Estructuras Algebraicas

Ejercicios propuestos - Open Course Ware

Javier Jiménez Garrido

Universidad de Cantabria

Para la elaboración de estas notas se ha empleado la *plantilla de LaTeX* 'The Legrand Orange Book' (via http://www.LaTeXTemplates.com) creada por M. Legrand con modificaciones de Vel.

Hoja 0. Números naturales y números enteros. Aritmética Modular

Aparte de realizar los ejercicios de las Secciones A.1 y A.2 (excepto A.2.33 y A.2.36) de los apuntes, se proponen los siguientes ejercicios:

Ejercicio 1 Calcular el máximo común divisor de las siguientes parejas de números:
792 y 702, 2024 y 1196, 4524 y 3002.
En cada caso determinar las identidades de Bézout correspondientes.

Ejercicio 2 A la hora de renovar los equipos de un laboratorio se han comprado N equipos a 2024 € e M equipos a 3234 €. Si el coste total han sido 220000 € y se han comprado la menor cantidad posible de ordenadores a 3234 €, ¿cuántos equipos se han comprado en total?

Ejercicio 3 Dado $k \in \mathbb{Z}$ calcular el máximo común divisor de $5k+3$ y $3k+2$ y determinar la identidad de Bézout correspondiente.

Ejercicio 4 Probar que la sucesión de Fibonacci $0,1,1,2,3,5,8,\ldots$ (definida por $a_1 = 1$, $a_2 = 1$ y $a_n = a_{n-1} + a_{n-2}$ para todo $n \geq 2$), dos términos consecutivos son siempre primos entre sí.

Ejercicio 5 ¿Se puede llenar, sin pasarse, un tanque de agua de 56 litros empleando garrafas de 9 y 6 litros?

Ejercicio 6 ¿Cuántas formas de dividir un año (no bisiesto) en 12 meses de 28, 30 y 31 días existen?

Ejercicio 7 Sea $n = \sum_{j=0}^{k} a_j 10^j$, con $0 \leq a_j \leq 9$. Demostrar los siguientes criterios de divisibilidad:

(I) n es divisible por 2 si y solo si su última cifra a_0 es par.

(II) n es divisible por 3 si y sólo si $\sum_{j=0}^{k} a_j$ es divisible por 3.

(III) n es divisible por 5 si y sólo si $a_0 = 0$ ó $a_0 = 5$.

(IV) n es divisible por 7 si y sólo si $a_0 \cdot 5 + \sum_{j=1}^{k} a_j 10^{j-1}$ es divisible por 7.

(V) n es divisible por 9 si y sólo si $\sum_{j=0}^{k} a_j$ es divisible por 9.

(VI) n es divisible por 11 si y sólo si $\sum_{j=0}^{k} (-1)^j a_j$ es divisible por 11.

Aplicar los criterios a $n = 2024$.

Ejercicio 8 Supongamos que hay un número desconocido de objetos. Si las contamos de tres en tres, nos sobran dos; de cinco en cinco, nos sobran tres; y de siete en siete, nos sobran dos. Pregunta: ¿Cuántos objetos hay?
Versión original: 今有物，不知其數。三、三數之，賸二；五、五數之，賸三；七、七數之，賸二。問：物幾何？

Ejercicio 9 Probar que:

(I) El cuadrado de cualquier número entero es congruente con 0,1 o 4 módulo 8.

(II) Probar que ningún número entero de la forma $8k+7$ con $k \in \mathbb{Z}$, puede escribirse como suma de tres cuadrados (enteros).

(III) Demostrar que si n es un número entero impar que no es divisible por 3, entonces $n^2 \equiv 1 (\text{mód } 24)$.

Ejercicio 10 Isaías, Vera, y Luisa tienen que medir el ancho de un tren para que entre por un túnel. Isaías tiene una regla de 10 cm que le ha prestado su hijo del colegio, después de medir no recuerda cuántas veces había usado la regla, pero sí recuerda que la última medición eran 7 cm. Vera hace uso del ancho de un folio, que mide 21 cm. Vera midió dos trenes que estaban juntos uno al lado de otro, tampoco recuerda cuántas veces usó el folio, pero al final recuerda que la última medición era un poco menos de un cuarto de folio, aproximadamente unos 5 cm. Por último, Luisa usó su bolígrafo de la suerte, que mide 11 cm, no recuerda cuantas veces lo usó, pero recuerda que si en el último paso quitaba la tapa, que mide 1 cm, la medición era exacta. Sabiendo que el ancho del tren mide menos de 5 m, ¿cuánto mide?

Ejercicio 11 (La prueba del nueve). Sea $N \in \mathbb{N}_{\geq 1}$, primero sumamos todas las cifras de N. Si el resultado obtenido tiene dos o más cifras, sumamos de nuevo las cifras de este entero natural, y seguimos así sucesivamente hasta obtener un número n que tenga solamente una cifra, es decir, $1 \leq n \leq 9$. Probar que:

(I) El procedimiento termina en un número finito de pasos.

(II) $N \equiv n \ (\text{mód } 9)$.

La **prueba del nueve** es una forma sencilla de comprobar, si una operación de suma, sustracción, multiplicación o división, realizada a mano, ha dado un resultado erróneo. Dados dos enteros N, M, se puede afirmar que el resultado de operar N con M es erróneo, si al tomar clases de N, M y $N*M$ módulo 9 (mediante el procedimiento anterior) tenemos que $\overline{N}*\overline{M} \neq \overline{N*M}$. Se pide:

(III) Emplear la prueba del nueve para determinar si las siguientes operaciones son falsas.

$$(i)\, 5783 \cdot 40162 = 233256846; \quad (ii)\, 9787 \cdot 1258 = 12342046;$$

$$(iii)\, 8901 \cdot 5743 = 52018443.$$

(IV) Encontrar un ejemplo de una suma, una resta y una multiplicación de dos enteros errónea para la cual la prueba del nueve no sea concluyente.

Ejercicio 12 Leer el artículo “What is the smallest prime?” C. K. Caldwell & Y. Xiong (2012)

Ejercicio 13 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Sean $a,b,c \in \mathbb{Z}/n\mathbb{Z}$. Con el producto de $\mathbb{Z}/n\mathbb{Z}$, si $a \cdot b = a \cdot c$ y $a \neq 0$, entonces $b = c$.

(II) Para todo $n \in \mathbb{N}_{\geq 2}$ se tiene que $\#U(\mathbb{Z}/n\mathbb{Z}) = n-1$.

(III) Para todos $n,m \in \mathbb{N}_{\geq 2}$ se tiene que $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

(IV) La ecuación $x^2 \equiv 2 \mod 7$ no tiene solución porque $\sqrt{2} \notin \mathbb{Q}$.

Ejercicio 14 (Dígitos de control). Los dígitos de control son un mecanismo para detectar errores en el tecleo o transmisión de los datos. Habitualmente consisten en uno o más caracteres numéricos o alfabéticos añadidos al dato original y calculados a partir de éste mediante un determinado algoritmo. Algunos de los ejemplos de uso frecuentes son los números de DNI, ISBN, códigos de barras, tarjetas de crédito o números de cuenta bancarios.

(i) Sea N tu número de DNI o documento similar, identifica a que hace referencia la letra o dígito de control que aparece en él.

(ii) Probar que si $N = \sum_{k=0}^{7} a_k 10^k$, es decir, $a_j \in \{0,1\ldots,9\}$ son las cifras decimales de tu DNI, entonces, el dígito de control, detecta siempre que hemos cambiado un dígito a_j por otro valor $b \in \{0,1\ldots,9\}$ con $b \neq a_j$.

(iii) Probar que si intercambiamos a_j con a_ℓ con $a_j \neq a_\ell$ y $j \neq \ell$, el dígito de control detecta el error.

(iv) Elige alguno de los libros que figuran en la guía docente de la asignatura, identifica a que hace referencia cada una de las partes del ISBN (International Standard Book Number).

(v) Buscar información sobre qué errores de tecleo permite detectar el ISBN y cuáles no. Realiza la demostración o da un ejemplo que muestre que no es capaz de detectar el error.

Hoja 1. Las nociones de grupo y subgrupo

Aparte de realizar los ejercicios de las secciones I.1 y I.2, se recomienda realizar los siguientes ejercicios:

Ejercicio 15 Probar que si a,b son elementos de un grupo $(G,\cdot)$, se cumple que

$$\begin{array}{ccc} (ab)^2 = a^2b^2 & \Leftrightarrow & ab = ba. \\ (ab)^{-1} = a^{-1}b^{-1} & \Leftrightarrow & ab = ba. \end{array}$$

Ejercicio 16 Escribir en notación aditiva las expresiones siguientes:

$$a^3b^4, \qquad a^{-2}(b^{-1}c)^3, \qquad (ab^4)^{-3}c^2 = 1.$$

Ejercicio 17 Se considera en $\mathbb{Q}$ la operación interna definida por $a*b = a+b+a\cdot b$ donde la suma $+$ y el producto $\cdot$ son las operaciones habituales en $\mathbb{Q}$.

(I) Probar que la operación $*$ tiene la propiedad asociativa y conmutativa.

(II) ¿Existe en $\mathbb{Q}$ elemento neutro para la operación $*$?

(III) ¿Qué elementos de $\mathbb{Q}$ poseen inverso para esta operación?

(IV) Determinar el mayor subconjunto de $\mathbb{Q}$ que sea grupo respecto de la operación $*$.

Ejercicio 18 Sea $(G,\cdot)$ un grupo conmutativo. Suponemos que se conocen $a,b,c \in G$, determinar $x \in G$ tal que:

$$abxc = cxax.$$

Ejercicio 19 Dado C un conjunto finito con $n \in \mathbb{N}$ elementos. ¿Cuántas leyes internas existen para C? De entre ellas, ¿cuántas son conmutativas?

Ejercicio 20 Probar que, si para cada elemento a de un grupo G se cumple que $a^2 = 1$, entonces G es abeliano.

Ejercicio 21 Sea $(G,\cdot)$ un grupo con la siguiente propiedad: "para todos $a,b,c,d,x \in G$ tenemos que

si se verifica la igualdad $a\cdot x\cdot b = c\cdot x\cdot d$,
entonces también se satisface la igualdad $a\cdot b = c\cdot d$."

Probar que G es abeliano.

Ejercicio 22 Dado $(C,\star)$ un semigrupo. Dados elementos $a_1,a_2,\ldots,a_n \in C$, para todo $n \in \mathbb{N}$ $n \geq 3$ se define recursivamente

$$a_1 \star a_2 \star \cdots \star a_n := (a_1 \star a_2 \star \cdots \star a_{n-1}) \star a_n.$$

Demostrar por inducción en m que

$$(a_1 \star a_2 \star \cdots \star a_n) \star (b_1 \star b_2 \star \cdots \star b_m) = a_1 \star a_2 \star \cdots \star a_n \star b_1 \star b_2 \star \cdots \star b_m.$$

Ejercicio 23 En este ejercicio demostraremos que en un semigrupo $(C,\star)$ el resultado obtenido al calcular una expresión de la forma

$$((a_1\star a_2)\star(a_3\star(a_4\star a_5)))\star(a_6\star(a_7\star a_8))$$

con $a_i\in C$ es independiente de la forma en la que se agrupen los términos con los paréntesis, siempre y cuando no se altere el orden de los elementos.

Para ello comenzaremos definiendo la **noción de árbol binario** en un conjunto C. Sea $k\in\mathbb{N}$, diremos que E es un **árbol binario de profundidad a lo más** k en un conjunto C si:

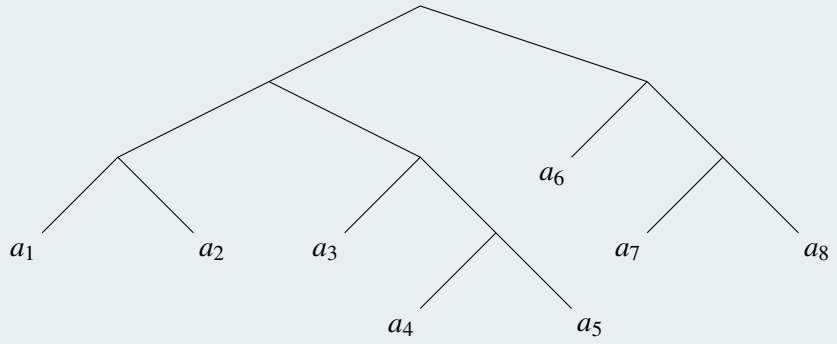
(I) $k=0$ y E es un elemento de C.

(II) $k>0$, y entonces $E=(E_1,E_2)$ siendo E_1 y E_2 árboles binarios de profundidad a lo más $k-1$.

Por ejemplo la expresión

$$A=(((a_1,a_2),(a_3,(a_4,a_5))),(a_6,(a_7,a_8)))$$

es un árbol binario de profundidad a lo más 4. La representación gráfica de este árbol binario es



Dado un árbol binario E en un conjunto S se define la **sucesión de sus hojas** $H(E)$ recursivamente: si E tiene profundidad a lo más 0, entonces $H(E)=(E)$; si E tiene profundidad a lo más k con $k>0$, entonces $E=(E_1,E_2)$, y se define $H(E)$ como la concatenación de $H(E_1)$ y $H(E_2)$. De forma que por ejemplo la sucesión de hojas del árbol anterior es $H(A)=(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$.

De la misma manera definimos el valor del un árbol binario E sobre $(S,\star)$ como $\text{valor}(E):=E$ si E tiene profundidad a lo más 0; en otro caso $E=(E_1,E_2)$ y se define

$$\text{valor}(E):=\text{valor}(E_1)\star\text{valor}(E_2).$$

En el ejemplo que manejamos $\text{valor}(A)=((a_1\star a_2)\star(a_3\star(a_4\star a_5)))\star(a_6\star(a_7\star a_8))$.

Demostrar que si E es un árbol binario sobre un semigrupo $(C,\star)$ cuya sucesión de hojas es $H(E)=(a_1,a_2,\ldots,a_n)$, entonces el valor de E es

$$a_1\star a_2\star\cdots\star a_n.$$

Pista: Hacer la demostración por inducción en la profundidad de árbol E y utilizar el ejercicio anterior.

Ejercicio 24 De un modo similar a la descripción de D_3 y D_4 realizada en el Ejercicio I.1.8 describe el grupo de isometrías del plano que dejan invariante un rectángulo que no es un cuadrado.

Ejercicio 25 Calcular la tabla de $\mathbb{Z}/2\mathbb{Z} \times D_3$. ¿Cuántos elementos tiene? ¿Podrías dar un ejemplo de un grupo distinto con el mismo número de elementos?

Ejercicio 26 Sea $(G,\cdot)$ un grupo abeliano. Fijamos un elemento $a \in G$ y definimos la operación $*_a$ de la siguiente manera

$$x *_a y = axy.$$

¿Es $(G,*_a)$ grupo? ¿Es $(G,*_a)$ grupo conmutativo?

Ejercicio 27 En el conjunto $\mathbb{Z}$ de los números enteros se definen las operaciones:

(I) $x *_1 y = 5x + 7y$.
(II) $x *_2 y = xy - 1$.
(III) $x *_3 y = x$.

