ESTRUCTURAS ALGEBRAICAS. GRUPO M3 (19-20).
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

100 Problemas de Anillos y Grupos para sacar un 10 en el Examen de EEAA.

1. Sea S un subgrupo propio de G. Probar que G está generado por su complementario.
2. Halla los polinomios irreducibles en los casos siguientes:
   (i) Aquellos de grado menor o igual que 3 en $\mathbb{Z}_3[x]$.
   (ii) Aquellos de grado menor o igual que 4 en $\mathbb{Z}_2[x]$.
3. Factoriza como producto de irreducibles $f(x) = 6x^2 - 12$ en $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{Z}_7[x]$.
4. Demuestra que $F = \mathbb{Z}_3[x]/(x^2+1)$ es un cuerpo finito, y halla su cardinal. ¿Son las unidades de F un grupo cíclico? (tanto en caso afirmativo como negativo, es necesario argumentarlo). Encontrar un generador de dicho grupo en caso afirmativo; o, por el contrario, escribir este como producto directo de subgrupos cíclicos.
5. Sean I el ideal de $\mathbb{Z}_3[x]$ generado por $x^3 - x + 1$ y $L = \mathbb{Z}_3[x]/I$. Consideremos
$$a = x^2 + x - 1 + I \in L.$$
   (i) Demostrar que L es un cuerpo, dando su cardinal.
   (ii) Hallar el inverso de a en L. Encuentra ahora un polinomio $f(x)$ sobre $\mathbb{Z}_3$ de grado menor que 3 verificando
$$a^{2000} = f(x) + I.$$
   (iii) ¿Es $\mathbb{Z}_3[x]/(x^3 - x^2 + 1)$ un cuerpo con el mismo número de elementos que L? ¿Son cuerpos isomorfos? En caso afirmativo, construye explícitamente dicho isomorfismo (sin olvidar demostrar que este es, efectivamente, un isomorfismo).
6. Dados n un entero libre de cuadrados y p un número primo,
   (i) demostrar que se tienen los isomorfismos siguientes:
$$\mathbb{Z}\left[\sqrt{n}\right] \cong \frac{\mathbb{Z}[x]}{(x^2-n)} \quad \text{y} \quad \frac{\mathbb{Z}[x]}{(p, x^2-n)} \cong \frac{\mathbb{Z}_p[x]}{(x^2-n)} \cong \mathbb{Z}_p\left[\sqrt{n}\right].$$
   (ii) ¿es el polinomio $x^2 - n$ irreducible sobre $\mathbb{Z}[x]$? ¿Es $\mathbb{Z}\left[\sqrt{n}\right]$ un cuerpo?
   (iii) estudiar la irreducibilidad de $x^2 + 1$ en $\mathbb{Z}_p[t]$ en función del primo p. ¿Cuándo es $\mathbb{Z}_p\left[\sqrt{-1}\right]$ un cuerpo?
   (iv) dar las definiciones de DFU, DIP y DE; recordando como vienen relacionadas todas estas entre sí y dando contraejemplos para las implicaciones que no se dan. Demostrar que para $n = 3$ estamos ante un DE.
7. Probar las afirmaciones siguientes para un DIP que denotamos por A:
   (i) Dados $a, b \in A$ arbitrarios, entonces $(a) + (b) = (\text{mcd}(a, b))$.
   (ii) Dados $a, b \in A$ arbitrarios, entonces $(a) \cap (b) = (\text{mcm}(a, b))$.
   (iii) Dados $a, b \in A$ arbitrarios, entonces $(a) \cdot (b) = (a \cdot b)$.
   ¿Qué pasa si sólo tenemos un DFU? (**probar las inclusiones que se den**, y dar **contraejemplos para aquellas que no sean ciertas en general** para los DFU).
8. Sea H un subgrupo propio de un grupo finito G. Demostrar que existe un elemento de G que no es conjugado a ningún otro elemento de H.
9. Demostrar que todo grupo de orden p^2q^2 con p y q primos distintos no es simple.
10. Dado G un **grupo arbitrario**, sean $H, K \trianglelefteq G$ tales que $H \cap K = \{1\}$ y $G = HK$. Demostrar que $G \cong H \times K$.

11. Este ejercicio tiene como objetivo demostrar que **los isomorfismos preservan las estructuras algebraicas** estudiadas.
    (i) Dado $\varphi\colon A \longrightarrow B$ un isomorfismo de anillos, probar que
        - A es cuerpo si, y sólo si, lo es B.
        - A es DE/DIP/DFU si, y sólo si, lo es B.
        - $a \in A$ es primo si, y sólo si, lo es $\varphi(a) \in B$.
        - ¿Qué más se preserva por φ? Demuéstralo.

    (ii) Dado $f\colon G \longrightarrow H$ un isomorfismo de grupos, probar que
        - G es cíclico si, y sólo si, lo es H.
        - G es simple si, y sólo si, lo es H.
        - $N \lhd G$ si, y sólo si, es $f(N) \lhd H$.
        - ¿Qué más se preserva por f? Demuéstralo.

