Álgebra Lineal y Estructuras Matemáticas

J. C. Rosales y P. A. García Sánchez

Departamento de Álgebra, Universidad de Granada

Capítulo 3

El anillo de los polinomios sobre un cuerpo

1. Divisibilidad

Un anillo es una terna $(R, +, \cdot)$, donde R es un conjunto, y $+$ y $\cdot$ son dos operaciones verificando:

1) la operación $+$ es asociativa, conmutativa, tiene elemento neutro, y todo elemento tiene inverso (lo que hace de $(R, +)$ un grupo abeliano),
2) la operación $\cdot$ es asociativa, tiene elemento neutro, y verifica la propiedad distributiva.

Diremos que el anillo R es conmutativo si además $\cdot$ cumple la propiedad conmutativa.

Un cuerpo es un anillo conmutativo en el que todo elemento distinto de cero (el elemento neutro de $+$) tiene inverso para $\cdot$.

Ejercicio 28: Da algunos ejemplos de cuerpos.

- $(\mathbb{Z}_m, +, \cdot)$ es un cuerpo si y sólo si m es primo.

Sea K un cuerpo. El conjunto de polinomios con coeficientes en K en la indeterminada x es

$$K[x] = \{a_0 + a_1x + \cdots + a_nx^n \text{ tales que } n \in \mathbb{N}, a_0, \ldots, a_n \in K\}.$$

- $K[x]$ es un anillo conmutativo con las operaciones usuales de suma y producto de polinomios.

Dado $a(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, con $a_n \neq 0$, decimos que n es el grado de $a(x)$, y lo notaremos por $\mathrm{gr}(a(x))$ ($\mathrm{gr}(0) = -\infty$). A a_n se le llama coeficiente líder de $a(x)$, y a a_nx^n término líder de $a(x)$.

- El grado del producto de dos polinomios es la suma de los grados.

Un elemento a de un anillo conmutativo R es una unidad si existe $b \in R$ de forma que $a \cdot b = 1$ (donde 1 es el elemento neutro de $\cdot$).

- El conjunto de las unidades de $K[x]$ es $K \setminus \{0\}$.

Sean $a(x), b(x) \in K[x]$. Decimos que $a(x)$ divide a $b(x)$, y lo denotamos por $a(x) \mid b(x)$, si existe $c(x) \in K[x]$ tal que $b(x) = a(x)c(x)$.

Un elemento $a(x) \in K[x]$ es irreducible si

1) $a(x) \neq 0$,
2) $a(x)$ no es una unidad de $K[x]$ (no es un polinomio constante),
3) si $a(x) = b(x)c(x)$, con $b(x), c(x) \in K[x]$, entonces $b(x)$ o $c(x)$ es una unidad de $K[x]$.

Ejercicio 29: Estudia la irreducibilidad de $x^2 + x \in \mathbb{Z}_3[x]$ y de $x^3 + x + 1 \in \mathbb{Z}_2[x]$.

Ejercicio 30: Demuestra que en $K[x]$ todo polinomio de grado uno es irreducible.

Un polinomio $a(x) \in K[x]$ es mónico si el coeficiente del término de mayor grado vale 1.

Teorema de factorización única de polinomios. Todo polinomio $a(x) \in K[x] \setminus K$ se puede expresar de forma única (salvo reordenación de los factores) como $a(x) = up_1(x)^{\alpha_1} \cdots p_r(x)^{\alpha_r}$, donde $u \in K \setminus \{0\}$, $\alpha_1, \ldots, \alpha_r \in \mathbb{N} \setminus \{0\}$ y $p_1(x), \ldots, p_r(x)$ son polinomios mónicos e irreducibles de $K[x]$.

A esa expresión la llamaremos la descomposición en irreducibles de $a(x)$.

Sean $a(x), b(x) \in K[x]$, con $a(x) \neq 0$ o $b(x) \neq 0$. Un polinomio $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$ si

1) $d(x) \mid a(x)$ y $d(x) \mid b(x)$,
2) si $c(x) \mid a(x)$ y $c(x) \mid b(x)$, con $c(x)$ otro polinomio, entonces $c(x) \mid d(x)$.