¿Qué propiedades tiene $(\mathbb{Z},*_1)$?¿y $(\mathbb{Z},*_2)$?¿y $(\mathbb{Z},*_3)$?

Ejercicio 28 Se definen las operaciones:

(I) $x *_1 y = \dfrac{xy}{(x-1)(y-1)}$ en $G_1 = \mathbb{Q}\backslash\{1\}$.

(II) $x *_2 y = \dfrac{xy}{x^2+y^2}$ en $G_2 = \mathbb{Q}\backslash\{0\}$.

¿Qué propiedades tiene $(G_1,*_1)$?¿y $(G_2,*_2)$?

Ejercicio 29 Sea $(G,\star)$ un semigrupo. Suponemos que existe $e \in G$ tal que:

(a) Para todo $g \in G$ se tiene que $g \star e = g$. *(Neutro por la derecha)*

(b) Para todo $g \in G$ existe $\widetilde{g} \in G$ tal que $g \star \widetilde{g} = e$. *(Inverso por la derecha)*

Probar que G es un grupo. Si sólo asumimos que $(G,\star)$ es un semigrupo que verifica (a), entonces ¿podemos concluir que $(G,\star)$ es un monoide?

Ejercicio 30 En el conjunto de pares de racionales $G = \mathbb{Q}\backslash\{0\} \times \mathbb{Q}$ se define la ley:

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

Probar que $(G,*)$ es un grupo y que $\{(1,b), : b \in \mathbb{Q}\}$ es un subgrupo de G. ¿Es $(G,*)$ conmutativo?

Ejercicio 31 Para todo entero $n \geq 1$, consideramos el conjunto de raíces n-ésimas de la unidad, es decir,

$$R_n = \{e^{2k\pi i/n} : k \in \{0,1\ldots,n-1\}\},$$

Probar que R_n es un subgrupo de $(\mathbb{C}\backslash\{0\},\cdot)$. Describir los elementos y calcular la tabla para $n = 4$. ¿Es $R = \cup_{n\in\mathbb{N}_{\geq 1}} R_n$ un subgrupo de $(\mathbb{C}\backslash\{0\},\cdot)$?

Ejercicio 32 Consideramos el grupo $G = (\mathbb{R}\backslash\{0\}, \cdot)$ y $H = \{x \in \mathbb{R}\backslash\{0\} : x^2 \text{es racional}\}$. Probar que H es un subgrupo de G. ¿Podemos remplazar el exponente 2 por cualquier entero positivo y que H siga siendo un grupo?

Ejercicio 33 Sea H un subgrupo de $(\mathbb{R}, +)$. Sea $K = \{2^a : a \in H\}$, probar que K es un subgrupo de $(\mathbb{R}\backslash\{0\}, \cdot)$.

Ejercicio 34 Determinar todos los subgrupos de $\mathbb{Z}$ que contienen a 20.

Ejercicio 35 Consideramos $\mathscr{C}(\mathbb{R})$: el conjunto de las funciones $f : \mathbb{R} \to \mathbb{R}$ continuas y definimos en $\mathscr{C}(\mathbb{R})$ una estructura de grupo mediante la suma de funciones $(f+g)(x) = f(x)+g(x)$ para todo $x \in \mathbb{R}$. Determinar si los siguientes subconjuntos de $\mathscr{C}(\mathbb{R})$ son subgrupos o no de $(\mathscr{C}(\mathbb{R}), +)$:

(I) $\mathscr{C}^1(\mathbb{R})$ (II) $\{f \in \mathscr{C}(\mathbb{R}) : \int_{\mathbb{R}} f(x)dx < \infty\}$.

(III) $\mathscr{C}^\infty(\mathbb{R})$ (IV) $\{f \in \mathscr{C}(\mathbb{R}) : f \text{ es uniformemente continua en} \mathbb{R}\}$.

Ejercicio 36 Determinar si los siguientes subconjuntos de $(\mathrm{GL}(n,\mathbb{C}), \cdot)$ son o no son subgrupos:

(I) Las matrices con coeficientes reales: $\mathrm{GL}(n,\mathbb{R}) = \{A \in \mathrm{GL}(n,\mathbb{C}) : A \in \mathrm{Mat}_{n\times n}(\mathbb{R})\}$.

(II) Las matrices ortogonales reales: $\mathscr{O}_n(\mathbb{R}) = \{O \in \mathrm{Mat}_{n\times n}(\mathbb{R}) : O^t = O^{-1}\}$.

(III) Las matrices con determinante igual a 1: $\mathrm{SL}(n,\mathbb{C}) = \{A \in \mathrm{GL}(n,\mathbb{C}) : \det(A) = 1\}$.

(IV) Las matrices con coeficientes enteros $\{A \in \mathrm{GL}(n,\mathbb{C}) : A \in \mathrm{Mat}_{n\times n}(\mathbb{Z})\}$.

(V) Las matrices unitarias: $\mathscr{U}_n(\mathbb{C}) = \{U \in \mathrm{GL}(n,\mathbb{C}) : U^* = U^{-1}\}$, donde U^* es la transpuesta de la conjugada de U.

(VI) Las matrices con coeficientes enteros y con determinante igual a 1: $\mathrm{SL}(n,\mathbb{Z}) = \{A \in \mathrm{GL}(n,\mathbb{C}) : A \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \text{ y } \det(A) = 1\}$.

(VII) Para $n = 2$, el conjunto de matrices de la forma $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ con $a \in \mathbb{R}$.

(VIII) Para $n = 3$, el **grupo de Heisenberg**: $H_3(\mathbb{R}) = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{R}\}$.

Ejercicio 37 Calcular el centro del grupo $Z(G)$ en cada caso:

(I) $G = \mathrm{GL}(2,\mathbb{R})$.

(II) $G = D_5$.

(III) El grupo de Heisenberg (ver ejercicio anterior).

Ejercicio 38 Probar que el conjunto $C = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ cuyos elementos son las aplicaciones f_j de $\mathbb{R}\backslash\{0,1\}$ en $\mathbb{R}\backslash\{0,1\}$ definidas por:

$$f_1(x) = x, \qquad f_2(x) = \frac{1}{x}, \qquad f_3(x) = 1-x,$$
$$f_4(x) = \frac{1}{1-x}, \qquad f_5(x) = \frac{x-1}{x}, \qquad f_6(x) = \frac{x}{x-1},$$

tiene estructura de grupo para la composición $f_i \circ f_j(x) = f_i[f_j(x)]$. Hallar todos los subgrupos de $(C, \circ)$.

Ejercicio 39 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) En $(D_n,\circ)$, el grupo de isometrías de un polígono regular de n lados, si $x\in D_n$ es tal que para todo $y\in D_n$ se tiene que $x\circ y = y\circ x$, entonces $x = \mathrm{Id}$.
(II) Dados dos elementos a y b de un grupo $(G,\cdot)$, entonces se cumple siempre que $(ab)^{-3} = b^{-3}a^{-3}$.
(III) Sea A un conjunto. Entonces $(\mathscr{P}(A),\cup)$ es un monoide.
(IV) Sea grupo $(G,\cdot)$ un grupo no conmutativo, entonces para todos $a,b\in G$ se tiene que $ab\neq ba$.
(V) Si H es un subgrupo de $(\mathbb{Z},+)$ y tal que $3,7\in H$, entonces $H=\mathbb{Z}$.
(VI) En el grupo $(\mathbb{Z},+)\times(\mathbb{Z},+)$ se tiene que $<(1,2),(-3,5)>=<(1,13),(0,11)>$.
(VII) En el grupo $(\mathbb{Z},+)\times(\mathbb{Z},+)$ consideramos $S_1 =<(1,2),(-3,5)>$, entonces $(1,0)\in S_1$.
(VIII) En el grupo $(\mathbb{Z},+)\times(\mathbb{Z},+)$ consideramos $S_2 =<(1,1)>$, entonces $S_2\neq\mathbb{Z}\times\mathbb{Z}$.
(IX) Los subgrupos de $(\mathbb{R}^2,+)$ son $\{(0,0)\}$, $\mathbb{R}^2$ y las rectas que pasan por el origen.
(X) $H=\{a+bi : a,b\in\mathbb{R},\ ab\geq 0\}$ es un subgrupo de $(\mathbb{C},+)$.
(XI) $H=\{a+bi : a,b\in\mathbb{R},\ a^2+b^2=1\}$ es un subgrupo de $(\mathbb{C}\backslash\{0\},\cdot)$.
(XII) $\mathbb{R}[x]$ es un subgrupo del conjunto de series de potencias formales $(\mathbb{R}[[x]],+)$.
(XIII) Se cumple que $(2+k)(3+4j)\neq(3+4j)(2+k)$ en $(\mathbb{H}\backslash\{0\},\cdot)$.
(XIV) Se tiene que $(3i-4j)^{-1} = ((-3/25)i+(4/25)j)$ en $(\mathbb{H}\backslash\{0\},\cdot)$.

Ejercicio 40 (Grupo Afín). Para realizar este ejercicio se recomienda haber cursado Álgebra Lineal II. Sea X un espacio afín euclídeo, consideramos el conjunto de todas los isomorfismos afines $f:X\to X$ (aplicaciones afines biyectivas), y lo denotamos por $GA(X)$. Probar que:

(I) $(GA(X),\circ)$ es un grupo, donde $\circ$ es la composición de funciones.
(II) Las semejanzas S son un subgrupo de $(GA(X),\circ)$:

$$S=\{f\in GA(X) : \text{existe } r>0 \text{ tal que } d(f(P),f(Q))=rd(P,Q) \text{ para todos } P,Q\in X\}.$$

(III) Los movimientos M son un subgrupo de $(GA(X),\circ)$:

$$M=\{f\in GA(X) : d(f(P),f(Q))=d(P,Q) \text{ para todos } P,Q\in X\}.$$

(IV) Las traslaciones T son un subgrupo de $(GA(X),\circ)$:

$$T=\{f\in GA(X) : d(f(P),f(Q))=d(P,Q) \text{ y } \overrightarrow{f(P)f(Q)}=\overrightarrow{PQ} \text{ para todos } P,Q\in X\}.$$

Ejercicio 41 Sean S,T subgrupos de un grupo $(G,\cdot)$. Probar que $S\cup T$ es subgrupo de G si y sólo si $S\subseteq T$ o $T\subseteq S$.

Ejercicio 42 Supongamos que H es un subconjunto no vacío de un grupo $(G,\cdot)$ que es cerrado para la operación de grupo y además verifica la siguiente propiedad: Si a no está en H entonces a^{-1} tampoco está en H. ¿Es H un subgrupo de G?

Hoja 2. Grupos cíclicos. Orden de un grupo y orden de un elemento

Aparte de realizar los ejercicios de la Sección I.3 se proponen los siguientes ejercicios.

Ejercicio 43 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) $(\mathbb{Q},+)$ es cíclico.
(II) $(\mathbb{Q}\backslash\{0\},\cdot)$ es cíclico.
(III) El conjunto de raíces $n-$ésimas de la unidad R_n es cíclico, ver Ejercicio31.
(IV) Si G y H son cíclicos, entonces $G\times H$ es cíclico.
(V) El conjunto $H=\{\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} : n\in\mathbb{Z}\}$ es un subgrupo cíclico de $(\mathrm{GL}(2,\mathbb{R}),\cdot)$.
(VI) Q_8 es cíclico.

Ejercicio 44 Leer el artículo "Group Theory in the Bedroom" B. Hayes (2005).

Ejercicio 45 Determinar todos los elementos de orden finito de $(\mathbb{R}\backslash\{0\},\cdot)$ y de $(\mathbb{C}\backslash\{0\},\cdot)$.

Ejercicio 46 Calcular los órdenes de todos los elementos de $(\mathbb{Z}/12\mathbb{Z},+)$ y $(\mathbb{Z}/13\mathbb{Z},+)$.

Ejercicio 47 Comprobar que $(U(\mathbb{Z}/24\mathbb{Z}),\cdot)$ no es cíclico y que posee 7 subgrupos de orden 2 y 7 subgrupos de orden 4.

Ejercicio 48 Determinar todos los subgrupos de $(\mathbb{Z}/225\mathbb{Z},+)$.

Ejercicio 49 Determinar todos los generadores de $(\mathbb{Z}/6\mathbb{Z},+)$, $(\mathbb{Z}/12\mathbb{Z},+)$, $(\mathbb{Z}/30\mathbb{Z},+)$ y $(U(\mathbb{Z}/25\mathbb{Z}),\cdot)$. Determinar todos los generadores un grupo cíclico $G=\langle a\rangle$ de orden n para $n=6$,8 o 20.

Ejercicio 50 Determinar el número de elementos de orden 6 que contiene un grupo cíclico de orden 1200.

Ejercicio 51 Probar que si $(G,\cdot)$ es cíclico e infinito, cada elemento de G distinto del neutro tiene orden infinito.

Ejercicio 52 Sea $(G,\cdot)$ un grupo finito de orden par, probar que $\{a\in G : a\neq a^{-1}\}$ tiene un número par de elementos. Deducir que todo grupo de orden par posee un número impar de elementos de orden 2.

Ejercicio 53 Consideramos el grupo lineal especial $\mathrm{SL}(2,\mathbb{R})$ formado por las matrices 2×2 reales con determinante 1 con la operación del producto de matrices. Consideramos

$$A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\qquad B=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\qquad \text{y}\qquad C=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Calcular $O(A)$, $O(B)$, $O(C)$ y $O(AB)$. Consideramos la matriz C como elemento del subgrupo $\mathrm{SL}(2,\mathbb{Z}/p\mathbb{Z}),\cdot)$ con p primo, ¿cuál es su orden?

Ejercicio 54 ¿Cuál es el orden del grupo $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$? ¿y de grupo $\mathrm{GL}(n,\mathbb{Z}/2\mathbb{Z})$ con $n\in\mathbb{N}$? ¿y de $\mathrm{GL}(n,\mathbb{Z}/p\mathbb{Z})$ con $p\in\mathbb{N}$ primo?

Ejercicio 55 Sean $n > 0$ y m enteros. Probar que la clase de m en $\mathbb{Z}/n\mathbb{Z}$ genera $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $m.c.d(m,n) = 1$.

Ejercicio 56 Consideramos el grupo de los polinomios con coeficientes en $\mathbb{Z}/10\mathbb{Z}$ con la suma, es decir, $(\mathbb{Z}/10\mathbb{Z}[X],+)$. Encontrar el orden de los siguientes elementos:

$$\text{(I)}\ f(x) = 7x^2+5x+4, \quad \text{(II)}\ g(x) = 4x^2+8x+6, \quad \text{(III)}\ f(x)+g(x).$$

Probar que el subconjunto de polinomios de grado menor o igual que 2 que denotamos por $(\mathbb{Z}/10\mathbb{Z})[x]_2$ es un subgrupo. ¿Cuántos elementos tiene? ¿Es cíclico?

