Capítulo 3

Anillos

Hemos utilizado estructuras en las que hay dos operaciones, como la suma y el producto en $\mathbb{Z}$. El objeto más básico de este tipo es un anillo, cuyos axiomas son bastante parecidos a los axiomas aritméticos de los enteros, aunque ligeramente más débiles; y, por lo tanto, más generales.

3.1 Anillos

Definición 3.1.1 *Un anillo es un conjunto A en el que hay definidas dos operaciones binarias $+$ y $\cdot$ que cumplen los axiomas siguientes:*

1. *$(A, +)$ es un grupo conmutativo*
2. *$\cdot$ es asociativa*
3. *$\cdot$ es distributiva respecto a $+$.*

Las operaciones $+$ y $\cdot$ se llaman suma y producto en el anillo (aunque pueden ser diferentes de la suma y producto usuales). El elemento neutro para $+$ se representa con el símbolo 0 (elemento cero) y el simétrico aditivo de a se escribe $-a$ y se denomina opuesto de a.

Si la operación $\cdot$ es conmutativa se dice que A es un anillo conmutativo. Si existe neutro para $\cdot$ se dice que A es un anillo unitario y el neutro se denota por el símbolo 1 (elemento uno).

Ejemplo 3.1.1

1. *$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$*
2. *El conjunto de matrices 2×2 con coeficientes enteros (o reales) con la suma y producto de matrices. Este anillo no es conmutativo, pero sí es unitario.*
3. *$(\mathbb{Z}, \oplus, \otimes)$ con $\oplus$ y $\otimes$ definidas, para cada par de números x, y por $x \oplus y = x+y-1$, $x \otimes y = x+y-xy$. Es un anillo conmutativo y unitario en el cual el neutro para $\oplus$ es el número entero 1 y el neutro para $\otimes$ es el número entero 0.*
4. *En $A = \{a, b, c, d, e\}$ se define las operaciones siguientes dadas por la tablas*

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

$\cdot$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

Es un anillo finito conmutativo y unitario. El elemento a es el neutro para la suma, mientras que b es el neutro para el producto.

A partir de aqui, consideraremos que $(A, +, \cdot)$ es un anillo.

Proposición 3.1.1 *1. Para todo elemento $a \in A$ se verifica que $0 = 0 \cdot a = a \cdot 0$.*

2. Si A es unitario y $A \neq \{0\}$ entonces $0 \neq 1$.

En efecto, para $a \neq 0$, $a \cdot 1 = a \neq 0 = a \cdot 0$, por lo tanto $0 \neq 1$.

3. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$, $\forall a, b \in A$.

4. $(-a) \cdot (-b) = a \cdot b$, $\forall a, b \in A$.

(Demostración.)

3.2 Divisores de cero y unidades

Definición 3.2.1 *Un elemento a de un anillo A se llama divisor de cero si existe un elemento no nulo $b \in A$ tal que $a \cdot b = 0$ ó $b \cdot a = 0$. Cuando $a \neq 0$ se denomina divisor de cero propio.*

Un elemento a de un anillo unitario A se llama inversible (o unidad) si a posee inverso multiplicativo, es decir, si existe un elemento $b \in A$ tal que $a \cdot b = 1 = b \cdot a$.

Observación 3.2.1 *Con la notación anterior, si a es unidad el elemento b es único, se denomina inverso de a y se representa por a^{-1}. Se denota por $U(A)$ el conjunto de los elementos inversibles del anillo A, que es un grupo con la operación producto, llamado grupo multiplicativo de A.*

Ejemplo 3.2.1 *1. $\mathbb{Z}$ no tiene divisores de cero propios y $U(\mathbb{Z}) = \{1, -1\}$.*

2. En $\mathbb{R}$ no hay divisores de cero propios y $U(\mathbb{R}) = R - \{0\}$.

3. En $\mathbb{Z}_m$ un elemento a es inversible si, y sólo si, m.c.d.$(a, m) = 1$, de lo que se deduce que $U(\mathbb{Z}_m)$ es un grupo de orden $\phi(m)$. Por ejemplo, $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$.

4. En el conjunto de matrices cuadradas de orden 2 con coeficientes reales, la matriz B es un divisor de cero, y las matrices inversibles son aquellas cuyo determinante es no nulo; por ejemplo, D es inversible.

$$B = \begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix} \quad D = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$$

5. En el apartado 4 del Ejemplo 3.1.1, todo elemento no nulo es inversible.

Proposición 3.2.2 *Sea $a \in A$, $a \neq 0$.*

1. El elemento a es un divisor de cero si, y sólo si, a no es simplificable para el producto.

2. Si a es un elemento inversible, a no es divisor de cero.

(Demostración.)

3.3 Dominios y cuerpos

Los conceptos de divisor de cero e inversible conducen a dos tipos importantes de anillos: los dominios y los cuerpos.

Definición 3.3.1 *Un anillo conmutativo unitario A, se denomina*

1. *dominio de integridad (o, simplemente, dominio) si no tiene divisores de cero propios;*
2. *cuerpo (conmutativo) si todo elemento distinto de 0 tiene inverso (es decir, $U(A) = A - \{0\}$).*

Observación 3.3.1 *Un cuerpo es un dominio. En efecto, si $a \cdot b = 0$ con $a \neq 0$ en un cuerpo K entonces existe $a^{-1} \in K$ y por tanto $b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$.*

Sin embargo, no todos los dominios son cuerpos, por ejemplo $\mathbb{Z}$ el anillo de los números enteros es un dominio pero no es cuerpo ya que, por ejemplo 2 no tiene inverso multiplicativo.

Proposición 3.3.2 *Todo dominio finito es un cuerpo.*

Demostración. Sea D un dominio cuyos elementos son $d_1, \cdots, d_n$. Veamos que si $a \neq 0$ es un elemento arbitrario distinto del 0 entonces existe su inverso multiplicativo.

Observemos que los productos $a.d_1, \cdots, a.d_n$ son distintos dos a dos pues si $a.d_i = a.d_j$ entonces $a.(d_i - d_j) = 0$ de donde se concluye que $d_i = d_j$. Luego el conjunto $C = \{a.d_1, \cdots, a.d_n\}$ tiene los mismos elementos que D. En particular, existe un i tal que $1 = ad_i$. Como D es conmutativo tenemos que $1 = d_i.a$ y por tanto $a^{-1} = d_i$.