    ¿Eres capaz de hallar alguna propiedad que no se preserve por isomorfismos en alguno de los dos casos? ¿Cuál? Demuéstralo en caso afirmativo.
12. Sean G y H dos grupos cíclicos arbitrarios.
    (i) Si se tiene que estos son **grupos finitos**, con órdenes n y m respectivamente, demostrar que $G \times H \cong C_{nm}$ si, y sólo si, son n y m coprimos.
    (ii) Demostrar que si estos son **grupos infinitos**, entonces $G \times H$ NO es cíclico. (**Sugerencia**: Probar que no existe un monomorfismo de grupos $f\colon \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$).
13. Demostrar que en todo grupo simple no abeliano los subgrupos propios tienen índice necesariamente mayor o igual que 5.
14. El objetivo que se propone ahora es demostrar que el conjunto $\left(\mathbb{S}^1\right)^n$ (con $n \in \mathbb{Z}$ positivo) es un grupo, que se conoce como *n-toro*; que es isomorfo a un cociente entre $\mathbb{R}^n$ y $\mathbb{Z}^n$. Para ello, los pasos a seguir son los siguientes:
    (i) Sean G_1 y G_2 dos grupos arbitrarios tales que $H_1 \trianglelefteq G_1$ y $H_2 \trianglelefteq G_2$ son dos subgrupos normales de G_1 y G_2 respectivamente. Demostrar que $H_1 \times H_2$ es un subgrupo normal de $G_1 \times G_2$. Probar que
    $$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}.$$
    (ii) Demostrar que $\mathbb{Z} < \mathbb{R}$ es un subgrupo normal de $\mathbb{R}$.
    (iii) Sea
    $$\mathbb{S}^1 = \left\{z \in \mathbb{C}^* : |z|^2 = 1\right\}.$$
    Demostrar que $\mathbb{S}^1$ es un subgrupo (normal) de $\mathbb{C}^*$.
    (iv) Sea $n \in \mathbb{Z}$ un entero positivo. Demostrar que
    $$\frac{\mathbb{R}^n}{\mathbb{Z}^n} \cong \left(\mathbb{S}^1\right)^n.$$
    El grupo $\left(\mathbb{S}^1\right)^n$ se conoce como *n-toro.*
15. Clasificar los grupos finitos de orden:
    (i) 8. (ii) 30. (iii) 46.
16. Demostrar que todo grupo de orden 957 es cíclico.
17. Sean G un grupo y $H \leq G$. Demostrar que H es normal en G si, y sólo si, se tiene que H es el núcleo para un homomorfismo de grupos con origen el propio grupo G.
18. Probar que un grupo G finito es cíclico si, y sólo si, para cada divisor positivo del orden de este grupo **existe un único** subgrupo de G con orden dicho divisor.
19. Probar que todo grupo de orden p^2 con p primo es abeliano. Deducir la clasificación para los grupos de orden el cuadrado de un primo.
20. Se considera el anillo $A = \mathbb{Z}_{84}$. Se pide:
    (i) Explicar si A es un DI.
    (ii) Decidir si $55 \in A$ es una unidad en A y, en caso afirmativo, calcular su inverso.

21. Decidir si las afirmaciones siguientes sobre teoría de anillos son verdaderas o falsas, razonando en cada caso de forma adecuada.
    (i) Dados A un DI e I un ideal I de A arbitrario, entonces A/I es también un DI.
    (ii) Los anillos $\mathbb{Z}_5[x]/\left(x^2+2x-1\right)$ y $\mathbb{Z}_5[x]/\left(x^2-x+3\right)$ son isomorfos.
    (iii) En los DI, un elementos es primo si, y sólo si, es irreducible.
    (iv) Si A es DIP, entonces $A[x]$ también es DIP.
    (v) Si $f\colon A \longrightarrow B$ es un **homomorfismo** de anillos y $\mathfrak{b} \subseteq B$ es un ideal, entonces la imagen inversa $f^{-1}(\mathfrak{b})$ es un ideal de A.
    (vi) Los ideales maximales de $\mathbb{Z}_n$ son los generados por $[p]_n$ con p primo tal que $p|n$.
    (vii) En un DFU, todos los ideales maximales son siempre principales y, además, están generados por un elemento irreducible.
    (viii) $\mathbb{R}[x]/\left(x^2+1\right)$ es el cuerpo de los complejos.
    (ix) En un DFU arbitrario, el máximo común divisor y mínimo común múltiplo de un conjunto finito de elementos fijo existen y son únicos.
    (x) Para todo polinomio $f(x) \in A[x]$ de grado $n \in \mathbb{N}$ con A anillo arbitrario, se tiene que f posee a lo más n raíces distintas.
22. Decidir si las afirmaciones siguientes sobre teoría de grupos son verdaderas o falsas, razonando en cada caso de forma adecuada.
    (i) Todo subgrupo normal de un cierto grupo dado es abeliano.
    (ii) Las unidades de un anillo unitario tienen estructura de grupo cíclico.
    (iii) Los grupos finitos con orden $p_1 \cdots p_r$ siendo cada par de enteros p_i distintos y coprimos para cada $i \in \{1, \ldots, r\}$ satisfacen el **Teorema Inverso de Lagrange**.
    (iv) Los grupos $\mathbb{Z}_{375} \times \mathbb{Z}_{62}$ y $\mathbb{Z}_{125} \times \mathbb{Z}_{93} \times \mathbb{Z}_2$ son isomorfos.
    (v) Los cocientes de grupos abelianos vuelven a serlo.
    (vi) Todo subgrupo cíclico de un grupo arbitrario es normal.
    (vii) Sean G un grupo y $H \leq G$ cualquiera. Si $H \subseteq [G,G]$ se tiene que $H \lhd G$. Como consecuencia, se prueba que $H \subseteq [G,G]$ si, y sólo si, es G/H abeliano.
    (viii) Si $G = \langle g \rangle$ tiene orden 40 y $f\colon G \longrightarrow G$ es un endomorfismo definido por
    $$f(g) := g^{12},$$
    entonces f es un monomorfismo necesariamente.
    (ix) Sea G un grupo tal que $|[G,G]| = m$ con q un primo que divide a $|G|$ coprimo con m. Entonces no existe $H \leq G$ de orden qm.
    (x) Dados G un grupo y $H \leq G$ con $x, y \in G$ arbitrarios, se tiene que $xH \subseteq yH$ si, y sólo si, es $xH = yH$.
23. Dar un ejemplo (demostrándolo) de **grupo no abeliano** que satisfaga el **Teorema Inverso de Lagrange**, y otro que no. (**Sugerencia**: para la segunda parte, basta demostrar que el grupo alternado $\mathcal{A}_4$ no posee ningún subgrupo de orden 6).
24. Escribir $\mathcal{U}_{33}$ (grupo multiplicativo de $\mathbb{Z}_{33}$) como producto directo de grupos cíclicos. Determinar todos los elementos de orden 2 para este.
25. Sean G un grupo con $g \in G$ arbitrario. Consideremos también $n, m \in \mathbb{N}$ tales que $\mathrm{mcd}(n,m) = 1$. Probar que si $g^m = 1 = g^n$ entonces $g = 1$ necesariamente. ¿Sucede lo mismo si n y m no son coprimos?
26. Si G es grupo abeliano finito, este verifica el **Teorema Inverso de Lagrange**.
27. (**Teorema Chino de los Restos en Anillos**) Demostrar que, dados $n, m \in \mathbb{Z}$ dos enteros coprimos arbitrarios, la aplicación
    $$\begin{array}{rccc} f\colon & \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & r + nm\mathbb{Z} & \mapsto & (r + n\mathbb{Z}, r + m\mathbb{Z}) \end{array}$$
    es un ismorfismo de anillos. ¿Qué pasa si n y m no son coprimos?

