Capítulo 3

Cuerpos finitos

En este capítulo vamos a construir cuerpos con un número finito de elementos. Esta construcción toma como base polinomios con coeficientes en $\mathbb{Z}_p$, con p un número primo. Antes de continuar, recordamos qué es un cuerpo.

Sea A un conjunto no vacío. Decimos que A tiene estructura de anillo conmutativo si en A tenemos definidas dos operaciones:

$$\begin{array}{ccc} A \times A & \xrightarrow{+} & A \\ (a,b) & \mapsto & a+b \end{array} \qquad\qquad \begin{array}{ccc} A \times A & \xrightarrow{\cdot} & A \\ (a,b) & \mapsto & a \cdot b \end{array}$$

denominadas respectivamente suma y producto, y que satisfacen las siguientes propiedades:

i) Para cualesquiera $a, b, c \in A$ se tiene que $(a+b)+c = a+(b+c)$.

ii) Para cualesquiera $a, b \in A$ se tiene que $a+b = b+a$.

iii) Existe un elemento $0 \in A$ tal que $a+0 = a$ para cualquier $a \in A$.

iv) Para cualquier $a \in A$ existe un elemento $b \in A$ tal que $a+b = 0$.

v) Para cualesquiera $a, b, c \in A$ se tiene que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

vi) Para cualesquiera $a, b \in A$ se tiene que $a \cdot b = b \cdot a$.

vii) Existe un elemento $1 \in A$ tal que $a \cdot 1 = a$ para cualquier $a \in A$.

viii) Para cualesquiera $a, b, c \in A$ se tiene que $a \cdot (b+c) = a \cdot b + a \cdot c$.

Si además, se cumple la propiedad adicional:

ix) Para cualquier $a \in A$, $a \neq 0$ existe un elemento b tal que $a \cdot b = 1$

se dice que A tiene estructura de cuerpo.

Son ejemplos de anillos conmutativos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_n$, con $n \geq 2$. De todos estos, son cuerpos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$, con p un número primo.

Aunque en $\mathbb{N}$ también tenemos definidas una suma y un producto, $\mathbb{N}$ no es un anillo conmutativo, pues falla la propiedad iv).

La propiedad iv) nos habla de la existencia de un elemento $b \in A$ para cualquier $a \in A$ tal que $a+b = 0$. Hay un único elemento que cumple esa propiedad, y a ese elemento se le denomina *opuesto* de a, y se le suele denotar como $-a$.

De la misma forma, al elemento que nos define la propiedad ix) se le llama *inverso* de a, y se le denota como a^{-1}.

En un anillo conmutativo A, a los elementos que tienen inverso (es decir, elementos $a \in A$ para los que existe un elemento $b \in A$ tal que $a \cdot b = 1$) se les llama unidades.

Dados $a, b \in A$, escribiremos $a - b$ en lugar de $a + (-b)$.

A partir de la definición de anillo, se pueden deducir algunas propiedades, de todos conocidas:

1. $a \cdot 0 = 0$ sea quien sea $a \in A$.

2. (Regla de los signos) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ y $(-a) \cdot (-b) = a \cdot b$.
3. $-(a - b) = b - a$.

De manera informal, podríamos decir que un anillo es un conjunto en el que podemos sumar, restar y multiplicar, con las propiedades usuales respecto a esas operaciones. Si además el producto es conmutativo, hablamos de un anillo conmutativo. Un cuerpo es un conjunto en el que podemos sumar, restar, multiplicar y dividir (salvo por cero).

3.1. Generalidades sobre polinomios

Definición 44. *Sea A un anillo conmutativo, y x un elemento que no pertenece a A. Un polinomio con coeficientes en A es una expresión de la forma*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde $n \in \mathbb{N}$ y $a_k \in A$.

Ejemplo 3.1.1. *Son polinomios con coeficientes en $\mathbb{Z}$*

$$2x^2 + 3x + (-1); \quad 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$$

En el primer caso $n = 2$, $a_2 = 2$, $a_1 = 3$ y $a_0 = -1$, mientras que en el segundo $n = 5$ y $a_5 = a_4 = a_3 = a_2 = a_1 = a_0 = 2$.

No son polinomios con coeficientes en $\mathbb{Z}$

$$3x^2 - x + 2 + x^{-1}; \quad sen(x) - 3$$

Nota: La definición que se ha dado no es muy rigurosa. De hecho, con esa definición, la expresión $x^2 + 1$ no es un polinomio, pues no se ajusta a lo explicitado en dicha definición, ya que no está dicho quien es a_1 ni a_2. Sí es un polinomio, de acuerdo con la definición dada $1x^2 + 0x + 1$. Obviamente, al referirnos al polinomio $1x^2 + 0x + 1$ lo haremos como $x^2 + 1$. De la misma forma, el primer polinomio que aparece en el ejemplo anterior lo escribiremos $2x^2 + 3x - 1$.

En general, si $a_k x^k + \cdots + a_1 x + a_0$ es un polinomio y $a_i = 0$, entonces el polinomio dado diremos que es igual a $a_k x^k + \cdots + a_{i+1} x^{i+1} + a_{i-1} x^{i-1} + \cdots + a_0$ (salvo que el polinomio de partida sea 0).

Tampoco se ajusta a la definición que hemos dado de polinomio, por ejemplo, la expresión $5+2x+3x^2$. Deberíamos escribir $3x^2 + 2x + 5$.

En lo que sigue no tendremos en cuenta estas deficiencias de la definición dada.

Dado un anillo A denotaremos por $A[x]$ al conjunto de todos los polinomios con coeficientes en A.

Definición 45. *Sea A un anillo.*

1. *Sean $p(x) = a_m x^m + \cdots + a_1 x + a_0$ y $q(x) = b_n x^n + \cdots + b_1 x + b_0$ dos elementos de $A[x]$, y supongamos que $m \leq n$. Se define la suma de los polinomios $p(x)$ y $q(x)$ como el polinomio*

$$p(x) + q(x) = b_n x^n + \cdots + b_{m+1} x_{m+1} + (a_m + b_m) x^m + \cdots + (a_1 + b_1) x + (a_0 + b_0)$$

2. *Sea $k \in \mathbb{N}$, $p(x) = a_m x^m + \cdots + a_1 x + a_0$, $q(x) = b_k x^k \in A[x]$ (si $k = 0$ entonces $q(x) = b_0$). Se define el producto de $p(x)$ y $q(x)$ como el polinomio:*

$$p(x) \cdot q(x) = a_n b_k x^{k+n} + \cdots + a_1 b_k x^{k+1} + a_0 b_k x^k$$

Sean ahora $p(x) = a_m x^m + \cdots + a_1 x + a_0$ y $q(x) = b_n x^n + \cdots + b_1 x + b_0$. Se define el producto de $p(x)$ y $q(x)$ como

$$p(x) \cdot q(x) = p(x) \cdot q_n(x) + \cdots + p(x) \cdot q_1(x) + p(x) \cdot q_0(x)$$

donde $q_k(x) = b_k x^k$.

Las dos operaciones definidas satisfacen las siguientes propiedades:

- La suma de polinomios es asociativa, es decir, $p(x) + (q(x) + r(x)) = p(x) + q(x)) + r(x)$. Nótese que esta propiedad es necesaria para poder definir el producto tal y como se ha hecho aquí.
- La suma de polinomios es conmutativa.
- La suma tiene un elemento neutro. Éste será denotado por 0.
- Dado $p(x) \in A[x]$ existe $q(x) \in A[x]$ tal que $p(x) + q(x) = 0$. Denotaremos como $-p(x)$ a este polinomio.
- El producto de polinomios es asociativo y conmutativo.
- El producto tiene un elemento neutro. Éste será denotado por 1.
- La suma es distributiva con respecto al producto.

Estas propiedades nos dicen que, si A es un anillo conmutativo, entonces $A[x]$ es también un anillo conmutativo.

Además, podemos identificar A como los elementos de $A[x]$ de la forma $p(x) = a$, en cuyo caso A es un subanillo de $A[x]$.

Ejemplo 3.1.2. *Sea* $A = \mathbb{Z}_{12}$*, y sean* $p(x) = 2x^3 + 3x^2 + 7x + 9$ *y* $q(x) = 6x^2 + 5x + 4$*. Entonces:*

$* \; p(x) + q(x) = 2x^3 + (3+6)x^2 + (7+5)x + (9+4) = 2x^3 + 9x^2 + 1$

$$\begin{aligned} * \; p(x) \cdot q(x) &= p(x) \cdot (6x^2) + p(x) \cdot (5x) + p(x) \cdot 4 \\ &= (0x^5 + 6x^4 + 6x^3 + 6x^2) + (10x^4 + 3x^3 + 11x^2 + 9x) + (8x^3 + 0x^2 + 4x + 0) \\ &= 4x^4 + 5x^3 + 5x^2 + x \end{aligned}$$

Normalmente, para efectuar la multiplicación dispondremos los datos de la siguiente forma:

$p(x)$			2	3	7	9
$q(x)$				6	5	4
$p(x) \cdot 4$			8	0	4	0
$p(x) \cdot 5x$		10	3	11	9	
$p(x) \cdot 6x^2$	0	6	6	6		
$p(x) \cdot q(x)$	0	4	5	5	1	0

luego el resultado final es $4x^4 + 5x^3 + 5x^2 + x$*.*

Daremos a continuación algunos conceptos referentes a los polinomios:

Definición 46. *Sea* A *un anillo conmutativo y* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$*.*

i) Si $a_n \neq 0$ *entonces se dice que el polinomio* $p(x)$ *tiene* **grado** n *(*$gr(p(x)) = n$*). Nótese que no se ha definido el grado del polinomio* 0*. En ocasiones, consideraremos que el grado del polinomio* 0 *es* -1*.*

ii) Al elemento $a_k \in A$ *se le llama* **coeficiente de grado k***, y a la expresión* $a_k x^k$*,* **término de grado k***.*

iii) El coeficiente de grado n *de un polinomio de grado* n *se llama* **coeficiente líder***, y a la expresión* $a_n x^n$ **término líder***.*

iv) El coeficiente de grado 0 *de un polinomio se le llama* **término independiente***.*

v) Un polinomio cuyo coeficiente líder valga 1 *se dice que es un* **polinomio mónico***.*

vi) Un polinomio que, bien tiene grado 0*, o bien es el polinomio* 0 *se dice que es un* **polinomio constante***.*

Ejemplo 3.1.3. *Sean* $p(x) = 3x^3+5x+2$ *y* $q(x) = x^4+2x^3+3x^2+5x+8$ *dos polinomios con coeficientes en* $\mathbb{Z}_{11}$*. Entonces:*

- $gr(p(x)) = 3$ *y* $gr(q(x)) = 4$*.*

- El coeficiente de grado 2 *de* $p(x)$ *es* 0*, mientras que el coeficiente de grado* 2 *de* $q(x)$ *es* 3*. El coeficiente de grado* 5 *de* $q(x)$ *es cero.*

- El coeficiente líder de $p(x)$ *es* 3*, mientras que el coeficiente líder de* $q(x)$ *es* 1*. Por tanto,* $q(x)$ *es mónico, mientras que* $p(x)$ *no lo es.*

- Los términos independientes de $p(x)$ *y* $q(x)$ *son* 2 *y* 8 *respectivamente.*

- Ninguno de los dos polinomios son constantes.

Proposición 3.1.1. *Sean* $p(x), q(x) \in A[x]$*. Entonces:*

$$gr(p(x) + q(x)) \leq máx\{gr(p(x), q(x)\}$$

$$gr(p(x) \cdot q(x)) \leq gr(p(x)) + gr(q(x))$$

La demostración de ambos hechos es fácil. Podría pensarse que en el segundo caso se da siempre la igualdad ($gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$). Sin embargo, el Ejemplo 3.1.2 nos muestra un caso en el que se da la desigualdad estricta.