Ejercicio 57 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Sea $(G,\cdot)$ un grupo finito con más de un elemento. Entonces G tiene un elemento de orden primo $p \geq 2$.
(II) Sean a y b elementos de un mismo grupo $(G,\cdot)$, entonces $O(ab) = \text{m.c.m.}(O(a),O(b))$.
(III) Sean a y b elementos de un mismo grupo $(G,\cdot)$, entonces si $O(a)$ y $O(b)$ son finitos entonces $O(ab)$ es finito.
(IV) Un grupo conmutativo de orden seis que contiene un elemento de orden 3 es un grupo cíclico.
(V) Un grupo cíclico $(G,\cdot)$ que tiene exactamente tres grupos: G, $\{1\}$ y un subgrupo de orden 7. Entonces G tiene 49 elementos.
(VI) Sea p un número primo. Si un grupo G tiene más de $p-1$ elementos de orden p, entonces G no es cíclico.
(VII) Para todo $n > 2$, el grupo $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$ no es cíclico.
(VIII) Un grupo infinito tiene que tener un número infinito de subgrupos.
(IX) Sean a y b elementos de un mismo grupo $(G,\cdot)$, tal que a tiene orden impar y $aba^{-1} = b^{-1}$, entonces $b^2 = 1_G$.

Ejercicio 58 Si a es un elemento de un grupo $(G,\cdot)$ con $O(a) = 7$, probar que a es el cubo de algún elemento de G. ¿Cómo se puede generalizar este resultado?

Ejercicio 59 Probar que un grupo no puede tener exactamente dos elementos de orden 2. Probar que si un grupo abeliano tiene más de tres elementos de orden 2, entonces tiene al menos 7 elementos de orden 2. Encontrar un ejemplo que demuestre que esto no es cierto, en general, para grupos no abelianos.

Ejercicio 60 Encontrar un ejemplo en cada caso:

(I) Un subgrupo propio de $(\mathbb{Z},+)$ que contiene a 18, 30 y 40. ¿Podrías dar otro diferente?
(II) Un grupo $(G,\cdot)$ no cíclico, tal que todos sus subgrupos propios (distintos de G) son cíclicos.
(III) Un grupo infinito con exactamente dos elementos de orden 4.
(IV) Dos subgrupos H_1, H_2 no triviales de $(\mathbb{R}[x],+)$ con $H_1 \cap H_2 = \{0\}$.
(V) Un grupo no abeliano con 8 elementos y exactamente 6 elementos de orden 4.

Ejercicio 61 Supongamos que $(G,\cdot)$ es un grupo finito con la propiedad de que todo elemento distinto del neutro tiene orden primo (por ejemplo D_3 y D_5). Si el centro del grupo $Z(G)$ es no trivial, probar que todo elemento distinto del neutro tiene el mismo orden.

Hoja 3. Grupos de permutaciones, alternados y diédricos

Aparte de realizar los ejercicios de la Sección I.4, se proponen los siguientes ejercicios.

Ejercicio 62 Sean β y γ en S_4 con $\beta\gamma=(1,4,3,2)$, $\gamma\beta=(1,2,4,3)$, y $\beta(1)=4$. Determinar β y γ. Si γ,β están en S_5 ¿es posible determinarlos?¿y si están en S_6?.

Ejercicio 63 ¿Cuál son los posibles órdenes para de los elementos de S_6, A_6, S_9 y A_9? ¿Qué relación aritmética tienen estos órdenes con el orden del grupo correspondiente? ¿Cuál es el mayor orden posible para un el elemento de A_{10}?

Ejercicio 64 Dadas $\alpha=(1,3,5)(4,2,6)$ y $\beta=(1,2,3)(1,4,5)$ en S_6, expresar α^{101} y β^{99} como producto de ciclos disjuntos y calcular su índice.

Ejercicio 65 Una máquina de barajar cartas eléctrica siempre reordena las cartas del mismo modo en relación al orden en que estas se introducen en la máquina. Todas las cartas de corazones ordenadas del AS (A) al REY (K) se introducen en la máquina, y una vez barajadas por la máquina se vuelven introducir de nuevo. Tras este procedimiento, las cartas salen en el siguiente orden 10, 9, Q, 8, K, 3, 4, A, 5, J, 6, 2, 7. ¿En qué orden estaban las cartas tras mezclarse la primera vez?

Ejercicio 66 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) El conjunto $H=\{\sigma\in S_5 :\ \sigma(2)=2 \text{ y } \sigma(5)=5\}$ es un subgrupo de S_7.
(II) A_n no es abeliano para todo $n\geq 4$.
(III) A_5 tiene un subgrupo de orden 12.
(IV) A_5 tiene un subgrupo de orden 30.
(V) A_5 no tiene subgrupos de orden k con $15\leq k\leq 20$.
(VI) A_5 es el único subgrupo de S_5 de orden 60.
(VII) $H=\{\alpha\in A_4 : \alpha^2=1\}$ es un subgrupo de A_4.
(VIII) $H=\{\alpha\in A_5 : \alpha^2=1\}$ es un subgrupo de A_5.

Ejercicio 67 Se supone que α es un ciclo de longitud 10. ¿Para qué valores $m\in\{2,3,\dots 10\}$ se cumple que $\alpha^m=\alpha\circ\alpha\circ\cdots(m \text{ veces})\cdots\circ\alpha$ es un ciclo de longitud 10?

Ejercicio 68 Demostrar que en S_7, la ecuación $x^2=(1,2,3,4)$ no tiene soluciones pero que la ecuación $x^3=(1,2,3,4)$ tiene al menos dos soluciones.

Ejercicio 69 Encontrar un ejemplo en cada caso:

(I) En S_4 un subgrupo cíclico de orden 4 y un subgrupo que no sea cíclico también de orden 4.
(II) Un subgrupo cíclico en A_8 de orden 4.
(III) Un subgrupo no cíclico en A_8 de orden 4.
(IV) Cinco subgrupos de S_5 de orden 24.
(V) Seis subgrupos de orden 60 en S_6.

Ejercicio 70 ¿Cuál es el menor entero positivo n tal que S_n tiene un elemento de orden mayor que $2n$?

Ejercicio 71 Demostrar que todo elemento de A_n con $n \geq 3$ puede expresarse como un ciclo de longitud 3 o un producto de ciclos de longitud 3.

Ejercicio 72 Sea $H = \{\alpha^2 : \alpha \in S_4\}$ y $K = \{\alpha^2 : \alpha \in S_5\}$. Probar que $H = A_4$ y que $K = A_5$.

Ejercicio 73 Para $n \geq 1$, sea H el conjunto de todas las permutaciones en S_n que se puede expresarse como el producto de un número de trasposiciones múltiplo de cuatro. Demostrar que $H = A_n$.

Ejercicio 74 Sean $\tau, \tilde{\tau} \in S_n$ dos trasposiciones probar que siempre se cumple alguna de las siguientes condiciones:

$$(i)\ \tau\tilde{\tau} = Id. \qquad (ii)\ (\tau\tilde{\tau})^2 = Id. \qquad (iii)\ (\tau\tilde{\tau})^3 = Id.$$

Ejercicio 75 Se recomienda responder las siguientes cuestiones del grupo diédrico empleando su representación como subgrupo de permutaciones, ver Ejercicio I.4.35. Sean s_1, s_2, s simetrías distintas de D_n y $r = r_\theta \in D_n$ una rotación de ángulo $\theta \in [0, 2\pi)$. Probar que:

(I) $s_1 s_2 \neq r_0$.
(II) Si $s_1 s_2 = s_2 s_1$, entonces $s_1 s_2 = r_\pi$.
(III) Para todo $k \in \mathbb{N}$, entonces $r^k s r^k = s$.
(IV) Para todo $k \in \mathbb{N}$, entonces $s r^k s = r^{-k}$, ¿por qué de esto se deduce que D_n es no abeliano?

Ejercicio 76 Se recomienda responder las siguientes cuestiones del grupo diédrico empleando su representación como subgrupo de permutaciones, ver Ejercicio I.4.35. Se pide:

(I) Probar que el conjunto $H_n = \{x^n : x \in D_4\}$ es un subgrupo de D_4.
(II) ¿Es el conjunto $\{x^n : x \in D_3\}$ subgrupo de D_3?
(III) Probar que $\{x^3 : x \in D_6\}$ no es subgrupo de D_6.
(IV) Calcular los órdenes de los elementos de los grupos D_4 y D_7.
(V) Probar que el grupo diédrico D_n contiene un subgrupo de orden m para todo m divisor de $2n$.
(VI) Si r_1, r_2, y r_3 son rotaciones en D_n y s_1, s_2 y s_3 son simetrías en D_n, determinar si $r_1 r_2 s_1 r_3 s_2 s_3 r_3$ es una rotación o un simetría.
(VII) Sea $n \in \mathbb{N}$ y d un entero positivo, $d \neq 2$, tal que d divide a n. Demostrar que el número de elementos de orden d en D_n es $\varphi(d)$. ¿Cuántos elementos de orden 2 hay en D_n?
(VIII) Probar que en todo subgrupo de D_n, o todo miembro del subgrupo es una rotación o exactamente la mitad de miembros son rotaciones.

Hoja 4. Clases laterales. Subgrupos normales. Grupo cociente

Aparte de realizar los ejercicios de la Sección I.5, se proponen los siguientes ejercicios.

Ejercicio 77 Determinar las clases laterales (a izquierda y derecha) que define S en G y el índice de S en G en cada caso:
(I) $S=\{1,b\}$ y $G=D_4$.
(II) $S=\mathrm{SL}(n,\mathbb{R})$ y $G=\mathrm{GL}(n,\mathbb{R})$.
(III) $S=<(2,2)>$ y $G=\mathbb{Z}\times\mathbb{Z}$.
(IV) $S=\{1,11\}$ y $G=U(\mathbb{Z}/30\mathbb{Z})$.
Dar dos sistemas completos de representantes distintos en cada caso.

Ejercicio 78 En el grupo $(\mathbb{C}\backslash\{0\},\cdot)$ consideramos $H=\{a+bi\in\mathbb{C}\backslash\{0\} : a^2+b^2=1\}$. Probar que H es un subgrupo y describir geométricamente la clase $(3+4i)H$.
Determinar todos los subgrupos finitos de $(\mathbb{C}\backslash\{0\},\cdot)$.

Ejercicio 79 Hallar:
(I) Todos los subgrupos de índice 2 de $(\mathbb{R}\backslash\{0\},\cdot)$.
(II) La lista de clases a la izquierda de $\langle a^4\rangle$ en $(\langle a\rangle,\cdot)$ donde a es un elemento de un grupo $(G,\cdot)$ con $O(a)=30$.
(III) El orden de un grupo $(G,\cdot)$ finito con menos de 100 elementos tal que G tiene subgrupos de orden 10 y 25.
(IV) El orden del elemento $4S$ en $U(\mathbb{Z}/105\mathbb{Z})/S$ donde $S=\langle 11\rangle$.
(V) El índice del subgrupo $S=\langle(1,2,3)(4,5)\rangle$ en S_6 y determinar si los siguientes elementos definen clases a izquierda iguales o distintas respecto de S: $a=(1,2,4,6)$, $b=(1,3,4,5,6)$, $c=(1,3,2,6)(4,5)$.
(VI) El tamaño mínimo de un grupo que contiene elementos con órdenes que van desde uno hasta diez.

Ejercicio 80 Sean $(G,\cdot)$ un grupo y H y K subgrupos de G, $a,b\in G$. Se pide:
(I) Probar que $a(H\cap K)=aH\cap aK$.
(II) Probar que si $aH\subseteq bK$, entonces $H\subseteq K$.
(III) Probar que si $\#H=n$ y $\#K=m$ con m.c.d.$(m,n)=1$, entonces $H\cap K=\{1\}$.
(IV) Probar que si $(G,\cdot)$ un grupo finito, y $k\in\mathbb{N}_{\geq 1}$ tal que $\#(G)=k\cdot\#(H)$, entonces para todo $g\in G$ se tiene que $g^{k!}\in H$.

Ejercicio 81 Sean $(G,\cdot)$ un grupo y H y K subgrupos de G. Suponemos que $\#(G)=n$, tomamos p un divisor primo de n y escribimos $n=p^rk$ donde $r\in\mathbb{N}_{\geq 1}$ y $p\nmid k$. Suponemos que $\#H=p^r$ y $\#K=p^\ell$ con con $0<\ell\leq r$ y K no es subgrupo de H. Probar que el conjunto producto $HK=\{hk : h\in H,\, k\in K\}$ no es subgrupo de G.

Ejercicio 82 Leer el artículo "Variations on a Theme: A_4 Definitely Has No Subgroup of Order Six!" M. Brennan & D. Machale (2000).

Ejercicio 83 Consideramos la sucesión definida por $a_1=3$ y $a_n=3^{a_{n-1}}$ para $n\in\mathbb{N}_{\geq 2}$. Encontrar los dos últimos dígitos de a_{2024}.

Ejercicio 84 Sea $(G,\cdot)$ un grupo y sea H un subgrupo normal de G. Si $a\in G$ es un elemento con $O(a)=2$, probar que el conjunto $K=H\cup aH$ es un subgrupo de G. Generalizar enunciado y demostración para el caso $O(a)=k>2$.

Ejercicio 85 Un ejército de hormigas obreras lleva terrones de azúcar a su colonia. Allí, las hormigas ponen 1 terrón de azúcar en la primera cámara, 2 en la segunda, 4 en la tercera, y doblando la cantidad así sucesivamente hasta la cámara número 101.

Entonces, la hormiga reina decide construir bloques cúbicos más grandes de $5\times5\times5$ terrones de azúcar con todo lo que habían recogido anteriormente. ¿Cuántos terrones de azúcar quedarían después de todas estas construcciones?

Ejercicio 86 Determinar en cada caso si S es normal en G o no.

(I) El subgrupo $S=\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix} : a,b,d\in\mathbb{R}, ad\neq 0\right\}$ en $G=\mathrm{GL}(2,\mathbb{R})$.
(II) El subgrupo $S=\{1,(1,2)\}$ en $G=S_3$.
(III) El subgrupo $S=\{\mathrm{Id},(1,2,3),(1,3,2)\}$ en $G=S_3$.
(IV) El subgrupo $S=\{\mathrm{Id},(1,2,3),(1,3,2)\}$ en $G=S_n$ con $n\geq 4$.
(V) El subgrupo $S=\{\sigma\in S_4 : \sigma(4)=4\}$ en $G=S_4$.
(VI) El subgrupo $S=\{1,-1\}$ en $G=Q_8$.
(VII) El subgrupo $S=\mathrm{SL}(n\mathbb{R})$ en $G=\mathrm{GL}(n,\mathbb{R})$.

Ejercicio 87 Dado K un subgrupo de $(\mathbb{R}\backslash\{0\},\cdot)$, consideramos en el grupo $G=\mathrm{GL}(2,\mathbb{R})$, el subconjunto

$$H(K)=\{A\in GL(2,\mathbb{R}) : \det(A)\in K\}.$$

Se pide:

(I) Probar que $H(K)$ es un subgrupo normal de G.
(II) Llamamos $T=H(\{1,-1\})$. Dados $a,b\in G$ con $aT=bT$, ¿qué relación hay entre $\det(a)$ y $\det(b)$?
(III) Llamamos $S=\mathrm{SL}(2,\mathbb{R})=H(\{1\})$. Dada $a\in G$ con $\det(a)=2$. Probar que aS es el conjunto de las matrices de G con determinante 2.

