3.5. Anillos de polinomios. Ideales maximales en $\mathbb{K}[x]$

Dado el anillo $(R,+,\cdot)$ un **polinomio sobre** R es una sucesión infinita de elementos de R, indexados con enteros no negativos, con la propiedad de que existe un entero $n \geq 0$ tal que $a_i = 0$ para todo $i > n$, $\quad (a_0, a_1, a_2, ..., a_n, 0_R, 0_R, ...) \overset{\text{notación}}{=} a_0 + a_1 x + a_2 x^2 + ... + a_n x^n = \sum_{i=0}^{n} a_i x^i$

- Si $f = \sum_{k=0}^{n} a_k x^k$ los elementos $a_0, a_1, ..., a_n \in R$ reciben el nombre de **coeficientes** de f.
  Se llama **polinomio nulo** o **cero** al polinomio cuyos coeficientes son todos iguales a $0_R \in R$.

- Si f es un polinomio no nulo, se llama **grado de** f al mayor entero no negativo $n \in \mathbb{N} \cup \{0\}$ para el cual $a_n \neq 0_R$ y se escribe $\text{gr}(f) = n$. El **grado del polinomio nulo** se dice que es $-\infty$. Si $\text{gr}(f) \leq 0$ se dice que f es un **polinomio constante**.

- Si $\text{gr}(f) = n \geq 0$, al coeficiente a_n se le llama **coeficiente principal** y se escribe $\text{cp}(f) = a_n$. En un anillo con identidad $1_R \in R$, un polinomio no nulo $f \in R[x] - \{0_{R[x]}\}$ se dice que es un **polinomio mónico** si su coeficiente principal es $\text{cp}(f) = 1_R$

- **Anillo de polinomios**: El conjunto de todos los **polinomios con coeficientes en** $(R,+,\cdot)$ se nota por $R[x]$. En $R[x]$ se definen las operaciones de **suma** y **producto** del siguiente modo:
  $\forall \quad f = \sum_{k=0}^{r} a_k x^k, \quad g = \sum_{k=0}^{s} b_k x^k \in R[x], \quad f+g = \sum_{k=0}^{max\{r,s\}} (a_k + b_k) x^k, \quad f \cdot g = \sum_{k=0}^{r+s} \left(\sum_{i+j=k} a_i b_j \right) x^k.$
  Si $(R,+,\cdot)$ es anillo conmutativo con identidad entonces $(R[x],+,\cdot)$ es anillo conmutativo con identidad $1_{R[x]} = (1_R, 0_R, ...) \in R[x]$. Su cero es el polinomio nulo: $0_{R[x]} = (0_R, 0_R, ...) \in R[x]$.
  $(R[x],+,\cdot)$ contiene un subanillo isomorfo a $(R,+,\cdot)$.

- **Función polinomial**: Sea $(R,+,\cdot)$ un anillo. Para cada polinomio $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ se llama función polinomial f a la aplicación $f : R \to R$, definida para $r \in R$ por $f(r) = \sum_{k=0}^{n} a_k \, r^k \in R$.
  Se dice que $\alpha \in R$ es una **raíz** de $f \in R[x]$ si verifica que $f(\alpha) = 0_R \in R$

Polinomios irreducibles sobre un dominio de integridad

Sea $(D,+,\cdot)$ un dominio de integridad. Un polinomio $f \in D[x]$, con $\text{gr}(f) \geq 0$, se dice que es **irreducible en** $D[x]$ si f no es unidad y siempre que se exprese como $f = g \cdot h$ con $g, h \in D[x]$ se verifica que uno de los polinomios g, h es unidad de $D[x]$.

Polinomios irreducibles sobre un cuerpo

Si $(\mathbb{K},+,\cdot)$ es un cuerpo, un polinomio $f \in \mathbb{K}[x]$, con $\text{gr}(f) = n > 0$, es **irreducible en** $\mathbb{K}[x]$ si no puede ser expresado como producto de polinomios de grado estrictamente menor que $\text{gr}(f) = n$.