Es fácil comprobar que si $p(x)$ o $q(x)$ es mónico, entonces se verifica que $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$.

Terminamos esta sección estudiando la evaluación de un polinomio en un punto.

Definición 47. *Sea* A *un anillo,* $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ *y* $a \in A$*. Se define la evaluación de* $p(x)$ *en el punto* a*,* $Ev_a(p(x))$ *como el elemento de* A*:*

$$Ev_a(p(x)) = a_n a^n + \cdots + a_1 a + a_0$$

Dicho de otra forma, $Ev_a(p(x))$ es el resultado de sustituir en la expresión de $p(x)$ el símbolo x por a. De esta forma tenemos definida una aplicación (morfismo de anillos) $Ev_a : A[x] \to A$.

Normalmente, escribiremos $p(a)$ en lugar de $Ev_a(p(x))$.

Proposición 3.1.2. *Dado* A *un anillo y* $p_1(x), p_2(x) \in A[x]$

1. *Si* $q(x) = p_1(x) + p_2(x)$ *entonces* $q(a) = p_1(a) + p_2(a)$ *(es decir,* $Ev_a(p_1(x) + p_2(x)) = Ev_a(p_1(x)) + Ev_a(p_2(x))$*).*

2. *Si* $q(x) = p_1(x) \cdot p_2(x)$ *entonces* $q(a) = p_1(a) \cdot p_2(a)$ *(es decir,* $Ev_a(p_1(x) \cdot p_2(x)) = Ev_a(p_1(x)) \cdot Ev_a(p_2(x))$*).*

Usando la aplicación evaluación, cada polinomio de $A[x]$ determina una aplicación $A \to A$, dada por $a \mapsto p(a)$.

Ejemplo 3.1.4.

1. *El polinomio* $x^3 + 3x^2 + 2x + 2 \in \mathbb{Z}_5[x]$ *determina la aplicación* $\mathbb{Z}_5 \to \mathbb{Z}_5$ *siguiente:*

$$0 \mapsto 2 \quad 1 \mapsto 3 \quad 2 \mapsto 1 \quad 3 \mapsto 2 \quad 4 \mapsto 2$$

2. *El polinomio* $x^2 + x + 1 \in \mathbb{Z}_2[x]$ *determina la aplicación*

$$0 \mapsto 1 \qquad 1 \mapsto 1$$

es decir, la aplicación constante 1*.*

3.2. Máximo común divisor y mínimo común múltiplo

Definición 48. *Sean $p(x), q(x) \in A[x]$. Se dice que $p(x)$ divide a $q(x)$, o que $q(x)$ es múltiplo de $p(x)$, y escribiremos $p(x)|q(x)$, si existe $c(x) \in A[x]$ verificando que $q(x) = p(x) \cdot c(x)$.*

Ejemplo 3.2.1.

1. *En $\mathbb{Z}_2[x]$ se verifica que $(x+1)|(x^2+1)$, ya que $x^2+1 = (x+1)(x+1)$.*
2. *En $\mathbb{Z}_3[x]$ se verifica que $(x+1) \not| (x^2+1)$, pues si $x^2+1 = (x+1) \cdot c(x)$, entonces $gr(c(x)) = 1$, luego $c(x) = c_1x + c_0$. Operando resulta que $c_0 = 1$, $c_0 + c_1 = 0$ y $c_1 = 1$, lo cual es imposible.*
3. *En $\mathbb{Z}_4[x]$ se verifica que $(x+2)|(2x^2+x+2)$, pues $2x^2+x+2 = (x+2)(2x+1)$ y $(2x^2+x+2)|(x+2)$ pues $x+2 = (2x^2+x+2)(2x+1)$.*
4. *Para cualquier $p(x) \in A[x]$ se verifica que $1|p(x)$ y $p(x)|0$.*

En lo que sigue nos centraremos en polinomios con coeficientes en $\mathbb{Z}_p$, con p un número primo. Notemos que en todos los casos, el anillo de coeficientes es un cuerpo.

Veamos a continuación algunas propiedades referentes a la relación de divisibilidad de polinomios.

Proposición 3.2.1. *Sea K un cuerpo y $p(x), q(x), r(x) \in K[x]$. Entonces:*

1. *$1|p(x)$ y $p(x)|0$.*
2. *$p(x)|p(x)$.*
3. *Si $p(x)|q(x)$ y $q(x)|p(x)$, entonces existe $a \in K^*$ tal que $q(x) = a \cdot p(x)$.*
4. *Si $p(x)|q(x)$ y $q(x)|r(x)$, entonces $p(x)|r(x)$.*
5. *Si $p(x)|q(x)$ y $p(x)|r(x)$, entonces $p(x)|(q(x) + r(x))$.*
6. *Si $p(x)|q(x)$, entonces $p(x)|q(x) \cdot r(x)$ para cualquier $r(x) \in K[x]$.*

La demostración de estas propiedades es casi inmediata.

Teorema 3.2.1 (Algoritmo de la división)**.** *Sea K un cuerpo, y $p(x), q(x)$ dos polinomios de $K[x]$, con $q(x) \neq 0$. Entonces existen únicos polinomios $c(x), r(x) \in K[x]$ tales que:*

$p(x) = q(x) \cdot c(x) + r(x)$

$r(x) = 0$ *o* $gr(r(x)) < gr(q(x))$.

Los polinomios $c(x)$ y $r(x)$ son llamados cociente y resto respectivamente.

Demostración:
Vamos a dar una indicación de como sería la demostración de existencia.
Supongamos que $gr(q(x)) = m$ y que b_m es el coeficiente líder de $q(x)$.
Distingamos dos casos:

- $gr(p(x)) < m$. En tal caso, basta tomar $c(x) = 0$ y $r(x) = p(x)$.
- $gr(p(x)) \geq m$. Llamemos entonces n al grado de $p(x)$ y sea a_n su coeficiente líder. Sea entonces $c_1(x) = a_n \cdot (b_m)^{-1}x^{n-m}$ y $p_1(x) = p(x) - q(x) \cdot c_1(x)$. Se tiene entonces que:

- $p(x) = q(x) \cdot c_1(x) + p_1(x)$. Esto es evidente por cómo hemos definido $p_1(x)$.
- $gr(p_1(x)) < gr(p(x))$ o $p_1(x) = 0$. Esto es así porque el término líder de $q(x) \cdot c_1(x)$ vale $-a_n x^n$. Por tanto, al hacer la resta $p(x) - q(x) \cdot c_1(x)$, el coeficiente líder de $p(x)$ se anula con el coeficiente líder de $q(x) \cdot c_1(x)$.

Si ahora $gr(p_1(x)) < m$ (o $p_1(x) = 0$), ya hemos terminado. Basta tomar $c(x) = c_1(x)$ y $r(x) = p_1(x)$. En caso contrario, repetimos con $p_1(x)$ el mismo proceso que con $p(x)$.

Obtenemos así dos polinomios $p_2(x)$ y $c_2(x)$ tales que $p_1(x) = q(x) \cdot c_2(x) + p_2(x)$ y $gr(p_2(x)) < gr(p_1(x))$ o $p_2(x) = 0$. En tal caso, se tiene que:

$$p(x) = q(x) \cdot c_1(x) + p_1(x) = q(x) \cdot c_1(x) + q(x) \cdot c_2(x) + p_2(x) = q(x) \cdot (c_1(x) + c_2(x)) + p_2(x)$$

Obtenemos así dos sucesiones de polinomios $c_1(x), c_2(x), \cdots c_k(x)$ y $p_1(x), p_2(x), \cdots, p_k(x)$ satisfaciendo

- $p(x) = q(x) \cdot (c_1(x) + c_2(x) + \cdots + c_k(x)) + p_k(x)$
- $p_k(x) = 0$ ó $gr(p_k(x)) < gr(p_{k-1}(x)) < \cdots < gr(p_1(x)) < gr(p(x))$.

Este proceso lo continuamos hasta que $gr(p_k(x))$ sea menor que m o $p_k(x)$ sea igual al polinomio cero. En tal caso, basta tomar $c(x) = c_1(x) + \cdots + c_k(x)$ y $r(x) = p_k(x)$.

La demostración de la unicidad se deja como ejercicio.

■

Nótese que si en lugar de considerar un cuerpo consideramos un anillo conmutativo cualquiera, y $p(x), q(x)$ son dos polinomios tales que el coeficiente líder de $q(x)$ es una unidad, entonces podría repetirse la demostración.

Por tanto, si $p(x), q(x) \in A[x]$ y $q(x)$ es mónico, existe únicos $c(x), r(x) \in A[x]$ tales que $p(x) = q(x) \cdot c(x) + r(x)$, y $gr(r(x)) < gr(q(x))$ o $r(x) = 0$.

Ejemplo 3.2.2. *Calculemos el cociente y el resto de la división del polinomio* $p(x) = 2x^4 + 3x^3 + 5x + 1$ *entre* $q(x) = 3x^3 + x + 6$ *en* $\mathbb{Z}_7[x]$. *Lo haremos siguiendo los pasos hechos en la demostración precedente.*

Notemos en primer lugar que $gr(p(x)) > gr(q(x))$.

Calculamos 3^{-1}. *Se tiene que* $3^{-1} = 5$.

Tomamos entonces el polinomio $c_1(x) = 2 \cdot 5 \cdot x^{4-3} = 3x$.

Hallamos $p_1(x) = p(x) - 3xq(x) = p(x) + 4xq(x) = 3x^3 + 4x^2 + x + 1$.

Dado que $gr(p_1(x)) \geq gr(q(x))$ *continuamos dividiendo. Tomamos el polinomio* $c_2(x) = 3 \cdot 5x^{3-3} = 1$

Hallamos $p_2(x) = p_1(x) - 1q(x) = p_1(x) + 6q(x) = 4x^2 + 2$.

Dado que $gr(p_2(x)) < gr(q(x))$ *la división ha terminado. El cociente es* $c(x) = c_1(x) + c_2(x) = 3x + 1$ *y el resto* $r(x) = 4x^2 + 2$.

Los cálculos podemos disponerlos como sigue:

2	3	0	5	1	|	3	0	1	6
5	0	4	3			3	1		
	3	4	1	1					
	4	0	6	1					
		4	0	2					

Vamos a continuación a detallar un algoritmo para realizar la división de polinomios. Dicho algoritmo se conoce como *algoritmo de Horner.*

Algoritmo de Horner:

Para explicar el algoritmo vamos a tomar $p(x) = x^5 - 2x^4 + 3x^3 - 5x^2 + 4x - 3$ y $q(x) = x^3 - 3x^2 + 2x - 5$ polinomios con coeficientes en $\mathbb{Q}$, y vamos a realizar la división de $p(x)$ entre $q(x)$. Disponemos los coeficientes como sigue:

	a_n	a_{n-1}	$\cdots$	a_1	a_0
$-b_{m-1}$					
$\vdots$					
$-b_1$					
$-b_0$					

En nuestro caso, tendríamos:

	1	-2	3	-5	4	-3
3						
-2						
5						

Sumamos los elementos de la segunda columna (en este caso sólo hay uno), y colocamos el resultado en la última fila.

	1	-2	3	-5	4	-3
3						
-2						
5						
	1					

Multiplicamos este elemento por cada uno de los de la primera columna, y los colocamos a partir de la tercera columna, en diagonal.

	1	-2	3	-5	4	-3
3		**3**				
-2			$\mathbf{-2}$			
5				**5**		
	1					

Sumamos los elementos de la tercera columna, y el resultado lo colocamos en la última fila.