Proposición 3.3.3 *El anillo de enteros módulo n, $\mathbb{Z}_n$, es un cuerpo si y sólo si n es un número primo.*

Demostración. Veamos en primer lugar que $\mathbb{Z}_n$ cuerpo implica que n es un número primo. Haremos un razonamiento por contradicción.

Supongamos que n no es un número primo. Si $n = 1$ entonces $\mathbb{Z}_n = \mathbb{Z}$ no es cuerpo. Si $n > 1$ entonces $n = ab$ con a y b enteros estrictamente menores que n. En $\mathbb{Z}_n$, tenemos que $[a][b] = [ab] = [n] = [0]$. Si $\mathbb{Z}_n$ fuese un cuerpo, necesariamente $[a] = [0]$ o bien $[b] = [0]$. Pero eso se cumple si $n \mid a$ o $n \mid b$ lo que contradice la hipótesis.

Veamos ahora que si n es primo entonces $\mathbb{Z}_n$, es un cuerpo. Para ello, probaremos que todo elemento no nulo tiene inverso multiplicativo. En efecto, consideremos $[m] \in \mathbb{Z}_n$ con $m < n$. Por ser n primo tenemos que m y n son primos entre sí y por tanto existen enteros tales que $1 = am + bn$, de donde $[1] = [a][m] + [b][n] = [a][m] + [b][0] = [a][m]$. Luego $[m]$ tiene inverso en $\mathbb{Z}_n$.

Ejemplo 3.3.1

1. *$(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son cuerpos.*
2. *Dado $a \in \mathbb{Z}_m$, $a \neq 0$, si $mcd(a, m) = 1$ entonces a es inversible en $\mathbb{Z}_m$, si $mcd(a, m) \neq 1$, entonces a es divisor de cero. En consecuencia, $\mathbb{Z}_m$ es cuerpo si, y sólo si $\mathbb{Z}_m$ es un dominio si, y sólo si, m es primo.*

3.4 Subanillos y subcuerpos

Definición 3.4.1 *Sea $(A, +, \cdot)$ un anillo (cuerpo), un subconjunto no vacío S de A se dice que es un subanillo (subcuerpo) de A si $(S, +, \cdot)$ (es decir, S con restricción de la suma y el producto de A) es un anillo (cuerpo).*

Ejemplo 3.4.1

1. *Para cualquier anillo A, los conjuntos $\{0\}$ y A son subanillos de A (subanillos triviales).*
2. *El conjunto de los enteros pares es un subanillo (aunque no unitario) de $(\mathbb{Z}, +, \cdot)$. De hecho, para cualquier entero $m > 0$, el conjunto $< m >$ de los múltiplos de m es un subanillo de $(\mathbb{Z}, +, \cdot)$.*
3. *$(\mathbb{Z}, +, \cdot)$ es subanillo de $(\mathbb{Q}, +, \cdot)$, y éste es subcuerpo de $(\mathbb{R}, +, \cdot)$.*

El resultado siguiente caracteriza los subconjuntos de A que son subanillos:

Proposición 3.4.1 *Sea $(A,+,\cdot)$ un anillo y S un subconjunto no vacío de A.*

1. *S es subanillo de A si, y sólo si, $\forall x,y \in S$ se verifica*
   (i) $x-y \in S$ (equivale a que $(S,+)$ sea subgrupo de $(A,+)$) y
   (ii) $x \cdot y \in S$.
2. *Si $(A,+,\cdot)$ es un cuerpo, S es subcuerpo de S si, y sólo si, $\forall x,y \in S$ se verifica*
   (i) $x-y \in S$ y
   (ii) $x \cdot y^{-1} \in S$, para $y \neq 0$.

(Demostración.)

Ejemplo 3.4.2 *1. El conjunto de enteros impares es un subanillo de $(\mathbb{Z},\oplus,\otimes)$ (Ejemplo 1, (3)).*

2. *El conjunto de las matrices de la forma $\begin{pmatrix} x & x \\ y & y \end{pmatrix}$ es un subanillo de las matrices de orden 2 con coeficientes enteros.*
3. *$\mathbb{Q}$ y $\{a+b\sqrt{2},\ a,b \in \mathbb{Q}\}$son subcuerpos de $\mathbb{R}$ con $(a+b\sqrt{2})^{-1} = a/(a^2-2b^2) + (-b/(a^2-2b^2))\sqrt{2}$.*
4. *$\mathbb{R}$ es un subcuerpo de $\mathbb{C}$.*

3.5 Ideales y anillo cociente

Definición 3.5.1 *Sea $(A,+,\cdot)$ un anillo, un subconjunto no vacío I de A se llama ideal de A si*

1. *$\alpha-\beta \in I$, $\forall \alpha,\beta \in I$ (equivalentemente, I es un subgrupo de $(A,+)$).*
2. *Para cada $\alpha \in I$, y cada $a \in A$. $\alpha \cdot a$ y $a \cdot \alpha \in I$.*

Observación 3.5.1 *Si S es un subanillo de A, S es un subgrupo del grupo conmutativo $(A,+)$ y, por lo tanto, la relación de equivalencia inducida por S en A es compatible con la operación $+$.*

Sin embargo, para definir el anillo cociente, se precisa una relación que también sea compatible con el producto.

Si $(A,+,\cdot)$ es un anillo e I un subgrupo de $(A,+)$, la relación inducida por I en A ($x \sim y$ si, y sólo si, $x-y \in I$) es compatible con la suma. Además, $\sim$ es compatible con $\cdot$ si, y sólo si, I es un ideal de A.

En este caso, el conjunto cociente A/I tiene estructura de anillo (llamado anillo cociente) con las operaciones suma y producto inducidas por las de A. Nótese que $[0]=I$, $[a]=a+I$, $\forall a \in A$.

