

UNIDAD 3: ANILLOS DE POLINOMIOS

En nuestra educación matemática se nos introdujo muy pronto -generalmente en los primeros años de secundaria- al estudio de los polinomios. Durante una temporada que parecía que no iba a tener fin, se nos obligaba, hasta el punto del aburrimiento insoportable, a factorizarlos, multiplicarlos, dividirlos y simplificarlos. La facilidad en factorizar un polinomio cuadrático, se interpretaba como una muestra de genuino talento matemático.

Posteriormente, en los primeros años de la educación superior, los polinomios hacen de nuevo su aparición en un marco algo distinto. Ahora son funciones, con sus valores, y nos preocupan su continuidad, sus derivadas, sus integrales y sus máximos y sus mínimos.

También aquí nos interesaremos en los polinomios, pero desde un punto de vista distinto de cualquiera de los dos que hemos enumerado. Para nosotros, los polinomios serán simplemente, elementos de un cierto anillo y lo que nos interesará serán las propiedades algebraicas de ese anillo.

Definiciones

Los conjuntos de polinomios con coeficientes en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o \mathbb{C} , que simbolizaremos mediante $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x]$ y $\mathbb{C}[x]$ respectivamente, son, con respecto a la suma y el producto habituales de polinomios, dominios de integridad conmutativos con unidad (Ejercicio).

En general, dado un anillo A , el conjunto $A[x]$ de **polinomios** a coeficientes en A se define como:

$$A[x] = \left\{ p(x) = \sum_{i=0}^n a_i x^i : a_i \in A, \forall i = 1, \dots, n \wedge n \in \mathbb{N} \right\}$$

El grado de un polinomio $p \in A[x]$ no nulo, que denotaremos $gr(p)$, se define como el mayor natural n tal que $a_n \neq 0$. Vale decir,

$$gr(p) = n \Rightarrow a_n \neq 0 \wedge a_{n+1} = a_{n+2} = \dots = 0$$

Un polinomio de grado n se llama **mónico** si $a_n = 1$.

En $A[x]$, la suma y el producto se definen de la siguiente manera.

Sean $p(x) = \sum_{i=0}^n a_i x^i$ y $q(x) = \sum_{j=0}^m b_j x^j$ dos elementos de $A[x]$ y, supongamos que $n = gr(p) \geq gr(q) = m$.

Entonces,

- la **suma** entre $p(x)$ y $q(x)$ es

$$p(x) + q(x) = \sum_{i=0}^m (a_i + b_i) x^i + \sum_{i=m+1}^n a_i x^i$$

- el **producto** entre $p(x)$ y $q(x)$ es

$$p(x)q(x) = \sum_{i=0}^{n+m} c_i x^i \text{ donde } c_i = \sum_{j=0, j \leq n, i-j \leq m}^i a_j b_{i-j}$$

Ejemplos

1. En $\mathbb{Z}[x]$, sean $p(x) = 3x^2 + x + 5$ y $q(x) = x^3 - x + 3$, es

- $p(x) + q(x) = x^3 + 3x^2 + 8$ (Ejercicio)
- $p(x)q(x) = 3x^5 + x^4 + 2x^3 + 8x^2 - 2x + 15$ (Ejercicio)

2. En $\mathbb{Z}_6[x]$, sean $p(x) = \bar{3}x^2 + x + \bar{5}$ y $q(x) = x^3 - x + \bar{3}$, es

- $p(x) + q(x) = x^3 + \bar{3}x^2 + \bar{2}$ (Ejercicio)
- $p(x)q(x) = \bar{3}x^5 + x^4 + \bar{2}x^3 + \bar{2}x^2 + \bar{4}x + \bar{3}$ (Ejercicio)

Proposición

Sea A un anillo conmutativo con identidad.

Con la suma y el producto, anteriormente definidos, el anillo de polinomios $(A[x], +, \cdot)$ es un anillo conmutativo y con identidad.

Dem.: Ejercicio

Proposición

Si A es un dominio de integridad, su anillo de polinomios $A[x]$ también es un dominio de integridad.