28. Definir qué es un *ideal bilátero* de un anillo. ¿Por qué no es suficiente la noción de *ideal a izquierda* o *derecha*? Definir qué es un *ideal principal* de un anillo conmutativo, y probar que los DIP satisfacen la condición de la cadena ascendente.
29. Indica cuáles de los siguientes conjuntos son grupos, indicando el orden en los casos tales que estos sean finitos. ¿Son abelianos? ¿Y cíclicos?
    (i) $\{A \in \mathrm{Mat}_n(\mathbb{R}) \mid \det(A) = \pm 1\}$ con el producto de matrices usual.
    (ii) $(\mathbb{Z} \times \mathbb{Q}, \circ)$ tal que $(a,b) \circ (c,d) := (a+c, 2cb+d)$ para $a, c \in \mathbb{Z}$ y $b, d \in \mathbb{Q}$.
    (iii) $\mathbb{Z}_5 \times \mathbb{Z}_7$ con la suma definida por componentes.
    (iv) $(\mathbb{Z}, \Delta)$ tal que $a \Delta b := a + b + 1$ para $a, b \in \mathbb{Z}$.
    (v) $G = \{x \in \mathbb{R} \mid x > 0\}$ con la operación $a * b := a^b$ para $a, b \in G$.
    (vi) $G = \langle a, b \mid a^5 = 1 = b^4, a^b = a^2 \rangle$.
30. Indica cuáles de los siguientes conjuntos son anillos, indicando si estos son conmutativos o unitarios. ¿Son DI? ¿Y cuerpos?
    (i) $\{n/m \mid n, m \in \mathbb{Z}, m \neq 0, \mathrm{mcd}(n,m) = 1, m \text{ par}\}$ con las operaciones de $\mathbb{Q}$.
    (ii) $\left\{ \sum_{i \geq 0} a_i x^i \in \mathbb{Z}_6[x] \;\middle|\; a_i = 0 \text{ si } i \text{ es impar} \right\}$.
    (iii) El cuerpo de fracciones asociado a un DI.
    (iv) $\{a/(2^n 3^m) \mid a \in \mathbb{Z}; n, m \in \mathbb{Z}^+\}$ con las operaciones de $\mathbb{Q}$.
    (v) El producto cartesiano de infinitos (numerable) anillos.
    (vi) El conjunto de matrices
    $$\left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \;\middle|\; a_{ij} \in \mathbb{Q}, \forall\, i,j \in \{1,2,3\} \right\}$$
    con las operaciones usuales.
31. Sea A un anillo tal que para todo $x \in A$ verifica que $x^2 - x$ conmuta con todo elemento del anillo. Demostrar entonces que A es conmutativo.
32. Dados los anillos $\mathbb{Z}\left[\sqrt{3}\right]$ y $\mathbb{Z}\left[\sqrt{-5}\right]$ responder a las siguientes cuestiones:
    (i) Hallar el grupo de unidades para $\mathbb{Z}\left[\sqrt{-5}\right]$. ¿Qué sucede para $\mathbb{Z}\left[\sqrt{3}\right]$?
    (ii) Decidir **razonadamente** si existen homomorfismos de anillos unitarios
    $$f \colon \mathbb{Z}\left[\sqrt{3}\right] \longrightarrow \mathbb{Z}\left[\sqrt{-5}\right].$$
    (iii) Hallar, si existe, un generador del ideal $\left(2+\sqrt{3}, 5\right)\mathbb{Z}\left[\sqrt{3}\right]$. ¿Es $\mathbb{Z}\left[\sqrt{3}\right]$ un DIP? Decidir razonadamente si $\mathbb{Z}\left[\sqrt{-5}\right]$ es DFU, DIP ó DE.
33. Definir las nociones de *subgrupo normal* y *grupo simple*. Enunciar los **Teoremas de Sylow**. Utilizar estos para resolver las siguientes cuestiones:
    (i) Probar que todo grupo de orden 44 es simple.
    (ii) Demostrar que todo grupo de orden 455 es cíclico.
34. Demostrar que si una permutación se descompone como producto de ciclos disjuntos, entonces su orden es el mínimo común múltiplo de los órdenes para cada ciclo disjunto. Definir lo que se conoce por *signatura* de una permutación. ¿Cuál es la manera más sencilla de obtener esta? Calcular los órdenes y las signaturas correspondientes a las permutaciones siguientes:
    (i) $\sigma = (1,4,7)(5,6,3,9) \in \mathcal{S}_{10}$.
    (ii) $\sigma = (5,3,2,5) \in \mathcal{S}_5$.
    (iii) $\sigma = (1) \in \mathcal{S}_{13}$.
    (iv) $\sigma = (1,2)(2,5)(5,7,8,4) \in \mathcal{S}_8$.
    (v) $\sigma = (2,3)(3,9,7)(5,6,5) \in \mathcal{S}9$.
    (vi) $\sigma = (12)(3685) \in \mathcal{S}_8$.
    (vii) $\sigma = (1,3,5,1)(2,4,6,2) \in \mathcal{S}_7$.
    (viii) $\sigma = (1,2,3,4,5,6,1) \in \mathcal{S}_6$.
    (ix) $\sigma = (1,2)(2,3,4,5) \in \mathcal{S}_5$.
    (x) $\sigma = (5,6,8)(11,9,4,7,10) \in \mathcal{S}_{12}$.
35. Demostrar que todo homomorfismo de cuerpos no nulo es necesariamente inyectivo. Deducir de este hecho que, si tenemos dos cuerpos finitos que tienen el mismo cardinal, entonces estos son necesariamente isomorfos.

