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

Factorización en polinomios. Criterios de irreducibilidad.

1. Dado n un número entero positivo, sea
$$\Phi_n(t) = t^{n-1} + t^{n-2} + \cdots + t + 1$$
el conocido como n-ésimo *polinomio ciclotómico.*
   (i) Demostrar que Φ_n es irreducible en $\mathbb{Z}[t]$ si, y sólo si, se tiene que n es primo.
   (ii) Demostrar que Φ_7 es irreducible en $(\mathbb{Z}[i])\,[t]$. ¿Pasa lo mismo con Φ_5?
2. Factorizar $f(t) = t^4 + 1$ en $\mathbb{Q}[t], \mathbb{R}[t]$ y $\mathbb{C}[t]$.
3. Estudiar la irreducibilidad en $\mathbb{Z}[t]$ de los polinomios siguientes **en función de los enteros dados** en cada caso, dando las factorizaciones correspondientes cuando toque:
   (i) $f_n(t) = t^2 + t - n$ para $n \in \{1, \ldots, 100\}$.
   (ii) $u_n(t) = t^n - 1$ para $n \in \{1, \ldots, 10\}$.
4. Estudiar si los polinomios $f(t) = t^4 - 5$ y $g(t) = t^3 - 2$ son irreducibles en $(\mathbb{Q}[i])\,[t]$.
5. Dado A un dominio de integridad, sea $a \in A\backslash\{0\}$ tal que $(a, t)A[t]$ es ideal principal. Demostrar que $a \in A^*$. Concluir que las siguientes afirmaciones son equivalentes:

   (i) A es un cuerpo; (ii) $A[t]$ es un DE; (iii) $A[t]$ es un DIP.

6. Dados $k \in \mathbb{Z}$ entero positivo, un polinomio $f \in \mathbb{Z}[t]$ arbitrario y el homomorfismo de anillos $\pi_k : \mathbb{Z}[t] \to \mathbb{Z}_k[t]$ *reducción módulo* k, demostrar que se tienen los isomorfismos
$$\frac{\mathbb{Z}[t]}{k\mathbb{Z}[t]} \cong \mathbb{Z}_k[t] \quad \text{y} \quad \frac{\mathbb{Z}[t]}{(k, f)\mathbb{Z}[t]} \cong \frac{\mathbb{Z}_k[t]}{\pi(f)\mathbb{Z}_k[t]}.$$
7. Estudiar si el ideal $\left(2, t^2 + 1\right)\mathbb{Z}[t]$ es primo.
8. Sean p un número primo y n un entero positivo.
   (i) Explicar cómo construir un cuerpo con p^n elementos.
   (ii) Constrúyase explícitamente un cuerpo que tenga un total de $5^3 = 125$ elementos.
9. Responder a las siguientes cuestiones:
   (i) Estudiar si el polinomio $f(t) = t^2 + 1$ es irreducible en $\mathbb{Z}_{11}[t]$.
   (ii) Determinar si $\mathbb{Z}_{11}[t]/f\mathbb{Z}_{11}[t]$ es un cuerpo o no. ¿Cuántos elementos tiene?
   (iii) Sea $\pi_{11} : \mathbb{Z}[t] \to \mathbb{Z}_{11}[t]$ el homomorfismo *reducción módulo* 11. Probar que
$$\ker \pi_{11} = 11\mathbb{Z}[t].$$
   (iv) Demostrar que se tiene la igualdad
$$\mathfrak{a}_{11} = \pi_{11}^{-1}\left(f\mathbb{Z}_{11}[t]\right) = \left(11, t^2 + 1\right)\mathbb{Z}[t].$$
   (v) Concluir que $\mathbb{Z}[t]/\mathfrak{a}_{11}$ es un cuerpo, y calcular su cardinal.
   (vi) ¿Cambia algo si usamos el primo 7? ¿Y si lo hacemos con 5? Deducir una **regla general** de los primos impares p tales que $\mathfrak{a}_p = \left(p, t^2 + 1\right)\mathbb{Z}[t]$ sea ideal maximal.

Algoritmo Extendido de Euclides en polinomios. Aplicaciones.

10. Estudiar (justificando) si son isomorfos los siguientes pares de anillos:

(i) $\frac{\mathbb{R}[x]}{(x^2+1)}$ y $\frac{\mathbb{R}[x]}{(x^2-1)}$.

(ii) $\mathbb{Z}_9$ y $\frac{\mathbb{Z}_3[x]}{(x^2+1)}$.