Análogamente, un polinomio $m(x)$ es un mínimo común múltiplo de $a(x)$ y $b(x)$ si

1) $a(x) \mid m(x)$ y $b(x) \mid m(x)$,
2) si $a(x) \mid c(x)$ y $b(x) \mid c(x)$, con $c(x)$ otro polinomio, entonces $m(x) \mid c(x)$.

De forma similar se puede definir el máximo común divisor y el mínimo común múltiplo de un conjunto de polinomios $\{a_1(x), \ldots, a_n(x)\}$ con n un entero positivo.

- Si $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$, también lo es $kd(x)$ para todo $k \in K \setminus \{0\}$, y éstos son los únicos máximos divisores comunes de $a(x)$ y $b(x)$. Lo mismo ocurre con el mínimo común múltiplo. Esto se debe a que si $a(x) \mid b(x)$, entonces $ka(x) \mid b(x)$ para cualquier $k \in K \setminus \{0\}$. Cuando escribamos $\gcd\{a(x), b(x)\}$ nos referiremos al máximo común divisor de $a(x)$ y $b(x)$ que sea mónico. Para el mínimo común múltiplo utilizaremos $\operatorname{lcm}\{a(x), b(x)\}$.
- Sean $a(x) = up_1(x)^{\alpha_1} \cdots p_r(x)^{\alpha_r}$ y $b(x) = vp_1(x)^{\beta_1} \cdots p_r(x)^{\beta_r}$, con $u, v \in K \setminus \{0\}$, $p_1(x), \ldots, p_r(x)$ polinomios mónicos e irreducibles, y $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$ enteros no negativos (algunos pueden ser cero, pues los factores que aparecen en $a(x)$ no tienen por qué aparecer en $b(x)$). Entonces

$$\gcd\{a(x), b(x)\} = p_1(x)^{\min\{\alpha_1, \beta_1\}} \cdots p_r(x)^{\min\{\alpha_r, \beta_r\}},$$

$$\operatorname{lcm}\{a(x), b(x)\} = p_1(x)^{\max\{\alpha_1, \beta_1\}} \cdots p_r(x)^{\max\{\alpha_r, \beta_r\}}.$$

- $\gcd\{a, b\}\operatorname{lcm}\{a, b\} = uab$, con $u \in K[x] \setminus \{0\}$.

Ejercicio 31: Calcula el máximo común divisor y el mínimo común múltiplo en $\mathbb{Z}_5[x]$ de $(x+1)(2x+3)$ y $(x+2)(4x+1)$.

Propiedad de la división. Dados $a(x), b(x) \in K[x]$, con $b(x) \neq 0$, existen $q(x), r(x) \in K[x]$ únicos de forma que $a(x) = q(x)b(x) + r(x)$ y $\operatorname{gr}(r(x)) < \operatorname{gr}(b(x))$.

A $q(x)$ y $r(x)$ los llamaremos respectivamente cociente y resto de dividir $a(x)$ entre $b(x)$, y los denotaremos por $a(x)$ div $b(x)$ y $a(x)$ mód $b(x)$.

Ejercicio 32: Calcula el cociente y el resto de dividir $3x^3 + 4x^2 + 2x + 3$ entre $2x^2 + x + 2$ en $\mathbb{Z}_5[x]$.

Algoritmo de Euclides para polinomios.
Entrada: $a(x), b(x) \in K[x] \setminus \{0\}$.
Salida: $\gcd\{a(x), b(x)\}$.

$(a_0(x), a_1(x)) := (a(x), b(x))$.
Mientras $a_1(x) \neq 0$
    $(a_0(x), a_1(x)) := (a_1(x), a_0(x)$ mód $a_1(x))$.
Devuelve $a_0(x)$ multiplicado por el inverso de su coeficiente líder.

Ejercicio 33: Calcula el máximo común divisor de los polinomios x^4+x+1 y x^2+2x+3 en $\mathbb{Z}_5[x]$.

Sea $a(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$. Un elemento $\alpha \in K[x]$ es una raíz de $a(x)$ si $a(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

Teorema del factor. Sea $a(x) \in K[x]$ y $\alpha \in K$. Entonces α es una raíz de $a(x)$ si y sólo si $x - \alpha \mid a(x)$.

- Un polinomio $a(x)$ es un múltiplo de un polinomio de grado uno si y sólo si $a(x)$ tiene una raíz en K.