36. Considérese la función $\varphi\colon \mathbb{Z}\left[\sqrt{-10}\right] \longrightarrow \mathbb{N}$ definida por
$$\varphi\left(a+b\sqrt{-10}\right) := a^2+6b^2.$$
Responder a las siguientes cuestiones:
(i) Demostrar que φ es una aplicación multiplicativa.
(ii) Deducir de lo anterior que un elemento $x \in \mathbb{Z}\left[\sqrt{-10}\right]$ es unidad si, y sólo si, es $\varphi(x)=1$. ¿Contiene $\mathbb{Z}\left[\sqrt{-10}\right]$ unidades distintas de ± 1?
(iii) Sea $x \in \mathbb{Z}\left[\sqrt{-10}\right]$ tal que $N(x)=p \in \mathbb{N}$ es un número primo. ¿Es x un elemento irreducible en el anillo dado? ¿Es primo?
(iv) ¿Es $\mathbb{Z}\left[\sqrt{-10}\right]$ un DIP?
(v) ¿Para todo $x \in \mathbb{Z}\left[\sqrt{-10}\right]$ irreducible, se tiene que el ideal generado por dicho elemento es primo? ¿Es cierto el recíproco?
37. Sean A y B dos anillos, e I un ideal de A. Probar que un homomorfismo de anillos $f\colon A/I \longrightarrow B$ está bien definido si, y sólo si, se tiene que $I \subseteq \ker(f)$. Deducir que se da la igualdad si, y sólo si, este es inyectivo. ¿Sucede lo mismo en teoría de grupos? Concluir que si se tiene un homomorfismo de cuerpos finitos del mismo cardinal no nulo, entonces este es isomorfismo de cuerpos si, y sólo si, está bien definido.
38. Demostrar que el conjunto A formado por las aplicaciones de $\mathbb{Z}_2$ en sí mismo tiene 4 elementos, y que se trata de un anillo con la suma y el producto ordinarios de aplicaciones. ¿Es este un anillo isomorfo a $\mathbb{Z}_4$?
39. Determinar el número de homomorfismos entre los grupos $\mathbb{Z}_6$ y $\mathcal{S}_5$ tales que
(i) sean inyectivos.
(ii) la imagen tenga orden 3.
40. Construir un cuerpo F de 25 elementos, enumerando todos estos. Utiliza el **Teorema de Clasificación para grupos abelianos finitamente generados** (enunciando este correctamente) para deducir que F^* es un grupo cíclico. Encuentra (o justifica porqué es imposible) elementos de órdenes 3 y 5 en este grupo.
41. Determinar si los ideales
$$\left(5, x^3+x+1\right) \quad \text{y} \quad \left(3, x^3+x+1\right)$$
son primos en $\mathbb{Z}[x]$. ¿Es alguno de estos maximal?
42. Resolver los siguientes sistemas de congruencias en $\mathbb{Z}$ y $\mathbb{Z}_5$:
(i) $\begin{cases} x \equiv 55 \pmod{73}; \\ x \equiv 15 \pmod{34}; \\ x \equiv 36 \pmod{47}. \end{cases}$
(ii) $\begin{cases} x \equiv 20 \pmod{29}; \\ x \equiv 8 \pmod{43}; \\ x \equiv 44 \pmod{69}. \end{cases}$
(iii) $\begin{cases} x \equiv 46 \pmod{71}; \\ 5x \equiv 3 \pmod{7}; \\ 3x \equiv 3 \pmod{9}. \end{cases}$
(iv) $\begin{cases} f(x) \equiv 1 \pmod{x}; \\ f(x) \equiv 1 \pmod{x+1}; \\ f(x) \equiv 1 \pmod{x-1}. \end{cases}$
(v) En una cesta hay $x<100$ manzanas, que si se reparten de dos en dos sobra 1, si se reparten de tres en tres sobran 2, si se reparten de cuatro en cuatro sobran 3 y si se reparten de cinco en cinco sobran 4. ¿Cuántas manzanas hay en el cesto?
43. Resolver las siguientes ecuaciones diofánticas en $\mathbb{Z}$ y $\mathbb{Z}[i]$:
(i) $18x-7y=48$.
(ii) $125x+476y=1$.
(iii) $(40+18i)x+(-23+10i)y=1$.
(iv) $5x+(3+4i)y=-2-i$.
(v) Estando en Estados Unidos, el Sr. Herrera se quedó sin dinero en efectivo y fue al banco a cambiar un cheque de viaje. El cajero, al pagarle, confundió el número de dólares con el número de centavos, y viceversa. Sin darse cuenta de este hecho, el Sr. Herrera gastó 49 y entonces, para su sorpresa, vio que la cantidad de dinero en efectivo que tenía era el doble al valor del cheque de viaje que había cambiado. Determina el valor mínimo que podría tener dicho cheque.

44. Probar que todo homomorfismo de grupos es además inyectivo si, y sólo si, se tiene que $\ker(f) = \{1\}$. ¿Sucede lo mismo para homomorfismos de anillos? Demuestra la caracterización correspondiente en teoría de anillos.
45. Dado $f\colon A \longrightarrow B$ demuestra que $\ker(f)$ es un ideal de A mientras que $\mathrm{Im}(f)$ es un subanillo de B. ¿Cuándo podemos asegurar que $\mathrm{Im}(f)$ es un ideal de B? Obtén (y prueba) resultados análogos para cuando se tienen homomorfismos de grupos.
46. ¿Cuántas clases de isomorfía hay de grupos abelianos con orden 3000? Determina los coeficientes de torsión y los divisores elementales para cada uno de estos. ¿Cuáles son cíclcos? De entre los grupos G anteriores, ¿para cuáles existe un epimorfismo de grupos $f\colon G \longrightarrow (\mathbb{Z}_{1500}, +)$?
47. Identificar el grupo G generado por los elementos x, y, z sujetos a las relaciones
$$\begin{cases} x + 2y + 3z = 0; \\ x + y + 2z = 0; \\ 2x + y + 8z = 0. \end{cases}$$
Identificar el orden de G y sus factores invariantes. Decidir si G contiene algún subgrupo cíclico de oren 8. ¿Existen subgrupos cíclicos de órdenes 5 y 12?
48. Consideremos la acción de un grupo G sobre un conjunto X arbitrario. Definir las *órbitas* y los *estabilizadores* de una acción, y enunciar cómo están relacionados los cardinales de ambos. Se pide demostrar lo siguiente:
    (i) Dados $x_1, x_2 \in X$ con estabilizadores H_1 y H_2 respectivamente, demostrar que estos dos son subgrupos conjugados si x_1 y x_2 están en la misma órbita.
    (ii) Supongamos que G tiene orden primo p y que X tiene cardinal finito m no múltiplo de p. Probar que la acción de G sobre X tiene algún punto fijo.
49. Halla el máximo orden posible para una permutación de $\mathcal{S}_{10}$ y encuentra un ejemplo explícito de permutación con dicho orden. ¿Pueden existir en dicho grupo permutaciones de orden 22? ¿Y de orden 16?
50. Sea $A = \mathbb{Z}_7[x]/\left(x^2 + 4x + 3\right)$.
    (i) Decidir si A es DI. En caso afirmativo, hallar un divisor de cero no trivial de A.
    (ii) Calcular el cardinal de A. Determinar su grupo de unidades, y listar estas.
    (iii) Justifica si la aplicación $\varphi\colon A \longrightarrow \mathbb{Z}_7 \times \mathbb{Z}_7$ definida por
    $$\left(f(x) + \left(x^2 + 4x + 3\right)\right) \mapsto (f(6), f(1))$$
    es un isomorfismo de anillos.
51. Probar que todo grupo de orden $p^a q$ con p y q primos (no ncesariamente distintos), siendo $a \in \mathbb{N}$ arbitrario, es resoluble.
52. (**Relaciones de Cardano-Vieta**) Dado
$$f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{C}[x]$$
con $u_1, u_2, u_3 \in \mathbb{C}$ sus raíces, demostrar que
$$\begin{cases} -a_2 = u_1 + u_2 + u_3; \\ a_1 = u_1u_2 + u_1u_3 + u_2u_3; \\ -a_0 = u_1u_2u_3. \end{cases}$$
Encontrar fórmulas similares para cualquier polinomio en $\mathbb{C}[x]$ de grado n arbitrario.
53. Sea G un grupo finito tal que $3 \nmid |G|$. Probar las afirmaciones siguientes:
    (i) La aplicación
    $$\begin{array}{rccc} f\colon & G & \longrightarrow & G \\ & x & \mapsto & f(x) := x^3 \end{array}$$
    es biyectiva.
    (ii) Si $(ab)^3 = a^3b^3$ para todo $a, b \in G$ arbitrarios, entonces G es un grupo abeliano.