Ejercicio 88 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Sea H es un subgrupo de S_4 que contiene a $(1,2)$ y a $(2,3,4)$, entonces $H=S_4$.
(II) Si $(G,\cdot)$ es un grupo de orden 25 que no es cíclico, entonces $a^5=1$ para todo $a\in G$.
(III) Sea $(G,\cdot)$ un grupo de orden 33, entonces G contiene un elemento de orden 3.
(IV) Si a es un elemento de un grupo $(G,\cdot)$, $O(a)$ es finito y H es un subgrupo normal de G, se cumple que $O(aH)$ en G/H divide a $O(a)$.
(V) Sea $(G,\cdot)$ un grupo de orden 420 y H,K subgrupos de G tales que $K\subseteq H$ y $K\neq H$. Si $\#K=42$, entonces $\#H=84$ o $H=G$.
(VI) Sea $(G,\cdot)$ un grupo abeliano con un número impar de elementos, entonces el producto de todos los elementos de G es la identidad.
(VII) Existe un grupo con menos de 25 elementos y más de un subgrupo de orden 5.
(VIII) Existe un grupo de orden 55 con exactamente 20 elementos de orden 11.
(IX) Sea H un subgrupo normal de un grupo $(G,\cdot)$ con $\#(H)=10$ y $a\in G$ tal que el orden de la clase de a en G/H es $O(aH)=3$. Entonces $O(a)\in\{3,6,15,30\}$.
(X) El grupo cociente $\mathbb{Z}\times\mathbb{Z}/<(4,2)>$ es cíclico.
(XI) Si N es normal en G y G/N es cíclico, entonces G es cíclico.
(XII) Todo grupo cociente de un grupo abeliano es abeliano.

Ejercicio 89 Dado $n \in \mathbb{N}$ consideramos el grupo $(n\mathbb{Z},+)$ formado por los múltiplos de n con la suma usual en $\mathbb{Z}$.

(I) Probar que $n\mathbb{Z}$ es cíclico.

(II) Probar que H es un subgrupo de $n\mathbb{Z}$ si y solo si $H = m\mathbb{Z}$ con $m \in \mathbb{N}$ y $n \mid m$.

(III) Si $m \in \mathbb{N}$ y $n \mid m$, entonces $n\mathbb{Z}/m\mathbb{Z}$ es un grupo cíclico de orden m/n.

Ejercicio 90 ¿Por qué podemos deducir del hecho de que A_4 no tenga subgrupos de orden seis que $\#(Z(A_4)) = 1$?

Comprobar que el único subgrupo de S_4 de orden 12 es A_4 y que A_4 tiene un sólo subgrupo S de orden 4. ¿Por qué la unicidad de un subgrupo de un orden prefijado implica que ese subgrupo es normal?

Ejercicio 91 (Espacio vectorial cociente). Dado V un $\mathbb{K}-$espacio vectorial y S un subespacio vectorial de V. Se pide:

(I) Demostrar que S es un subgrupo normal de $(V,+)$.

(II) Sobre el grupo cociente V/S cuya operación suma sabemos que está definida para todos $v+S, w+S \in V/S$ por

$$(v+S) \boxplus (w+S) = (v+w)+S$$

se define también una ley externa para todo $\lambda \in \mathbb{K}$ y todos $v+S \in V/S$ por

$$\lambda \boxdot (v+S) = (\lambda v)+S$$

Demostrar que V/S es un $\mathbb{K}-$espacio vectorial sobre con las operaciones mencionadas.

(III) Supongamos ahora que $\dim V = n$ y que $\dim S = r$. Tomamos una base $B_S = \{u_1, \ldots, u_r\}$ de S y la extendemos a una base $B = \{u_1, \ldots, u_r, w_{r+1}, \ldots, w_n\}$ de V.
Probar que $\widetilde{B} = \{w_{r+1}+S, \ldots, w_n+S\}$ es una base de V/S y deducir que

$$\dim V = \dim(S) + \dim(V/S).$$

(IV) ¿Cuál es el espacio vectorial cociente que resulta si $S = V$? ¿Y si $S = \{0_V\}$?

(V) En $\mathbb{R}^4$ se considera el subespacio vectorial

$$S = \{(x,y,z,t) \in \mathbb{R}^4 \,:\, x+y-z+2t = 0, x-y+3z+6t = 0\}.$$

Hallar una base de $\mathbb{R}^4/S$ y hallar las coordenadas del vector $(1,-3,2,6)+S$ en esa base.

(VI) Consideremos (X,Σ,μ) un espacio de medida. Se define el espacio vectorial: $\mathscr{L}^1_\mu(X)$ como el espacio de todas las funciones $f : X \to \mathbb{R}$ medibles que cumplen

$$\int_X |f| d\mu < \infty.$$

Una norma natural para definir en estos espacios sería $\|f\|_1 = \int_X |f| d\mu$, Sin embargo, una aplicación así definida no resulta norma, ya que no se cumple $\|f\|_1 = 0 \Rightarrow f = 0$, pues cualquier función que sea igual a la función nula, salvo en un conjunto de medida nula, tendrá norma cero. Probar que $\mathscr{N} = \{f \in \mathscr{L}^1_\mu(X) : \|f\|_1 = 0\}$ es un subespacio vectorial de $\mathscr{L}^1_\mu(X)$. Dada $f \in \mathscr{L}^1_\mu(X)$ describir la clase de equivalencia $f+\mathscr{N}$. Probar que $L^1_\mu(X) = \mathscr{L}^1_\mu(X)/\mathscr{N}$ es un espacio vectorial normado.

Ejercicio 92 Definir una acción de $GL(2,\mathbb{R})$ sobre $\mathbb{R}^2$. ¿Es fiel? ¿y transitiva?

Ejercicio 93 Consideramos el conjunto $X = \text{Aplic}(G,\mathbb{C}) = \{f : G \to \mathbb{C} \ : \ f \text{ es aplicación}\}$ y la aplicación $A : X \times G \to X$ donde para todos $g,h \in G$ toda $f \in X$ se define $(A(f,g))(h) := f(gh)$. Probar que A es una acción de grupo de G sobre X. ¿Es fiel? ¿y transitiva?

Ejercicio 94 Probar que el grupo de rotaciones de un cubo tiene 24 elementos.
(Pista: Considerar X el conjunto de caras del cubo y G el conjunto de permutaciones de las caras que se pueden realizar sin romper el cubo y emplear la fórmula que relaciona el cardinal de G con los cardinales de las órbitas y los estabilizadores)

Ejercicio 95 (Estabilizador y Órbita de un punto). Sea G un grupo de permutaciones de un conjunto I, para cada $i \in I$ se define el **estabilizador de i en G** mediante:

$$stab_G(i) = \{\sigma \in G : \sigma(i) = i\},$$

y la **órbita de i bajo la acción G** como:

$$orb_G(i) = \{\sigma(i) : \sigma \in G\}.$$

El número de elementos de $orb_G(i)$ se denomina **longitud de la órbita**. Probar que:

(I) Probar que para cada $i \in I$, $stab_G(i)$ es subgrupo de G.

(II) Probar que la siguiente relación es una relación de equivalencia:

$$j R_{orb} k \quad \text{si y solo si} \quad \text{existe} \quad i \in I \quad \text{tal que} \quad j,k \in orb_G(i).$$

(III) Sea G un grupo finito de permutaciones de un conjunto I. Probar que para cada $i \in I$ se cumple que:

$$\#G = \#(orb_G(i))\#(stab_G(i)).$$

Ejercicio 96 Consideramos el subgrupo de S_7 dado por

$$G = \{(1),(12)(34),(1234)(56),(13)(24),(1432)(56),(56)(13),(14)(23),(24)(56)\}.$$

Encontrar el estabilizador y la órbita de 1,3,5,7.

Hoja 5. Homomorfismos e isomorfismos de grupos

Aparte de realizar los ejercicios del Bloque I, se proponen los siguientes ejercicios.

Ejercicio 97 Comprobar que las siguientes aplicaciones son homomorfismos. Determinar su núcleo y su imagen.

(I) $f:(\mathbb{R}[x],+)\to(\mathbb{R}[x],+)$ definida por $f(P(x))=\frac{dP}{dx}(x)$.
(II) $f:(S_n,\circ)\to(\{1,-1\},\cdot)$ definida por $f(\sigma)=i(\sigma)$.
(III) $r>0$ y $f_r:(\mathbb{R}_{>0},\cdot)\to(\mathbb{R}_{>0},\cdot)$ dada por $f(x)=x^r$.
(IV) $f:(\mathbb{R}[[x]],+)\to(\mathbb{R}[x],+)$ definida por $f((\sum_{i=0}^{\infty}a_ix^i))=a_0+a_2x+a_4x^2+a_6x^3+a_8x^4$.
(V) $f:\mathbb{Z}/72\mathbb{Z}\to\mathbb{Z}/100\mathbb{Z}$ definida por $f(a+72\mathbb{Z})=25a+100\mathbb{Z}$.

Ejercicio 98 Probar que cada endomorfismo f de $(\mathbb{Q},+)$ queda determinado por $f(1)$ y determinar todos los endomorfismos de $\mathbb{Q}$.

Ejercicio 99 Hallar:

(I) Todos los subgrupos de S_4/V_4 (ver Ejercicio I.5.33) y $(\mathbb{Z}/84\mathbb{Z})/\langle 30\rangle$.
(II) Todos los homomorfismos de $\mathbb{Z}$ en S_3.
(III) Todos los homomorfismos de $\mathbb{Z}/4\mathbb{Z}$ en $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.
(IV) Todos los homomorfismos de grupos de $\mathbb{Z}/2024\mathbb{Z}$ en $\mathbb{Z}/2040\mathbb{Z}$.

Ejercicio 100 Sean α y β endomorfismos de un grupo G y sean $H=\{g\in G:\alpha(g)=\beta(g)\}$. ¿Es H un subgrupo de G? ¿Es H normal en G?

Ejercicio 101 Sea $(G,\cdot)$ es un grupo y sea $f:G\to G$ la aplicación dada por $f(a)=a^2$. Probar que f es homomorfismo si y sólo si G es abeliano.

Ejercicio 102 Encontrar, si es posible, un ejemplo en cada caso:

(I) Un isomorfismo de grupos entre $(\mathbb{R}_{>0},\cdot)$ y $(\mathbb{R},+)$.
(II) Un homomorfismo de $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ sobreyectivo.
(III) Un homomorfismo f de $\mathbb{Z}/17\mathbb{Z}$ a un grupo G arbitrario, pero fijo, que no es inyectivo.
(IV) Un isomomorfismo entre $\mathbb{C}\backslash\{0\}/H$ y $(\mathbb{R}_{>0},\cdot)$ donde $H=\{z\in\mathbb{C}\backslash\{0\}:|z|=1\}$.
(V) Un isomorfismo entre G/H y $\mathbb{Z}/4\mathbb{Z}$ donde G es el grupo $(\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z},+)$ y $H=\{(0,0),(2,0),(0,2),(2,2)\}$.
(VI) Un isomorfismo entre G/K y $\mathbb{Z}/4\mathbb{Z}$ donde $G=\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ y $K=\langle(1,2)\rangle$.
(VII) Un endomorfismo f de $(U(\mathbb{Z}/30\mathbb{Z}),\cdot)$ tal que $f(7)=7$ y $Kerf=\{1,11\}$.

Ejercicio 103 Sean H,K subgrupos normales de un grupo G tales que $H\cap K=\{1\}$. Probar que G es isomorfo a un subgrupo de $G/H\times G/K$.

Ejercicio 104 Sea $(G,\cdot)$ tal que $G/Z(G)$ es cíclico. Probar que G es abeliano. Deducir que no puede existir un homomorfismo de grupos f de D_4 en $\mathbb{Z}$ tal que $\mathrm{Ker}(f)=\{\mathrm{Id},r^2\}$.

Ejercicio 105 Dado $f:G\to H$ un homomorfismo de grupos sobreyectivo, $a\in G$ y $N\lhd G$.

(I) Probar que $f(N)\lhd H$.
(II) Si además f es inyectivo, probar que $f(C(a))=C(f(a))$ (Ejercicio I.6.54).

Dar un ejemplo, en cada caso, que demuestre que la sobreyectividad es necesaria.

Ejercicio 106 Probar que todo grupo de orden 77 es cíclico.

Ejercicio 107 Consideramos el subgrupo $\mathbb{Z}$ de $(\mathbb{Q},+)$, y estudiar si $\mathbb{Q}/\mathbb{Z}$ es isomorfo a $\mathbb{Q}$.

Ejercicio 108 Sea $f: G \to H$ un homomorfismo de grupos. Probar que si $f(g)=h$, entonces $f^{-1}(h) = g\ker f$. Emplear este resultado para:

(I) Determinar $f^{-1}(3)$ probando previamente que la aplicación $f:(\mathbb{Z}\oplus\mathbb{Z},+)\to(\mathbb{Z},+)$ dada por $f(a,b)=a-b$ es un homomorfismo.

(II) Encontrar todos los elementos de $U(\mathbb{Z}/40\mathbb{Z})$ que van a parar a 11 por f con f es un endomorfismo de $(U(\mathbb{Z}/40\mathbb{Z}),\cdot)$ tal que $\mathrm{Ker} f = \{1,9,17,33\}$ y $f(11)=11$.

(III) Probar que si x es una solución particular de un sistema lineal de ecuaciones y S es el conjunto de soluciones del sistema homogéneo asociado, entonces $x+S$ es el conjunto de soluciones del sistema de partida.

Ejercicio 109 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Si S es un subgrupo de G, entonces $S \lhd N(S)$ (ver Ejercicio I.2.23) y si además $N(S)/S$ es abeliano, entonces $N(S)/Z(S)$ es abeliano.

(II) Si G_1, G_2, H_1, H_2 son subgrupos de un grupo G tales que $G_1 \approx H_1$ y $G_2 \approx H_2$, entonces se cumple que $G_1 \times G_2 \approx H_1 \times H_2$.

(III) $U(\mathbb{Z}/8\mathbb{Z}) \approx U(\mathbb{Z}/10\mathbb{Z})$.

(IV) $U(\mathbb{Z}/8\mathbb{Z}) \approx U(\mathbb{Z}/12\mathbb{Z})$.

(V) $(\mathbb{Z},+) \approx (\mathbb{Q},+)$.

(VI) Para todo par de grupos G y H tenemos que $(G\times H)/(G\times\{1_H\}) \approx H$.

(VII) Sea N un subgrupo normal de un grupo finito G. Entonces el orden de gN en G/N divide al orden de g en G para todo $g \in G$.

(VIII) $(\mathbb{R},*) \approx (\mathbb{R},+)$ con $a*b = a\sqrt{1+b^2} + b\sqrt{1+a^2}$.

Ejercicio 110 Sea $G = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$ y

$$H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a,b \in \mathbb{Q} \right\}.$$

Probar que $(G,+)$ y $(H,+)$ son isomorfos. ¿Son $(G\backslash\{0\},\cdot)$ y $(H\backslash\{0_{2\times 2}\},\cdot)$ isomorfos?