Dem.: Sean $p(x) = \sum_{i=0}^n a_i x^i$ y $q(x) = \sum_{i=0}^m b_i x^i$ en $A[x]$, con $a_n \neq 0$ y $b_m \neq 0$. Si $p(x)q(x) = \sum_{i=0}^{n+m} c_i x^i \Rightarrow c_{m+n} = a_n b_m \neq 0$, ya que A es un dominio de integridad.

$$\therefore p(x)q(x) \neq 0$$

Corolario

Si A es un dominio de integridad y p y q son dos polinomios no nulos, entonces

$$gr(pq) = gr(p) + gr(q)$$

Ejemplo

Si el anillo no es un dominio de integridad, el resultado del corolario anterior no es cierto (Ejercicio).

En general, si a es un divisor de cero y $b \neq 0$ es tal que $ab = 0$ o $ba = 0$, entonces:

$$\begin{aligned} (ax^n)(bx^m) &= 0 \\ (bx^n)(ax^m) &= 0 \end{aligned}$$

Corolario

Si A es un dominio de integridad, los elementos invertibles de $A[x]$ coinciden con los elementos invertibles de A .

Dem.: Llamemos $U(A[x])$ y $U(A)$ a los conjuntos formados por los elementos invertibles de $A[x]$ y A , respectivamente. Queremos ver que $U(A[x]) = U(A)$.

⊃) Puesto que A es un subanillo de $A[x]$, todo elemento invertible de A lo es, obviamente, de $A[x]$.

⊂) Sea $p(x) \in U(A[x]) \Rightarrow \exists q(x) \in U(A[x]) / p(x)q(x) = 1 \wedge 0 = gr(1) = gr(pq) = gr(p) + gr(q)$ pues A es dominio de integridad. Luego,

$$\begin{aligned} gr(p) = 0 &\Rightarrow p(x) = a \in A \\ gr(q) = 0 &\Rightarrow q(x) = b \in A \end{aligned}$$

Pero entonces $ab = 1 \wedge a \in U(A)$.

Ejemplos

1. $U(\mathbb{Z}[x]) = \{-1, 1\}$
2. $U(\mathbb{Q}[x]) = \mathbb{Q} - \{0\}$
3. Si F es cuerpo $\Rightarrow U(F[x]) = F - \{0\}$

Teorema

Sea C un cuerpo y $p(x), q(x) \in C[x]$ con $q \neq 0$. Entonces, existen $s(x), r(x) \in C[x]$ tales que $p(x) = s(x)q(x) + r(x)$ y $r(x) = 0$ o $gr(p) < gr(q)$.

Dem.:

Supongamos que $p(x) = \sum_{i=0}^m a_i x^i$ y $q(x) = \sum_{i=0}^n b_i x^i$.

- Si $gr(p) < gr(q)$, basta tomar $s(x) = 0$ y $r(x) = p(x)$.
- Si $gr(p) \geq gr(q)$ (vale decir, $m \geq n$), al ser C un cuerpo, b_n tiene un inverso multiplicativo, que escribiremos $\frac{1}{b_n}$; entonces

$$p(x) = \frac{a_m}{b_n} x^{m-n} q(x) + \left(p(x) - \frac{a_m}{b_n} x^{m-n} q(x) \right) = \frac{a_m}{b_n} x^{m-n} q(x) + \tilde{r}(x)$$

Ahora bien,

$$\tilde{r}(x) = \sum_{i=0}^m a_i x^i - \frac{a_m}{b_n} x^{m-n} \sum_{i=0}^n b_i x^i = a_m x^m - a_m x^m + a_{m-1} x^{m-1} + \dots = a_{m-1} x^{m-1} + \dots$$

y $gr(\tilde{r}) \leq m-1 < gr(p)$

- Si $\tilde{r} \equiv 0$ o $gr(\tilde{r}) < gr(q)$, el teorema está probado.
- Si $\tilde{r}(x) = c_p x^p + c_{p-1} x^{p-1} + \dots$, con $p \geq n$, escribimos

$$p(x) = \left(\frac{a_m}{b_n} x^{m-n} + \frac{c_p}{b_n} x^{p-n} \right) q(x) + \left(\tilde{r}(x) - \frac{c_p}{b_n} x^{p-n} q(x) \right) = \tilde{c}(x) q(x) + \tilde{\tilde{r}}(x)$$

con $gr(\tilde{\tilde{r}}) < gr(\tilde{r})$.

Este proceso nos permite llegar en, a lo sumo, $m-n+1$ pasos a la descomposición $p(x) = s(x)q(x) + r(x)$.