	1	-2	3	-5	4	-3
3		3				
-2			-2			
5				5		
	1	**1**				

Y ahora multiplicamos este elemento por los de la primera columna y comenzamos a colocar los resultados a partir de la cuarta columna.

	1	-2	3	-5	4	-3
3		3	**3**			
-2			-2	$\mathbf{-2}$		
5				5	**5**	
	1	1				

Repetimos el proceso. Sumamos los elementos de la cuarta columna, y el resultado lo colocamos en la última fila.

	1	-2	3	-5	4	-3
3		3	3			
-2			-2	-2		
5				5	5	
	1	1	**4**			

Y multiplicamos por los elementos de la primera columna. Los resultados los situamos a partir de la quinta.

	1	−2	3	−5	4	−3
3		3	3	**12**		
−2			−2	−2	**−8**	
5				5	5	**20**
	1	1	4			

Puesto que ya hemos llegado a la columna de la derecha, sólo nos queda sumar los elementos de las columnas de la derecha.

	1	−2	3	−5	4	−3
3		3	3	12		
−2			−2	−2	−8	
5				5	5	20
	1	1	4	**10**	**1**	**17**

Y ya hemos terminado. Estos últimos resultados constituyen los coeficientes del resto. Los demás elementos de la última fila constituyen los coeficientes del cociente. Por tanto, tenemos que:

$$c(x) = x^2 + x + 4; \qquad r(x) = 10x^2 + x + 17$$

En el caso de que el divisor no sea un polinomio mónico, hay que incluir una pequeña variante. Al colocar los coeficientes del divisor, hemos de multiplicar cada uno por el inverso de su coeficiente líder (además de cambiarlos de signo). Y una vez finalizado el algoritmo, el cociente que nos resulte hemos de multiplcarlo también por este inverso. Para recordar este inverso, lo situaremos inicialmente en la esquina superior izquierda de la tabla.

Por ejemplo, vamos a realizar la división del polinomio $p(x) = 6x^4 - 7x^3 - 10x^2 + 9x - 3$ entre $q(x) = 2x^2 + x - 3$.

La situación de partida es:

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$					
$\frac{3}{2}$					

Y ahora vamos completando la tabla al igual que antes:

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$					
$\frac{3}{2}$					
	6				

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$		−3			
$\frac{3}{2}$			9		
	6				

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$		−3			
$\frac{3}{2}$			9		
	6	−10			

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$		−3	5		
$\frac{3}{2}$			9	−15	
	6	−10			

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$		−3	5		
$\frac{3}{2}$			9	−15	
	6	−10	4		

$\frac{1}{2}$	6	−7	−10	9	−3
$\frac{-1}{2}$		−3	5	−2	
$\frac{3}{2}$			9	−15	6
	6	−10	4	−8	3

Y ahora, el cociente hay que multiplicarlo por el inverso del coeficiente líder del divisor (que está calculado arriba a la izquierda). Por tanto, nos quedaría:

$$c(x) = \frac{1}{2}(6x^2 - 10x + 4) = 3x^2 - 5x + 4, \quad \text{y} \quad r(x) = -8x + 3.$$

Vamos por último a hacer un ejemplo de una división de dos polinomios con coeficientes en $\mathbb{Z}_7$. El procedimiento es el mismo. Los polinomios son $p(x) = 2x^5 + 4x^3 + 5x^2 + 3x + 2$ y $q(x) = 3x^3 + x^2 + 5$.

El inverso del coeficiente líder del divisor es $3^{-1} = 5$. Ahora multiplicamos los opuestos del resto de coeficientes por 5, y obtenemos $(-1) \cdot 5 = 6 \cdot 5 = 2$ y $(-5) \cdot 5 = 2 \cdot 5 = 3$. Por tanto, comenzamos el algoritmo con la siguiente tabla:

5	2	0	4	5	3	2
2						
0						
3						

Y ahora realizamos la división:

5	2	0	4	5	3	2
2						
0						
3						
	2					

5	2	0	4	5	3	2
2		4				
0			0			
3				6		
	2					

5	2	0	4	5	3	2
2		4				
0			0			
3				6		
	2	4				

5	2	0	4	5	3	2
2		4	1			
0			0	0		
3				6	5	
	2	4				

5	2	0	4	5	3	2
2		4	1			
0			0	0		
3				6	5	
	2	4	5			

5	2	0	4	5	3	2
2		4	1	3		
0			0	0	0	
3				6	5	1
	2	4	5			

5	2	0	4	5	3	2
2		4	1	3		
0			0	0	0	
3				6	5	1
	2	4	5	0	1	3

Luego el cociente es $c(x) = 5 \cdot (2x^2 + 4x + 5) = 3x^2 + 6x + 4$ y el resto es $r(x) = x + 3$.

Si analizamos el estudio que hicimos de los números enteros, podemos ver cómo el algoritmo de la división resultó clave en el desarrollo posterior. A partir de él se pudo probar la existencia de máximo común divisor y calcularlo; encontrar los coeficientes de Bezout, que luego fueron la base para la resolución de congruencias.

Ahora, en $\mathbb{Z}_p[x]$ tenemos también un algoritmo de división, luego todo lo dicho para números enteros vale también para polinomios.

En el capítulo anterior, a partir de un anillo (los números enteros), gracias al algoritmo de la división, construimos, para cada número primo p, un cuerpo que denominamos $\mathbb{Z}_p$.

Ahora, a partir de otro anillo ($\mathbb{Z}_p[x]$), y también apoyándonos en el algoritmo de la división, vamos a construir para cada polinomio irreducible $m(x)$ (que definiremos en su momento), un cuerpo que denominaremos $\mathbb{Z}_p[x]_{m(x)}$.

> **Nota:** Un anillo A, se dice que es un dominio euclídeo si en él tenemos definida una aplicación *grado*, $g : A^* \to \mathbb{N}$ satisfaciendo dos propiedades:
>
> - $g(ab) \geq g(a)$ para $b \neq 0$
> - Para todo $a, b \in A$, $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ y $g(r) < g(a)$ ó $r = 0$.
>
> Es decir, un Dominio Euclídeo viene a ser un anillo en el que tenemos definida una división, con resto.
>
> Tenemos entonces que $\mathbb{Z}$ y $K[x]$ son dominios euclídeos (las funciones grado son, en el caso de $\mathbb{Z}$ el valor absoluto, y en el caso de $K[x]$ el grado).
>
> En un dominio euclídeo se verifica el teorema de Bezout, el teorema chino del resto, el teorema de factorización única, etc.

Definición 49. *Sean $p(x), q(x) \in K[x]$, con $q(x) \neq 0$. Se definen los polinomios $p(x)$ mód $q(x)$ y $p(x)$ div $q(x)$ como el resto y el cociente de dividir $p(x)$ entre $q(x)$.*

Cuando $p(x)$ mód $q(x) = 0$, denotaremos por $\frac{p(x)}{q(x)}$ al polinomio $p(x)$ div $q(x)$.

Ejemplo 3.2.3.

1. *En* $\mathbb{Z}_3[x]$*, se verifica que:*

   $x^5+x^4+2x^3+x^2+x+1$ *mód* $x^2+2x+1=2$
   $x^5+x^4+2x^3+x^2+x+1$ *div* $x^2+2x+1=x^3+2x^2+2$.

2. *En* $\mathbb{Z}_5[x]$*:*

   $x^5+x^4+2x^3+x^2+x+1$ *mód* $x^2+2x+1=6x$
   $x^5+x^4+2x^3+x^2+x+1$ *div* $x^2+2x+1=x^3+4x^2+3x+1$.

Definición 50. *Sea* $p(x)\in K[x]$ *y* $a\in K$*. Se dice que* a *es una raíz de* $p(x)$ *si* $p(a)=0$*.*

Ejemplo 3.2.4. *El polinomio* $p(x)=x^5+x^4+x^3+2x^2+1\in\mathbb{Z}_3[x]$ *tiene a* $x=1$ *por raíz, pues* $p(1)=1+1+1+2+1=0$*. Sin embargo,* 0 *no es raíz pues* $p(0)=1$ *y* 2 *tampoco es raíz pues* $p(2)=2^5+2^4+2^3+2\cdot 2^2+1=2+1+2+2+1=2$*.*

El siguiente resultado es un conocido teorema referente a la división por el polinomio $x-a$.

Teorema 3.2.2 (Teorema del resto)**.** *Sea* $p(x)\in K[x]$ *y* $a\in K$*. Entonces el resto de dividir* $p(x)$ *entre* $x-a$ *es el resultado de evaluar* $p(x)$ *en el punto* a*. Dicho de otra forma*

$$p(x)\ \textit{mód}\ x-a=p(a)$$

Demostración: Si dividimos $p(x)$ entre $x-a$ nos da un polinomio de grado menor que 1, luego debe ser un polinomio constante. Se tiene entonces que $p(x)=c(x)\cdot(x-a)+r$. Evaluando en a nos queda que $p(a)=c(a)\cdot(a-a)+r$, es decir, $r=p(a)$. ■

Corolario 3.2.1 (Teorema del factor)**.** *Sea* $p(x)\in K[x]$ *y* $a\in K$*. Entonces* a *es raíz de* $p(x)$ *si, y sólo si,* $(x-a)|p(x)$*.*

Nota: Si trabajamos con polinomios con coeficientes en un anillo conmutativo cualquiera (por ejemplo, $\mathbb{Z}$, o $\mathbb{Z}_n$ con n un número compuesto), los resultados anteriores son igualmente válidos.

Ejemplo 3.2.5. *Vamos a hallar el cociente y el resto de la división de* $x^5+x^4+x^3+2x^2+1$ *entre* $x+9=x-2$ *en* $\mathbb{Z}_{11}[x]$*. Lo hacemos según el algoritmo de Horner.*

	1	1	1	2	0	1
2						

Tras aplicar el algoritmo, nos quedaría así

	1	1	1	2	0	1
2		2	6	3	10	9
	1	3	7	5	10	10

Nótese que $x^5+x^4+x^3+2x^2+1=(x^4+3x^3+7x^2+5x+10)(x+9)+10$*, y que* $p(2)=10$*.*

Vamos a dividir ahora $x^5+x^4+x^3+2x^2+1$ *entre* $x+1$ *en* $\mathbb{Z}_3[x]$*. Puesto que* $x+1=x-2$*, se tiene que*

	1	1	1	2	0	1
2		2	0	2	2	1
	1	0	1	1	2	2

es decir, el cociente es x^4+x^2+x+2 *y el resto es* 2*.*

Definición 51. *Sea $p(x) \in K[x]$, y $a \in K$. Se dice que a es una raíz de multiplicidad m si $(x-a)^m | p(x)$ y $(x-a)^{m+1} \not| p(x)$.*

Nótese que decir que a es una raíz de multiplicidad m es decir que $p(x) = (x-a)^m c(x)$ con $c(a) \neq 0$.

A las raíces de multiplicidad 1 se les llama raíces simples; a las de multiplicidad 2, raíces dobles, a las de multiplicidad 3, raíces triples, y así sucesivamente.

En ocasiones, si a no es una raíz se dice que es una raíz de multiplicidad 0.

Ejemplo 3.2.6. *El polinomio $x^5+x^3+x^2+1 \in \mathbb{Z}_2[x]$ tiene a $x=1$ como raíz triple, pues $x^5+x^3+x^2+1 = (x+1)^3(x^2+x+1)$, y x^2+x+1 no tiene a 1 como raíz.*

	1	0	1	1	0	1
1		1	1	0	1	1
	1	1	0	1	1	0
1		1	0	0	1	
	1	0	0	1	0	
1		1	1	1		
	1	1	1	0		
1		1	0			
	1	0	1			

Aquí vemos las sucesivas divisiones por $x+1$. Se aprecia como las tres primeras son exactas, mientras que la cuarta da resto 1.