54. (**Teorema Chino de los Restos en Grupos**) Demostrar que, dados $n, m \in \mathbb{Z}$ dos enteros coprimos arbitrarios, la aplicación
$$\begin{array}{rccc} f\colon & (\mathbb{Z}/nm\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \\ & r + nm\mathbb{Z} & \mapsto & (r + n\mathbb{Z}, r + m\mathbb{Z}) \end{array}$$
es un ismorfismo de grupos. (**Sugerencia**: Se sigue del **Teorema Chino de los Restos en Anillos**). Obtén que la función de Euler es multiplicativa por coprimos[1].
55. Determina la estructura del grupo $\mathcal{U}_{4991}$ (grupo multiplicativo de $\mathbb{Z}_{4991}$).
56. Determinar cuáles de los siguientes conjuntos son subanillos ó ideales:
    (i) En el anillo de las matrices cuadradas reales que tienen orden 2×2 el subconjunto formado por aquellas matrices de la forma
    $$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
    donde $a - d = 0$ y $b + c = 0$ con $a, b, c, d \in \mathbb{R}$.
    (ii) $\left\{ \sum_{i\geq 0} a_i x^i \;\middle|\; a_i \in \mathbb{Z}; \forall\ i \in \mathbb{N}, a_0 \in 2\mathbb{Z} \right\}$.
    (iii) El producto de dos ideales en cualquier anillo.
    (iv) La imagen recíproca por un homomorfismo de anillos para un ideal.
    (v) El centro de un anillo.
    (vi) $\left\{ \sum_{i\geq 0} a_i x^i \;\middle|\; a_i \in \mathbb{Z}; \forall\ i \in \mathbb{N}, a_i \in 2\mathbb{Z}, \forall\ i \in 2\mathbb{Z} \right\}$.
57. Determinar cuáles de los siguientes conjuntos son subgrupos. ¿Cuáles son normales?
    (i) En el grupo de las matrices cuadradas reales que tienen orden 2×2 el subconjunto formado por aquellas matrices de la forma
    $$\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}$$
    bajo la multiplicación de matrices, para $x \in \mathbb{R}$.
    (ii) La imagen recíproca por un homomorfismo de grupos para un subgrupo normal.
    (iii) La intersección finita de subgrupos normales.
    (iv) El conjunto de todos los conmutadores entre elementos de un grupo.
    (v) La raíces n-ésimas de la unidad en $\mathbb{C}^*$ (con el producto).
    (vi) $\{(1), (1,2)(3,4), (1,2), (3,4)\}$ es $\mathcal{S}_4$.
58. Demostrar que $x^3 + x^2 + 1$ es un polinomio irreducible sobre $\mathbb{Z}_2[x]$. Determinar si $\mathbb{Z}_2[x]/\left(x^3 + x^2 + 1\right)$ es un cuerpo, y hallar su cardinal. ¿Es este isomorfo a $\mathbb{Z}_8$?
59. Sean A un anillo y $\mathfrak{p}$ un ideal primo de A. Probar que si A es DIP, entonces $A/\mathfrak{p}$ es también DIP. ¿Es cierto el recíproco? ¿Qué sucede si en vez de DIP ponemos DFU?
60. Se considera el anillo $A = \mathbb{Z}\left[\sqrt{-80}\right]$ con la norma multiplicativa usual inducida del conjugado complejo dado en $\mathbb{C}$.
    (i) Demostrar que 2 y 3 son irreducibles en A.
    (ii) Probar que 3 no es primo en A.
    (iii) Enunciar que es un DE. ¿Es A un DE?
61. Sea $G = \langle \alpha, \beta \rangle$ el subgrupo de $\mathcal{S}_{10}$ generado por las permutaciones
$$\alpha = (1,2,3,4)(5,6,7)(8,9,10) \quad \text{y} \quad \beta = (1,3)(2,4)(5,8,7,10,6,9).$$
    (i) Probar que G es abeliano, y calcular $|G|$.
    (ii) Expresar G como producto directo de subgrupos.
    (iii) ¿Cuántos elementos de orden 12 tiene G?

[1]En ocasiones, se dice que una aplicación del tipo $f\colon A \longrightarrow B$ entre dos anillos A y B es multiplicativa si $f(ab) = f(a)f(b)$ sólo cuando a y b son coprimos. Nosotros diremos, para distinguir con lo que llamamos aplicación multiplicativa en la **Hoja de Ejercicios** 1, que esta es una *aplicación multiplicativa por coprimos*.

