2 sobre $\mathbb{R}$ con la suma ordinaria de matrices. se pide:

(1). Probar que $(G, +)$ es un grupo abeliano.

(2). Probar que el conjunto $\{A \in G \mid \det(A) \neq 0\} \subset G$ no es un subgrupo de G.

(3). Probar que el conjunto $\{A \in G \mid A \text{ es simétrica}\} \subset G$ es un subgrupo de G.

(4). Probar que G no es cíclico.

Ejercicio 91.– Sea el conjunto G de las matrices cuadradas invertibles de orden 2 sobre $\mathbb{R}$ con el producto de matrices. Se pide:

(1). Probar que $(G, \cdot)$ es un grupo no abeliano.

(2). Probar que el conjunto $\{A \in G \mid \det(A) = \pm 1\} \subset G$ es un subgrupo de G.

(3). Probar que el conjunto $\{A \in G \mid A \text{ es simétrica}\} \subset G$ no es un subgrupo de G.

(4). Probar que G no es cíclico.

Ejercicio 92.– 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 (multiplicativo) de $\mathrm{GL}_2(\mathbb{R})$.

Ejercicio 93.– 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 $d = \mathrm{m}cd(m, n)$.

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

Ejercicio 94.– Sea $(G, \star)$ un grupo finito, y sean H y K subgrupos de G con índices (en G) primos entre sí. Pruebe que $G = H \star K$.

Ejercicio 95.– Sea G un grupo. Pruebe que son equivalentes:

(1). G es abeliano.

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

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

Ejercicio 96.– Denotaremos por C_n al grupo multiplicativo cíclico de órden n. Probar que $C_n \times C_m$ es un grupo cíclico si y sólo si $\mathrm{mcd}(n, m) = 1$.

Ejercicio 97.– Sea G un grupo tal que todo elemento tiene orden 2. Entonces G es abeliano.

Ejercicio 98.– 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 99.– Pruebe que un grupo es finito si y sólo si contiene un número finito de subgrupos (Idea: Pruébelo primero para grupos cíclicos).

Ejercicio 100.– 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 $C_2 \times C_3$.

Ejercicio 101.– 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 $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z} \times \mathbb{Z}/\mathbb{Z}4$.

Nota.- En lo que sigue G denotará un grupo multiplicativo, salvo que se diga lo contrario.

Ejercicio 102.– (•) Sea G un grupo. Pruebe que la intersección arbitraria de subgrupos normales de G es un subgrupo normal de G.

Ejercicio 103.– (•) 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 104.– 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 105.– 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 106.– Estudiar cuántos homomorfismos existen:

(1). De $\mathbb{Z}$ en $\mathbb{Z}$.

(2). De $\mathbb{Z}/\mathbb{Z}4$ en $\mathbb{Z}/\mathbb{Z}12$, de $\mathbb{Z}/\mathbb{Z}9$ en $\mathbb{Z}/\mathbb{Z}3$, de $\mathbb{Z}$ en $\mathbb{Z}/\mathbb{Z}2$, y de $\mathbb{Z}$ en $\mathbb{Z}/\mathbb{Z}8$.

(3). De $\mathbb{Z}$ en $\mathbb{Z}/\mathbb{Z}m$.

(4). De $\mathbb{Z}/\mathbb{Z}n$ en $\mathbb{Z}/\mathbb{Z}m$.

Ejercicio 107.– 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 108.– Sea G un grupo, sea $C(G) = \{x \in G \mid xy = yx \text{ para todo } y \in G\}$ 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 109.– 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 110.– Si H es un subgrupo de G de índice 2, entonces H es normal en G.

Ejercicio 111.– 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 112.– 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 113.– 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 114.– Sea $f : G \to K$ un homomorfismo de grupos, con G finito. Entonces $|\operatorname{im}(f)|$ divide a $|G|$.

Ejercicio 115.– 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 116.– 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 117.– Sea H un subgrupo normal de orden dos de un grupo G. Pruebe que $H \subset C(G)$.

Ejercicio 118.– 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 119.– Encuentre todos los subgrupos de $(\mathbb{Z}/\mathbb{Z}2)^3$, indicando los que son normales y hallando los cocientes, en esos casos.

Ejercicio 120.– 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 121.– Sea G un grupo finito y $K \subset H \subset G$ subgrupos. Pruebe que $i(H : G)i(K : H) = i(K : G)$.

Ejercicio 122.– Pruebe que $\operatorname{Aut}(\mathbb{Z}) \simeq \mathbb{Z}/\mathbb{Z}2$.

Ejercicio 123.– Sea G un grupo. Pruebe que las aplicaciones definidas por

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

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

Ejercicio 124.– 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 $a - b$.

Ejercicio 125.– (Teorema de Cayley) Sea G un grupo finito de orden n. Entonces $\exists H \subset S_n$ subgrupo tal que $G \simeq H$.