Definición 52. *Sea K un cuerpo, y $p(x), q(x) \in K[x]$. Se dice que $d(x) \in K[x]$ es un máximo común divisor de $p(x)$ y $q(x)$ si:*

1. *$d(x) | p(x)$ y $d(x) | q(x)$.*
2. *Si $c(x) | p(x)$ y $c(x) | q(x)$ entonces $c(x) | d(x)$.*

Nota:

1. La primera condición de la definición nos dice que $d(x)$ debe ser un divisor común de $p(x)$ y $q(x)$. La segunda condición nos dice que este divisor común es el "más grande" de los divisores comunes.

   El máximo común divisor de dos polinomios $p(x)$ y $q(x)$ es entonces un polinomio que es divisor común de ambos polinomios, y que es múltiplo de todos los divisores comunes.

2. Si $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$ y $a \in K^*$ entonces $a \cdot d(x)$ es también un máximo común divisor de $p(x)$ y $q(x)$. De hecho, cualquier polinomio que sea un máximo común divisor de $p(x)$ y $q(x)$ es de la forma $a \cdot d(x)$. De todos estos, hay uno, y sólo uno que es mónico (salvo en el caso de que $p(x) = q(x) = 0$). Denotaremos por $mcd(p(x), q(x))$ al único máximo común divisor de $p(x)$ y $q(x)$ que es mónico.

3. Aquí se ha definido el máximo común divisor de dos polinomios. Podría haberse definido de forma análoga el máximo común divisor de 3 ó más.

Ejemplo 3.2.7. *Sean $p(x) = x^2+4x+4$ y $q(x) = x^2+1$. El polinomio $p(x)$ tiene 12 divisores. Estos son:*

$$1, 2, 3, 4, x+2, 2x+4, 3x+1, 4x+3, x^2+4x+4, 2x^2+3x+3, 3x^2+2x+2, 4x^2+x+1$$

mietras que $q(x)$ tiene 16, que son:

$$1, 2, 3, 4, x+2, 2x+4, 3x+1, 4x+3, x+3, 2x+1, 3x+4, 4x+2, x^2+1, 2x^2+2, 3x^2+3, 4x^2+4$$

El conjunto de los divisores comunes de $p(x)$ y $q(x)$ es:

$$\{1,\ 2,\ 3,\ 4,\ x+2,\ 2x+4,\ 3x+1,\ 4x+3\}$$

De ellos:

- *$x+2$ es múltiplo de todos, pues $x+2 = 1\cdot(x+2)$, $x+2 = 2\cdot(3x+1)$, $x+2 = 3\cdot(2x+4)$, $x+2 = 4\cdot(4x+3)$. Por tanto, $x+2$ es un máximo común divisor de $p(x)$ y $q(x)$.*
- *$2x+4$ es múltiplo de todos, pues $2x+4 = 1\cdot(2x+4)$, $2x+4 = 2\cdot(x+2)$, $2x+4 = 3\cdot(4x+3)$, $2x+4 = 4\cdot(3x+1)$, luego $2x+4$ es también un máximo común divisor de $p(x)$ y $q(x)$.*
- *$3x+1$ es múltiplo de todos, ya que $3x+1 = 1\cdot(3x+1)$, $3x+1 = 2\cdot(4x+3)$, $3x+1 = 3\cdot(x+2)$, $3x+1 = 4\cdot(2x+4)$. También $3x+1$ es un máximo común divisor de $p(x)$ y $q(x)$.*
- *$4x+3$ es múltiplo de todos: $4x+3 = 1\cdot(4x+3)$, $4x+3 = 2\cdot(2x+4)$, $4x+3 = 3\cdot(3x+1)$, $4x+3 = 4\cdot(x+2)$. Es decir, $4x+3$ es un máximo común divisor de $p(x)$ y $q(x)$.*

Vemos entonces que $p(x)$ tiene cuatro polinomios que satisfacen la definición de máximo común divisor. Son $x+2$, $2x+4$, $3x+1$ y $4x+3$. Elegido uno cualquiera de ellos, $d(x)$, podemos ver que los restantes son $2\cdot d(x)$, $3\cdot d(x)$ y $4\cdot d(x)$.

Vemos también que hay uno que es mónico, y es $x+2$. Escribiremos por tanto $mcd(p(x),q(x)) = x+2$.

Se deja como ejercicio dar la definición de mínimo común múltiplo.

Veremos a continuación algunas propiedades referentes al máximo común divisor. Supongamos que tenemos $p(x), q(x), r(x), d(x) \in K[x]$, y supondremos que los cuatro polinomios son mónicos.

Propiedades:

1. $mcd(p(x),q(x)) = mcd(a\cdot p(x), q(x)) = mcd(p(x), a\cdot q(x))$, donde $a \in K^*$.
2. $mcd(p(x),0) = p(x)$ y $mcd(p(x),1) = 1$
3. Si $p(x)|q(x)$ entonces $mcd(p(x),q(x)) = p(x)$.
4. $mcd(p(x), mcd(q(x),r(x)) = mcd(mcd(p(x),q(x)),r(x)) = mcd(p(x),q(x),r(x))$.
5. $mcd(p(x)\cdot r(x), q(x)\cdot r(x)) = mcd(p(x),q(x))\cdot r(x)$
6. Si $d(x)|p(x)$ y $d(x)|q(x)$ entonces $mcd\left(\frac{p(x)}{d(x)}, \frac{q(x)}{d(x)}\right) = \frac{mcd(p(x),q(x))}{d(x)}$.

Los siguientes resultados son análogos a los dados para números enteros.

Lema 3.2.1. *Sean $p(x), q(x) \in K[x]$. Entonces, para cualquier $c(x) \in K[x]$ se tiene que $mcd(p(x),q(x)) = mcd(q(x), p(x) - c(x)q(x))$.*

Corolario 3.2.2. *Sean $p(x), q(x) \in K[x]$, con $q(x) \neq 0$. Entonces $mcd(p(x),q(x)) = mcd(q(x), p(x)\ mód\ q(x))$.*

Para calcular ahora el máximo común divisor de dos polinomios procedemos de igual forma que a la hora de calcular el máximo común divisor de dos números enteros. Vamos realizando divisiones hasta obtener un resto nulo. El resto anterior es el máximo común divisor.

$$\begin{aligned}
p(x) &= q(x)\cdot c_1(x) + r_1(x)\\
q(x) &= r_1(x)\cdot c_2(x) + r_2(x)\\
r_1(x) &= r_2(x)\cdot c_3(x) + r_3(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{i-2}(x) &= r_{i-1}(x)\cdot c_i(x) + r_i(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{k-2}(x) &= r_{k-1}(x)\cdot c_k(x) + r_k(x)\\
r_{k-1}(x) &= r_k(x)\cdot c_{k+1}(x) + 0
\end{aligned}$$

Sin embargo, el polinomio $r_k(x)$ no tiene por qué ser mónico, luego el resultado final, $r_k(x)$, no sería el máximo común divisor de $p(x)$ y $q(x)$. Necesitamos multiplicar por el inverso del coeficiente líder para obtener el máximo común divisor.

El algoritmo EUCLIDES del capítulo anterior vale ahora para el cálculo del máximo común divisor de dos polinomios con coeficientes en un cuerpo. Únicamente, al final hay que multiplicar el resultado por el inverso del coeficiente líder de $p(x)$.

En el caso de que los dos polinomios, $p(x)$ y $q(x)$ fueran nulos, el algoritmo daría error.

Algoritmo EUCLIDES$(p(x), q(x))$

Entrada: $p(x), q(x) \in K[x]$

Salida: $d(x) = mcd(p(x), q(x))$

  Mientras $q(x) \neq 0$

    $(p(x), q(x)) := (q(x), p(x) \text{ mód } q(x))$

$a = c.l.(p(x))^{-1}$.

$p(x) := a \cdot p(x)$.

Devuelve $p(x)$

Ejemplo 3.2.8.

1. *Vamos a calcular el máximo común divisor de los polinomios $p(x)$ y $q(x)$ del ejemplo 3.2.7. Para esto, vamos realizando las divisiones sucesivas hasta que nos dé resto cero.*

   - $x^2 + 4x + 4 = (x^2 + 1)\cdot 1 + 4x + 3$.
   - $x^2 + 1 = (4x + 3)\cdot(4x + 2) + 0$.

   Y al haber obtenido resto cero, tenemos que un máximo común divisor es $4x + 3$ (último resto no nulo). Multiplicamos por el inverso del coeficiente líder (es decir, multiplicamos por 4), y tenemos que $mcd(p(x), q(x)) = 4 \cdot (4x + 3) = x + 2$.

2. *Vamos a calcular en $\mathbb{Z}_5[x]$ el máximo común divisor de $x^3 + 4x + 3$ y $x^3 + x^2 + 1$.*

$$\begin{array}{rcrlcr}
x^3 + 4x + 3 &=& (x^3 + x^2 + 1) & 1 & + & (4x^2 + 4x + 2)\\
x^3 + x^2 + 1 &=& (4x^2 + 4x + 2) & (4x) & + & 2x + 1\\
4x^2 + 4x + 2 &=& (2x + 1) & (2x + 1) & + & 1
\end{array}$$

   Luego el máximo común divisor de $x^3 + 4x + 3$ y $x^3 + x^2 + 1$ es 1.

El teorema de Bezout se tiene también en el caso de los polinomios.

Teorema 3.2.3. *Sean $p(x), q(x) \in K[x]$, y sea $d(x) = mcd(p(x), q(x))$. Entonces existen $u(x), v(x) \in K[x]$ tales que $d(x) = p(x)\cdot u(x) + q(x)\cdot v(x)$*

La demostración del teorema, así como el algoritmo para calcular $u(x)$ y $v(x)$ es análogo al hecho en el caso de los números enteros. Hay que tener en cuenta que al final, hay que multiplicar el resultado por el inverso del coeficiente líder.

Algoritmo BEZOUT$(p(x), q(x))$
Entrada: $p(x), q(x) \in K[x]$
Salida: $(d(x), u(x), v(x))$: $d(x) = mcd(p(x), q(x))$; $d(x) = p(x) \cdot u(x) + q(x) \cdot v(x)$
  Si $q(x) = 0$
    $a := c.l.(p(x))^{-1}$
    Devuelve $(a \cdot p(x), a, 0)$;
    Fin
  $r_{-1}(x) := p(x)$, $r_0(x) := q(x)$.
  $u_{-1}(x) := 1$, $u_0(x) := 0$.
  $v_{-1}(x) := 0$, $v_0(x) := 1$.
  $i := 1$.
  $r_1(x) := r_{-1}(x)$ mód $r_0(x)$
  Mientras $r_i(x) \neq 0$
    $c_i(x) := r_{i-2}(x)$ div $r_{i-1}(x)$.
    $u_i(x) := u_{i-2}(x) - u_{i-1}(x) \cdot c_i(x)$.
    $v_i(x) := v_{i-2}(x) - v_{i-1}(x) \cdot c_i(x)$.
    $i := i + 1$.
    $r_i(x) := r_{i-2}(x)$ mód $r_{i-1}(x)$.
  $a := c.l.(r_{i-1}(x))^{-1}$
  $r(x) := a \cdot r_{i-1}(x)$; $u(x) := a \cdot u_{i-1}(x)$; $v(x) := a \cdot v_{i-1}(x)$.
  Devuelve $(r(x), u(x), v(x))$.
  Fin

Ejemplo 3.2.9.