Ejercicio 34: Calcula todos los polinomios irreducibles de grado 2 de $\mathbb{Z}_3[x]$.

Ejercicio 35: Determina la reducibilidad o irreducibilidad de los siguientes polinomios en $\mathbb{Z}_3[x]$: x^4+x+2, x^3+x+1, x^2+1, x^4+x^2+2.

Teorema del resto. Sea $a(x) \in K[x]$ y $\alpha \in K$. Entonces $a(x)$ mód $(x-\alpha) = a(\alpha)$.

Ejercicio 36: Calcula en $\mathbb{Z}_5[x]$ el resto de dividir $x^{1000}+1$ entre $x+3$.

Si α es una raíz de $a(x) \in K[x]$, entonces aplicando reiteradamente el teorema del factor, tenemos que $a(x) = (x-\alpha)^m b(x)$, con $m \in \mathbb{N} \setminus \{0\}$ y $b(\alpha) \neq 0$. El número natural m es la multiplicidad de la raíz α en $a(x)$. Si $m = 1$, decimos que α es una raíz simple. Si $m \geq 2$, entonces es una raíz múltiple.

Ejercicio 37: Calcula las raíces (y sus multiplicidades) del polinomio $x^3+2x+3 \in \mathbb{Z}_5[x]$.

- Si $a(x) \in K[x] \setminus \{0\}$, entonces la suma de las multiplicidades de las raíces de $a(x)$ es menor o igual que $\mathrm{gr}(a(x))$.

Caracterización de las raíces múltiples. Si α es una raíz de $a(x) \in K[x]$. Entonces α es una raíz múltiple si y sólo si α es también raíz de $a'(x)$, la derivada de $a(x)$.

Ejercicio 38: Demuestra que el polinomio $x^{70}-1 \in \mathbb{R}[x]$ no tiene raíces múltiples.

Maxima 20: `maxima` no factoriza en polinomios mónicos. El comando `factor` muestra una descomposición en irreducibles.

```
(%i1) factor(3*x^3-2*x+1);
```

$$(\%o1) \qquad (x+1)\left(3x^2-3x+1\right)$$

```
(%i2) gcd(3*x^3+3,x^2-1);
```

$$(\%o2) \qquad x+1$$

```
(%i3) (x-1)^2*(x+1);
```

$$(\%o3) \qquad (x-1)^2\,(x+1)$$

```
(%i4) expand(%);
```

$$(\%o4) \qquad x^3-x^2-x+1$$

```
(%i5) gcd(%,diff(%,x));
```

$$(\%o5) \qquad x-1$$

```
(%i6) quotient(x^3+1,x-3);
```

```
(%o6)                                  x^2+3*x+9
(%i7) remainder(x^3+1,x-3);
(%o7)                                     28
(%i8) expand((x^2+3*x+9)*(x-3)+28);
(%o8)                                  x^3+1
```

Maxima 21: Calculemos las raices y sus multiplicidades del polinomio $x^6+3x^5+6x^3+2x^2+6x+3$ con coeficientes en $\mathbb{Z}_7$.

```
(%i1) modulus:7$
(%i2) p:x^6+3*x^5+6*x^3+2*x^2+6*x+3$
(%i3) gcd(p,diff(p,x));
(%o3)                                x^3+2*x^2+x+3
(%i4) factor(%);
(%o4)                              (x-2)^2 (x-1)
(%i5) factor(p);
(%o5)                            (x-3) (x-2)^3 (x-1)^2
```

Consequencia Si $a(x) \in K[x] \setminus \{0\}$, entonces las raíces múltiples de $a(x)$ son las raíces de $\gcd\{a(x), a'(x)\}$.

Ejercicio 39: Calcula las raíces múltiples del polinomio $x^3 - 3x + 2 \in \mathbb{R}[x]$.