Ideales en $\mathbb{K}[x]$

1. Sea $(\mathbb{K},+,\cdot)$ un cuerpo $\Rightarrow$ todo ideal en $(\mathbb{K}[x],+,\cdot)$ es un ideal principal.
2. Sea $(\mathbb{K},+,\cdot)$ un cuerpo y $f \in \mathbb{K}[x]$. El ideal (f) es maximal en $\mathbb{K}[x] \Leftrightarrow f$ es irreducible en $\mathbb{K}[x]$.

Resultados sobre raíces

Sea $(\mathbb{K}, +, \cdot)$ un cuerpo y $f \in \mathbb{K}[x]$ con $\text{gr}(f) = n > 0$.

1. **Teorema del resto**: Si $\alpha \in \mathbb{K}$ entonces $f(\alpha)$ es el resto obtenido al dividir f entre $x - \alpha$
2. **Teorema del factor**: $\alpha \in \mathbb{K}$ es raíz de f si y sólo si $(x - \alpha)$ divide a f en $\mathbb{K}[x]$.
3. f puede tener a lo sumo n raíces en $\mathbb{K}$

Resultados sobre polinomios irreducibles en $\mathbb{C}[x]$ y en $\mathbb{R}[x]$

1. Un polinomio $f \in \mathbb{C}[x]$ es irreducible en $\mathbb{C}[x] \Leftrightarrow \text{gr}(f) = 1$
2. Un polinomio $f \in \mathbb{R}[x]$ es irreducible en $\mathbb{R}[x] \Leftrightarrow \text{gr}(f) = 1$ o bien es $f = a_0 + a_1 x + a_2 x^2$, tal que $a_1^2 - 4a_2 a_0 < 0$

Lema de Gauss

Sean $f \in \mathbb{Z}[x]$ y $\alpha, \beta \in \mathbb{Q}[x]$ tales que $f = \alpha \cdot \beta$ con $\text{gr}(\alpha) < \text{gr}(f)$ y $\text{gr}(\beta) < \text{gr}(f)$, entonces existen polinomios $a, b \in \mathbb{Z}[x]$ verificando que $f = a \cdot b$ con $\text{gr}(a) = \text{gr}(\alpha) < \text{gr}(f)$ y $\text{gr}(b) = \text{gr}(\beta) < \text{gr}(f)$.

Criterio de raíces racionales

Si $\frac{r}{s} \in \mathbb{Q}$, con $\text{mcd}(r, s) = 1$, es una raíz racional de
$f = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, polinomio de grado $n \geq 1$ y con $a_0 \neq 0 \Rightarrow r | a_0$ y $s | a_n$.

Criterio de Eisenstein

Sea $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ con $\text{mcd}(a_0, \cdots, a_n) = 1$ y tal que existe un número primo $p \in \mathbb{Z}$ verificando que $p | a_i$ para todo $i \in \{0, 1, ..., n-1\}$, $p \nmid a_n$ y $p^2 \nmid a_0$ entonces f es irreducible en $\mathbb{Q}[x]$.

Criterio de reducción módulo primo

Sea $f = a_0 + ... + a_n x^n \in \mathbb{Z}[x]$ con $\text{gr}(f) = n \geq 2$. Si existe p primo tal que $[f]_p = [a_0]_p + ... + [a_n]_p \, x^n \in \mathbb{Z}_p[x]$ tiene grado n y es irreducible en $\mathbb{Z}_p[x]$ entonces f es irreducible en $\mathbb{Q}[x]$.