Ejemplos (Ejercicios)

1. ¿Cuál es la descomposición en $\mathbb{Q}[x]$ si $p(x) = x^4 - x^2 + 1$ y $q(x) = 2x^2 + 1$?
2. ¿Cuál es la descomposición en $\mathbb{Z}_7[x]$ si $p(x) = x^4 - x^2 + \bar{1}$ y $q(x) = \bar{2}x^2 + \bar{1}$?

Definiciones

Dado un polinomio $p(x)$ con coeficientes en un anillo A y un elemento a de A , $p(a)$ es el resultado de realizar en el anillo las operaciones que se obtienen sustituyendo x por a en el polinomio.

Dados dos polinomios $p(x)$ y $q(x)$ con coeficientes en un anillo A , diremos que $q(x)$ **divide a** $p(x)$ si $\exists c(x) \in A[x]/p(x) = c(x)q(x)$

Corolario

Sea C cuerpo; si $p(x) \in C[x]$ y $a \in C$, $x - a$ divide a $p(x)$ sii $p(a) = 0$.

Dem.: Ejercicio

Ejemplo

$x - \bar{3}$ divide a $p(x) = x^2 + x + \bar{1}$ en $\mathbb{Z}_{13}[x]$, pero $x - 3$ no divide a $p(x) = x^2 + x + 1$ en $\mathbb{Q}[x]$.

Definiciones

Dado un polinomio $p(x) \in A[x]$, $a \in A$ se dice **raíz** de p si $p(a) = 0$; por tanto, de acuerdo con el corolario anterior, en un cuerpo, a es una raíz de p sii $x - a$ divide a $p(x)$. Si $(x - a)^n$ divide a $p(x)$ pero $(x - a)^{n+1}$ no lo divide, se dice que la raíz a tiene **multiplicidad** n .

Ejemplo

1 es raíz simple de $x^2 - 1$ en $\mathbb{Q}[x]$, pero es raíz doble de $x^2 - 2x + 1$ en el mismo anillo.

Corolario

Sea C cuerpo, dado un polinomio $p(x) \in C[x]$ con $gr(p) = n \geq 1$, $p(x)$ tiene a lo sumo n raíces, contando cada raíz tantas veces como indica su multiplicidad.

Dem.: Ejercicio

Sug.: Realizar inducción sobre $n = gr(p)$.

Ejemplo (Ejercicio)

¿Qué sucede si C no es cuerpo?

Corolario

Sea C un cuerpo y $p(x)$ un polinomio de grado n en $C[x]$. Si existen m elementos distintos a_1, a_2, \dots, a_m de C tales que $p(a_i) = 0, \forall i = 1, 2, \dots, m$ y m es mayor que n , el polinomio $p(x)$ es el polinomio nulo.

Dem.: Ejercicio

Definiciones

Una consecuencia de que el polinomio 0 sea el neutro de $A[x]$ es que dos polinomios $p(x) = \sum_{i=0}^n a_i x^i$ y $q(x) = \sum_{i=0}^n b_i x^i$ son **iguales** sii $a_i = b_i, \forall i = 1, \dots, n$. Además, todo polinomio $p(x) = \sum_{i=0}^n a_i x^i$ de $A[x]$ define una

función polinómica $p : A \rightarrow A$ dada por $p(a) = \sum_{i=0}^n a_i a^i$.

Corolario

Sea $p(x) = \sum_{i=0}^n a_i x^i$ un polinomio con coeficientes en un cuerpo C , que posee n raíces r_1, \dots, r_n (contando raíces múltiples por separado). Entonces,

$$p(x) = a_n(x - r_1)\dots(x - r_n)$$

Dem.: Ejercicio

CRITERIOS DE IRREDUCIBILIDAD PARA POLINOMIOS

Uno de los conceptos más fructíferos cuando estudiamos, alguna vez, los números enteros fue el de número primo. En los anillos de polinomios también se puede definir un concepto análogo al de número primo en el anillo $(\mathbb{Z}, +, \cdot)$; en el caso de los anillos de polinomios, los elementos que satisfacen propiedades similares a las de los primos en \mathbb{Z} se llamarán irreducibles.