62. Sea $\mathbb{K}$ un cuerpo arbitrario. Examinar si el ideal
$$\left(x^2+y^2+z^2, z-x^3\right) \subseteq \mathbb{K}\left[x,y,z\right]$$
es un ideal primo. (**Sugerencia**: Distinguir los casos $\operatorname{car}(\mathbb{K})=2$ y $\operatorname{car}(\mathbb{K})\neq 2$).
63. Demuestra que $F=\mathbb{Z}_3[x]/(x^2+1)$ es un cuerpo finito y halla su cardinal. Encuentra un generador del grupo multiplicativo de F y expresa todos los elementos de F^* como potencia de dicho generador. Haz lo mismo con $K=\mathbb{Z}_2[x]/(x^3+x+1)$.
64. Construye cuerpos finitos con 16, 25, 81 y 125 elementos.
65. Demuestra las siguientes afirmaciones en orden para conlcuir un procedimiento que te permite saber si un número dado es primo, el cual se conoce por **Test de primalidad de Lucas (versin mejorada de Kraitchik y Lehmer)**.
    (i) Sea $n>1$ un entero. Demuestra que
    $$n \text{ es primo } \iff n-1=\varphi(n) \iff n-1 \text{ divide a } \varphi(n).$$
    Concluye de esto que, si n no es primo, entonces existen un primo q y $r\geq 1$ tales que q^r divide a $n-1$ pero no a $\varphi(n)$.
    (ii) Supón ahora que nuestro n no es primo y que, para el q del apartado anterior, existe un entero a tal que $a^{n-1}\equiv 1 \mod n$ y
    $$a^{\frac{n-1}{q}} \not\equiv 1 \mod n.$$
    Observa que $a\in(\mathbb{Z}/n)^*$ y sea m el orden de a en $(\mathbb{Z}/n)^*$. Demuestra que q^r divide a m y, por tanto, también a $\varphi(n)$.
    (iii) Demuestra que si $n>1$ es un entero, y para cualquier factor primo q de $n-1$ existe un entero a tal que $a^{n-1}\equiv 1 \mod n$ y
    $$a^{\frac{n-1}{q}} \not\equiv 1 \mod n,$$
    entonces n es primo.
66. Demuestra que el *número de Fermat* $F_k := 2^{2^k}+1$ es primo si, y sólo si, existe un entero a tal que
$$a^{\frac{F_k-1}{2}} \equiv -1 \mod F_k.$$
(**Sugerencia**: Utiliza el **Ejercicio** 65 anterior).
67. Sean $\mathbb{R}[t]$ y $\mathbb{R}[x,y]$ los anillos con coeficientes reales en una y dos indeterminadas, respectivamente. Considerar el homomorfismo de anillos evaluación dado por
$$\begin{array}{rccc}\varphi\colon & \mathbb{R}[x,y] & \longrightarrow & \mathbb{R}[t] \\ & p(x,y) & \mapsto & p\left(t^3,t^7\right)\end{array}.$$
    (i) Demostrar (argumentando) si $\mathbb{R}[t]$ y $\mathbb{R}[x,y]$ son DFUs. ¿Es alguno de ellos DIP?
    (ii) Decidir si φ es sobreyectivo, y calcular su núcleo.
    (iii) Estudiar si el núcleo es un ideal primo o maximal.
68. El objetivo que se propone en este ejercicio es determinar la estructura del anillo cociente $\mathbb{Z}\left[\sqrt{-2}\right]/\mathfrak{a}$ con $\mathfrak{a}=\left(5-\sqrt{-2},3\right)\mathbb{Z}\left[\sqrt{-2}\right]$ un ideal
    (i) Calcular el máximo común divisor de $-5+2\sqrt{-2}$ y $1+5\sqrt{-2}$. Obtener también unos coeficientes para una Identidad de Bézout en el anillo $\mathbb{Z}\left[\sqrt{-2}\right]$.
    (ii) Encontrar, si es posible, un generador del ideal $\mathfrak{a}$. ¿Es este un elemento primo?
    (iii) Determinar el núcleo y la imagen del único homomorfismo de anillos unitarios (demostrar que, efectivamente, no hay más) $f\colon\mathbb{Z}\longrightarrow\mathbb{Z}\left[\sqrt{-2}\right]/\mathfrak{a}$.
    (iv) Deducir de esto la estructura del anillo $\mathbb{Z}\left[\sqrt{-2}\right]/\mathfrak{a}$ y calcular su cardinal.
69. Sea $f\colon G_1\longrightarrow G_2$ un homomorfismo de grupos. Si tenemos que la aplicación f no se corresponde con el homomorfismo trivial, siendo $|G_1|=18$ y $|G_2|=15$ por ejemplo, ¿cuánto vale $|f(G_1)|$?