3.5.31 Problemas

1. Encontrar todas las unidades de los siguientes anillos: *a)* $(\mathbb{Z}[x],+,\cdot)$ *b)* $(\mathbb{R}[x],+,\cdot)$ *c)* $(\mathbb{Z}_{11}[x],+_{11},\cdot_{11})$
2. Estudiar si en el anillo $(\mathbb{Z}_4[x],+_4,\cdot_4)$, el polinomio $f=2x+1$ es una unidad.
3. ¿Es válido el algoritmo de la división en $(\mathbb{Z}[x],+,\cdot)$?
4. Calcular $d=\text{mcd}(f,g)$ y polinomios λ y μ tales que $d=\lambda f+\mu g$ en los siguientes casos:
   a) En $(\mathbb{Q}[x],+,\cdot)$: $f=x^4-x^3+x-1$, $g=x^3+x-2$
   b) En $(\mathbb{Z}_2[x],+_2,\cdot_2)$:
   $f_1=x^4+1$, $g_1=x^2+1$; $f_2=x^5+1$, $g_2=x^2+1$; $f_3=x^9+1$, $g_3=x^6+1$
   c) En $(\mathbb{Z}_3[x],+_3,\cdot_3)$: $f_1=x^3+x^2+x+1$, $g_1=x^2+2$; $f_2=x^5+x^2+2x$, $g_2=x^4+x$
   d) En $(\mathbb{Z}_5[x],+_5,\cdot_5)$: $f_1=x^4+2x^3+x^2+4x+2$, $g_1=x^2+3x+1$; $f_2=x^5+x^4+2x^3+x^2+4x+2$, $g_2=x^2+2x+3$
   e) En $(\mathbb{Z}_7[x],+_7,\cdot_7)$: $f=x^4+2x^3+2x^2+2x+1$ y $g=x^3-x^2+x-1$
5. Estudiar si la siguiente igualdad es verdadera o falsa en $\mathbb{Z}_{15}[x]$
$$(x+1)(x+14)=(x+4)(x+11)$$
6. En $(\mathbb{Z}[x],+,\cdot)$ sea $I=\{p\in\mathbb{Z}[x]:p(0)=0\}$. Demostrar que I no es un ideal maximal.
7. Encontrar el resto que resulta al dividir $f=x^{100}+x^{90}+x^{80}+x^{50}+1$ entre $g=x-1$ en $\mathbb{Z}_2[x]$
8. Encontrar las raíces
   a) $x^2-5x+6\in\mathbb{Z}[x]$, *b)* $x^2-5x+6\in\mathbb{Z}_{12}[x]$, *c)* $3x^3-4x^2-x+4\in\mathbb{Z}_5[x]$,
   d) $x^3+x+1\in\mathbb{Z}_2[x]$, *e)* $x^2-x+2\in\mathbb{Z}_3[i][x]$, *f)* $x^4-16\in\mathbb{Q}[x]$, *g)* $x^4-16\in\mathbb{C}[x]$
9. Determinar si son irreducibles en $\mathbb{Q}[x]$
   a) $x^5+9x^4+12x^2+6$, *b)* x^4+x+1, *c)* x^4+3x^2+3,
   d) x^5+5x^2+1, *e)* x^2+3x-1, *f)* $\frac{5}{2}x^5+\frac{9}{2}x^4+15x^3+\frac{3}{7}x^2+6x+\frac{3}{14}$
10. Expresar el polinomio como producto de polinomios irreducibles en el anillo indicado en cada caso:
    a) $x^2+1\in\mathbb{Z}_5[x]$, *b)* $x^3+5x^2+5\in\mathbb{Z}_{11}[x]$, *c)* $x^2+x+1\in\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_7[x]$
    d) x^4+x^3+1, $x^3+x^2+x+1\in\mathbb{Z}_2[x]$, *e)* x^3+6, $3x^2+x+4\in\mathbb{Z}_7[x]$
11. Encontrar en cada caso, si fuera posible, un polinomio irreducible $p\in\mathbb{K}[x]$ con el grado indicado
    a) $p\in\mathbb{Q}[x]$ con $\text{gr}(p)=3$
    b) $p\in\mathbb{R}[x]$ con $\text{gr}(p)=4$
    c) $p\in\mathbb{Z}_3[x]$ con $\text{gr}(p)=2$