Todo número entero positivo puede descomponerse en un producto de números primos; éste es el *teorema fundamental de la aritmética*. Algo similar ocurre en algunos anillos de polinomios. Los elementos primos de un anillo de polinomios serán llamados polinomios irreducibles. En caso contrario diremos que el polinomio es reducible. En esta sección estudiaremos algunos criterios de irreducibilidad para polinomios en $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{C}[x]$; en algunos casos la reducibilidad o irreducibilidad de un polinomio puede estudiarse mirando sus raíces, por lo que también veremos cómo encontrar raíces de polinomios en algunos casos particulares.

Definiciones

Sea A un anillo conmutativo con identidad. Un polinomio $p(x) \in A[x]$ que no sea invertible en $A[x]$, se dice que es **irreducible** si para toda descomposición de la forma $p(x) = q(x)r(x)$ con $q(x), r(x) \in A[x]$, se tiene que o bien $gr(q) = 0$ o bien $gr(r) = 0$.

Un polinomio que no es irreducible, se dice **reducible**.

Ejemplos

$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ es irreducible en $\mathbb{Q}[x]$ pero no en $\mathbb{R}[x]$, y $x^2 + 1$ aún siendo irreducible en $\mathbb{Q}[x]$ y $\mathbb{R}[x]$, no lo es en $\mathbb{C}[x]$.

Observación

La irreducibilidad de un polinomio depende del anillo que se considere.

Proposición

Sea C cuerpo y $p(x) \in C[x]$ un polinomio de grado 2 o 3. $p(x)$ es reducible en $C[x]$ sii $p(x)$ tiene una raíz en C .

Dem.:

Si $p(x)$ tiene una raíz a en C , podemos escribir $p(x) = (x - a)q(x)$ y, por tanto, $p(x)$ es reducible.

Recíprocamente, si $p(x)$ es reducible, podemos escribir $p(x) = q(x)r(x)$ donde al menos uno de estos dos polinomios en los que se descompone $p(x)$ es de grado uno; como C es cuerpo, este polinomio de grado uno, tiene una raíz en C este polinomio de grado uno, tiene una raíz en C , y ésta es a su vez raíz de $p(x)$.

Ejemplos

1. El polinomio $p(x) = x^2 + x + 1$ no tiene raíces en \mathbb{Q} ; por tanto, es irreducible en $\mathbb{Q}[x]$.
2. El resultado anterior no es cierto para polinomios de grado superior a tres. Si tomamos $p(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2$, $p(x)$ no tiene raíces en \mathbb{Q} y sin embargo puede reducirse en $\mathbb{Q}[x]$.

Proposición

Sea $p(x) = \sum_{i=0}^n a_i x^i$ un polinomio con coeficientes en \mathbb{Z} . Si $\frac{a}{b}$ es una raíz de $p(x)$ con a y b primos entre sí, a debe ser divisor de a_0 y b debe ser divisor de a_n .

Dem.:

Si $\frac{a}{b}$ es una raíz de $p(x)$ se tiene

$$p\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \dots + a_1 \left(\frac{a}{b}\right) + a_0 = 0$$

Multiplicando por b^n , obtenemos

$$a_n a^n + a_{n-1} a^{n-1} b + \dots + a_1 a b^{n-1} = -a_0 b^n$$

Como a es común a todos los términos de la parte izquierda de esta igualdad, sacando factor común se deduce que a divide a $a_0 b^n$; como a y b son primos entre sí, a no puede dividir a b^n y por tanto debe ser un divisor de a_0 .

La igualdad anterior también puede escribirse de la forma

$$a_n a^n = -a_{n-1} a^{n-1} b - \dots - a_1 a b^{n-1} - a_0 b^n$$

Ejercicio: Completar la prueba para este caso.

Ejemplo

$x^2 + 1$ no tiene raíces en \mathbb{Q} ya que si las tuviera, tendrían que ser -1 o 1 .

Teorema Fundamental del Álgebra (Gauss)

Todo polinomio $p(x)$ no constante con coeficientes complejos tiene al menos una raíz en \mathbb{C} .

Dem.: No la haremos pues, si bien pueden darse varias demostraciones de este teorema, la más sencilla hace uso de la teoría de funciones de variable compleja.

Corolario

Un polinomio de $\mathbb{C}[x]$ es irreducible sii es de grado 1.

Dem.: Ejercicio

Proposición

Si $r = a + bi$ es una raíz compleja de $p(x) \in \mathbb{R}[x]$, su conjugada, $\bar{r} = a - bi$ también lo es.