70. Resolver las siguientes cuestiones sobre homomorfismos de grupos:
    (i) Determinar (y el núcleo e imagen) los homomorfismos de grupos entre $\mathbb{Z}_n$ y $\mathbb{Z}$.
    (ii) ¿Puede existir algún homomorfismo de grupos que vaya de $\mathbb{Z}_8$ en $\mathbb{Z}_{12}$?
    (iii) Calcula todos los endomorfismos de grupos del grupo simétrico $\mathcal{S}_3$.
    (iv) ¿Cuántos homomorfismos de grupos suprayectivos existen de $\mathcal{D}_{13}$ en $\mathbb{Z}_{12}$?
    (v) Estudia si existe un ismorfismo de grupos entre $\mathcal{D}_6$ y $\mathbb{Z}_2 \times \mathcal{S}_3$.
71. Resolver las siguientes cuestiones sobre homomorfismos de anillos:
    (i) ¿Es posible que exista algún homomorfismo de anillos unitario entre $\mathbb{Z}$ y $\mathbb{Z}[i]$?
    (ii) Enumerar todos los homomorfismos de anillos unitarios que vayan de $\mathbb{Z}_n$ en $\mathbb{Z}_m$.
    (iii) Probar si existe $f\colon \mathbb{Z}\left[\sqrt{-2}\right] \longrightarrow \mathbb{Z}\left[\sqrt{23}\right]$ homomorfismo de anillos unitario.
    (iv) ¿Eres capaz de dar algún monomorfismo de anillos unitario con origen $\mathbb{Z}$ en $\mathbb{Q}$?
    (v) Construye explícitamente un homomorfismo de anillos no nulo y no unitario.
72. Demostrar que $Z(\mathcal{S}_n)$ es trivial para $n \geq 3$.
73. Sea $G \leq \mathcal{S}_n$. Considerar la acción natural de G sobre el conjunto $X = \{1, 2, 3, 4\}$. Escribir las órbitas de dicha acción y encontrar los estabilizadores de cada punto, para cada uno de los siguientes grupos:
    (i) $G = \langle 1, 2, 3\rangle$; (ii) $G = \langle 1, 2, 3, 4\rangle$; (iii) $G = \mathcal{A}_4$.
74. Demostrar que el grupo alternado $\mathcal{A}_5$ tiene subgrupos de índices 6 y 10. ¿Puede tener este algún subgrupo de índice 3 ó 4? Razónalo.
75. Sea $H \leq K \lhd G$ donde se tiene que K es cíclico y finito. Demostrar que $H \lhd G$.
76. Supongamos que $H \leq G$ y $x^2 \in H$ para todo $x \in G$. Demostrar que $H \lhd G$ y concluir que el grupo cociente G/H es abeliano.
77. Consideremos el grupo aditivo $(\mathbb{Z}_{220}, +)$.
    (i) Determinar el índice del subgrupo H de $\mathbb{Z}_{220}$ generado por $[28]_{220}$.
    (ii) ¿A qué grupo conocido es isomorfo H?
    (iii) ¿Cuántos subgrupos de $\mathbb{Z}_{220}$ existen con el mismo índice que H?
78. Da un ejemplo de grupo con las siguientes características en cada caso:
    (i) Grupo G infinito que tenga exactamente un elemento de orden 2.
    (ii) Grupo G no abeliano que sea simple de orden mayor que 60.
    (iii) Grupo G abeliano de orden no primo tal que no tenga ningún cociente cíclico.
    (iv) Grupo G infinito en el que todo elemento no trivial tenga orden 2.
    (v) Grupo G de orden impar tal que para cada $x \in G$ exista $y \in G$ con $y^2 = x$.
79. Da un ejemplo de anillo con las siguientes características en cada caso:
    (i) Un anillo A que sea DFU, pero sin embargo no DIP.
    (ii) Un anillo A que tenga, al menos, un ideal infinitamente generado.
    (iii) Un anillo A que no sea cuerpo y tenga infinitas unidades.
    (iv) Un anillo A no conmutativo, y que tampoco sea unitario.
    (v) Un anillo A con infinitos elementos divisores de cero.
80. Decidir si $\mathbb{R}[x, y]/\left(y - x^3\right)$ es DE, DIP ó DFU. Calcular sus unidades.
81. Estudiar si los siguientes polinomios son irreducibles:
    (i) $x^4 + 5x^3 + 4x + 6$ en $\mathbb{Q}$.
    (ii) $x^6 + x^5 + x^4 + x^3 + x^2 + 1$ en $\mathbb{Z}_2$.
    (iii) $x^5 + 2x^4 + 3x^3 + 3x^2 + 2x + 1$ en $\mathbb{R}$.
    (iv) $x^4 + 4x^3 + 6x^2 + 2x + 1$ en $\mathbb{Z}$.
    (v) $x^3 + 2x^2 + 1$ en $\mathbb{Z}_{17}$.
    (v) $5x^{10} + 10x^7 + 20x^3 + 10$ en $\mathbb{Z}[i]$.
    (vi) $2x^4 - 8x + 1$ en $\mathbb{Q}[i]$.
    (vii) $x^6 + 30x^5 - 15x^3 + 6x - 120$ en $\mathbb{C}$.
    (ix) $x^n + 22$ en $\mathbb{Z}_{23}$ para $n \geq 2$.
    (x) $x^4 + 15x^3 - 5$ en $\mathbb{Z}_7$.
82. Sea A un anillo conmutativo con unidad. Vamos a denotar por $\mathrm{Nil}(A)$ el ideal formado por los elementos nilpotentes de A. Demostrar que son equivalentes:
    (i) A tiene exactamente un ideal primo.
    (ii) Cada elemento de A es nilpotente o unidad.
    (iii) $A/\mathrm{Nil}(A)$ es un cuerpo.

83. Sea G un grupo de orden 27125.
    (i) Demostrar que G tiene un único subgrupo normal de orden 217.
    (ii) Probar que G satisface el **Teorema Inverso de Lagrange**.
    (iii) Demostrar que G es resoluble.
84. Examinar si los siguientes ideales son primos ó maximales para $\mathbb{K}$ un cuerpo:
    (i) $\left(x^3+y^2+z\right)$ en $\mathbb{K}[x,y,z]$.
    (ii) $\left(x^3-3xyz+y^3+z^3\right)$ en $\mathbb{K}[x,y,z]$.
    (iii) $\left(x^5+xyz^5+y^5zt^5\right)$ en $\mathbb{K}[x,y,z,t]$.
    (iv) $\left(y^6-x^4z\right)$ en $\mathbb{K}[x,y,z]$.
    (v) $\left(x^4y+y^5z+z^6x\right)$ en $\mathbb{K}[x,y,z]$.
    (vi) $(x-yz,z-xy)$ en $\mathbb{K}[x,y,z]$.
    (vii) $\left(y+2x^2,z+3x^3,t-x^4-y-z\right)$ en $\mathbb{K}[x,y,z,t]$.
    (viii) $\left(y+2x^2,z+3x^3,t^5-x^4-y-z\right)$ en $\mathbb{K}[x,y,z,t]$.
85. Sea $f(x)\in\mathbb{Z}[x]$. Demostrar que si $f(0)$ y $f(1)$ son impares, entonces $f(x)$ no tiene raíces enteras. Concluir que $f(x)=x^3+x+1\in\mathbb{Z}[x]$ es irreducible sobre $\mathbb{Z}$.
86. Sea $A=\mathbb{Z}\times\mathbb{Z}\times\dots$ el producto directo de una cantidad numerable de copias enteras, y sea $R=\mathrm{End}(A,+)$. Sea $\varphi,\psi\in R$ definidos por
$$\varphi(a_1,a_2,a_3,\cdots):=(a_2,a_3,\cdots),\quad \forall\, a_1,a_2,a_3,\cdots\in\mathbb{Z}$$
y
$$\psi(a_1,a_2,a_3,\cdots):=(0,a_1,a_2,a_3,\cdots),\quad \forall\, a_1,a_2,a_3,\cdots\in\mathbb{Z}.$$
    (i) Probar que $\varphi\psi=1_{\mathrm{End}(\mathbb{Z}^\infty)}$ y $\psi\varphi\neq 1_{\mathrm{End}(\mathbb{Z}^\infty)}$. Es decir, demostrar que ψ es un inverso por la derecha de φ pero no por la izquierda.
    (ii) Encontrar infinitos ejemplos distintos de inversos por la derecha de φ que no lo son por la izquierda.
    (iii) Encontrar un elemento no nulo $f\in\mathrm{End}(\mathbb{Z}^\infty)$ de forma que $\varphi f=0$ pero $f\varphi\neq 0$.
    (iv) Probar que no existe $g\in\mathrm{End}(\mathbb{Z}^\infty)$ no nulo de forma que $g\varphi=0$.
87. ¿Cuántos 2-subgrupos de Sylow tiene $\mathcal{S}_4$? Probar que si T es un 2-subgrupo de Sylow para $\mathcal{S}_4$ entonces $T\cong\mathcal{D}_8$. Hallar todos los subgrupos de Sylow para $\mathcal{S}_5$.
88. ¿Cuántos subgrupos de orden p primo tiene un grupo isomorfo a $\mathcal{C}_p\times\mathcal{C}_p$? Deducir el número de elementos con orden p. Lo mismo para grupos isomorfos a $\mathcal{C}_p\times\mathcal{C}_p\times\mathcal{C}_p$.
89. Sean
$$H=\left\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\;\middle|\; ad\neq 0; a,b,c\in\mathbb{R}\right\}$$
y
$$N=\left\{\begin{pmatrix}1&b\\0&1\end{pmatrix}\;\middle|\; b\in\mathbb{R}\right\}.$$
Responder razonadamente a las cuestiones siguientes:
    (i) ¿Es H un subgrupo normal de $\mathrm{GL}(2,\mathbb{R})$?
    (ii) ¿Es N un subgrupo normal de H?
90. Sea G un grupo finito de orden impar que contiene un subgrupo normal N de orden $|N|=5$. Demostrar que en la acción por conjugación de G en N todas las órbitas son unitarias, y concluir que N es un subgrupo de centro G.
91. Calcular el número de elementos que tengan orden 5 en los posibles grupos G de orden 45. ¿Es posible determinar estos para cualquier grupo de orden 50?
92. Demostrar que dado un grupo G así como un subgrupo $N\leq G$ para este, se tiene que $N\lhd G$ si, y sólo si, este es unión entre algunas clases de conjugación para G nuestro grupo, entre las cuales debe estar la clase del 1 necesariamente. Determina el número de todas las clases de conjugación que tienen los grupos alternados de órdenes $2,3,4$ y 5 en cada caso, así como el número de elementos en cada una de esta. Comprueba que se satisface la **Ecuación de Clases** para cada uno de estos. Utilizar lo demostrado al principio para conlcuir que $\mathcal{A}_5$ es simple. ¿Qué sucede con los grupos alternados de orden $n<5$? Dar ejemplos de subgrupos normales para estos.