1. *Vamos a expresar* $mcd(x^3+4x+3, x^3+x^2+1)$ *en función de los polinomios* x^3-x+3 *y* x^3+x^2+1.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		x^3+4x+3		1	0
0		x^3+x^2+1		0	1
1		$4x^2+4x+2$	1	1	4
2		$2x+1$	$4x$	x	$4x+1$
3		1	$2x+1$	$\mathbf{3x^2+4x+1}$	$\mathbf{2x^2+4x+3}$

Aquí vemos cómo se han obtenido las dos últimas columnas:

$1 = 1 - 1 \cdot 0$
$x = 0 - (4x) \cdot 1$
$3x^2 + 4x + 1 = 1 - (2x+1) \cdot x = 1 + (3x+4) \cdot x$

$4 = 0 - 1 \cdot 1$
$4x + 1 = 1 - (4x) \cdot (4)$
$2x^2 + 4x + 3 = 4 - (2x+1) \cdot (4x+1) = 4 + (3x+4) \cdot (4x+1)$

Nótese que se verifica que

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

2. *Sean* $p(x) = x^5 + 2x^4 + x^2 + 2x + 2$, $q(x) = x^5 + 2x^3 + x^2 + x + 1 \in \mathbb{Z}_3[x]$. *Vamos a calcular su máximo común divisor y a exprearlo en función de* $p(x)$ *y* $q(x)$.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		$x^5 + 2x^4 + x^2 + 2x + 2$		1	0
0		$x^5 + 2x^3 + x^2 + x + 1$		0	1
1		$2x^4 + x^3 + x + 1$	1	1	2
2		$2x^2 + 2$	$2x + 2$	$x + 1$	$2x$
3	2	0			
		$\mathbf{x^2 + 1}$		$\mathbf{2x + 2}$	$\mathbf{x}$

Luego $mcd(x^5 + 2x^4 + x^2 + 2x + 2, x^5 + 2x^3 + x^2 + x + 1) = x^2 + 1$ *y*

$$x^2 + 1 = (x^5 + 2x^4 + x^2 + 2x + 2)(2x + 2) + (x^5 + 2x^3 + x^2 + x + 1)(x)$$

En el primer ejemplo, como el último resto distinto de cero es mónico, no ha sido necesario multiplicar por el inverso del coeficiente líder. En el segundo ejemplo, el último resto no nulo era $2x^2 + 2$, *que no es mónico. Por tanto, hemos tenido que multiplicar tanto* $u(x)$ *como* $v(x)$ *por el inverso del coeficiente líder.*

Los Corolarios 2.3.2, 2.3.3 y 2.3.4, así como la Proposición 2.3.1 pueden ahora trasladarse al contexto de polinomios con coeficientes en un cuerpo.

3.3. Factorización de polinomios en $\mathbb{Z}_p[x]$

Para la construcción de los cuerpos finitos, necesitamos el concepto análogo al de número primo en el contexto de polinomios con coeficientes en $\mathbb{Z}_p$.

Comenzamos con la definición de polinomios irreducibles.

Definición 53. *Sea* $p(x) \in K[x]$ *no constante. Se dice que* $p(x)$ *es irreducible si sus únicos divisores son los polinomios constantes (no nulos) y los polinomios de la forma* $a \cdot p(x) : a \in K^*$.
Si $p(x)$ *no es irreducible, se dice que es reducible.*

Observación: Nótese que si $p(x) \in K[x]$ es reducible y $gr(p(x)) = n$ entonces $p(x)$ tiene un divisor no constante, mónico, de grado menor o igual que $\frac{n}{2}$.

Ejemplo 3.3.1.

1. *Cualquier polinomio de grado* 1 *en* $K[x]$ *es irreducible.*
2. *El polinomio* $x^3 + x + 1 \in \mathbb{Z}_2[x]$ *es irreducible. Si fuera reducible, por la observación anterior debería tener un divisor de grado menor o igual que* $\frac{3}{2}$. *Los únicos polinomios en esas condiciones son* x *y* $x + 1$, *y ninguno de ellos divide a* $x^3 + x + 1$.
3. *Dado* $p(x) = ax^2 + bx + c \in \mathbb{R}[x]$ *entonces* $p(x)$ *es irreducible si, y sólo si,* $b^2 - 4ac < 0$.

Al igual que teníamos en $\mathbb{Z}$, tenemos ahora una caracterización de los polinomios irreducibles.

Proposición 3.3.1. *Sea $p(x) \in K[x]$ no constante. Entonces:*

$$p(x) \text{ es irreducible } \iff \big(p(x)|q_1(x)\cdot q_2(x) \Longrightarrow p(x)|q_1(x) \text{ ó } p(x)|q_2(x)\big)$$

Con esta proposición estamos ya en condiciones de dar el teorema de factorización.

Teorema 3.3.1. *Sea K un cuerpo, y $p(x) \in K[x]$ no constante. Entonces $p(x)$ se expresa de forma única como*

$$p(x) = a p_1(x)p_2(x)\cdots p_k(x)$$

donde $a \in K$ y $p_i(x)$ es un polinomio mónico e irreducible.

La demostración es similar a la que se hizo del teorema fundamental de la aritmética.

En $\mathbb{Z}_8[x]$ se tiene que $x^2+7 = (x+1)(x+7) = (x+3)(x+5)$. Vemos entonces que podemos factorizar un polinomio de dos formas distintas. Sin embargo, puesto que $\mathbb{Z}_8$ no es un cuerpo, este ejemplo no está en contradicción con la afirmación de la factorización única que nos da el teorema 3.3.1.

Dado un polinomio $q(x) \in \mathbb{Z}_p[x]$ que no sea una potencia de un polinomio irreducible, existe un algoritmo (algoritmo de Berlekamp) que nos proporciona un divisor propio de este polinomio, caso de existir. Sin embargo, ese algoritmo escapa de los objetivos de estas notas, por lo que no lo estudiaremos aquí. Para factorizar un polinomio, seguiremos el método de ensayo-error.

Si tenemos un número entero, y queremos descomponerlo como producto de números primos, la forma más sencilla para hacerlo (aunque no la más eficiente, especialmente si se trata de números grandes) es ir probando con cada uno de los números primos, para ver si hay alguno que lo divida. Normalmente, comenzamos probando con el primo $p = 2$, si no lo divide seguimos con el primo $p = 3$ y así sucesivamente. En prncipio, habría que seguir hasta que encontremos un divisor primo, o hasta que hayamos llegado a la raíz cuadrada del número a factorizar.

Ahora, si tenemos un polinomio $q(x) \in \mathbb{Z}_p[x]$ de grado n, seguiremos una estrategia análoga. Probaremos por los irreducibles de grado uno, si ninguno lo divide pasaremos a los irreducibles de grado 2, y así sucesivamente, bien hasta que encontremos un divisor irreducible, bien hasta que hayamos probado por todos los irreducibles de grado menor o igual que $\frac{n}{2}$.

Supongamos que tenemos un polinomio $q(x) \in \mathbb{Z}_p[x]$ que queremos factorizar. Como acabamos de comentar, lo primero que hemos de hacer es comprobar si lo divide algún polinomio mónico de grado 1. Los polinomios mónicos de grado 1 son $x, x+1, \cdots, x+(p-1)$. Por tanto, tenemos que comprobar si el resto de la división de $q(x)$ por alguno de estos polinomios vale o no cero. Pero los restos de estas divisiones son respectivamente $q(0),\ q(p-1), \cdots, q(1)$ (ver teorema 3.2.2).

Entonces, lo primero que hemos de hacer para factorizar un polinomio $q(x) \in \mathbb{Z}_p[x]$ es ver si tiene raíces o no.

Ejemplo 3.3.2.

1. *Sea $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Entonces $p(0) = 1$ y $p(1) = 1$. Como $\mathbb{Z}_2 = \{0, 1\}$, el polinomio $p(x)$ no tiene raíces.*

   Con esto, sabemos que el polinomio no tiene divisores de grado 1. Dado que $p(x)$ tiene grado 3 esto es suficiente para asegurarnos que el polinomio es irreducible.

2. *Sea ahora $p(x) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$. Al igual que antes, podemos comprobar que este polinomio no tiene raíces (pues $p(0) = p(1) = 1$). Sin embargo, esto no es suficiente para asegurar que el polinomio sea irreducible (de hecho, este polinomio es reducible, pues $x^4 + x^2 + 1 = (x^2 + x + 1)^2$).*

3. *Sea ahora $p(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$. Ahora se tiene que $p(1) = 0$, luego $x = 1$ es una raíz. Probamos a dividir por $x - 1$.*

$$\begin{array}{c|cccc} & 1 & 0 & 1 & 1 \\ 1 & & 1 & 1 & 2 \\ \hline & 1 & 1 & 2 & 0 \end{array}$$

Luego $p(x) = (x+2)\cdot(x^2+x+2)$. *Puede comprobarse fácilmente que* x^2+x+2 *no tiene raíces, y por ser de grado 2 tendríamos que es irreducible.*

4. *Sea* $p(x) = x^4+3x^3+2x^2+6x+5 \in \mathbb{Z}_7[x]$. *Vamos a encontrar sus raíces. Para eso, vamos a ir probando por los distintos elementos de* $\mathbb{Z}_7$. *Claramente,* $p(0) = 5 \neq 0$.

	1	3	2	6	5
1		1	4	6	5
	1	4	6	5	3

	1	3	2	6	5
2		2	3	3	4
	1	5	5	2	2

	1	3	2	6	5
3		3	4	4	2
	1	6	6	3	0

Luego $x = 3$ *es una raíz, y* $p(x) = (x-3)\cdot(x^3+6x^2+6x+3)$. *Ahora seguimos buscando raíces, pero lo hacemos con el polinomio* x^3+6x^2+6x+3. *Con* $x = 0$, $x = 1$ *y* $x = 2$ *ya no tenemos que probar, pues lo hemos hecho antes.*

	1	6	6	3
3		3	6	1
	1	2	5	4

	1	6	6	3
4		4	5	2
	1	3	4	5

	1	6	6	3
5		5	6	4
	1	4	5	0

Y vemos que $x = 5$ *es otra raíz. Tenemos entonces que* $p(x) = (x-3)\cdot(x-5)\cdot(x^2+4x+5)$. *Continuamos ahora con* x^2+4x+5.

	1	4	5
5		5	3
	1	2	1

	1	4	5
6		6	4
	1	3	2

Y por tanto, $p(x)$ *no tiene más raíces. Tendríamos entonces la siguiente factorización del polinomio* $p(x)$*:*

$$p(x) = (x+4)\cdot(x+2)\cdot(x^2+4x+5).$$

Una vez que hayamos encontrado todas las raíces, y hayamos dividido por los correspondientes factores, nos toca buscar divisores irreducibles de grado 2, continuar con divisores irreducibles de grado 3 y así sucesivamente. Para esto, nos vendría bien tener una lista de estos polinomios irreducibles (de la misma forma que tenemos una lista $2, 3, 5, 7, 11, \cdots$ de los números primos a la que recurrimos cuando queremos factorizar un número entero).

A continuación vamos a dar una lista con los polinomios irreducibles mónicos de grados bajos en $\mathbb{Z}_p[x]$ para valores pequeños de p.