2. Cuerpos finitos

Sea $m(x) \in K[x] \setminus \{0\}$. Denotamos por

$$K[x]_{m(x)} = \{a(x) \in K[x] \text{ tales que } \operatorname{gr}(a(x)) < \operatorname{gr}(m(x))\},$$

que es el conjunto de los restos posibles de dividir por $m(x)$. Este conjunto es un anillo con las siguientes operaciones.

$$a(x) \oplus b(x) := (a(x) + b(x)) \text{ mód } m(x),$$

$$a(x) \otimes b(x) := (a(x)b(x)) \text{ mód } m(x).$$

- $a(x)$ es una unidad de $K[x]_{m(x)}$ si y sólo si $\gcd\{a(x), m(x)\} = 1$. Por tanto $K[x]_{m(x)}$ es un cuerpo si y sólo si $m(x)$ es irreducible.
- $\mathbb{Z}_p[x]_{m(x)}$, con p un entero primo, tiene cardinal $p^{\operatorname{gr}(m(x))}$.

Ejercicio 40: Encuentra un cuerpo con 8 elementos.

- Si $a(x)s(x) + m(x)t(x) = 1$, entonces $s(x)$ mód $m(x)$ es el inverso para el producto de $a(x)$ en $K[x]_{m(x)}$.

Algoritmo extendido de Euclides.
Entrada: $a(x), b(x) \in K[x] \setminus \{0\}$.
Salida: $s(x), t(x), d(x) \in K[x]$ tales que $d(x) = \gcd\{a(x), b(x)\}$ y $a(x)s(x) + b(x)t(x) = d(x)$.

$(a_0(x), a_1(x)) := (a(x), b(x))$.
$(s_0(x), s_1(x)) := (1, 0)$.
$(t_0(x), t_1(x)) := (0, 1)$.
Mientras $a_1(x) \neq 0$
  $q(x) := a_0(x)$ div $a_1(x)$.
  $(a_0(x), a_1(x)) := (a_1(x), a_0(x) - a_1(x)q(x))$.
  $(s_0(x), s_1(x)) := (s_1(x), s_0(x) - s_1(x)q(x))$.
  $(t_0(x), t_1(x)) := (t_1(x), t_0(x) - t_1(x)q(x))$.
$d(x) := a_0(x)$, $s(x) := s_0(x)$, $t(x) := t_0(x)$.
Devuelve $s(x), t(x), d(x)$.

Maxima 22: Veamos si tiene solución la ecuación

$$(6x^3 + 6)X + (4x^2 - 4)Y = x^2 + 2x + 1$$

en el anillo de polinomios con coeficientes racionales y con incógnita x.

```
(%i1) gcdex(6*x^3+6,4*x^2-4);
```

$$(\%o1) \qquad [1, -\frac{3x}{2}, 6x + 6]$$

Como no nos ha devuelto un máximo común divisor mónico, dividimos por su coeficiente líder.

```
(%i2) %/6;
```

$$(\%o2) \qquad [\frac{1}{6}, -\frac{x}{4}, x + 1]$$

```
(%i3) %*(x+1);
```

$$(\%o3) \qquad [\frac{x+1}{6}, -\frac{x^2+x}{4}, x^2 + 2x + 1]$$

```
(%i4) %[1]*(6*x^3+6)+%[2]*(4*x^2-4);
```

$$(\%o4) \qquad x^2 + 2x + 1$$

Así $X = \frac{x+1}{6}$, $Y = -\frac{x^2+x}{4}$ es una solución a nuestra ecuación.

Ejercicio 41: Calcula el inverso para el producto de $x + 1$ en $\mathbb{Z}_5[x]_{x^2+x+1}$.

Maxima 23: En $\mathbb{Z}_2[x]$, el conjunto de posibles restos módulo un polinomio de grado dos viene dado por la siguiente lista.

```
(%i1) f4:[0,1,x,x+1];
```

$$(\%o1) \qquad [0, 1, x, x + 1]$$

Hagamos la tabla de multiplicar de $\mathbb{Z}_2[x]_{x^2+1}$. Al ser $x^2 + 1 = (x + 1)(x + 1)$ en $\mathbb{Z}_2[x]$, lo que obtenemos no es un cuerpo.

```
(%i2) genmatrix(lambda([i,j],polymod(remainder(f4[i]*f4[j],x^2+1),2)),4,4);
```

(%o2)
$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & x & x+1 \\ 0 & x & 1 & x+1 \\ 0 & x+1 & x+1 & 0 \end{pmatrix}$$

Si hacemos las cuentas módulo x^2+x+1, que es irreducible, obtenemos un cuerpo con cuatro elementos.

```
(%i3) genmatrix(lambda([i,j],polymod(remainder(f4[i]*f4[j],x^2+x+1),2)),4,4);
```

(%o3)
$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & x & x+1 \\ 0 & x & x+1 & 1 \\ 0 & x+1 & 1 & x \end{pmatrix}$$

Como se puede ver en la tabla, el inverso de x es $x+1$.