Dem.: Ejercicio

Corolario

Si $p(x) \in \mathbb{R}[x]$ es irreducible en $\mathbb{R}[x]$, su grado es 1 ó 2. Además, si el grado es 2 y p es irreducible, $p(x) = ax^2 + bx + c$, con $b^2 - 4ac < 0$.

Dem.:

Los polinomios de grado 0 no nulos son invertibles en $\mathbb{R}[x]$. Todo polinomio de grado 1 es obviamente irreducible. Si $p(x) = ax^2 + bx + c$ es irreducible, no puede tener raíces reales y, por tanto, el discriminante de la ecuación $ax^2 + bx + c = 0$, que es $b^2 - 4ac$, debe ser negativo. Si $gr(p) \geq 3$, sea $r \in \mathbb{C}$ una raíz de p ; si $r \in \mathbb{R}$, $x - r$ divide a $p(x) \in \mathbb{R}[x]$ y $p(x)$ no es irreducible; si $r = a + bi \notin \mathbb{R}$, $\bar{r} = a - bi$ es también una raíz de $p(x)$, y en $\mathbb{C}[x]$, se tiene

$$p(x) = (x - (a - bi))(x - (a + bi))q(x) = ((x - a) - bi)((x - a) + bi)q(x) = (x^2 - 2ax + a^2 + b^2)q(x)$$

por tanto q ha de pertenecer a $\mathbb{R}[x]$, $gr(q) \geq 1$ y $p(x)$ no es irreducible.

Ejemplos

- $x^2 - 4x + 5$ es irreducible sobre $\mathbb{R}[x]$ (Verificarlo).
- $x^4 + 3x^3 + 4x^2 + x - 3$ es reducible en $\mathbb{Z}[x]$ (Verificarlo).

Definiciones

El **contenido** de un polinomio $p(x) = \sum_{i=0}^n a_i x^i$ se define como

$$C(p) = \text{mcd}(a_n, \dots, a_1, a_0)$$

El polinomio se dice **primitivo** si su contenido, $C(p)$, es 1.

Ejemplos

$2x^2 + 4x + 5$ y $x^3 + 7$ son primitivos, mientras que $2x^2 + 4x + 6$ no lo es.

Lema de Gauss

Si $p(x)$ y $q(x)$ son dos polinomios primitivos en $\mathbb{Z}[x]$, entonces $p(x)q(x)$ también lo es.

Dem.: No la haremos.

Proposición

Sean $p(x)$ y $q(x)$ dos polinomios en $\mathbb{Z}[x]$ y $p(x)$ primitivo. Si $p(x)$ divide a $q(x)$ en $\mathbb{Q}[x]$, $p(x)$ divide a $q(x)$ en $\mathbb{Z}[x]$.

Dem.: Como $p(x)|q(x)$ en $\mathbb{Q}[x]$, existe $a(x) \in \mathbb{Q}[x]$ tal que $q(x) = p(x)a(x)$, y escribiendo dicho polinomio $a(x)$ como $a(x) = (\frac{1}{b})\tilde{a}(x)$ con $\tilde{a}(x) \in \mathbb{Z}[x]$ se sigue que $bq(x) = p(x)\tilde{a}(x)$.

Tomando contenidos, tendríamos, $C(bq) = C(p\tilde{a}) = C(p)C(\tilde{a})$; es decir, $bC(q) = C(\tilde{a})$ (*¿Por qué?*). En estas condiciones se obtiene que $b|C(\tilde{a})$, lo que implica que $a(x) = (\frac{1}{b})\tilde{a}(x)$ ya pertenecía, de entrada, a $\mathbb{Z}[x]$. Por lo tanto, la factorización $q(x) = p(x)a(x)$ es también una factorización en $\mathbb{Z}[x]$.

Teorema

Sea $p(x)$ un polinomio primitivo en $\mathbb{Z}[x]$, entonces $p(x)$ es irreducible en $\mathbb{Q}[x]$ sii es irreducible en $\mathbb{Z}[x]$.