Definición 3.5.2 *Si A es un anillo conmutativo unitario y $a \in A$, el conjunto $(a)=\{x\cdot a = a\cdot x,\ x \in A\}$ es un ideal, llamado ideal principal generado por a.*

Ejemplo 3.5.1 *1. Para todo entero m, $< m >$ es un ideal de $(\mathbb{Z},+,\cdot)$ y $\mathbb{Z}/< m >= \mathbb{Z}_m$*

2. *En $\mathbb{Z}$, $(m)=\{s\cdot m,\ s \in \mathbb{Z}\}$ coincide con $< m >$, pues $2+2+\overset{n}{\cdots}+2 = n\cdot m$.*

   Pero, no siempre se verifica; por ejemplo, en $(\mathbb{Q},+,\cdot)$, $< 2 >= \{2+2+\overset{n}{\cdots}+2,\ n \in \mathbb{Z}\}$ mientras que $(2)=\{q\cdot 2,\ q \in \mathbb{Q}\}=\mathbb{Q}$.
3. *En $\mathbb{Z}$ todos los ideales son principales.*
4. *Si K es un cuerpo e I un ideal de K, entonces $I=\{0\}$ o bien $I=K$.*
5. *Todo ideal es un subanillo, pero el recíproco no siempre se cumple. Por ejemplo, $\mathbb{Z}$ es un subanillo, pero no ideal de $\mathbb{Q}$.*
6. *El conjunto de las matrices $\begin{pmatrix} x & x \\ y & y \end{pmatrix}$ es un subanillo de las matrices de orden 2 con coeficientes enteros y no es un ideal.*

3.6 Morfismos de anillos

Definición 3.6.1 *Sean $(A,+,\cdot)$ y $(B,+,\cdot)$ anillos. Una aplicación $f: A \to B$ se denomina morfismo de anillos si $\forall a_1, a_2 \in A$*

1. $f(a_1 + a_2) = f(a_1) + f(a_2)$
2. $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$.

Proposición 3.6.1 1. $f(0_A) = 0_B$

2. $f(-a) = -f(a), \forall a \in A$.
3. *Si A' es un subanillo de A, entonces $f(A')$ es un subanillo de B'.*
   En particular, $\mathrm{Im}(f) = f(A)$ *es un subanillo de B.*
4. *Si B' es un subanillo de B, entonces $f^{-1}(B')$ es un subanillo de A.*
   En particular, $\mathrm{Ker}(f) = \{a \in A,\ f(a) = 0_B\}$*es un subanillo de A.*
5. $\mathrm{Ker}(f)$ *es ideal de A.*
6. *f es inyectiva si, y sólo si,* $\mathrm{Ker}(f) = \{0_A\}$.
7. *Sean A un cuerpo y $f: A \to B$ un morfismo de anillos. Si $f \neq 0$ entonces f es inyectiva.*

(Demostración.)

Ejemplo 3.6.1 1. $f: Z \to \mathbb{Z}_m$, *con $f(x) = [x]$ es un epimorfismo.*

2. $f: Z \to \mathbb{Z}_6$, *definida por $f(2n) = 0$, $f(2n+1) = 3$ es un morfismo de anillos, ambos son unitarios, pero $f(1) \neq 1$.*
3. $f: \mathbb{Z}_4 \to \mathbb{Z}_8$, *definida por $f(a) = a^2$ no es un morfismo de anillos, pues conserva el producto, pero no la suma (por ejemplo, $f(2+3) \neq f(2) + f(3)$).*
4. $f: \mathbb{Z}_4 \to \mathbb{Z}_8$, *definida por $f(a) = 2a$ no es un morfismo de anillos, pues conserva la suma, pero no el producto (por ejemplo, $f(1 \cdot 2) \neq f(1) \cdot f(2)$).*

Observación 3.6.2 *La definición de morfismo de cuerpos es la misma que la de morfismo de anillos, es decir, una aplicación entre cuerpos que conserva las operaciones. Por la Proposición 3.6.1, apartado 7, todo morfismo de cuerpos es nulo o es inyectivo. Si $f: K \to K'$ es un morfismo no nulo, entonces $f: K - \{0\} \longrightarrow K' - \{0\}$ es un morfismo de grupos (con el producto) y, en consecuencia, $f(1_K) = 1_{K'}$ y $f(x^{-1}) = (f(x))^{-1}$.*

3.7 Característica de un cuerpo

Sea $(K,+,\cdot)$ un cuerpo, se llama característica de K al orden del elemento 1 en el grupo $(K,+)$. Puede ocurrir que:

1. El orden del elemento 1 sea un natural $n \in \mathbb{N}$ (por ejemplo, cuando K es finito). En este caso, n es primo y $\mathrm{ord}\ (x) = n, \forall x \in K,\ x \neq 0$.
2. El 1 tenga orden infinito, es decir, $1 + \overset{n}{\cdots} + 1 \neq 0$, $\forall n \in \mathbb{N}$ (por ejemplo, $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$). En este caso se dice que K es un cuerpo de característica 0.

Ejercicio. Si K es un cuerpo de característica $p \neq 0, (x+y)^p = x^p + y^p$.

Observación 3.7.1 *Si K es un cuerpo finito de característica p, entonces $|K| = p^n$, para algún entero positivo n. Recíprocamente, para cualquier entero positivo n, existe un cuerpo finito de cardinal p^n. En la construcción de estos cuerpos se utilizan polinomios con coeficientes en el cuerpo $\mathbb{Z}_p$.*

3.8 Anillo de polinomios con coeficientes en un cuerpo

Sea $(K, +, \cdot)$ un cuerpo.

Definición 3.8.1 *Un polinomio en la indeterminada x con coeficientes en K es una expresión de la forma $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ donde $a_i \in K$, para todo $0 \leq i \leq n$.*

El conjunto de polinomios en la indeterminada x con coeficientes en K se denota por $K[x]$.