Ejercicio 111 Sea $(G,\cdot)$ un grupo y N,H subgrupos normales de G con $N \subseteq H$ tales que G/H es abeliano. Probar que G/N es abeliano. Si G/H es cíclico, ¿podemos deducir que G/N es cíclico?

Ejercicio 112 Demostrar que el grupo $(\mathbb{Z},+)$ no se puede expresar como suma directa de dos subgrupos propios.

Ejercicio 113 Sea $G = \{(x,y) \in \mathbb{R}^2 : y \neq 0\}$ definimos la operación:

$$(x_1,y_1) * (x_2,y_2) = (x_2y_1 + x_1,\ y_1y_2).$$

Probar que:

(I) $(G,\cdot)$ es un grupo.

(II) La aplicación $\varphi: G \to (\mathbb{R}\backslash\{0\},\cdot)$ dada por $\varphi(x,y)=y$, es un homomorfismo de grupos.

(III) $\varphi^{-1}(1)$ es un subgrupo de G isomorfo a $(\mathbb{R},+)$.

(IV) $H = \{(0,y) \in \mathbb{R}^2\}$ es un subgrupo de G isomorfo a $(\mathbb{R}\backslash\{0\},\cdot)$.

Ejercicio 114 Leer el artículo "The Groups of Order Sixteen Made Easy" M. Wild (2005)

Ejercicio 115 (Representación matricial de cuaterniones y complejos). Consideramos el conjunto $H(2,\mathbb{C})$ de las matrices $A \in \mathrm{Mat}_{2\times 2}(\mathbb{C})$ de la forma

$$A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \qquad z,w \in \mathbb{C}.$$

(I) Probar que $(H(2,\mathbb{C}),+)$ es un subgrupo de $(\mathrm{Mat}_{2\times 2}(\mathbb{C}),+)$ y que $(H(2,\mathbb{C})\backslash\{0_{2\times 2}\},\cdot)$ es un subgrupo de $(\mathrm{GL}(2,\mathbb{C}),\cdot)$.
(II) Probar que $(H(2,\mathbb{C}),+) \approx (\mathbb{H},+)$ y que $(H(2,\mathbb{C})\backslash\{0_{2\times 2}\},\cdot) \approx (\mathbb{H}\backslash\{0\},\cdot)$ donde $\mathbb{H}$ es el conjunto de los cuaterniones.
(III) Encontrar un subconjunto C de $H(2,\mathbb{C})$ de matrices con coeficientes reales tales que $(\mathbb{C},+) \approx (C,+)$ y que $(\mathbb{C}\backslash\{0\},\cdot) \approx (C\backslash\{0_{2\times 2}\},\cdot)$. Dada $Z \in C$, ¿Qué representa, a través de este isomorfismo, $\det(Z)$?¿y $\mathrm{tr}(Z)$? Usar estas matrices para interpretar geométricamente el producto de números complejos.
(IV) Encontrar un subconjunto M_8 de 8 matrices de $H(2,\mathbb{C})$ que forme un grupo con la multiplicación isomorfo al grupo de los cuaterniones Q_8.
(V) Encontrar un subconjunto A_n de $2n$ matrices reales de $H(2,\mathbb{C})$ que forme un grupo con la multiplicación isomorfo a D_n.
(VI) Probar que Q_8 no es isomorfo a D_4.

Ejercicio 116 (Grupo de automorfismos). Sea G un grupo consideramos el conjunto de automorfismos:

$$\mathrm{Aut}(G) = \{f : G \to G; \text{con } f \text{ isomorfismo}\}.$$

Se pide:
(I) Probar que $(\mathrm{Aut}(G),\circ)$ es un grupo donde $\circ$ es la ley de composición.
(II) Sea R el subgrupo de todas las rotaciones en D_n. Sea $f \in \mathrm{Aut}(D_n)$ probar que $f(R) = R$.
(III) Encontrar $\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$ y $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ para $n \in \mathbb{Z}$.
(IV) Encontrar $\mathrm{Aut}(D_6)$ y $\mathrm{Aut}(D_7)$.
(V) Encontrar dos grupos G y H tales que $G \not\approx H$, pero $\mathrm{Aut}(G) \approx \mathrm{Aut}(H)$.

Ejercicio 117 (Grupo de automorfismos internos). Sea G un grupo y $a \in G$. Consideramos la función $\phi_a(x) = axa^{-1}$ para todo $x \in G$, se llama **automorfismo interno inducido por** a. Probar que:
(I) ϕ_a es un automorfismo de G para todo $a \in G$.
(II) $\mathrm{AutInt}(G) = \{\phi_a : a \in G\}$ es un subgrupo de $\mathrm{Aut}(G)$.
(III) La correspondencia de G en $\mathrm{AutInt}(G)$ que a cada elemento a lo envía en ϕ_a es un homomorfismo de grupos y que $\mathrm{AutInt}(G) \approx G/Z(G)$.
(IV) Encontrar el grupo de los automorfismos internos para los grupos D_6 y D_7. ¿Qué sucede si G es conmutativo?

Ejercicio 118 (Grupo derivado). Sea $(G,\cdot)$ un grupo, $x,y \in G$. Llamamos **conmutador de** x **e** y al elemento:

$$[x,y] := x^{-1}y^{-1}xy$$

y llamamos **subgrupo derivado de** G al subgrupo generado por todos los conmutadores:

$$G' = < \{[x,y] : \text{para todos} \quad x,y \in G\} >,$$

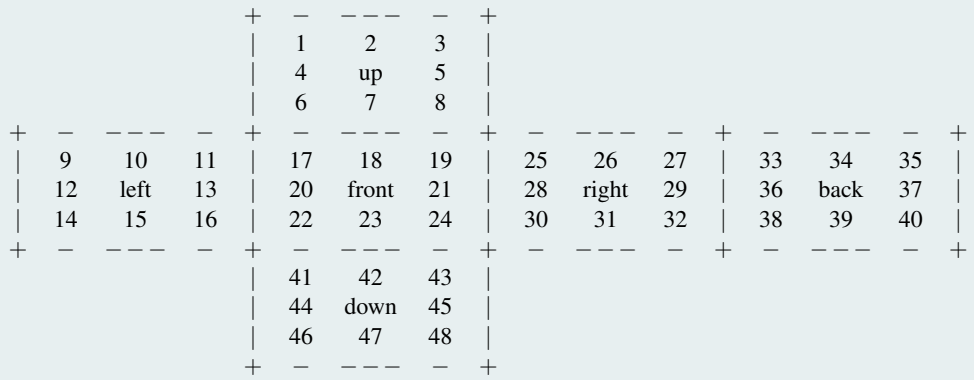
Sea H un subgrupo de G. Probar que:

(I) $[x,y] = 1_G$ si y solo si x e y conmutan.
(II) $[x,y]^{-1} = [y,x]$.
(III) G' es un subgrupo normal en G.
(IV) G/G' es abeliano.
(V) si $H \lhd G$ y G/H es abeliano, entonces $G' \subseteq H$.
(VI) si $G' \subseteq H$, entonces H es normal en G.

Calcular el subgrupo derivado en cada caso:

$$(a)\ \mathbb{Z} \qquad (b)\ Q_8 \qquad (c)\ S_5 \qquad (d)\ A_4 \qquad (e)\ \mathrm{GL}(n,\mathbb{R}).$$

Ejercicio 119 El conjunto de todas las configuraciones del Cubo de Rubik forman un grupo, que puede identificarse con un subgrupo de S_{48} generado por 6 elementos, es decir, Rubik $=< \{F,B,U,D,L,R\} >$ donde F es la permutación producida al girar sobre la cara frontal, B sobre la cara opuesta a la cara frontal (back), U sobre la cara situada en la parte superior (up), D sobre la cara opuesta (down), L sobre la cara izquierda (left) y R sobre la cara derecha (right).



Se pide:

(I) Describir F,B,U,D,L,R como elementos de S_{48}.
(II) Emplear SAGE para calcular el orden del grupo del Cubo de Rubik.
(III) Emplear SAGE para calcular el orden de $U \circ L$, $U \circ L \circ F$ y $U \circ L \circ B$.
(IV) Clasificar el grupo $< \{L,\ R\} >$.

Ejercicio 120 (Representación de una acción de grupo como un homomorfismo). Probar que definir una acción A de G sobre X equivale a definir un homomorfismo de grupos $f : G \to S(X)$. En otras palabras, probar que la correspondencia dada por:

$$\Psi: \ \{\text{Acciones de } G \text{ sobre } X\} \ \to \ \{\text{Homomorfismos de } G \text{ en } S(X)\}$$

$$A \qquad\qquad \Psi(A) = f_A: \begin{array}{ccc} G & \to & S(X) \\ g & \to & A_g: \begin{array}{ccc} X & \to & X \\ x & \to & A(x,g) \end{array} \end{array}$$

es una aplicación biyectiva. *(Nota: Debemos probar que $A_g \in S(X)$, que f_A es homomorfismo de grupos y, finalmente que Ψ es biyectiva)* Si sabemos que A es fiel, ¿qué podemos decir de f_A? Relacionar las nociones de órbita y estabilizador del Ejercicio 95 con las nociones del Ejercicio I.5.51.

Hoja 6. Anillos. Subanillos. Ideales. Anillo Cociente. Característica

Se recomienda realizar los ejercicios de las secciones II.1 y II.2.

Ejercicio 121 Dar un ejemplo de:

(I) un anillo finito no conmutativo.

(II) un anillo infinito no conmutativo sin elemento unidad.

(III) un subconjunto de un anillo que es un subgrupo para la suma pero no es un subanillo.

Ejercicio 122 Sea X un conjunto. Para todos $A, B \in R = \mathscr{P}(X)$ definimos:

$$\begin{array}{rcl} A \,\Delta\, B & := & (A \backslash B) \cup (B \backslash A). \\ A \,\square\, B & := & A \cap B. \end{array}$$

Probar que $(R, \Delta, \square)$ es un anillo. ¿Quién es 0_R?¿Quién es el opuesto de $A \in R$ para Δ? ¿Es R conmutativo?¿Es R unitario? Si la respuesta a la última pregunta es afirmativa, ¿quién es 1_R? Hallar las tablas de Δ y $\square$ para $X = \{a, b, c\}$.

Ejercicio 123 Probar que el conjunto $R = \{0, 2, 4, 6, 8\}$ es un anillo para la suma y el producto módulo 10. Probar que es unitario y encuentra 1_R.

Ejercicio 124 Sea $(R, +, \cdot)$ un anillo en el que se satisface la siguiente propiedad (Ley de Cancelación):

$(\star)$ para todos $a, b, c \in R$ con $a \neq 0$ si $ab = ca$, entonces $b = c$.

Probar que R es conmutativo.

Ejercicio 125 Sea $(R, +, \cdot)$ un anillo y supongamos que existe $n \in \mathbb{N}_{\geq 2}$ tal que $x^n = x$ para todos los elementos $x \in R$. Probar que:

(I) Si m es un entero positivo y $a^m = 0$ con $a \in R$, entonces $a = 0$.

(II) Si $ab = 0$ con $a, b \in R$, entonces $ba = 0$.

(III) Si n es par, entonces $-a = a$ para todo $a \in R$.

Ejercicio 126 Leer el artículo "Finite Rings of Odd Order with Few Nilpotent and Idempotent Elements" A. Y. M. Chin (2018)

Ejercicio 127 (Elementos Nilpotentes). Sea $(R, +, \cdot)$ un anillo y $a \in R$ decimos que a es **nilpotente** si existe $n \in \mathbb{N}_{\geq 1}$ tal que $a^n = 0_R$. Probar que:

(I) si R es unitario y a es nilpotente, entonces $1_R - a$ tiene inverso para el producto en R.

(II) si R es conmutativo, entonces $S = \{a \in R : a \text{ es nilpotente}\}$ es un subanillo de R.

(III) el anillo $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ tiene un elemento no nulo nilpotente si y solo si n es divisible por el cuadrado de un número primo.

Ejercicio 128 (Matrices Nilpotentes - Caracterización). Sea $n \in \mathbb{N}_{\geq 1}$ y $N \in \mathrm{Mat}_{n\times n}(\mathbb{R})$, probar que son equivalentes:

(I) N es nilpotente.

(II) el polinomio característico de N ($P_N(x) = \det(x\mathrm{Id}_n - N)$) es igual a x^n.

(III) el polinomio mínimo de N es x^k para algún entero $k \leq n$.

(IV) el único valor propio (complejo) de N es 0.

(V) la traza de N^k es nula, es decir, $\mathrm{tr}(N^k) = 0$ para cada $k \in \mathbb{N}_{\geq 1}$.

Ejercicio 129 (Matrices Nilpotentes). Sea $n \in \mathbb{N}_{\geq 1}$ consideramos el anillo $(\mathrm{Mat}_{n\times n}(\mathbb{R}), +, \cdot)$. Probar que:

(I) si N es una matriz nilpotente, entonces necesariamente $\det(N) = 0$. Mostrar que el recíproco no es cierto.

(II) si N es una matriz triangular con ceros a lo largo de la diagonal, entonces es nilpotente. Mostrar que existen matrices nilpotentes con todas las entradas no nulas.

(III) si N es una matriz nilpotente, entonces $\det(\mathrm{Id}_n + N) = 1$. Recíprocamente, probar que si para todo $t \in \mathbb{R}$ se tiene que $\det(\mathrm{Id}_n + tN) = 1$, entonces N es nilpotente.

(IV) la única matriz diagonalizable y nilpotente de $Mat_{n\times n}(\mathbb{R})$ es la matriz nula.

Ejercicio 130 (Elementos Idempotentes). Sea $(R, +, \cdot)$ y $a \in R$ decimos que a es **idempotente** si $a^2 = a$. Probar que:

(I) si a es idempotente, entonces $a^n = a$ para todo $n \in \mathbb{N}_{\geq 1}$.

(II) si R es conmutativo y a y b son idempotentes, entonces también son idempotentes ab, $a - ab$, $a + b - ab$ y $a + b - 2ab$.

(III) si R conmutativo y unitario y a es idempotente, entonces también es idempotente $1_R - a$.

Ejercicio 131 En cada caso, encontrar todas las unidades, todos los divisores del cero, todos los elementos idempotentes y todos los elementos nilpotentes.

(I) En el anillo de los enteros de Gauss $\mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$.

(II) En el anillo producto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

(III) En el anillo de matrices $\mathrm{Mat}_{2\times 2}(\mathbb{R})$.

(IV) En el anillo de matrices $\mathrm{Mat}_{2\times 2}(\mathbb{Z}/3\mathbb{Z})$.

Ejercicio 132 En un anillo unitario, encontrar:

(I) todos los elementos que son a la vez idempotentes y nilpotentes.

(II) todos los elementos que son a la vez idempotentes y unidades.

Ejercicio 133 Sea $A = Aplic(\mathbb{R},\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$ el conjunto de todas las funciones reales con valores reales. Definimos una estructura de anillo en este conjunto mediante la suma y el producto de funciones usual [$(f+g)(x) = f(x)+g(x)$ y $(fg)(x) = f(x)g(x)$ para todo x en $\mathbb{R}$]. Determinar todos los divisores del cero de A. Determinar todos los elementos nilpotentes de A. Probar que todo elemento no nulo es o bien un divisor del cero o bien una unidad.