1. **Polinomios irreducibles de** $\mathbb{Z}_2[x]$**.**

   - Grado 1. Aquí, los irreducibles son todos, es decir,
   $$x \qquad x+1.$$
   - Grado 2. Los no irreducibles son x^2, $x(x+1) = x^2+x$ y $(x+1)(x+1) = x^2+1$. El único que queda es
   $$x^2+x+1.$$
   - Grado 3. También aquí los únicos que hay son los que no tienen raíces. Estos son:
   $$x^3+x+1 \qquad x^3+x^2+1.$$
   - Grado 4. Aquí hemos de eliminar todos los que tengan raíces y $(x^2+x+1)^2 = x^4+x^2+1$. Nos quedan entonces tres polinomios, que son:
   $$x^4+x+1 \qquad x^4+x^3+1 \qquad x^4+x^3+x^2+x+1.$$

- Grado 5. Los reducibles son los que tienen raíces y los dos que toman una factorización de la forma (grado 2) · (grado 3). Estos dos son $(x^2+x+1)(x^3+x+1) = x^5+x^4+1$ y $(x^2+x+1)(x^3+x^2+1) = x^5+x+1$.

  Nos quedan entonces 6 polinomios que son:

$$x^5+x^2+1 \qquad x^5+x^3+1 \qquad x^5+x^4+x^3+x^2+1 \qquad x^5+x^4+x^3+x+1$$

$$x^5+x^4+x^2+x+1 \qquad\qquad x^5+x^3+x^2+x+1.$$

2. **Polinomios mónicos irreducibles en $\mathbb{Z}_3[x]$.**

   - Grado 1. Al igual que antes, todos son irreducibles. Tenemos por tanto

$$x \qquad x+1 \qquad x+2.$$

   - Grado 2. Son aquellos que no tiene raíces. Hay un total de 3, que son:

$$x^2+1 \qquad x^2+x+2 \qquad x^2+2x+2.$$

   - Grado 3. Son también los que no tienen raíces. En este caso hay 8.

$$x^3+2x+1 \qquad x^3+2x+2 \qquad x^3+x^2+2 \qquad x^3+2x^2+1$$

$$x^3+x^2+x+2 \qquad x^3+x^2+2x+1 \qquad x^3+2x^2+x+1 \qquad x^3+2x^2+2x+2.$$

   - De grado 4 hay 18 polinomios irreducibles.

3. **Polinomios mónicos irreducibles en $\mathbb{Z}_5[x]$.**

   - Grado 1. Tenemos 5 irreducibles:

$$x \qquad x+1 \qquad x+2 \qquad x+3 \qquad x+4.$$

   - Grado 2. Los que no tienen raíces son 10.

$$x^2+2 \qquad x^2+3 \qquad x^2+x+1 \qquad x^2+x+2 \qquad x^2+2x+3$$

$$x^2+2x+4 \qquad x^2+3x+3 \qquad x^2+3x+4 \qquad x^2+4x+1 \qquad x^2+4x+2.$$

   - Para grados mayores el número de polinomios es muy grande. Así, de grado 3 la lista tendría 40 polinomios, mientras que la de grado 4 sería de 150.

4. **Polinomios mónicos irreducibles en $\mathbb{Z}_7[x]$.**

   - Grado 1. Como siempre aquí son todos irreducibles.

$$x \qquad x+1 \qquad x+2 \qquad x+3 \qquad x+4 \qquad x+5 \qquad x+6.$$

   - Grado 2. Aquí la lista es ya muy grande. Tenemos un total de 21 polinomios.

$$x^2+1 \quad x^2+2 \quad x^2+4 \quad x^2+x+3 \quad x^2+x+4 \quad x^2+x+6 \quad x^2+2x+2$$

$$x^2+2x+3 \quad x^2+2x+5 \quad x^2+3x+1 \quad x^2+3x+5 \quad x^2+3x+6 \quad x^2+4x+1 \quad x^2+4x+5$$

$$x^2+4x+6 \quad x^2+5x+2 \quad x^2+5x+3 \quad x^2+5x+5 \quad x^2+6x+3 \quad x^2+6x+4 \quad x^2+6x+6.$$

   - De grado 3 hay un total de 112 polinomios irreducibles.

Ejemplo 3.3.3.

1. *Sea* $q(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$.

   En primer lugar, buscamos divisores de grado 1. Esto, es equivalente a buscar raíces. En este caso, puesto que $q(0) = q(1) = 1$, *el polinomio no tiene ningún divisor de grado* 1.

   Continuamos buscando divisores de grado 2. El único irreducible de grado 2 es x^2+x+1. *Probamos a dividir entonces* $q(x)$ *por* $x^2 + x + 1$, *y nos queda que* $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$. *Los dos polinomios que aparecen son irreducibles (pues no tienen raíces).*

2. *Sea* $q(x) = x^7 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$. *Entonces:*

   Evaluamos en $x = 0$ *y* $x = 1$. *En ambos casos nos sale* 1, *luego* $q(x)$ *no tiene divisores de grado* 1.

   Dividimos por x^2+x+1, *y nos queda* $q(x) = (x^2+x+1)(x^5+x^4+x+1)+x$. *Por tanto no tiene divisores de grado* 2.

   Dividimos por $x^3 + x + 1$ *y* $x^3 + x^2 + 1$. *En el primer caso nos queda* $q(x) = (x^3 + x + 1)(x^4 + x^2) + (x^2 + x + 1)$ *y en el segundo* $q(x) = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1)$.

   Puesto que $x^4 + x^3 + x^2 + x + 1$ *no tiene divisores de grado* 1 *y grado* 2 *(ya que de tenerlos serían también divisores de* $q(x)$ *deducimos que* $x^4 + x^3 + x^2 + x + 1$ *es irreducible.*

   La factorización de $q(x)$ *como producto de irreducibles es*

   $$x^7 + x^4 + x^3 + x + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1).$$

3. *Sea* $p(x) = x^7 + 2x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$. *Vamos a factorizar este polinomio como producto de irreducibles.*

   - *Buscamos los divisores de grado 1. Para esto, realizamos las divisiones según el algoritmo de Horner:*

	1	0	0	0	2	1	0	2
1		1	1	1	1	0	1	1
	1	1	1	1	0	1	1	0
1		1	2	0	1	1	2	
	1	2	0	1	1	2	0	
1		1	0	0	1	2		
	1	0	0	1	2	1		

   Vemos que nos ha salido dos veces el factor $(x - 1) = (x + 2)$, *por lo que tenemos que* $q(x) = (x + 2)^2(x^5 + 2x^4 + x^2 + x + 2)$.
   Comprobamos si el último polinomio tiene a $x = 2$ *como raíz:*

	1	2	0	1	1	2
2		2	2	1	1	1
	1	1	2	2	2	0
2		2	0	1	0	
	1	0	2	0	2	

   Es decir, el polinomio $x^5 + 2x^4 + x^2 + x + 2$ *tiene a* $x = 2$ *como una raíz simple. Tenemos ahora la factorización*

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

   Y ya hemos terminado con los divisores de grado uno.

   - *Buscamos ahora los divisores irreducibles de grado 2, pero ya lo hacemos con el polinomio* $x^4+x^3+2x^2+2x+2$. *Como los únicos irreducibles de grado 2 en* $\mathbb{Z}_3[x]$ *son* x^2+1, x^2+x+2 *y* $x^2 + 2x + 2$, *realizamos las correspondientes divisiones:*

   $$\begin{array}{rcrcrcr} x^4 + x^3 + 2x^2 + 2x + 2 & = & (x^2 + 1) & \cdot & (x^2 + x + 1) & + & x + 1 \\ x^4 + x^3 + 2x^2 + 2x + 2 & = & (x^2 + x + 2) & \cdot & (x^2) & + & 2x + 2 \\ x^4 + x^3 + 2x^2 + 2x + 2 & = & (x^2 + 2x + 2) & \cdot & (x^2 + 2x + 2) & + & 1 \end{array}$$

y vemos como los restos son, respectivamente, $x+1$, $2x+2$ *y* 1. *Por tanto, el polinomio* $x^4+x^3+2x^2+2x+2$ *no tiene divisores de grado 2.*

Como el polinomio tiene grado cuatro, y no tiene divisores de grado 1 ni de grado 2 es irreducible.

La factorización de $p(x)$ *como producto de irreducibles es:*

$$x^7+2x^3+x^2+2=(x+1)\cdot(x+2)^2\cdot(x^4+x^3+2x^2+2x+2)$$

3.4. Anillos cocientes de polinomios. Cuerpos finitos

En los capítulos anteriores, dado un número natural $n\geq 2$, construimos el conjunto $\mathbb{Z}_n$, y después definimos su aritmética.

Ahora, sustituimos $\mathbb{Z}$ por $\mathbb{Z}_p[x]$, con p un número primo. Si $m(x)\in\mathbb{Z}_p[x]$ vamos a definir el conjunto $\mathbb{Z}_p[x]_{m(x)}$. Para esto, necesitamos definir la relación de congruencia entre polinomios, de forma análoga a como se hizo con números enteros.

Definición 54. *Sea* p *un número primo y* $a(x),b(x),m(x)\in\mathbb{Z}_p[x]$. *Se dice que* $a(x)$ *es congruente con* $b(x)$ *módulo* $m(x)$, *y se escribe* $a(x)\equiv b(x)(\text{mód } m(x))$ *si* $m(x)|(b(x)-a(x))$. *Es decir:*

$$a(x)\equiv b(x)(\text{mód } m(x)) \text{ si existe } c(x)\in\mathbb{Z}_p[x] \text{ tal que } b(x)-a(x)=c(x)m(x).$$

Nótese que la relación de congruencia módulo 0 es la relación de igualdad ($a(x)\equiv b(x)(\text{mód } 0)$ si, y sólo si, $a(x)=b(x)$), mientras que si $\lambda\in\mathbb{Z}_p^*$ entonces $a(x)\equiv b(x)(\text{mód } \lambda)$ cualesquiera que sean $a(x)$ y $b(x)$. Por tanto, nos centraremos en congruencias módulo $m(x)$ con $m(x)$ un polinomio de grado mayor o igual que 1.

Además, se tiene que $a(x)\equiv b(x)(\text{mód } m(x))$ si, y sólo si, $a(x)\equiv b(x)(\text{mód } \lambda\cdot m(x))$, donde $\lambda\in K^*$. Por tanto, al hablar de congruencias módulo $m(x)$ podemos suponer que $m(x)$ es un polinomio mónico.

Ejemplo 3.4.1. *Sea* $m(x)=x^2+2\in\mathbb{Z}_3[x]$. *Entonces:*

$x^4+2x^3+x^2+x+2\equiv 2x^4+x^3+2x^2+2x(\text{mód } x^2+2)$

pues $(2x^4+x^3+2x^2+2x)-(x^4+2x^3+x^2+x+2)=(x^2+2)(x^2+2x+2)$.

$x^4+x^3+2x^2+1\not\equiv x^3+x+2(\text{mód } x^2+2)$

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

Proposición 3.4.1. *Sea* $m(x)\in\mathbb{Z}_p[x]$. *Entonces la relación de congruencia módulo* $m(x)$ *es una relación de equivalencia.*

La demostración es igual a la que se hizo para congruencias en $\mathbb{Z}$.

Para cada $m(x)\in\mathbb{Z}_p[x]$ vamos a denotar por $\mathbb{Z}_p[x]_{m(x)}$ al conjunto cociente de $\mathbb{Z}_p[x]$ por la relación de congruencia módulo $m(x)$. A la clase de equivalencia de un polinomio $a(x)$ la denotaremos inicialmente por $[a(x)]_{m(x)}$, o simplemente $[a(x)]$.

Al igual que en el caso de los números enteros, se tiene que $a(x)\equiv b(x)(\text{mód } m(x))$ si, y sólo si, $a(x)$ mód $m(x)$ $=$ $b(x)$ mód $m(x)$ (es decir, dan el mismo resto al dividir por $m(x)$). A partir de aquí puede verse que el conjunto $\mathbb{Z}_p[x]_{m(x)}$ está en biyección con los polinomios de $\mathbb{Z}_p[x]$ de grado menor que el de $m(x)$, pues hay tantos elementos como posibles restos de la división por $m(x)$.