Definición 3.8.2 *Sea $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un polinomio en $K[x]$.*

1. *Si $a_i = 0$, para todo $0 \leq i \leq n$, $a(x)$ se llama polinomio cero.*
2. *Si $a(x)$ no es el polinomio cero,*
   (a) *el mayor entero s tal que $a_s \neq 0$ se llama grado del polinomio $a(x)$, denotado por $\partial a(x)$.*
   (b) *a_s se llama coeficiente principal y a_sx^s término principal;*
   (c) *a_i es el coeficiente de grado i*
   (d) *a_ix^i el término de grado i, para $0 \leq i \leq n$.*
3. *Un polinomio de grado 0 se llama polinomio constante.*
4. *Cuando el coeficiente principal es 1, el polinomio se llama mónico.*
5. *Dos polinomios, $a(x)$ y $b(x)$, son iguales si tienen el mismo grado y $a_i = b_i$, para todo i, $0 \leq i \leq \partial a(x) = \partial b(x)$.*
6. *Los símbolos $x, x^2, x^3, \cdots$ sólo indican las posiciones de los coeficientes, por ello, también se define un polinomio con coeficientes en un cuerpo K como una sucesión finita $(a_0, a_1, a_2, \cdots, a_n)$ de elementos de K o una aplicación $a : \mathbb{N} \to K$ tal que $a(n) = 0$, si $n > \partial a$.*

Ejemplo 3.8.1 *En $(\mathbb{Z}_5, +, \cdot)$ la expresión $3x^6 + 4x^5 + x^2 + 4x + 2$ es un polinomio de grado 6, con coeficiente principal 3 y término constante 2.*

3.8.1 Suma y producto en K[x]

Sean $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ y $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ polinomios de $K[x]$.

Podemos suponer que $n \geq m$, y si $n > m$ ponemos $b_{m+1} = b_{m+2} = \cdots = b_n = 0$.

Se define la suma $a(x) + b(x)$ y el producto $a(x)\cdot b(x)$ de los polinomios de la forma siguiente:

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n$$

$$a(x)\cdot b(x) = (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0)x + (a_0 \cdot b_1 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 + \cdots + a_n \cdot b_m x^{n+m}$$

Es decir, el coeficiente de x^i en $a(x) + b(x)$ es $a_i + b_i$, para cada $0 \leq i \leq n$.

El coeficiente de x^i en $a(x)\cdot b(x)$ para $0 \leq i \leq n + m$, es

$$a_0 \cdot b_i + a_1 \cdot b_{i-1} + a_2 \cdot b_{i-2} + \cdots + a_i \cdot b_0 = \sum_{k=0}^{i} a_k \cdot b_{i-k} = \sum_{j+k=i} a_j \cdot b_k$$

donde las sumas y productos son en K.

De estas definiciones se deduce que los coeficientes de $a(x) + b(x)$ y de $a(x)\cdot b(x)$ pertenecen a K, es decir, la suma y el producto son operaciones internas en $K[x]$.

Además, si $a(x) + b(x) \neq 0$ y $a(x)\cdot b(x) \neq 0$ entonces

$$\partial(a(x) + b(x)) \leq max\{\partial a(x), \partial b(x)\} \text{ y } \partial(a(x)\cdot b(x)) = \partial a(x) + \partial b(x).$$

Ejemplo 3.8.2 *1. Si* $a(x) = 3 + 2x + 4x^2 + 4x^5$ *y* $b(x) = 3x + 2x^2 + 4x^3$ *en* $\mathbb{R}[x]$,

$a(x)+b(x) = (3+0)+(2+3)x+(4+2)x^2+(0+4)x^3+(4+0)x^5 = 3+5x+6x^2+4x^3+4x^5$ $a(x)\cdot b(x) = (3\cdot 0)+(3\cdot 3+2\cdot 0)x+(3\cdot 2+2\cdot 3+4\cdot 0)x^2+\cdots\cdots = 16x^8+8x^7+12x^6+16x^5+16x^4+28x^3+12x^2+9x.$

2. En $\mathbb{Z}_5[x]$, *si* $a(x) = 3 + 2x + 4x^2 + 4x^5$ *y* $b(x) = 3x + 2x^2 + 4x^3$

$a(x) + b(x) = (3 + 0) + (2 + 3)x + (4 + 2)x^2 + (0 + 4)x^3 + (4 + 0)x^5 = 3 + 1x^2 + 4x^3 + 4x^5$
$a(x)\cdot b(x) = (3\cdot 0)+(3\cdot 3+2\cdot 0)x+(3\cdot 2+2\cdot 3+4\cdot 0)x^2+\cdots\cdots = x^8+3x^7+2x^6+x^5+x^4+3x^3+2x^2+4x.$

Observación 3.8.1 *Con estas operaciones* $(K[x], +, \cdot)$ *es un anillo conmutativo unitario sin divisores de cero propios, es decir, es un dominio. Sin embargo,* $K[x]$ *no es un cuerpo, los únicos elementos inversibles son los polinomios constantes no nulos.*

En los apartados que siguen, veremos cómo las propiedades de divisibilidad (y los resultados que de ellas se deducen) en $K[x]$ son las mismas que en Z.

3.8.2 Algoritmo de división en K[x]

En cursos anteriores se aprendió a dividir polinomios con coeficientes reales, se vió cómo se obtiene el cociente y el resto. La misma técnica se aplica cuando los coeficientes de los polinomios se toman en un cuerpo K.

Proposición 3.8.2 *Algoritmo de división. Sean* $a(x)$ *y* $b(x)$ *polinomios con coeficientes en un cuerpo* K, *siendo* $b(x) \neq 0$. *Se verifica que existen polinomios únicos* $q(x)$, $r(x)$ *de* $K[x]$ *tales que*

$$a(x) = q(x)b(x) + r(x), \text{ donde } \partial r(x) < \partial b(x) \text{ ó } r(x) = 0.$$

Demostración. Para obtener la existencia, se considerará $b(x)$ fijo y se demostrará por inducción en el grado de $a(x)$.

1. Caso $\partial a(x) = 0$. Si $\partial b(x) = 0$, $b(x) = b_0 \neq 0$ y $a(x) = a_0 = (a_0 b_0^{-1})b_0 + 0$ y basta tomar $q(x) = (a_0 b_0^{-1})$ y $r(x) = 0$. Si $\partial b(x) > 0$, el resultado se cumple para $q(x) = 0$ y $r(x) = a(x)$.

2. Paso inductivo. Supongamos $\partial a(x) > 0$ y que el teorema se cumple para polinomios de grado estrictamente menor que el grado de a(x). En primer lugar, observemos que si $\partial a(x) < \partial b(x)$, el resultado se cumple para $q(x) = 0$ y $r(x) = a(x)$. Veamos el caso $\partial a(x) \geq \partial b(x)$.