Ejercicio 134 Sea $(R,+,\cdot)$ un anillo conmutativo y unitario y $a,b,c \in R$. Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Si $a^2 = a$, entonces o bien $a = 0$ o bien $a = 1$.
(II) Si $ab = 0$, entonces o bien $a = 0$ o bien $b = 0$.
(III) Si $a \in U(R)$ y $b \mid c$, entonces $ab \mid c$.
(IV) Si $a \in U(R)$ y $b^2 = 0$, entonces $a+b \in U(R)$.
(V) Si $ab = ac$ y $a \neq 0$, entonces $b = c$.

Ejercicio 135 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Si R es un anillo tal que $x^3 = x$ para todo $x \in R$, entonces $6x = 0$ para todo $x \in R$.
(II) En el conjunto de las sucesiones de números reales $\mathbb{R}^{\mathbb{N}}$ definimos las operaciones

$$(a_j)_{j\in\mathbb{N}} \boxplus (b_j)_{j\in\mathbb{N}} = (a_j + b_j)_{j\in\mathbb{N}} \qquad (a_j)_{j\in\mathbb{N}} \boxdot (b_j)_{j\in\mathbb{N}} = (a_j \cdot b_j)_{j\in\mathbb{N}}$$

entonces $(\mathbb{R}^{\mathbb{N}}, \boxplus, \boxdot)$ es un anillo conmutativo y unitario sin divisores del cero no nulos.
(III) $(\mathbb{Z},+,+)$ es un anillo.
(IV) Para todo anillo $(R,+,\cdot)$ se cumple que $0_R \notin U(R)$.
(V) En $\mathbb{Z}/8\mathbb{Z}$ se tiene que $3|7$.
(VI) Si un anillo es cíclico para la suma, entonces es conmutativo.
(VII) Si $(R,+,\cdot)$ es un anillo conmutativo y unitario y $(S,+)$ es subgrupo de $(R,+)$, entonces S es subanillo de R.
(VIII) Sea R un anillo y $a \in R$. Entonces $S = \{x \in R : ax = 0_R\}$ es un subanillo de R.
(IX) El subconjunto $S = \{(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} : a+b=c\}$ es un subanillo de $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$.
(X) Sea R un anillo unitario y $a \in R$ tal que $a^2 = 1_R$. Entonces $S = \{ara : r \in R\}$ es un subanillo de R.
(XI) Sean A,B y C subanillos de un anillo R. Si $A \subseteq B \cup C$, entonces $A \subseteq B$ o $A \subseteq C$.
(XII) Sea R un anillo, si $a^2 - b^2 = (a+b)(a-b)$ para todos $a,b \in R$, entonces R es conmutativo.

Ejercicio 136 Encontrar:

(I) Todos los subanillos de $(\mathbb{Z},+,\cdot)$.
(II) Todos los subanillos de $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$.
(III) El subanillo más pequeño de $\mathbb{Q}$ que contiene a $2/3$.

Ejercicio 137 Determinar si los siguientes subconjuntos de $\mathrm{Mat}_{2\times2}(\mathbb{Z})$ son subanillos o no:

$$S_1 = \left\{ \begin{pmatrix} a & a+b \\ a+b & b \end{pmatrix} : a,b \in \mathbb{Z} \right\}, \qquad S_2 = \left\{ \begin{pmatrix} a & a-b \\ a-b & b \end{pmatrix} : a,b \in \mathbb{Z} \right\},$$

$$S_3 = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} : a,b \in \mathbb{Z} \right\}, \qquad S_4 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in \mathbb{Z} \right\}$$

Ejercicio 138 (Anillo de Matrices). Dado $(R,+,\cdot)$ un anillo conmutativo y unitario y $n,m\in\mathbb{N}_{\geq 1}$. Decimos que A es **una matriz de tamaño** $n\times m$ **con coeficientes en** R si A es una aplicación de $\{1,\dots,n\}\times\{1,\dots,m\}$ en R, es decir,

$$A:\{1,\dots,n\}\times\{1,\dots,m\}\to R.$$

La imagen de un elemento (i,j) se denota por $a_{i,j}:=A(i,j)$ y se denomina entrada $(i,j)-$ésima de la matriz A. Habitualmente, en lugar de la notación funcional, representamos la matriz A de la siguiente forma:

$$A=\left(a_{ij}\right)_{1\leq j\leq m}^{1\leq i\leq n}=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m}\\ a_{21} & a_{22} & a_{23} & \cdots & a_{2m}\\ a_{31} & a_{32} & a_{33} & \cdots & a_{3m}\\ \vdots & \vdots & \vdots & \cdots & \vdots\\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nm}\end{pmatrix}.$$

De la misma manera, el conjunto de matrices de tamaño $n\times m$ con coeficientes en R que se denota por $\mathrm{Mat}_{n\times m}(R):=\mathrm{Aplic}(\{1,\dots,n\}\times\{1,\dots,m\},R)$. Dadas $A,B\in\mathrm{Mat}_{n\times m}(R)$, definimos la operación suma del modo usual:

$$\begin{array}{ccccc} +:\mathrm{Mat}_{n\times m}(R)\times\mathrm{Mat}_{n\times m}(R) & & \to & & \mathrm{Mat}_{n\times m}(R)\\ A \quad , \quad B & & \to & & A+B=\left(a_{ij}\right)_{1\leq j\leq m}^{1\leq i\leq n}+\left(b_{ij}\right)_{1\leq j\leq m}^{1\leq i\leq n}:=\left(a_{ij}+b_{ij}\right)_{1\leq j\leq m}^{1\leq i\leq n}.\end{array}$$

Por otra parte, dadas $A=\left(a_{ij}\right)_{1\leq j\leq m}^{1\leq i\leq n}\in\mathrm{Mat}_{n\times m}(R)$ y $B=\left(b_{ij}\right)_{1\leq j\leq \ell}^{1\leq i\leq m}\in\mathrm{Mat}_{m\times \ell}(R)$. Llamamos **matriz producto de** A **por** B a la matriz de tamaño $n\times\ell$ que denotamos

$$A\cdot B:=C=(c_{ij})_{1\leq j\leq \ell}^{1\leq i\leq n}\in\mathrm{Mat}_{n\times\ell}(R)$$

y cuyos coeficientes están dados por la expresión

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{im}b_{mj}=\sum_{k=1}^{m}a_{ik}b_{kj},\qquad \forall\, i\in\{1,\dots,n\}\quad \forall\, j\in\{1,\dots,\ell\}.$$

(observe que para que el producto sea una operación binaria e interna las matrices deben ser cuadradas) Empleando las propiedades de R, probar que:

(I) $(\mathrm{Mat}_{n\times m}(R),+)$ es un grupo abeliano.

(II) Dadas $A,A_1,A_2\in\mathrm{Mat}_{n\times m}(R)$, $B,B_1,B_2\in\mathrm{Mat}_{m\times\ell}(R)$ y $C\in\mathrm{Mat}_{\ell\times s}(R)$, se cumple que

a) $A\cdot(B\cdot C)=(A\cdot B)\cdot C$.

b) $(A_1+A_2)B=A_1B+A_2B$.

c) $A(B_1+B_2)=AB_1+AB_2$.

d) Si Id_r es la **matriz identidad** de tamaño $r\in\mathbb{N}_{\geq 1}$ definida por

$$\mathrm{Id}_r(\ell,k)=\begin{cases}1_R & \text{si}\quad \ell=k,\\ 0 & \text{si}\quad \ell\neq k.\end{cases}$$

entonces se verifica que $I_nA=A$ y $AI_m=A$.

(III) Concluir que $(\mathrm{Mat}_{n\times n}(R),+,\cdot)$ es un anillo unitario.

(IV) $(\mathrm{Mat}_{n\times n}(R),+,\cdot)$ no es en general conmutativo.

Ejercicio 139 El el anillo de los números enteros $(\mathbb{Z},+,\cdot)$.

(I) En cada caso, encontrar $a \in \mathbb{N}$ tal que:

$$\begin{array}{lll} (a)=(2)+(3) & (a)=(6)+(8) & (a)=(m)+(n). \\ (a)=(3)(4) & (a)=(6)(8) & (a)=(m)(n). \\ (a)=(3)\cap(4) & (a)=(6)\cap(8) & (a)=(m)\cap(n). \end{array}$$

(II) Dados dos ideales I y J de $\mathbb{Z}$ tales que $(35) \subsetneq J \subsetneq I$ ¿Qué podemos decir de I y J?

Ejercicio 140 (Radical de un ideal). Sea R un anillo conmutativo y sea I un ideal de R, se define el **radical de un ideal** I como

$$\text{rad}(I) = \{r \in R; \text{existe } n \in \mathbb{N} \text{ tal que } r^n \in I\}.$$

Se pide:

(I) Probar que $\text{rad}(I)$ es un ideal de R y que contiene a I.

(II) Probar que $\text{rad}(\text{rad}(I)) = \text{rad}(I)$ y que si J es otro ideal entonces $\text{rad}(I \cap J) = \text{rad}(I) \cap \text{rad}(J)$.

(III) En $\mathbb{Z}/36\mathbb{Z}$, calcular $\text{rad}((0))$, $\text{rad}((4))$, $\text{rad}((7))$ y $\text{rad}((6))$.

(IV) En $\mathbb{Z}$, calcular $\text{rad}(4\mathbb{Z})$, $\text{rad}(5\mathbb{Z})$ y $\text{rad}(12\mathbb{Z})$. ¿Qué se puede decir en general de $\text{rad}(m\mathbb{Z})$?

(V) Determinar los elementos nilpotentes de $R/\text{rad}((0))$.

Ejercicio 141 (Anulador). Sea R un anillo conmutativo y sea A un subconjunto de R, definimos el **anulador de** A en R por

$$\text{Ann}(A) := \{r \in R : ra = 0 \text{ para todo } a \in A\}.$$

Probar que:

(I) $\text{Ann}(A)$ es un ideal de R.

(II) Si $A \subseteq B$, entonces $\text{Ann}(B) \subseteq \text{Ann}(A)$.

(III) $A \subseteq \text{Ann}(\text{Ann}(A))$. ¿Se puede dar la contención estricta?

Ejercicio 142 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Todo subanillo de $\mathbb{Z} \oplus \mathbb{Z}$ es un ideal de $\mathbb{Z} \oplus \mathbb{Z}$.

(II) El subconjunto $S = \{a+bi : a \in \mathbb{Z}, b \in 2\mathbb{Z}\}$ es un subanillo de $\mathbb{Z}[i]$.

(III) El subconjunto $S = \{a+bi : a \in \mathbb{Z}, b \in 2\mathbb{Z}\}$ es un ideal de $\mathbb{Z}[i]$.

(IV) Dado R un anillo conmutativo y unitario y sean $I_1, I_2, \ldots, I_k$ ideales de R tales que $I_i + I_j = R$ si $i \neq j$. Entonces $I_i + \cap_{i \neq j} I_j = R$.

(V) Dados R un anillo unitario, I un ideal de R y $u \in U(R)$. Si $u \in I$, entonces $I = R$.

(VI) En el anillo $R = Mat_{2\times 2}(\mathbb{Z})$ y el subconjunto $I = Mat_{2\times 2}(2\mathbb{Z})$ es un ideal de R.

(VII) Sea $\mathscr{C} = \mathscr{C}(\mathbb{R},\mathbb{R})$ el anillo de las funciones continuas de $\mathbb{R}$ en $\mathbb{R}$ con la suma y el producto de funciones usual $[(f+g)(x) = f(x)+g(x)$ y $(fg)(x) = f(x)g(x)$ para todo x en $\mathbb{R}]$. Entonces $S = \{f \in \mathscr{C} : f(0) \in 2\mathbb{Z}\}$ un subanillo de $\mathscr{C}$.

(VIII) Sea $\mathscr{C} = \mathscr{C}(\mathbb{R},\mathbb{R})$ el anillo de las funciones continuas de $\mathbb{R}$ en $\mathbb{R}$ con la suma y el producto de funciones usual. Entonces $S = \{f \in \mathscr{C} : f(0) \in 2\mathbb{Z}\}$ un ideal de $\mathscr{C}$.

(IX) Sea $(R,+,\cdot)$ un anillo conmutativo y unitario y $a \in R$. Entonces el subgrupo aditivo generado por a es igual que el ideal generado por a, es decir, $< a >= (a)$.

(X) Sea R un anillo e I un ideal de R. Entonces R/I es conmutativo si y sólo si $rs - sr \in I$

para todos $r,s \in R$.

(XI) Sea R un anillo conmutativo y unitario con $\text{car}(R) = p$ y p primo. Entonces R es finito.

(XII) Sea R un anillo conmutativo y unitario con $\text{car}(R) = p$ y p primo. Si $a \in R$ es nilpotente, entonces existe $k \in \mathbb{N}_{\geq 1}$ de modo que $(1_R + a)^k = 1_R$.

(XIII) En un anillo conmutativo y unitario de característica 2 los elementos idempotentes forman un subanillo.

Ejercicio 143 En el anillo de polinomios $(\mathbb{Z}[x], +, \cdot)$ consideramos:

$$I = (2x+1) \qquad \text{y} \qquad J = \{f \in \mathbb{Z}[x] \ : \ f(0) = 0\}$$

Se pide:

(I) Determinar si J es un ideal o no.

(II) Probar que para todo $n \in \mathbb{N}_{\geq 1}$ existen ideales $I_1, I_2, \ldots I_n$ tales que $J \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n$.

(III) Hallar $I \cap J$ y un ideal que contenga a $I \cup J$.

(IV) ¿Cuál es el inverso de $x + I$ en $\mathbb{Z}[x]/I$?

Ejercicio 144 ¿Cuántos elementos hay en $(\mathbb{Z}/5\mathbb{Z})[i]/(1+i)$? Hallar la clase de $3+4i$ en $(\mathbb{Z}/5\mathbb{Z})[i]/(1+i)$. ¿Tiene $3+4i+(1+i)$ inverso en $(\mathbb{Z}/5\mathbb{Z})[i]/(1+i)$?

Hoja 7. Homomorfismos e isomorfismos de anillos

Se recomienda realizar los ejercicios de las Sección II.3.

Ejercicio 145 Determinar si las siguientes aplicaciones son o no homomorfismos de anillos:

(I) $f : \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \to \mathbb{Z}$ dada por $f(A) = a_{11}$ donde $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$.

(II) $R = \{A \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) : a_{21} = 0\}$ y $f : R \to \mathbb{Z}$ dada por $f(A) = a_{11}$.

¿Son homomorfismos de anillos unitarios?

Ejercicio 146 Determinar todos los homorfismos de anillos:

(I) de $\mathbb{Z}/6\mathbb{Z}$ en $\mathbb{Z}/6\mathbb{Z}$,
(II) de $\mathbb{Z}/20\mathbb{Z}$ en $\mathbb{Z}/30\mathbb{Z}$,
(III) de $\mathbb{Z}/n\mathbb{Z}$ en $\mathbb{Z}$ con $n \in \mathbb{N}$.
(IV) de $\mathbb{R}$ en $\mathbb{R}$.
(V) de $\mathbb{R}$ en un anillo cualquiera R tal que su núcleo sea $\mathbb{Z}$.
(VI) de $\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/2n\mathbb{Z}$ si n es impar.
(VII) de $\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/2n\mathbb{Z}$ si n es par.