Dem.:

\Rightarrow) Si $p(x)$ fuera reducible en $\mathbb{Z}[x]$, se tendría $p(x) = q(x)r(x)$ con $q(x)$ y $r(x)$ polinomios con coeficientes enteros y ninguno de ellos una unidad; por tanto, $1 = C(q)C(r)$, ya que $p(x)$ es primitivo, de donde se deduce que $C(q) = C(r) = 1$; esto implica que el grado de $q(x)$ y $r(x)$ es mayor o igual que 1, ya que ninguno de los dos es una unidad en $\mathbb{Z}[x]$. Así pues, $p(x) = q(x)r(x)$ es una factorización de p en $\mathbb{Q}[x]$ donde ni $q(x)$ ni $r(x)$ son invertibles en $\mathbb{Q}[x]$, ya que tienen grado superior a 1, y $p(x)$ también sería reducible en $\mathbb{Q}[x]$.

\Leftarrow) Recíprocamente, si $p(x) = q(x)r(x)$ fuera una factorización de $p(x)$ en $\mathbb{Q}[x]$, con factores que no son unidades, podemos escribir $q(x) = (\frac{a}{b})\tilde{q}(x)$, con $\tilde{q}(x) \in \mathbb{Z}[x]$ y primitivo. Pero entonces, $\tilde{q}(x)|p(x)$ en $\mathbb{Q}[x]$ y, por la proposición anterior, $\tilde{q}(x)|p(x)$ en $\mathbb{Z}[x]$; esto es, $p(x)$ también sería reducible en $\mathbb{Z}[x]$.

Proposición (Criterio de irreducibilidad de Eisenstein)

Sea $p(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ un polinomio primitivo con coeficientes enteros tal que existe un entero primo p que divide a a_i , $i = 0, 1, \dots, n-1$, pero que no divide a A_0 y p^2 no divide a a_0 ; entonces p es irreducible en $\mathbb{Z}[x]$.

Dem.: No la haremos.

Ejemplos

1. El polinomio $x^4 - 3x^2 + 6x + 3$ es irreducible en $\mathbb{Z}[x]$ ya que puede aplicarse el criterio de Eisenstein con $p = 3$; como es primitivo, es también irreducible en $\mathbb{Q}[x]$.
2. El criterio de Eisenstein proporciona únicamente una condición suficiente de irreducibilidad, pero no necesaria (*Analizar el polinomio $x^2 + 4$*).
3. Si p es un entero positivo primo, los polinomios $x^n + p$ son irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ para cualquier exponente natural n . Así pues, al contrario de lo que ocurre en $\mathbb{C}[x]$ y $\mathbb{R}[x]$, es posible encontrar en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ polinomios irreducibles de cualquier grado.

FIN

Bibliografía

- DORRONSORO, J. y HERNÁNDEZ, E. *Números, grupos y anillos*. Madrid, España: Ed. Addison-Wesley Iberoamericana España, S.A., 1996.
- HERSTEIN, I.N. *Álgebra moderna*. México: Editorial F. Trillas, 1970.

PRÁCTICA 3: Anillos de polinomios

1. Encontrar las raíces racionales de:
 - (a) $3x^3 - 7x - 5 = 0$
 - (b) $2x^3 - 3x + 1 = 0$
2. Probar que $30x^n = 91$ no tiene raíces racionales para ningún $n > 1$.
3. Estudiar la irreducibilidad de $x^2 + \bar{1}$ y $x^3 + x + \bar{2}$ en $\mathbb{Z}_3[x]$ y en $\mathbb{Z}_5[x]$.
4. Encontrar todos los polinomios cuadráticos mónicos con coeficientes en \mathbb{Z}_3 .
5. Descomponer $x^4 - 5x^2 + 6$ sobre $\mathbb{Q}[x]$ y sobre $\mathbb{R}[x]$.
6. Descomponer $x^6 - 1$ sobre $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}[x]$ y $\mathbb{Z}_7[x]$.
7. Descomponer $x^8 - 1$ sobre $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $[x]$ y sobre $\mathbb{Z}_5[x]$.
8. Estudiar la irreducibilidad en $\mathbb{Q}[x]$ de los siguientes polinomios:
 - (a) $x^3 + 2x^2 + 4x + 2$
 - (b) $x^4 + 3x^3 + 4x^2 + 6x + 4$
 - (c) $x^3 + 6x^2 + 5x + 25$
 - (d) $x^3 + 6x^2 + 11x + 8$
 - (e) $2x^4 - 8x^2 + 1$
 - (f) $x^4 - 2x^2 + 8x + 1$
 - (g) $x^4 + 2x^2 - x + 2$