   Si $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, con $a_n \neq 0$ y $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, con $b_m \neq 0$, el polinomio $\alpha(x) = a(x) - a_n b_{m-1} x^{n-m} b(x)$ cumple que $\partial\alpha(x) < \partial a(x)$. Por hipótesis de inducción, existen polinomios $\gamma(x), \rho(x)$ tales que $\alpha(x) = \gamma(x)b(x) + \rho(x)$ con $\partial\rho(x) < \partial b(x)$, o bien $\rho(x) = 0$. Así pues, $a(x) = a_n b_{m-1} x^{n-m} b(x) + \alpha(x) = (a_n b_{m-1} x^{n-m} + \gamma(x))b(x) + \rho(x)$ y tomando $q(x) = a_n b_{m-1} x^{n-m} + \gamma(x)$ y $r(x) = \rho(x)$ se obtiene $a(x) = q(x)b(x) + r(x)$, donde $\partial r(x) < \partial b(x)$ ó $r(x) = 0$. Esto completa la inducción y el resultado es cierto para todos los valores de $\partial a(x)$.

Unicidad: si $a(x) = q_1(x)b(x) + r_1(x) = q_2(x)b(x) + r_2(x)$, donde $\partial r_i(x) < \partial b(x)$ o $r_i(x) = 0, (i = 1, 2)$ entonces $(q_1(x) - q_2(x))b(x) = r_2(x) - r_1(x)$. Si $q_1(x) \neq q_2(x)$, $\partial[(q_1(x) - q_2(x))b(x)] \geq \partial b(x)$, mientras que $\partial(r_2(x) - r_1(x)) \leq max\{\partial r_1(x), \partial r_2(x)\} < \partial b(x)$. Se llega así a una contradicción y, en consecuencia, $q_1(x) = q_2(x)$ y $r_1(x) = r_2(x)$.

Los polinomios $q(x)$ y $r(x)$ se llaman cociente y resto, respectivamente, de dividir $a(x)$ por $b(x)$. Nótese que la construcción de $\alpha(x)$ en la demostración indica la manera (algoritmo) de dividir dos polinomios.

Ejemplo 3.8.3 *Si* $a(x) = 5x^4 + 2x^3 + 4x^2 + 3x + 2$ *y* $b(x) = 3x^2 + 5$ *en* $(\mathbb{Z}_7[x], +, \cdot)$, *el cociente es* $c(x) = 4x^2 + 3x + 4$ *y el resto* $r(x) = 2x + 3$.

Definición 3.8.3 *Al igual que en* $\mathbb{Z}$, *si* $a(x)$ *y* $b(x)$ *son polinomios con coeficientes en* K *tales que el resto de dividir* $a(x)$ *por* $b(x)$ *es* 0, *se dice que* $a(x)$ *es múltiplo de* $b(x)$ *o que* $b(x)$ *es divisor (o factor) de* $a(x)$; *es decir,* $a(x) = q(x)b(x)$ *para algún* $q(x)$ *de* $K[x]$. *Se representa* $b(x) \mid a(x)$.

Ejemplo 3.8.4 *1. $x-1$ es divisor de x^2-1 en $\mathbb{R}[x]$.*

2. $x+3$ es divisor de x^2+1 en $\mathbb{Z}_5[x]$ pero no lo es en $\mathbb{R}[x]$.

Definición 3.8.4 *Sean $a(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in K[x]$ y $\alpha\in K$, se llama valor del polinomio $a(x)$ en α al elemento de K, $a(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n\in K$.*

Se dice que α es raíz de $a(x)$ si $a(\alpha)=0$.

Proposición 3.8.3 *Teorema del resto.*

Sean $a(x)\in K[x]$ y $\alpha\in K$; el resto de la división de $a(x)$ por $x-\alpha$ es $a(\alpha)$.

Demostración. Por el teorema de división, $a(x)=(x-\alpha)q(x)+r(x)$ con $r=0$ o $\partial r(x)<\partial(x-\alpha)=1$. Por lo tanto, $r(x)=r$ es un elemento de K. Si evaluamos $a(x)$ en α se obtiene $a(\alpha)=(\alpha-\alpha)q(\alpha)+r(\alpha)=0+r$.

Proposición 3.8.4 *Teorema del factor.*

Sean $a(x)\in K[x]$ y $\alpha\in K$; $x-\alpha$ divide a (es un factor de) $a(x)$ si, y sólo si, α es raíz de $a(x)$.

Demostración. $x-\alpha$ divide a $a(x)$ si y sólo si $r(x)=0$ si y sólo si $a(\alpha)=0$.

Ejemplo 3.8.5 *1. $a(x)=-7+3x-x^2+4x^4-6x^5+x^7\in\mathbb{Q}[x]$. El resto de dividir $a(x)$ por $x-2$ es $a(2)=-5$ y el resto de dividir $a(x)$ por $x+1$ es $a(-1)=-2$.*

2. Si se divide $b(x)=2+2x+x^2+x^3+3x^4+x^5\in\mathbb{Z}_5[x]$ por $x+4=x-1$, el resto es $b(1)=0$ en $\mathbb{Z}_5$. En consecuencia, $x+4$ divide a $b(x)$, es decir, $b(x)=(x+4)q(x)$ con $\partial q(x)=4$. El polinomio $q(x)=3+x+4x^3+x^4$, tiene a 3 como raíz, y por lo tanto, también $b(x)$, con lo cual $b(x)=(x-1)(x-3)(x^3+2x^2+x+4)$.

Observación 3.8.5 *Si $\alpha\in K$ es una raíz de $a(x)$, entonces $a(x)=(x-\alpha)q_1(x)$. Si α es de nuevo raíz de $q_1(x)$, entonces $q_1(x)=(x-\alpha)q_2(x)$ y así $a(x)=(x-\alpha)^2q_2(x)$. Siguiendo este proceso se llegará a un m, con $1\leq m\leq\partial a(x)$, tal que $a(x)=(x-\alpha)^mq_m(x)$ con $q_m(\alpha)\neq 0$ y se dice que α es raíz de multiplicidad m del polinomio $a(x)$.*

Proposición 3.8.6 *Si $a(x)\in K[x]$ tiene grado $n\geq 1$, entonces $a(x)$ tiene a lo sumo n raíces en K (considerando cada una de ellas tantas veces como indica su multiplicidad como raíz de a(x)).*

Demostración. Por inducción en $\partial a(x)$.