(iii) $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$ y $\frac{\mathbb{Z}_2[x]}{(x^3+x^2+1)}$.

(iv) $\mathbb{Z}_4[x]$ y $\mathbb{Z}_2[x]$.

11. Hallar una identidad de Bézout para el máximo común divisor de los polinomios
    (i) $f(x) = x^4 + 6x^3 + 13x^2 + 12x + 3$ y $g(x) = x^4 + 5x^5 + 9x^2 + 8x + 2$ en $\mathbb{Q}[x]$.
    (ii) $f(x) = x^5 + 3x^3 + 4x + 2$ y $g(x) = x^4 + 2x^3 + 1$ en $\mathbb{Z}_5[x]$.
12. Sean $f(t) = t^3 + t^2 + 2 \in \mathbb{Z}_3[t]$ y $g(t) = t^3 + t + 1 \in \mathbb{Z}_2[t]$.
    (i) Probar si el ideal $f\mathbb{Z}_3[t]$ es maximal, y determinar el cardinal de $\mathbb{Z}_3[t]/f\mathbb{Z}_3[t]$.
    (ii) Demostrar que $\mathbb{Z}_2[t]/g\mathbb{Z}_2[t]$ es un cuerpo.
    (iii) Estudiar si
    $$(1+t) + f\mathbb{Z}_3[t] \in \frac{\mathbb{Z}_3[t]}{f\mathbb{Z}_3[t]}$$
    tiene inverso (calcularlo si es así).
    (iv) Calcular el cardinal de $\mathbb{Z}_2[t]/g\mathbb{Z}_2[t]$ y describir explícitamente sus elementos.
13. Consideremos el ideal $\mathfrak{a} = \big(t^2+1\big)\mathbb{Z}_5[t]$.
    (i) Estudiar si el cociente
    $$A = \frac{\mathbb{Z}_5[t]}{\mathfrak{a}}$$
    es un cuerpo, y calcular el inverso de $\big(t^2+t-3\big) + \mathfrak{a}$ en A.
    (ii) Estudiar si A tiene divisores de cero y, en caso afirmativo, dar un ejemplo.
14. Sea $\mathfrak{a} = \big(x^3 + x^2 + 2\big)$ un ideal de $\mathbb{Z}_3[x]$.
    (i) Demostrar que es maximal, y determinar el cardinal del cociente $\mathbb{Z}_3[x]/\mathfrak{a}$.
    (ii) Hallar, si es posible, el inverso de $x+1$ en el cociente anterior.
15. Sea $f(x) = x^4 + x^3 + x^2 + x + 1$ un polinomio en $\mathbb{Z}_2[x]$. Considerar el anillo cociente
    $$F = \frac{\mathbb{Z}_2[x]}{f\mathbb{Z}_2[x]}.$$
    (i) Probar que F es un cuerpo. ¿Cuántos elementos tiene?
    (ii) Demostrar que, si tenemos $\alpha \in F$ una raíz del polinomio $t^7 - 1 \in F[t]$ arbitraria, necesariamente esta verifica que $\alpha = 1$.
16. Sean $\mathbb{K}$ un cuerpo y $m \in \mathbb{N}$.
    (i) Si m es impar, probar que el polinomio $y^2 - x^m$ es irreducible en $\mathbb{K}[x,y]$. ¿Qué sucede si m es par?
    (ii) Si m no es múltiplo de 3, probar que el polinomio $y^3 - x^m$ es irreducible en $\mathbb{K}[x,y]$. ¿Qué sucede si m es múltiplo de 3?
17. Sean $\mathbb{K}$ un cuerpo, y sean $m, n \in \mathbb{N}$ enteros coprimos. Probar que el polinomio $y^n - x^m$ es irreducible en $\mathbb{K}[x,y]$. ¿Qué sucede si n y m no son coprimos? (**Sugerencia**: Definir el **homomorfismo de anillos evaluación**
    $$\begin{array}{rccc} \varphi\colon & \mathbb{K}[x,y] & \longrightarrow & \mathbb{K}[t] \\ & x & \mapsto & t^n; \\ & y & \mapsto & t^m, \end{array}$$
    y razonar como en el ejercicio anterior).
18. Resolver el sistema de congruencias en $\mathbb{Z}_3[x]$ dado por
    $$\begin{cases} f(x) & \equiv & x & \big(\text{mod } x^2+x\big); \\ f(x) & \equiv & 1 & \big(\text{mod } x^2+1\big). \end{cases}$$