Ejemplo 3.4.2.

1. *Vamos a calcular los elementos del conjunto* $\mathbb{Z}_2[x]_{(x^2+1)}$.

   Sea $p(x) \in \mathbb{Z}_2[x]$. *Al dividir* $p(x)$ *entre* x^2+1, *el resto es un polinomio de grado menor que 2 o es el polinomio nulo. Por tanto, sólo tenemos cuatro posibles restos, que son* 0, 1, x *y* $x+1$. *Tenemos entonces que*

   $$\mathbb{Z}_2[x]_{x^2+1} = \{[0], [1], [x], [x+1]\}.$$

   En la clase de equivalencia $[0]$ *están todos los polinomios que dan resto cero al dividir por* x^2+1, *es decir, todos los múltiplos de* x^2+1, *por ejemplo,* 0, x^2+1, x^3+x, x^4+1, *etc.; en la clase* $[1]$ *están los polinomios que al dividir por* x^2+1 *dan resto* 1, *como por ejemplo,* 1, x^2, x^3+x+1, x^4, *etc.*

   En resumen, se tiene:

   $$[0] = \{0,\ x^2+1,\ x^3+x,\ x^3+x^2+x+1,\ x^4+x^2,\ x^4+1, x^4+x^3+x^2+x,\ x^4+x^3+x+1, \cdots\}.$$
   $$[1] = \{1,\ x^2,\ x^3+x+1,\ x^3+x^2+x,\ x^4+x^2+1,\ x^4,\ x^4+x^3+x^2+x+1,\ x^4+x^3+x, \cdots\}.$$
   $$[x] = \{x,\ x^2+x+1,\ x^3,\ x^3+x^2+1,\ x^4+x^2+x,\ x^4+x+1,\ x^4+x^3+x^2,\ x^4+x^3+1, \cdots\}.$$
   $$[x+1] = \{x+1,\ x^2+x,\ x^3+1,\ x^3+x^2,\ x^4+x^2+x+1,\ x^4+x,\ x^4+x^3+x^2+1,\ x^4+x^3, \cdots\}.$$

   O si queremos,

   $$[0] = (x^2+1)\mathbb{Z}_2[x]; \qquad [1] = 1 + (x^2+1)\mathbb{Z}_2[x];$$
   $$[x] = x + (x^2+1)\mathbb{Z}_2[x]; \qquad [x+1] = x + 1 + (x^2+1)\mathbb{Z}_2[x].$$

   Y por ejemplo, se tiene que $x^8+x^7+x^6+x+1 \in [1]$, *ya que*

   $$x^8+x^7+x^6+x+1 = 1 + (x^2+1)\cdot(x^6+x^5+x^3+x).$$

2. *El conjunto* $\mathbb{Z}_2[x]_{x^2+x+1}$ *tiene también cuatro elementos, que son* $[0]$, $[1]$, $[x]$ *y* $[x+1]$. *Sin embargo, aunque se representen igual que los de* $\mathbb{Z}_2[x]_{x^2+1}$, *los conjuntos* $\mathbb{Z}_2[x]_{x^2+x+1}$ *y* $\mathbb{Z}_2[x]_{x^2+1}$ *son distintos, pues en cada uno* $[0]$, $[1]$, $[x]$ *y* $[x+1]$ *representa cosas diferentes. Veámoslo.*

   $$[0] = \{0,\ x^2+x+1,\ x^3+x^2+x,\ x^3+1,\ x^4+x^3+x^2,\ x^4+x^3+x+1,\ x^4+x,\ x^4+x^2+1, \cdots\}.$$
   $$[1] = \{1,\ x^2+x,\ x^3+x^2+x+1,\ x^3,\ x^4+x^3+x^2+1,\ x^4+x^3+x,\ x^4+x+1,\ x^4+x^2, \cdots\}.$$
   $$[x] = \{0,\ x^2+1,\ x^3+x^2,\ x^3+x+1,\ x^4+x^3+x^2+x,\ x^4+x^3+1,\ x^4,\ x^4+x^2+x+1, \cdots\}.$$
   $$[x+1] = \{0,\ x^2,\ x^3+x^2+1,\ x^3+x,\ x^4+x^3+x^2+x+1,\ x^4+x^3,\ x^4+1,\ x^4+x^2+x, \cdots\}.$$

   Y vemos como, por ejemplo, en el primer caso, es decir, $\mathbb{Z}_2[x]_{x^2+1}$ *se tiene que* $x^3 \in [x]$ *(o* $[x^3] = [x]$*), mientras que en el segundo caso, es decir,* $\mathbb{Z}_2[x]_{x^2+x+1}$ *se tiene que* $x^3 \in [1]$.

3. *El conjunto* $\mathbb{Z}_2[x]_{x^3+x^2+x+1}$ *tiene ocho elementos, mientras que* $\mathbb{Z}_3[x]_{x^2+1}$ *tiene nueve. Determínalos en ambos casos.*

Lema 3.4.1. *Sean* $a(x), b(x), c(x), d(x), m(x) \in \mathbb{Z}_p[x]$. *Entonces:*

1. $\left.\begin{array}{l} a(x) \equiv c(x) (mód\ m(x)) \\ b(x) \equiv d(x) (mód\ m(x)) \end{array}\right\} \Longrightarrow a(x)+b(x) \equiv c(x)+d(x) (mód\ m(x)).$

2. $\left.\begin{array}{l} a(x) \equiv c(x) (mód\ m(x)) \\ b(x) \equiv d(x) (mód\ m(x)) \end{array}\right\} \Longrightarrow a(x)b(x) \equiv c(x)d(x) (mód\ m(x)).$

Y con este lema podemos ya definir las operaciones suma y producto

Definición 55. *Sean* $a(x), b(x) \in \mathbb{Z}_p[x]$ *y* $m(x) \in \mathbb{Z}_p[x]$ *mónico y no constante. Se definen en* $\mathbb{Z}_p[x]_{m(x)}$ *las operaciones:*

$$[a(x)] + [b(x)] = [a(x)+b(x)], \qquad [a(x)][b(x)] = [a(x)b(x)].$$

Como era de esperar, la definición hecha no depende de los representantes elegidos, y eso es consecuencia del lema 3.4.1

Ejemplo 3.4.3.

1. *Supongamos que estamos trabajando en* $\mathbb{Z}_3[x]_{x^2+1}$.

   $[x+2]+[x+1]=[2x]$.

   $[x+2][x+1]=[x^2+2]=[1]$.

   Puesto que $[x+2]=[x^2+x]$ *y* $[x+1]=[2x^2+x]$ *podíamos haber efectuado las operaciones anteriores*

   $[x^2+x]+[2x^2+x]=[3x^2+2x]=[2x]$.

   $[x^2+x][2x^2+x]=[2x^4+x^2]=[1]$, *ya que* $2x^4+x^2=(x^2+1)(2x^2+2)+1$.

   Y los resultados coinciden, como no podía ser de otra forma.

2. *Vamos a fijarnos ahora en las clases de equivalencia que hemos obtenido en el ejemplo 3.4.2. En ese ejemplo, calculamos las clases de equivalencia que determinanban el conjunto* $\mathbb{Z}_2[x]_{x^2+1}$ *y las que determinaban el conjunto* $\mathbb{Z}_2[x]_{x^2+x+1}$.

   Vamos a sumar un elemento cualquiera de $[1]$ *con un elemento cualquiera de* $[x]$. *El resultado va a ser un elemento de* $[x+1]$. *Lo vamos a hacer cuatro veces.*

   - *Primero lo vamos a hacer con clases de* $\mathbb{Z}_2[x]_{x^2+1}$.

     $1+x=x+1\in[x+1]$ $\qquad$ $(x^3+x^2+x)+(x^2+x+1)=x^3+1\in[x+1]$

     $x^2+(x^4+x^3+x^2)=x^4+x^3\in[x+1]$ $\qquad$ $(x^4+x^3+x)+(x^4+x^3+x^2)=x^2+x\in[x+1]$.

     Y así para cualesquiera dos polinomios que tomemos, el primero perteneciente a $[1]$ *y el segundo a* $[x]$.

   - *Ahora lo hacemos en* $\mathbb{Z}_2[x]_{x^2+x+1}$.

     $(x^2+x)+(x^2+1)=x+1\in[x+1]$ $\qquad$ $x^3+(x^4+x^3+1)=x^4+1\in[x+1]$

     $(x^4+x^3+x)+(x^3+x+1)=x^4+1\in[x+1]$ $\qquad$ $(x^4+x^2)+x^4=x^2\in[x+1]$.

De ahora en adelante, si $a\in K\subseteq\mathbb{Z}_p[x]$, denotaremos por a a la clase de equivalencia $[a]\in\mathbb{Z}_p[x]_{m(x)}$, mientras que a la clase de equivalencia $[x]$ la denotaremos por α o simplemente por x.

Nótese que siguiendo la notación $\alpha=[x]$, dado $a_kx^k+\cdots+a_1x+a_0\in\mathbb{Z}_p[x]$ el elemento $[a_kx^k+\cdots+a_1x+a_0]$ se representa como $a_k\alpha^k+\cdots+a_1\alpha+a_0$. Dicho de otra forma, $[p(x)]$ se representa como $p(\alpha)$.

Nótese también que con esta notación se verifica que $m(\alpha)=0$, pues $m(\alpha)=[m(x)]=[0]$. Además, esta condición es suficiente para realizar las operaciones en $\mathbb{Z}_p[x]_{m(x)}$

$$\mathbb{Z}_p[x]_{m(x)}=\{p(\alpha):p(x)\in\mathbb{Z}_p[x];m(\alpha)=0\}.$$

Ejemplo 3.4.4.

1. *En el conjunto* $\mathbb{Z}_2[x]_{x^3+x+1}$ *vamos a multiplicar* $[x^2+x+1]$ *y* $[x^2+1]$. *Podemos proceder de dos formas:*

   a) *Multiplicamos los dos polinomios:*
   $[x^2+x+1][x^2+1]=[x^4+x^3+x+1]$.
   Dividimos x^4+x^3+x+1 *entre* x^3+x+1. $x^4+x^3+x+1=(x^3+x+1)(x+1)+x^2+x$.
   Por tanto $[x^2+x+1][x^2+1]=[x^2+x]$.

   b) $(\alpha^2+\alpha+1)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha+1$.
   Puesto que $\alpha^3+\alpha+1=0$ *deducimos que* $\alpha^3=\alpha+1$, *luego* $\alpha^4=\alpha^2+\alpha$. *Por tanto*
   $(\alpha^2+\alpha+1)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha+1=(\alpha^2+\alpha)+(\alpha+1)+\alpha+1=\alpha^2+\alpha$.

   En los dos casos se obtiene el mismo resultado.

2. $\mathbb{Z}_2[x]_{x^2+1} = \{0, 1, \alpha, \alpha+1 : \alpha^2+1=0\}$, *o si preferimos:*

$$\mathbb{Z}_2[x]_{x^2+1} = \{0, 1, \alpha, \alpha+1 : \alpha^2 = 1\}.$$

Proposición 3.4.2. *Sea $m(x) \in \mathbb{Z}_p[x]$ mónico y no constante. Las operaciones suma y producto en $\mathbb{Z}_p[x]_{m(x)}$ verifican las siguientes propiedades (aquí vamos a denotar a $[x]$ por x):*

i) $p(x) + (q(x) + r(x)) = (p(x) + q(x)) + r(x)$

ii) $p(x) + q(x) = q(x) + p(x)$

iii) $p(x) + 0 = p(x)$

iv) Para cada $p(x) \in \mathbb{Z}_p[x]_{m(x)}$ *existe* $q(x) \in \mathbb{Z}_p[x]_{m(x)}$ *tal que* $p(x) + q(x) = 0$.

v) $p(x)(q(x)r(x)) = (p(x)q(x))r(x)$

vi) $p(x)q(x) = q(x)p(x)$

vii) $p(x) \cdot 1 = p(x)$

viii) $p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x)$

Estas propiedades nos dicen que $\mathbb{Z}_p[x]_{m(x)}$ es un anillo conmutativo.