Ejemplo 3.8.6 *1. $a(x)=9-6x+x^2\in\mathbb{R}[x]$ tiene a lo sumo dos raíces, en este caso 3 es raíz de multiplicidad 2 y $a(x)=(x-3)(x-3)$ es una factorización" de $a(x)$.*

2. $a(x)=4+x^2\in\mathbb{R}[x]$ no tiene raíces reales, lo que no contradice la nota anterior.

3. $a(x)=4+x^2\in\mathbb{C}[x]$ tiene dos raíces complejas, $2i$ y $-2i$, se factoriza como $a(x)=(x-2i)(x+2i)$.

4. Si $a(x)=6+2x+x^2\in\mathbb{Z}_7[x]$, entonces $a(2)=0$, $a(3)=0$ y éstas son las únicas raíces del polinomio. Así, $a(x)=(x-2)(x-3)=(x+5)(x+4)$.

Observación 3.8.7 *En general, si $a(x)\in K[x]$ y $\alpha_1,\alpha_2,\cdots,\alpha_s$ son las raíces de $a(x)$ en K, entonces $a(x)=a_n(x-\alpha_1)\cdots(x-\alpha_s)q(x)$ donde a_n es el coeficiente principal de $a(x)$ y $q(x)$ un polinomio mónico sin raíces.*

El algoritmo de división, permite demostrar, al igual que para el anillo $\mathbb{Z}$, el siguiente resultado

Proposición 3.8.8 *Todo ideal de $K[x]$ es un ideal principal.*

Demostración. Sea I un ideal de $K[x]$. Consideremos $d(x)$, el polinomio mónico de menor grado en I. Claramente, $(d(x))$ está contenido en I. Por otra parte, si $a(x)\in I$, por el algoritmo de división $a(x)=q(x)d(x)+r(x)$ con $\partial r(x)<\partial d(x)$ o $r(x)=0$. Pero si $a(x),d(x)\in I$, entonces $r(x)=a(x)-q(x)d(x)\in I$, y por la elección de $d(x)$ no puede ocurrir $\partial r(x)<\partial d(x)$. Así pues, $r(x)=0$, es decir, $a(x)\in(d(x))$ y $(d(x))=I$.

3.8.3 Máximo común divisor de polinomios.

A partir del algoritmo de división en $K[x]$, veremos definiciones y resultados sobre divisibilidad de polinomios análogos a los ya conocidos en $\mathbb{Z}$.

Definición 3.8.5 *Dados dos polimonios $a(x)$ y $b(x)$ de $K[x]$, se dice que $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$ si*

1. *$d(x)$ es divisor de $a(x)$ y $b(x)$*
2. *todo divisor de $a(x)$ y $b(x)$ es también divisor de $d(x)$.*

3.8.9 *Según esta definición, en general no existe un único mcd de dos polinomios. Si $d_1(x)$ y $d_2(x)$ verifican las condiciones 1 y 2, entonces $d_1(x) = \lambda d_2(x)$, para alguna constante λ. De esta forma, existirá un único máximo común divisor mónico y definiremos el mcd(a(x), b(x)) como el polinomio mónico que verifica las condiciones 1 y 2.*

Observemos que si $a(x) = b(x)q(x) + r(x)$ entonces

$$\mathrm{mcd(a(x), b(x)) = mcd(b(x), r(x)).}$$

Observación 3.8.10 *Para calcular el mcd de $a(x)$ y $b(x)$ en $K[x]$ imitaremos el método utilizado en $\mathbb{Z}$ de dividir repetidamente; éste es el algoritmo de Euclides para $K[x]$. Sean $a(x), b(x) \in K[x]$, supongamos $\partial a(x) \geq \partial b(x)$, con $b(x) \neq 0$. Llamamos $a_0(x) = a(x)$, $a_1(x) = b(x)$ y hacemos las divisiones siguientes:*

$$\begin{array}{ccc}
a_0(x) = q_1(x)a_1(x) + a_2(x) & con & \partial a_2(x) < \partial a_1(x) \\
a_1(x) = q_2(x)a_2(x) + a_3(x) & & \partial a_3(x) < \partial a_2(x) \\
a_2(x) = q_3(x)a_3(x) + a_4(x) & & \partial a_4(x) < \partial a_3(x) \\
\cdots & \cdots & \cdots \\
a_{s-2}(x) = q_{s-1}(x)a_{s-1}(x) + a_s(x) & & \partial a_s(x) < \partial a_{s-1}(x) \\
a_{s-1}(x) = q_s(x)a_s(x) + 0 & &
\end{array}$$

Dado que el grado de los restos decrece estrictamente, se llegará a un resto $a_{s+1}(x) = 0$. La última ecuación indica que $a_s(x)$ es divisor de $a_{s-1}(x)$; en consecuencia, $a_s(x)$ es un mcd de $a_{s-1}(x)$ y $a_s(x)$.

Utilizando las igualdades anteriores en orden inverso se tiene:

$a_s(x) = mcd(a_s(x), a_{s-1}(x)) = mcd(a_{s-1}(x), a_{s-2}(x)) = \cdots = mcd(a_2(x), a_1(x)) = mcd(a_1(x), a_0(x)) = mcd(a(x), b(x))$. Entonces el último resto no nulo, $a_s(x)$, es un mcd de $a(x)$ y $b(x)$ y es un múltiplo del mcd mónico de estos polinomios. Para obtener el $mcd(a(x), b(x))$ bastará multiplicar $a_s(x)$ por el inverso de su coeficiente principal.

Por substituciones sucesivas en las ecuaciones, podemos expresar $a_s(x)$ de la forma $\lambda(x)a(x) + \mu(x)b(x)$, donde $\lambda(x)$ y $\mu(x)$ son polinomios de $K[x]$. La existencia del mcd de dos polinomios en $K[x]$ viene dada por el teorema de Bezout.

Teorema 3.8.11 *Teorema de Bezout. Sean $a(x), b(x) \in K[x]$, existe $d(x) = mcd(a(x), b(x))$. Además existen polinomios $\lambda(x)$ y $\mu(x)$ en $K[x]$ tales que $d(x) = \lambda(x)a(x) + \mu(x)b(x)$.*

(Demostración).