93. Todo grupo G en el que su cociente por el centro $Z(G)$ sea cíclico verifica que este es necesariamente el grupo trivial $\left\{1_{G/Z(G)}\right\}$.
94. Sea G un grupo de orden p^3q donde tenemos que p y q primos diferentes. Demostrar que dos q-subgrupos de Sylow distintos tienen intersección trivial siempre. ¿Sucede lo mismo con los p-subgrupos de Sylow? Dar ejemplos de grupos que tengan el orden dado para los que existan (y darlos como ejemplos, obviamente) dos p-subgrupos de Sylow distintos que tengan intersección $1, p$ y p^2.
95. Demostrar que la característica de un anillo A divide al entero n si $na = 0$ para algún $a \in A$ no nulo cuando este es un DI. ¿Qué sucede en caso de que A no sea DI?
96. Sean G un grupo finito y $H \leq G$ arbitrario. Se define como *exponente* de G (el cual se denota por $\exp(G)$) al menor entero positivo n tal que $g^n = 1$ para todo $g \in G$ arbitrario. Demostrar las afirmaciones siguientes:
    (i) El entero $\exp(G)$ es el mínimo común múltiplo de los órdenes para todos los elementos en G. Por tanto, este divide a $|G|$ y puede no darse la igualdad.
    (ii) $\exp(H)$ divide a $\exp(G)$.
    (iii) Si $H \lhd G$ se tiene que $\exp(G/H)$ divide a $\exp(G)$.
    (iv) Para todo entero $n \geq 2$ se tiene que
    $$\exp\left(\mathbb{S}^n\right) = \begin{cases} \exp\left(\mathbb{S}^{n-1}\right) & \text{si } n \text{ no es potencia de un primo;} \\ p\exp\left(\mathbb{S}^{n-1}\right) & \text{si } n \text{ es potencia de un primo } p. \end{cases}$$
97. Sea $A = \mathbb{Z}_{12}[x]/\left(x^2\right)$.
    (i) Estudiar si A es un cuerpo, explicando razonadamente los motivos. ¿Es DI?
    (ii) Demostrar que todo elemento de A viene unívocamente determinado por un representante del tipo $ax + b \in \mathbb{Z}_{12}[x]$.
    (iii) Probar que A tiene exactamente 48 unidades.
98. Utilizar el homomorfismo de grupos inducido por la acción de G multiplicación a izquierda de coclases para demostrar que todo grupo G con orden $|G| = p^r n > n!$ siendo $p \nmid n$ primo con $r \geq 1$ no puede ser simple.
99. Sea $\mathbb{K}$ un cuerpo. Considerar el anillo
    $$A = \left\{ \sum_{i,j\geq 0} a_{ij}x^i y^j \in \mathbb{K}[x,y] \;\middle|\; a_{ij} = 0 \text{ cuando } i+j \text{ es impar} \right\}.$$
    Este es el anillo de polinomios en el que todos los monomios que aparecen tienen grado total par. Se comprueba que este es un subanillo de $\mathbb{K}[x,y]$. ¿Es ideal?
    (i) Dar las unidades de A y probar que los elementos xy, x^2 e y^2 son irreducibles en A. ¿Hay algún otro monomio del tipo $x^i y^j$ con $i, j \geq 0$ que sea irreducible en A?
    (ii) Deducir que A no es un DFU.
    (iii) Probar que x^3y e y^2x^2 no tienen máximo común divisor en A.
100. Consideramos el anillo $A = \mathbb{Z}_7[x]/\left(x^2 - x + 4\right)$.
    (i) Demostrar que este es un cuerpo de $7^2 = 49$ elementos.
    (ii) Determinar $\alpha = \left[x^3\right]$ como elemento de A que tenga orden menor que 2.
    (iii) Obtén el inverso de $\left[x^3 + x^2 + x\right]$ en A.
    (iv) Demuestra (o justifica) que el grupo de las unidades para A es un grupo cíclico de orden $48 = 2^4 \cdot 3$. Halla un generador del mismo para asegurar que este es un grupo cíclico, explicando el procedimiento empleado para ello.
    (v) Prueba que A^* no es simple, dando un subgrupo normal propio concreto. ¿Existe algún grupo de orden 48 que sea simple? Justifica adecuadamente tu respuesta. Determinar todos los posibles grupos abelianos (salvo isomorfismo) que tengan orden 48 señalando sus factores invariantes.