Maxima 24: Resolvamos la congruencia

$$(x+3)X \equiv x^2 \pmod{x^3+1}$$

en $\mathbb{Z}_5[x]$.

Primero fijamos el módulo a 5 (`maxima` representa $\mathbb{Z}_5$ como $\{-2,-1,0,1,2\}$).

```
(%i1) modulus:5;
```

(%o1) 5

Luego comprobamos si el máximo común divisor de $x+3$ y x^3+1 divide a x^2.

```
(%i2) gcdex(x+3,x^3+1);
```

(%o2) $[x^2+2x-1,-1,1]$

De esta forma sabemos además que el inverso de $x+3$ módulo x^3+1 es x^2+2x-1. Despejamos y tenemos que $X=(x^2+2x-1)x^2 \pmod{x^3+1}$, que podemos calcular de la siguiente forma.

```
(%i3) remainder(%[1]*x^2,x^3+1);
```

(%o3) $-x^2-x-2$

Finalmente podemos comprobar el resultado obtenido.

```
(%i4) remainder(%*(x+3),x^3+1);
```

(%o4) x^2

Así las soluciones son de la forma $X=-x^2-x-2+(x^3+1)t(x)$, para cualquier $t(x)\in\mathbb{Z}_5[x]$.

Maxima 25:

Encontremos ahora el conjunto de soluciones del sistema de ecuaciones

$$\begin{cases} (x+3)X = x^2 \pmod{x^3+1}, \\ (2x+1)X = x \pmod{x^2}. \end{cases}$$

Por el ejercicio anterior, sabemos que de la primera ecuación obtenemos que $X=-x^2-x-2+(x^3+1)t(x)=4x^2+4x+3+t(x)(x^3+1)$. Así que substituyendo este valor en la segunda y despejando $t(x)$, obtenemos lo siguiente.

```
(%i1)  modulus:5$
```

```
(%i2)  remainder(x-(2*x+1)*(4*x^2+4*x+3),x^2);
```
$$(\%o2) \qquad x+2$$

```
(%i3)  remainder((2*x+1)*(x^3+1),x^2);
```
$$(\%o3) \qquad 2x+1$$

Por tanto $(2x+1)t(x) = x+2 \pmod{x^2}$. Calculamos ahora el inverso de $2x+1$ módulo x^2 en $\mathbb{Z}_5[x]$ con el algoritmo extendido de Euclides.

```
(%i4)  gcdex(2*x+1,x^2);
```
$$(\%o4)/R/ \qquad [-2x+1,-1,1]$$

```
(%i4)  gcdex(2*x+1,x^2);
```
$$(\%o4)/R/ \qquad [-2x+1,-1,1]$$

De esta forma, $t(x) = 2x+2+s(x)x^2$ y en consecuencia $X = 4x^2+4x+3+(2x+2+s(x)x^2)(x^3+1)$. Como

```
(%i6)  expand(4*x^2+4*x+3+(2*x+2)*(x^3+1));
```
$$(\%o6) \qquad 2x^4+2x^3+4x^2+6x+5$$

```
(%i7)  rat(%);
```
$$(\%o7)/R/ \qquad 2x^4+2x^3-x^2+x$$

Llegamos a que $X = 2x^4+2x^3+4x^2+x+s(x)(x^5+x^2)$, para cualquier $s(x) \in \mathbb{Z}_5[x]$.

Índice alfabético

algoritmo de Euclides, 23
anillo, 22
  conmutativo, 22

cociente, 23
coeficiente líder, 22
cuerpo, 22

grado de un polinomio, 22

mínimo común múltiplo, 23
máximo común divisor, 23
multiplicidad, 24

polinomio, 22
  irreducible, 22
  monico, 22

raíz de un polinomio, 24
  múltiple, 24
  simple, 24
resto, 23

término líder, 22

unidad, 22