Ejemplo 3.8.7

1. *Hallar el $mcd(x^3 + 2x^2 + x + 1, x^2 + 5)$ en $\mathbb{Z}_7[x]$*

   $x^3 + 2x^2 + x + 1 = (x + 2)(x^2 + 5) + (3x + 5)$

   $x^2 + 5 = (3x + 5)(5x + 1)$. *Entonces* $mcd(x^3 + 2x^2 + x + 1, x^2 + 5) = 3^{-1}(3x + 5) = x + 4$.

2. *Hallar el $mcd(x^4 + x^3 + x^2 + 1, x^4 + 1)$ en $\mathbb{Z}_2[x]$*

   $x^4 + x^3 + x^2 + 1 = 1.(x^4 + 1) + (x^3 + x^2)$

   $x^4 + 1 = (x + 1)(x^3 + x^2) + (x^2 + 1)$

   $x^3 + x^2 = (x + 1)(x^2 + 1) + (x + 1)$

   $x^2 + 1 = (x + 1)(x + 1) + 0$. *Entonces* $mcd(x^4 + x^3 + x^2 + 1, x^4 + 1) = x + 1$.

Definición 3.8.6 *Dados dos polimonios $a(x)$ y $b(x)$ de $K[x]$, se dice que $m(x)$ es un mínimo común múltiplo de $a(x)$ y $b(x)$ si*

1. *$m(x)$ es múltiplo de $a(x)$ y $b(x)$*
2. *todo múltiplo de $a(x)$ y $b(x)$ es también múltiplo de $m(x)$.*

3.8.12 *Al igual que para el máximo común divisor, si pedimos que el polinomio $m(x)$ sea mónico se obtiene la unicidad; por ello, definiremos el $mcm(a(x), b(x))$ como el polinomio mónico que verifica las condiciones 1 y 2.*

El mínimo común múltiplo de dos polimonios $a(x)$ y $b(x)$ de $K[x]$, se obtiene de la siguiente igualdad $mcm(a(x), b(x)) = a(x)\cdot b(x)/mcd(a(x), b(x))$ convertido en polinomio mónico si es necesario.

3.8.4 Polinomios irreducibles

En el estudio de los números enteros se vio cómo todo entero mayor o igual que 2, puede escribirse como producto de primos de forma única. En este apartado veremos los resultados análogos para $K[x]$, donde los primos serán los llamados polinomios irreducibles.

En primer lugar, nótese que la existencia de polinomios constantes no nulos permite factorizar trivialmente cualquier polinomio. Esto se debe a que una constante no nula α tiene inverso en K, que también es su inverso en $K[x]$; de manera que $a(x) = \alpha(\alpha^{-1}(a(x))$ es una factorización de $a(x)$ en $K[x]$. Por ese motivo los polinomios irreducibles se definen de la forma siguiente.

Definición 3.8.7 *Un polinomio $a(x) \in K[x]$ se denomina reducible si existen polinomios $b(x), c(x) \in K[x]$ con $\partial b(x), \partial c(x) \geq 1$ tales que $a(x) = b(x)c(x)$. En caso contrario, se dice que $a(x)$ es irreducible.*

Observación 3.8.13

1. *Como consecuencia de la definición, todo polinomio de grado menor o igual que 1 es irreducible.*
2. *Sea $a(x) \in K[x]$ con $\partial a(x) \geq 2$. Si $a(x)$ tiene alguna raíz en K, entonces $a(x)$ es reducible. Si $\alpha \in K$ una raíz de $a(x)$, entonces $a(x) = (x - \alpha)q(x)$ donde $\partial q(x) = \partial a(x) - 1 \geq 2 - 1 = 1$. Por lo tanto, $a(x)$ es reducible.*
3. *El recíproco no siempre es cierto; por ejemplo, $(x^2 + 1)(x^2 + 1)$ es reducible en $\mathbb{R}[x]$, pero no tiene raíces en $\mathbb{R}$.*
4. *Sin embargo, para $\partial a(x) = 2$ ó $\partial a(x) = 3$, $a(x)$ es reducible en $K[x]$ si, y sólo si, $a(x)$ tiene alguna raíz en K (o, si se prefiere, es irreducible en $K[x]$ si, y sólo si, no tiene raíces en K).*

   En efecto, si $a(x)$es reducible, $a(x) = b(x)c(x)$ con $\partial b(x), \partial c(x) \geq 1$. Como $\partial a(x) = 2$ ó 3, $\partial b(x) = 1$ ó $\partial c(x) = 1$, por lo tanto $b(x)$ ó $c(x)$ tiene una raíz en K (si $b(x) = b_0 + b_1 x$, entonces $-b_0 b_1^{-1}$ es una raíz de $b(x)$ en K).

Ejemplo 3.8.8

1. *$x^2 + 1$ es irreducible en $\mathbb{Q}[x]$ y $\mathbb{R}[x]$, pero $x^2 + 1 = (x + i)(x - i)$ y, por lo tanto, es reducible en $\mathbb{C}[x]$.*
2. *En $\mathbb{Z}_2[x]$, $a(x) = x^3 + x^2 + x + 1$ es reducible ya que $a(1) = 0$, de lo que se deduce que $a(x) = (x - 1)q(x)$. Sin embargo, $b(x) = x^2 + x + 1$ es irreducible porque $b(0), b(1) \neq 0$.*
3. *$x^4 + 3x^2 + 2 = (x^2 + 2)(x^2 + 1)$ es reducible en $\mathbb{R}[x]$, aunque no tiene raíces en $\mathbb{R}$.*
4. *El polinomio $x^4 + 1$ no tiene raíces en $\mathbb{Z}_3$, por lo que la única posible factorización sería como producto de dos polinomios de grado 2, $x^4 + 1 = (x^2 + \alpha x + \beta)(x^2 + \mu x + \delta)$. Las ecuaciones que se obtienen de la igualdad de los polinomios anteriores, permiten calcular los coeficientes: $\alpha = 1, \beta = 2, \mu = 2, \delta = 2$. Por lo tanto $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$ y es reducible en $\mathbb{Z}_3[x]$.*
5. *El polinomio $b(x) = x^4 + x^3 + x^2 + x + 1$ tampoco tiene raíces en $\mathbb{Z}_3$, la posible factorización sería como producto de dos polinomios de grado 2, $x^4 + x^3 + x^2 + x + 1 = (x^2 + \alpha x + \beta)(x^2 + \mu x + \delta)$. Pero el sistema de ecuaciones que se obtiene de la igualdad de los polinomios anterior no tiene solución en $\mathbb{Z}_3$, por lo que $b(x)$ es irreducible en $\mathbb{Z}_3[x]$.*

Siguiendo el paralelismo con $\mathbb{Z}$, también en $K[x]$ todo polinomio no constante se puede expresar como producto de una constante (su coeficiente principal) por polinomios mónicos irreducibles de una única forma, salvo el orden de los factores. Igualmente, el mcd y el mcm de polinomios puede obtenerse a partir de la factorización de éstos en irreducibles.