¿Cuántos homomorfismos de anillos unitarios existen en cada caso?

Ejercicio 147 Sean R un anillo cualquiera y $f, g : \mathbb{Q} \to R$ homomorfismos de anillos tales que $f_{|\mathbb{Z}} = g_{|\mathbb{Z}}$. Probar que $f = g$.

Ejercicio 148 Encontrar un ideal I de forma que $\mathbb{Z}[x]/I$ sea isomorfo, como anillo, a $\mathbb{Z}/7\mathbb{Z}$.

Ejercicio 149 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Todo homomorfismo de anillos lleva elementos idempotentes en idempotentes.
(II) La suma del cuadrado de tres números enteros consecutivos no es un cuadrado.
(III) Existe un isomorfismo de grupos entre $(3\mathbb{Z}, +)$ y $(5\mathbb{Z}, +)$.
(IV) Existe un isomorfismo de anillos entre $(3\mathbb{Z}, +, \cdot)$ y $(5\mathbb{Z}, +, \cdot)$.
(V) Existe un isomorfismo de grupos entre $(\mathbb{Z}/4\mathbb{Z}, +)$ y $(2\mathbb{Z}/8\mathbb{Z}, +)$.
(VI) Existe un isomorfismo de anillos entre $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ y $(2\mathbb{Z}/8\mathbb{Z}, +, \cdot)$.
(VII) Existe un isomorfismo de anillos entre $\mathbb{R}$ y $\mathbb{C}$.
(VIII) El único automorfismo de anillos de $\mathbb{R}$ en $\mathbb{R}$ es la identidad.
(IX) El único automorfismo de anillos de $\mathbb{C}$ en $\mathbb{C}$ es la identidad.
(X) Sea $P(x) \in \mathbb{Q}[x]$. Entonces $a + bi$ es una raíz de $P(x)$ si y sólo si su conjugado $a - bi$ es una raíz de $P(x)$.
(XI) Sea $P(x) \in \mathbb{R}[x]$. Entonces $a + bi$ es una raíz de $P(x)$ si y sólo si su conjugado $a - bi$ es una raíz de $P(x)$.
(XII) Sea $P(x) \in \mathbb{C}[x]$. Entonces $a + bi$ es una raíz de $P(x)$ si y sólo si su conjugado $a - bi$ es una raíz de $P(x)$.

Ejercicio 150 Probar que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ y $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ no son anillos isomorfos.

Ejercicio 151 Leer el artículo "Orders for finite noncommutative rings" D. B. Erickson (1966)

Ejercicio 152 Sea R un anillo, probar que existe un anillo unitario S y un monomorfismo $f : R \to S$.

Ejercicio 153 Sea R un anillo conmutativo y unitario con $car(R) = p$ y p primo. Dados $a, b \in R$, demostrar que:

$$\forall n \in \mathbb{N}, \qquad (a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Ejercicio 154 (Polinomios de Lagrange y Teorema chino del resto). Dado $n \in \mathbb{N}$, consideramos $\alpha_1, \alpha_2, \ldots \alpha_n, \beta_1, \beta_2, \ldots \beta_n \in \mathbb{R}$ con $\alpha_i \neq \alpha_j$ si $i \neq j$. Se pide:

(I) Empleado el Teorema chino del resto, probar que existe un polinomio $P(x) \in \mathbb{R}[x]$ tal que $P(\alpha_j) = \beta_j$ para todo $j \in \{1, 2, \ldots, n\}$.

(II) Deducir que si $\tilde{P}(x) \in \mathbb{R}[x]$ es otro polinomio tal que $\tilde{P}(\alpha_j) = \beta_j$ para todo $j \in \{1, 2, \ldots, n\}$, entonces existe $Q(x) \in \mathbb{R}[x]$ de modo que

$$\tilde{P}(x) = P(x) + Q(x) \prod_{j=1}^{n} (x - \alpha_j).$$

(III) Para cada $j \in \{1, \ldots, n\}$, hallar empleando el Algoritmo de Euclides en $\mathbb{R}[x]$ dos polinomios $A_j(x), B_j(x) \in \mathbb{R}[x]$ tales que

$$\beta_j = A_j(x)(x - \alpha_j) + B_j(x) \prod_{k=1, k\neq j}^{n} (x - \alpha_k).$$

(IV) Con la notación del apartado anterior, comprobar que el polinomio

$$P(x) = B_1(x) \prod_{k=1, k\neq 1}^{n} (x - \alpha_k) + B_1(x) \prod_{k=1, k\neq 2}^{n} (x - \alpha_k) + \cdots + B_n(x) \prod_{k=1, k\neq n}^{n} (x - \alpha_k)$$

coincide con el **polinomio interpolador de Lagrange**.

(V) Empleado el Teorema chino del resto, hallar un polinomio $P(x) \in \mathbb{R}[x]$ tal que

$$P(0) = -2, \quad P(1) = 3, \quad P(-1) = 2, \quad P(-2) = 5$$

y $\text{gr}(P(x)) > 4$.

(VI) Empleado el Teorema chino del resto, hallar un polinomio $P(x) \in \mathbb{R}[x]$ tal que

$$P(0) = -2, \quad P(1) = 3, \quad P(-1) = 2, \quad P(i) = 0.$$

Hoja 8. Dominios y cuerpos

Se recomienda realizar los ejercicios de la Sección II.4.

Ejercicio 155 Consideramos el conjunto de matrices

$$R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \ : \ a,b \in \mathbb{Z} \right\}$$

y $f : R \to \mathbb{Z}$ la función dada por $f(A) = a - b$. Se pide:

(I) Demostrar que R es un anillo y f es un homorfismo de anillos.
(II) Determinar $\mathrm{Ker}(f)$.
(III) Probar que $R/\mathrm{Ker}(f)$ es isomorfo a $\mathbb{Z}$.
(IV) Determinar si $\mathrm{Ker}(f)$ es o no un ideal primo. ¿Es $\mathrm{Ker}(f)$ maximal?

Ejercicio 156 En el anillo $\mathbb{Z}[x]$ consideramos los subconjuntos:

$$I_1 = 2\mathbb{Z}[x] = \{P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] \ : \ a_i \in 2\mathbb{Z}\}.$$

$$I_2 = \{P(x) \in \mathbb{Z}[x] \ : \ P(0) = 0\}.$$

$$I_3 = \{P(x) \in \mathbb{Z}[x] \ : \ P(0) \in 2\mathbb{Z}\}.$$

Se pide

(I) Determinar si I_1, I_2 e I_3 son ideales de $\mathbb{Z}[x]$.
(II) Determinar si I_1, I_2 e I_3 son ideales maximales de $\mathbb{Z}[x]$.
(III) Un sistema completo de representantes de $\mathbb{Z}[x]/I_1$, $\mathbb{Z}[x]/I_2$ y $\mathbb{Z}[x]/I_3$.

Ejercicio 157 Encontrar:

(I) Elementos a,b y c en el anillo $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ tales que ab, ac y bc son divisores del cero pero que $a+b+c$ no es un divisor del cero.
(II) Todos los divisores del cero y todas las unidades de $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$.
(III) Un anillo conmutativo sin divisores del cero no nulos que no sea un dominio de integridad.
(IV) Encontrar un anillo R dos elementos a y b de R que sean divisores del cero de modo que $a+b \neq 0$ y que $a+b$ no sea un divisor del cero.
(V) Un cuerpo de característica 2 con más de dos elementos.
(VI) Un anillo con exactamente dos ideales maximales.
(VII) Todos los ideales M maximales de $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$.

Ejercicio 158 Probar que no existe un dominio de integridad con exactamente 6 elementos.

Ejercicio 159 Supongamos que a y b son elementos de un cuerpo F de orden 8 y que $a^2 + ab + b^2 = 0$. Probar que $a = b = 0$. ¿Qué ocurre si suponemos que en lugar de ser $\#F = 8$ tenemos que $\#F = 2^n$ con n impar?

Ejercicio 160 Si F es un cuerpo de característica 2 con más de dos elementos, demostrar que existen $x,y \in F$ tales que $(x+y)^3 \neq x^3 + y^3$.

Ejercicio 161 Dar un ejemplo de un cuerpo de característica 2 con infinitos elementos. Sea F un cuerpo de característica distinta de 2 y tal que los elementos no nulos de F forman un grupo cíclico para la multiplicación. Probar que $\#F < \infty$.

Ejercicio 162 Consideramos un dominio de integridad D y $f : D \to \mathbb{N}$ una función no constante tal que $f(xy) = f(x)f(y)$. Demostrar que si $u \in U(D)$ entonces $f(u) = 1$.

Ejercicio 163 Consideramos el conjunto de matrices

$$R = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a,b \in \mathbb{Z}/7\mathbb{Z} \right\}$$

Se considera en R la suma y el producto habitual en $\mathrm{Mat}_{2\times 2}(\mathbb{Z}/7\mathbb{Z})$. Probar que R es un anillo conmutativo. ¿Cuántos elementos hay en R?¿Es R un dominio de integridad?¿Es R un cuerpo?¿Se satisfacen las mismas propiedades si reemplazamos $\mathbb{Z}/7\mathbb{Z}$ por $\mathbb{Z}/5\mathbb{Z}$?

Ejercicio 164 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Los ideales maximales de $\mathbb{Z}/36\mathbb{Z}$ son (2) y (3).
(II) El ideal $(x+a)$ es maximal de $\mathbb{R}[x]$ para todo $a \in \mathbb{R}$.
(III) Todo ideal maximal de $\mathbb{R}[x]$ es de la forma $(x+a)$ con $a \in \mathbb{R}$.
(IV) El anillo $\mathscr{C}([-1,1],\mathbb{R})$ de las funciones continuas $f : [-1,1] \to \mathbb{R}$ es un dominio.
(V) Se cumple que 0 es el único elemento nilpotente de un dominio de integridad.
(VI) Supongamos que R y S son anillos conmutativos y unitarios. Sea $f : R \to S$ un homomorfismo de anillos sobreyectivo y sea I un ideal de S. Si I es primo en S, entonces $f^{-1}(I)$ es primo en R.
(VII) Supongamos que R y S son anillos conmutativos y unitarios. Sea $f : R \to S$ un homomorfismo de anillos y sea I un ideal de S. Si I es primo en S, entonces $f^{-1}(I)$ es primo en R.
(VIII) Supongamos que R y S son anillos conmutativos y unitarios. Sea $f : R \to S$ un homomorfismo de anillos sobreyectivo y sea I un ideal de S. Si I es maximal en S entonces $f^{-1}(I)$ es maximal en R.
(IX) Supongamos que R y S son anillos conmutativos y unitarios. Sea $f : R \to S$ un homomorfismo de anillos y sea I un ideal de S. Si I es maximal en S entonces $f^{-1}(I)$ es maximal en R.
(X) Los únicos ideales de un cuerpo F son $\{0_F\}$ y F.
(XI) Las fracciones racionales $\mathbb{R}(x)$ y las series de potencias formales $\mathbb{R}[[x]]$ son anillos isomorfos.
(XII) El ideal $I = \{(3x,y) \ : \ x,y \in \mathbb{Z}\}$ es un ideal maximal de $\mathbb{Z} \oplus \mathbb{Z}$.
(XIII) Dado F un cuerpo con 27 elementos, entonces para todo $a \in F$, $5a = -a$.
(XIV) Todo cuerpo es isomorfo, como anillo, a su cuerpo de fracciones.
(XV) Sea R un anillo conmutativo y unitario con $\#R = 30$. Si I es un ideal de R con $\#I = 10$, entonces I es maximal.
(XVI) Sea $\mathscr{C} = \mathscr{C}(\mathbb{R},\mathbb{R})$ el anillo de las funciones continuas de $\mathbb{R}$ en $\mathbb{R}$. Entonces el conjunto $I = \{f \in \mathscr{C} \ : \ f(0) = 0\}$ es un ideal maximal.

Ejercicio 165 Probar que (x^2+x+1) es maximal en $\mathbb{R}[x]$ y deducir que $\mathbb{R}[x]/(x^2+x+1)$ es un cuerpo.

Ejercicio 166 Probar que $I = (2+2i)$ no es un ideal primo de $\mathbb{Z}[i]$ ¿Cuántos elementos hay en $\mathbb{Z}[i]/I$? ¿cuál es la característica de $\mathbb{Z}[i]/I$?

Ejercicio 167 Sea R un anillo unitario tal que $a^2 = a$ para todo $a \in R$. Probar que R es conmutativo. Sea I un ideal primo, probar que $\#(R/I) = 2$.

Ejercicio 168 Calcular los cuerpos de fracciones de $\mathbb{Z}[x]$, $(\mathbb{Z}/3\mathbb{Z})[x]$ y $\mathbb{Z}[i]$.

Ejercicio 169 (Endomorfismo de Frobenius). Sea R un anillo conmutativo y unitario con característica p con p primo. Probar que:

(I) $F : R \to R$ dado por $F(x) = x^p$ es un homorfismo de anillos, que denominamos **endomorfismo de Frobenius**.

(II) Probar que F no es en general un automorfismo.

(III) Probar que si R no tiene elementos nilpotentes, entonces F es monomorfismo

Ejercicio 170 (Series de potencias formales). Sea D un dominio de integridad, representamos por $D[[x]]$ el conjunto de las **series de potencias formales con coeficientes en** D y consideramos la suma y el producto de series de potencias definidos por:

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k := \sum_{k=0}^{\infty} (a_k + b_k) x^k.$$

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} b_k x^k\right) := \sum_{k=0}^{\infty} c_k x^k, \qquad c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

Probar que:

(I) $(D[[x]], +, \cdot)$ es un dominio de integridad.

(II) Las unidades de $D[[x]]$ son las series de potencias $\sum_{k=0}^{\infty} a_k x^k$ con $a_0 \in U(D)$.

(III) Calcular el inverso de $(1+x)$ en $\mathbb{Z}[[x]]$.

Ejercicio 171 (Subcuerpo). Dado $(F, +, \cdot)$ un cuerpo, decimos que un subconjunto no vacío $L \subseteq F$ es un **subcuerpo** de F si las restricciones de las operaciones internas $+|_{L\times L}$ y $\cdot|_{L\times L}$ dotan L de estructura de cuerpo. Demostrar que L es un cuerpo de F si y solo si L es no vacío y se satisfacen las siguientes propiedades:

(SCI) si $a \in L$, entonces $-a \in L$.
(SCII) si $a, b \in L$, entonces $a + b \in L$.
(SCIII) si $a, b \in L$, entonces $a \cdot b \in L$.
(SCIV) si $a \in L$ y $a \neq 0$, entonces $a^{-1} \in L$.

Demostrar que si L es un subcuerpo de F, entonces $(F, +)$ es un espacio vectorial sobre L.

Hoja 9. Dominios de factorización única, dominios de ideales principales y dominios euclídeos. Anillos de Polinomios

Se recomienda realizar los ejercicios de las Secciones II.5 y II.6.