Ejemplo 3.4.5.

1. *Consideramos el anillo $\mathbb{Z}_2[x]_{x^3+1}$. Vamos a escribir las tablas de sumar y multiplicar de dicho anillo. Antes de ello, enumeramos sus elementos*

$$\mathbb{Z}_2[x]_{x^3+1} = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

Para realizar la tabla del producto tenemos en cuenta que $\alpha^3 + 1 = 0$, es decir, $\alpha^3 = 1$.

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	1	$\alpha+1$	α^2+1	$\alpha^2+\alpha+1$
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2+1	$\alpha^2+\alpha$	$\alpha+1$	0
α^2	0	α^2	1	α^2+1	α	$\alpha^2+\alpha$	$\alpha+1$	$\alpha^2+\alpha+1$
α^2+1	0	α^2+1	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha+1$	α^2+1	0
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	α^2+1	$\alpha+1$	$\alpha+1$	α^2+1	$\alpha^2+\alpha$	0
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	0	0	$\alpha^2+\alpha+1$

Donde algunas de las celdas se han completado como sigue:

$$\alpha \cdot \alpha^2 = \alpha^3 = 1$$

$$(\alpha^2+1)(\alpha^2+\alpha+1) = \alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha+1 = \alpha+1+\alpha^2+\alpha^2+\alpha+1 = 0$$

Y se ha tenido en cuenta que $\alpha^4 = \alpha^3 \cdot \alpha = \alpha$.

$$(\alpha^2+1)(\alpha^2+1) = \alpha^4+2\alpha^2+1 = \alpha+1.$$

2. *Vamos a dar ahora la tabla de multiplicar de* $\mathbb{Z}_3[x]_{x^2+1}$. *Los elementos son ahora*

$$\mathbb{Z}_3[x]_{x^2+1} = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

$\cdot$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α

Proposición 3.4.3. *Sea* p *un número primo,* $m(x) \in \mathbb{Z}_p[x]$ *no constante y* $q(\alpha) \in \mathbb{Z}_p[x]_{m(x)}$. *Entonces:*

- $q(\alpha)$ *es una unidad si, y sólo si,* $mcd(q(x), m(x)) = 1$.
- $q(\alpha)$ *es un divisor de cero si, y sólo si,* $mcd(q(x), m(x)) \neq 1$.

Recordemos que si A es un anillo conmutativo, un elemento $a \in A$ se dice unidad si existe $b \in A$ tal que $a \cdot b = 1$, mientras que se dice divisor de cero si existe $b \neq 0$ tal que $a \cdot b = 0$.

Demostración: La demostración de la primera parte es análoga a la demostración de la proposición 2.5.2

En cuanto a la segunda, si $p(\alpha)$ es un divisor de cero, entonces $p(\alpha)$ no es una unidad (¿por qué?), luego $mcd(p(x), m(x)) \neq 1$.

Recíprocamente, si $mcd(p(x), m(x)) \neq 1$, consideramos $q(x) = \frac{m(x)}{d(x)}$ donde $d(x) = mcd(p(x), m(x))$. Entonces $gr(q(x)) < gr(m(x))$, lo que implica que $q(\alpha) \neq 0$, y puesto que $p(x)q(x)$ es múltiplo de $m(x)$ ya que

$$p(x)q(x) = p(x)\frac{m(x)}{d(x)} = \frac{p(x)}{d(x)}m(x)$$

se verifica que $p(\alpha)q(\alpha) = 0$. ■

Ejemplo 3.4.6. *En* $\mathbb{Z}_2[x]$ *se verifica que* $mcd(x^2+1, x^3+1) = x+1$. *Por tanto,* α^2+1 *es un divisor de cero en* $\mathbb{Z}_2[x]_{x^3+1}$. *Además, para encontrar un elemento que al multiplicarlo por él nos de cero, calculamos* $\frac{x^3+1}{x+1}$. *Ese cociente vale* x^2+x+1. *Deducimos entonces que* $(\alpha^2+1)(\alpha^2+\alpha+1) = 0$, *como podemos ver en el ejemplo anterior.*

A partir de la proposición anterior se deduce fácilmente que si $m(x)$ es un polinomio irreducible en $\mathbb{Z}_p[x]$, entonces $\mathbb{Z}_p[x]_{m(x)}$ es un cuerpo. Si $m(x)$ es un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$ entonces $\mathbb{Z}_p[x]_{m(x)}$ es un cuerpo con p^n elementos.

Por otra parte, si K es un cuerpo con un número finito de elementos, entonces su característica es un número primo p[1] En tal caso se tiene que $\mathbb{Z}_p \subseteq K$. Utilizando resultados de álgebra lineal se puede ver que existe un número natural n de forma que K tiene p^n elementos.

Es decir, por una parte hemos visto que el número de elementos de un cuerpo finito es una potencia de un primo. Por otra parte, hemos visto como, dado un número primo p y un número natural n podemos construir un cuerpo con p^n elementos. Basta encontrar un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$. Hay un teorema que nos asegura la existencia de polinomios irreducibles de cualquier grado en $\mathbb{Z}_p[x]$.

La existencia de varios polinomios irreducibles de un mismo grado en $\mathbb{Z}_p[x]$ daría lugar, en principio, a distintos cuerpos con p^n elementos. Sin embargo, todos los cuerpos con el mismo cardinal son isomorfos, en el sentido que vamos a explicar a continuación.

Ejemplo 3.4.7.

1. *Hemos visto que $\mathbb{Z}_3[x]_{x^2+1}$ es un cuerpo con nueve elementos, cuya tabla del producto calculamos en el ejemplo 3.4.5. Puesto que x^2+x+2 es también un polinomio irreducible en $\mathbb{Z}_3[x]$ tenemos que $\mathbb{Z}_3[x]_{x^2+x+2}$ es también un cuerpo con nueve elementos. Si llamamos β al elemento $[x]$, entonces la tabla del producto de este cuerpo es:*

$(\mathbb{Z}_3[x]_{x^2+x+2},\cdot)$	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
2	0	2	1	2β	$2\beta+2$	$2\beta+1$	β	$\beta+2$	$\beta+1$
β	0	β	2β	$2\beta+1$	1	$\beta+1$	$\beta+2$	$2\beta+2$	2
$\beta+1$	0	$\beta+1$	$2\beta+2$	1	$\beta+2$	2β	2	β	$2\beta+1$
$\beta+2$	0	$\beta+2$	$2\beta+1$	$\beta+1$	2β	2	$2\beta+2$	1	β
2β	0	2β	β	$\beta+2$	2	$2\beta+2$	$2\beta+1$	$\beta+1$	1
$2\beta+1$	0	$2\beta+1$	$\beta+2$	$2\beta+2$	β	1	$\beta+1$	2	2β
$2\beta+2$	0	$2\beta+2$	$\beta+1$	2	$2\beta+1$	β	1	2β	$\beta+2$

donde se ha usado que $\beta^2 = 2\beta+1$, relación que se deduce de $\beta^2+\beta+2=0$ (es decir, $m(\beta)=0$). Si ahora hacemos el cambio $\alpha = \beta+2$, es decir, $\beta = \alpha+1$, la tabla nos quedaría

$(\mathbb{Z}_3[x]_{x^2+x+2},\cdot)$	0	1	2	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
2	0	2	1	$2\alpha+2$	$2\alpha+1$	2α	$\alpha+1$	α	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	2α	1	$\alpha+2$	α	$2\alpha+1$	2
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	1	α	$2\alpha+2$	2	$\alpha+1$	2α
α	0	α	2α	$\alpha+2$	$2\alpha+2$	2	$2\alpha+1$	1	$\alpha+1$
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	α	2	$2\alpha+1$	2α	$\alpha+2$	1
2α	0	2α	α	$2\alpha+1$	$\alpha+1$	1	$\alpha+2$	2	$2\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	2	2α	$\alpha+1$	1	$2\alpha+2$	α

Si comparamos esta tabla con la que obtuvimos para $\mathbb{Z}_3[x]_{x^2+1}$ vemos que es exactamente la misma (salvo el orden de las filas y columnas). Vemos entonces que los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ son iguales, o más precisamente, son isomorfos.

De hecho, lo único que diferencia a los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ es, aparte del camino para obtenerlos, el nombre que se le ha dado a los elementos. Lo que en un cuerpo se llama α en el otro se llama $\beta+2$. Una vez hecha la correcta correspondencia entre los elementos de uno y del otro, se opera de igual forma en un caso y en el otro.

[1] la característica de un anillo A se define como el menor número natural m tal que $1+1+\overset{m \text{ veces}}{\cdots}+1=0$, si dicho número existe.

Nota:*Dados dos cuerpos K y K', se dice que son isomorfos si existe una aplicación $f : K \to K'$ satisfaciendo:*

a) *f preserva la suma, es decir, $f(a+b) = f(a) + f(b)$.*

b) *f preserva el producto, es decir, $f(ab) = f(a)f(b)$.*

c) *f es biyectiva.*

f es lo que se llama un isomorfismo de cuerpos.

En el caso de $K = \mathbb{Z}_3[x]_{x^2+x+2}$ y $K' = \mathbb{Z}_3[x]_{x^2+1}$, la aplicación $f : K \to K'$ dada por

$$0 \mapsto 0 \quad 1 \mapsto 1 \quad 2 \mapsto 2 \quad \beta \mapsto \alpha + 1 \quad \beta + 1 \mapsto \alpha + 2$$

$$\beta + 2 \mapsto \alpha \quad 2\beta \mapsto 2\alpha + 2 \quad 2\beta + 1 \mapsto 2\alpha \quad 2\beta + 2 \mapsto 2\alpha + 1$$

es un isomorfismo de cuerpos. Obviamente, este isomorfismo queda totalmente determinado por $\beta \mapsto \alpha + 1$.

Nota:

Aunque en la última sección nos hemos centrado en el caso de polinomios con coeficientes en $\mathbb{Z}_p$, todo el desarrollo podría haberse hecho para el caso de polinomios con coeficientes en un cuerpo cualquiera.

Vamos a tomar como cuerpo K el conjunto de los números reales, y $m(x) = x^2+1$. Este polinomio es irreducible (tiene grado 2 y no tiene raíces), luego $\mathbb{R}[x]_{x^2+1}$ es un cuerpo.

Vamos a denotar por i a $[x]$ (en lugar de α). Entonces, los elementos de $\mathbb{R}[x]_{x^2+1}$ son de la forma $a+bi$, donde $a, b \in \mathbb{R}$. Además, $i^2 + 1 = 0$, es decir, $i^2 = -1$.

Por tanto,

$$\mathbb{R}[x]_{x^2+1} = \{a + bi : a, b \in \mathbb{R}; i^2 = -1\}$$

luego el cuerpo obtenido resulta ser igual (o isomorfo) a $\mathbb{C}$.

Dado p es un número primo y n es un número natural no nulo, denotaremos como $\mathbb{F}_{p^n}$ al único cuerpo que existe con p^n elementos. Así, por ejemplo, $\mathbb{F}_4 = \mathbb{Z}_2[x]_{x^2+x+1}$ y $\mathbb{F}_9 = \mathbb{Z}_3[x]_{x^2+1}$. Obviamente, $\mathbb{F}_p = \mathbb{Z}_p$ para cualquier primo p.