3.9 Cuerpos finitos

Se pueden construir cuerpos finitos siguiendo el mismo procedimiento que en la construcción de $(\mathbb{Z}_p, +, \cdot)$, con p un número primo, pero partiendo del anillo de polinomios.

Observación 3.9.1 *Recordemos que si $I = (p(x))$ es un ideal de $K[x]$ con $p(x)$ un polinomio mónico de grado $\partial p(x)$, los elementos del anillo cociente $K[x]/(p(x))$ son las clases de equivalencia de la relación definida en $K[x]$ por $a(x) \sim b(x) \Leftrightarrow a(x) - b(x) \in (p(x)) \Leftrightarrow a(x), b(x)$ dan el mismo resto al dividirlos por $p(x)$.*

Consideremos el subconjunto de $K[x]$ formado por los posibles restos al dividir un polinomio por $p(x)$,

$$R = \{a(x) \in K[x]/\partial a(x) < \partial p(x)\}.$$

Consideremos la aplicación $K[x]/(p(x)) \xrightarrow{f} R$ dada por $f([a(x)]) = r(x)$ siendo $r(x)$ el resto de dividir $a(x)$ por $p(x)$. Se verifica que f es una aplicación biyectiva. En efecto,

1. *f esta bien definida: $[a(x)] = [b(x)] \Leftrightarrow a(x) \sim b(x) \Leftrightarrow a(x), b(x)$ tienen el mismo resto al dividirlos por $p(x)$. Luego $f([a(x)]) = f([b(x)])$.*
2. *f es inyectiva: $f([a(x)]) = f([b(x)]) \Leftrightarrow a(x), b(x)$ tienen el mismo resto al dividirlos por $p(x) \Leftrightarrow a(x) \sim b(x) \Leftrightarrow [a(x)] = [b(x)]$.*
3. *f es sobreyectiva: Dado $r(x) \in K[x]/(p(x))$ consideramos la clase del propio polinomio $r(x)$ en $K[x]/(p(x))$ y tenemos que $f([r(x)]) = r(x)$.*

En consecuencia $K[x]/(p(x))$ y R tienen el mismo cardinal y se podrían identificar al conjunto K^n, siendo $n = \partial p(x)$ (usando que $R = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1},\ a_i \in K\}$).

Al igual que sucede en $\mathbb{Z}_n$, los elementos de $K[x]/(p(x))$ son inversibles o son divisores de cero según sean primos con $p(x)$ como pone de manifiesto la siguiente proposición

Proposición 3.9.2 *Sea $[a(x)] \in K[x]/(p(x))$, se verifica que,*

1. *si $mcd(a(x), p(x)) = 1$ entonces $[a(x)]$ es unidad en el anillo $K[x]/(p(x))$.*
2. *Si $mcd(a(x), p(x)) \neq 1$ entonces $[a(x)]$ es un divisor de cero en el anillo $K[x]/(p(x))$.*

(Demostración similar al caso $\mathbb{Z}_n$).

Corolario 3.9.3 *El anillo cociente $K[x]/(q(x))$ es un cuerpo si y sólo si $q(x)$ es un polinomio irreducible. En ese caso, su característica coincide con la característica de K.*

Demostración. La primera afirmación se prueba de forma análoga al caso $\mathbb{Z}_n$. La característica de $K[x]/(q(x))$ coincide con la característica del cuerpo K pues para todo natural n se verifica que $n \cdot [1_K] = [0_K]$ si y sólo si $n \cdot 1_K = 0_K$.

Podemos describir la construcción de cuerpos finitos cuyo cardinal sea distinto de un número primo. Consideramos como cuerpo base $\mathbb{Z}_p$, siendo p es un número primo y q(x) un polinomio irreducible de grado n con coeficientes en $\mathbb{Z}_p$. Por lo visto anteriormente el anillo cociente $F = \mathbb{Z}_p[x]/(q(x))$ tiene estructura de cuerpo, su cardinal es p^n y su característica es p.

Todo cuerpo finito F tiene la estructura descrita en el párrafo anterior. Es decir, si F es un cuerpo finito, su caracteristica es un número primo p y su cardinal es un potencia de p, siendo F isomorfo a un cuerpo $\mathbb{Z}_p[x]/(q(x))$ con $q(x)$ un polinomio irreducible de grado n.

Ejemplo 3.9.1 *1. $p(x) = x^2 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$, el cuerpo $\mathbb{Z}_2[x]/(p(x))$ tiene $2^2 = 4$ elementos que son de la forma $ax + b$ con $a, b \in \mathbb{Z}_2$, $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, 1 + x\}$.*

Teniendo en cuenta que $x^2 + x + 1 = 0$ en el anillo cociente, se pueden facilitar los cálculos en el cociente. Por ejemplo, $x^2 + 1 = -x = x$, entonces $(x + 1)(x + 1) = x^2 + 1 = x$.

2. El mismo polinomio $p(x) = x^2+x+1$ no es irreducible en $\mathbb{Z}_3[x]$, de hecho, $p(1) = 0$ y $p(x) = (x-1)^2$. El anillo cociente $\mathbb{Z}_3[x]/(x^2 + x + 1)$ no es un cuerpo, como lo demuestra, entre otras cosas que $(x - 1)(x - 1) = p(x) = 0$. Aunque algunos elementos tienen inverso, por ejemplo, $(x + 1)$ ya que $(x + 1)2x = 2x^2 + 2x = 1$ en $\mathbb{Z}_3[x]/(x^2 + x + 1)$.