Ejercicio 172 Consideramos el homomorfismo de evaluación $\Phi : \mathbb{Z}[x] \to \mathbb{Z}$ definido por $\Phi(P(x)) = e_1(P(x)) = P(1)$. Encontrar un polinomio $Q(x) \in \mathbb{Z}[x]$ tal que $\mathrm{Ker}(\Phi) = (Q(x))$. ¿Existe una única posibilidad para $Q(x)$? ¿A qué anillo es isomorfo $\mathbb{Z}[x]/\mathrm{Ker}(\Phi)$?
Repetir el ejercicio sustituyendo $\mathbb{Z}$ por $\mathbb{Q}$.

Ejercicio 173 Se considera el ideal $I = (6, x-1)$ en $\mathbb{Z}[x]$. Dar un sistema completo de representantes para las clases de $\mathbb{Z}[x]/I$. Dar un ideal maximal de $\mathbb{Z}[x]$ que contenga a I.

Ejercicio 174 Encontrar:

(I) Un ejemplo de un cuerpo que contenga estrictamente a los números complejos $\mathbb{C}$.
(II) Un cuerpo con 25 elementos.
(III) Un cuerpo con 27 elementos.
(IV) El valor de $P(3)$ donde $P(x) = x^{233} + 3x^{119} + 3x^{55} + 1$ es un polinomio de $(\mathbb{Z}/5\mathbb{Z})[x]$.
(V) Un D.F.U. D donde no se satisfaga la Identidead de Bezout, es decir, que existan $a, b \in D$ tales que para todos $x, y \in D$ las combinaciones $ax + by$ no representen nunca un máximo común divisor de a y b.
(VI) Un polinomio $P(x) \in \mathbb{Q}[x]$ tal que $x^2 + 1 | P(x)$ y $x^3 + 1 | (P(x) - 1)$.
(VII) Un polinomio $P(x) \in (\mathbb{Z}/2\mathbb{Z})[x]$ tal que $x^2 + 1 | P(x)$ y $x^3 + 1 | (P(x) + 1)$.

Ejercicio 175 (Polinomios vs funciones polinómicas). Sea $(R, +, \cdot)$ un anillo conmutativo y unitario. Dado un polinomio $P(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ definimos la **función polinomial asociada a** P por

$$\begin{array}{rccc} f_P : & R & \to & R \\ & \alpha & \to & P(\alpha) \end{array}$$

Se pide:

(I) Probar que los polinomios $P(x) = x^4 + x$ y $Q(x) = x^2 + x$ en $(\mathbb{Z}/3\mathbb{Z})[x]$ determinan la misma función de $(\mathbb{Z}/3\mathbb{Z})$ en $(\mathbb{Z}/3\mathbb{Z})$, es decir, $f_P = f_Q$.
(II) Encontrar dos polinomios cúbicos distintos en $\mathbb{Z}/2\mathbb{Z}[x]$ que determinen la misma función polinomial de $(\mathbb{Z}/2\mathbb{Z})$ en $(\mathbb{Z}/2\mathbb{Z})$.
(III) Sean $P(x), Q(x) \in \mathbb{Z}[x]$ polinomios cúbicos tales que $f_P(\alpha) = f_Q(\alpha)$ para cuatro valores distintos de $\alpha \in \mathbb{Z}$. Probar que $P(x) = Q(x)$.
(IV) Sea F un cuerpo infinito y $P(x) \in F[x]$ un polinomio. Suponemos que $f_P(\alpha) = 0$ para un número infinito de elementos $\alpha \in F$, probar que $P(x) = 0$.
(V) Sea F un cuerpo infinito y $P(x), Q(x) \in F[x]$ polinomios. Suponemos que para un número infinito de $\alpha \in F$ se tiene que $f_P(\alpha) = f_Q(\alpha)$, probar que $P(x) = Q(x)$.
(VI) Sea $P(x)$ un polinomio no constante de $\mathbb{Z}[x]$, probar que $f_P(\alpha)$ toma infinitos valores en $\mathbb{Z}$.

Ejercicio 176 Se pide:
(I) Probar que $P(x) = x^2 + x + 4$ es irreducible en $(\mathbb{Z}/11\mathbb{Z})[x]$.
(II) Escribir $P(x) = x^3 + 6$ como producto de irreducibles en $(\mathbb{Z}/7\mathbb{Z})[x]$.
(III) Escribir $P(x) = x^3 + x^2 + x + 1$ como producto de irreducibles en $(\mathbb{Z}/2\mathbb{Z})[x]$.
(IV) Demostrar que $P(x) = x^4 + 1$ es reducible en $(\mathbb{Z}/p\mathbb{Z})[x]$ para todo p primo.
En cada caso, determinar, si es posible, cuatro polinomios diferentes asociados a $P(x)$.

Ejercicio 177 Sea F un cuerpo. Se pide:
(I) Dado $P(x) = \sum_{k=0}^{n} a_k x^k \in F[x]$. Probar que $(x-1)|P(x)$ si y solamente si $\sum_{k=0}^{n} a_k = 0$.
(II) Probar que para todo cuerpo F hay infinitos elementos irreducibles en $F[x]$.
(III) Demostrar que el conjunto

$$I = \{P(x) = \sum_{k=0}^{n} a_k x^k \in F[x] \ : \ n \in \mathbb{N} \text{ y } \sum_{k=0}^{n} a_k = 0\}.$$

es un ideal de $F[x]$ y encontrar un generador de I.
(IV) Demostrar que

$$I = \{P(x) \in F[x] \ : \ P(a) = 0 \text{ para todo } a \in F\}$$

es un ideal en $F[x]$. Probar que I es infinito si F es finito y que $I = \{0\}$ si F es infinito. Cuando F es finito, encontrar un polinomio mónico $Q(x)$ tal que $I = (Q(x))$.
(V) Probar que existen $a, b \in F$ con la propiedad: $(x^2 + x + 1)|(x^{43} + ax + b)$.
(VI) Denotamos por $F(x)$ al cuerpo de fracciones de $F[x]$. Probar que no hay ningún elemento en $F(x)$ cuyo cuadrado sea x.

Ejercicio 178 Dados R y S dos anillos conmutativos y unitarios. Se pide:
(I) Dado I un ideal de un anillo R, probar que $I[x]$, los polinomios con coeficientes en I, es ideal de $R[x]$.
(II) Probar que si I es un ideal primo de R, entonces $I[x]$ es un ideal primo de $R[x]$.
(III) Dar un ejemplo de un anillo conmutativo y unitario R y un ideal maximal I de R de forma que $I[x]$ no sea ideal maximal de $R[x]$.
(IV) Probar que $P(x) = \sum_{k=0}^{n} a_k x^k$ es unidad en $R[x]$ si y solo si a_0 es unidad en R y a_k es nilpotente para $1 \leq k \leq n$.
(V) Dado f un homomorfismo de anillos $f : R \to S$ definimos $\tilde{f} : R[x] \to S[x]$ por

$$\tilde{f}(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} f(a_k) x^k.$$

Probar que $\tilde{f}$ es un homomorfismo de anillos. Deducir que si R y S son isomorfos entonces $R[x]$ y $S[x]$ son también isomorfos.

Ejercicio 179 En $(\mathbb{Z}/3\mathbb{Z})[x]$ consideramos los polinomios

$$P(x) = x^3 + x^2 + x + 1 \quad \text{y} \quad Q(x) = x^4 + x^3 + 2x^2 + x + 1$$

y el ideal $I = (P(x), Q(x))$.
(I) Encontrar un polinomio $D(x) \in (\mathbb{Z}/3\mathbb{Z})[x]$ tal que $I = (D(x))$.
(II) Probar que $(\mathbb{Z}/3\mathbb{Z})[x]/I$ es un cuerpo.
(III) ¿Cuántos elementos tiene?
(IV) ¿Cuál es el inverso de $x + I$?

Ejercicio 180 (Identidad de Bezout). Sea D un *D.I.P.*, $a,b \in D$ y sea $d \in D$ un máximo común divisor de a y b. Demostrar que existen elementos $x,y \in D$ tales que $ax+by=d$. Calcular un máximo común divisor y escribir la identidad de Bezout correspondiente en los siguientes casos:

(I) Para $A(x)=x^2+x-6$ y $B(x)=x^2-1$ en $\mathbb{Q}[x]$.

(II) Para $A(x)=x^4+6x^3+4x^2+6x+3$ y $B(x)=6x^3+3x^2+6x+3$ en $\mathbb{Q}[x]$.

(III) Para $a=4+22i$ y $b=17+i$ en $\mathbb{Z}[i]$.

(IV) Para $a=-2398+642i$ y $b=318+2462i$ en $\mathbb{Z}[i]$.

(V) Para $P_{n+1}(x)=x^{n+1}+x^n+x^{n-1}+\cdots+x+1$ y $P_n(x)=x^n+x^{n-1}+\cdots+x+1$ en $F[x]$ donde $n \in \mathbb{N}$ y F es un cuerpo.

Ejercicio 181 Sea F un cuerpo, $P(x),Q(x) \in F[x]$, $I=(P(x))$ y $A=F[x]/I$. Estudiar si A es o no un cuerpo, determinar cuántos elementos tiene y, si es posible, calcular el inverso de $Q(x)+I$ en los siguientes casos:

(I) Para $F=\mathbb{Z}/5\mathbb{Z}$, $P(x)=x^2+x+2$ y $Q(x)=2x+3$

(II) Para $F=\mathbb{Z}/3\mathbb{Z}$, $P(x)=x^2+x+1$ y $Q(x)=2x+3$.

(III) Para $F=\mathbb{Z}/3\mathbb{Z}$, $P(x)=x^3+2x+1$ y $Q(x)=x^2+x+1$.

(IV) Para $F=\mathbb{Z}/5\mathbb{Z}$, $P(x)=x^3+3x+2$ y $Q(x)=x^2+1$.

(V) Para $F=\mathbb{Z}/2\mathbb{Z}$, $P(x)=x^2+x+1$ y $Q(x)=x+1$.

Ejercicio 182 Empleando las propiedades del Ejercicio II.5.42, se pide:

(I) Probar que $1-i$ y 3 son irreducibles en $\mathbb{Z}[i]$.

(II) Probar que 2 y 5 no son irreducibles en $\mathbb{Z}[i]$.

(III) Dado $p \in \mathbb{Z}$ primo tal que $p=a^2+b^2$ con $a,b \in \mathbb{Z}$, demostrar que $a+bi$ es irreducible en $\mathbb{Z}[i]$.

(IV) Dar tres ejemplos de primos que satisfacen la propiedad anterior y determinar sus correspondientes irreducibles.

(V) Demostrar que 21 no factoriza de forma única como producto de irreducibles en $\mathbb{Z}[i\sqrt{5}]$.

Ejercicio 183 Comprobar que $3x^2+4x+3$ factoriza en $\mathbb{Z}/5\mathbb{Z}[x]$ como $(3x+2)(x+4)$ y como $(4x+1)(2x+3)$ ¿Contradice esto el hecho de que $F[x]$ sea un D.F.U. cuando F es cuerpo?

Ejercicio 184 Escribir la lista de polinomios irreducibles y mónicos en $\mathbb{Z}/3\mathbb{Z}[x]$ de grado menor o igual que 2. ¿Es $P(x)=x^5+x^4+x^3+2x^2+x+2$ irreducible en $\mathbb{Z}/3\mathbb{Z}[x]$?

Ejercicio 185 Leer el artículo "Divisibility properties of integral functions" O. Helemer (1940)

Ejercicio 186 Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) Sea D un D.I.P. y p un elemento irreducible de D, entonces $D/(p)$ es un cuerpo.
(II) Sea D un D.I.P, entonces $D[x]$ es un D.I.P.
(III) Sea D un D.I.P e $I \subseteq D$ un ideal, entonces D/I es un D.I.P.
(IV) Para todo $p \in \mathbb{N}$ primo $\mathbb{Z}[x]/(p,x) \approx \mathbb{Z}/p\mathbb{Z}$.
(V) Sean $P(x), Q(x) \in \mathbb{R}[x]$ dos polinomios tales que $(P(x), Q(x)) = \mathbb{R}[x]$, entonces se cumple que $(P(x)+Q(x),\, P(x)Q(x)) = \mathbb{R}[x]$.
(VI) Sea $P(x) \in \mathbb{Z}[x]$ un polinomio tal que $P(0) \equiv P(1) \equiv 1 \,(\text{mód}\, 2)$, entonces $P(x)$ no tiene raíces enteras.

Ejercicio 187 Sea F un cuerpo y $\alpha \in F$. Probar que:

(I) $F[x]/(x-\alpha) \approx F$.
(II) (x) es un ideal primo de $F[x,y]$ que no es maximal.
(III) $F[x,y]$ es un dominio de integridad que no es un D.I.P.

Ejercicio 188 Empleando las propiedades del Ejercicio II.5.43 cuando sea necesario, se pide:

(I) Probar que si $\alpha \cdot \beta \in U(\mathbb{Z}[\sqrt{2}])$, entonces α y β son unidades.
(II) Probar que $U(\mathbb{Z}[\sqrt{2}]) = \{\pm(1+\sqrt{2})^n \,:\, n \in \mathbb{Z}\}$.
(III) Comprobar que en $\mathbb{Z}[\sqrt{2}]$ se cumple que

$$(5+\sqrt{2})(2-\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2}).$$

¿Se puede deducir de esta igualdad que $\mathbb{Z}[\sqrt{2}]$ no es un D.F.U.?

Ejercicio 189 (Anillos Noetherianos). Sea R un anillo conmutativo y unitario decimos que satisface la condición la **cadena ascendente dada ideales** si cada sucesión $\{I_k\}_{k=1}^{\infty}$ de ideales de R creciente, es decir, $I_k \subseteq I_{k+1}$ para todo $k \in \mathbb{N}_{\geq 1}$ es estacionaria: existe $k_0 \in \mathbb{N}_{\geq 1}$ tal que $I_k = I_{k_0}$ para todo $k \geq k_0$. Un anillo R conmutativo y unitario con la propiedad de la cadena ascendente dada ideales se dice que es **noetheriano**.

(I) Probar que R/I es noetheriano, si R es un anillo noetheriano e I es un ideal de R.
(II) Sea R un anillo conmutativo y unitario decimos que un ideal I de R está **finitamente generado** si existe un conjunto finito de elementos $a_1, a_2, \ldots a_n \in I$ tal que $I = (a_1, a_2, \ldots a_n)$. Sea D un dominio de integridad, demostrar que:
D es noetheriano si y sólo si todo ideal de D está finitamente generado.

Ejercicio 190 Sea D un dominio, consideramos $D[[x]]$ el dominio de series formales de potencias (ver Ejercicio 170).

(I) Probar que dado $f = \sum_{k=0}^{\infty} a_k x^k \in D[[x]]$ si a_0 es irreducible en D, entonces f es irreducible en $D[[x]]$.
(II) Sea F un cuerpo. Probar que $F[[x]]$ (Ver Ejercicio 170) es un dominio euclídeo para la aplicación definida para todo $f = \sum_{k=0}^{\infty} a_k x^k \in F[[x]] \backslash \{0\}$ por

$$\delta(f) = \text{mín}\{k \in \mathbb{N} \,:\, a_k \neq 0\}.$$

Determinar todos los ideales de $F[[x]]$.