Tema 2: Polinomios

TEORÍA

Índice

En muchas de las aplicaciones del Álgebra a la Informática se requiere elegir un cuerpo finito de un cardinal adecuado. En este tema aprenderemos entre otras cosas a construir nuevos cuerpos finitos a partir de congruencias de polinomios.

A lo largo del tema, $\mathbb{K}$ denotará un cuerpo fijado.

1. Polinomios con coeficientes en un cuerpo

Definición 1.1. Llamaremos *polinomio de grado n en la variable X con coeficientes en* $\mathbb{K}$ a cualquier expresión formal

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_2 X^2 + a_1 X + a_0,$$

donde cada $a_i \in \mathbb{K}$, y siendo $a_n \neq 0$.

Notación 1.2. Los polinomios se suelen denotar con las letras p, q, r y sucesivas. Escribiremos $\deg(p(X))$ para denotar el *grado* del polinomio $p(X)$. Denotaremos por $\mathbb{K}[X]$ el conjunto de polinomios en la variable X con coeficientes en el cuerpo $\mathbb{K}$.

Ejemplo 1.3. El polinomio $p(X) = 5X^3 + \left(-1/2\right) X + 1$ cumple que $p(X) \in \mathbb{Q}[X]$ cuando es considerado como polinomio con coeficientes en $\mathbb{Q}$. Su grado es $\deg(p(X)) = 3$.

El polinomio $q(X) = X^9 + \overline{4}X^6 + \overline{2}X$ considerado como polinomio con coeficientes en $\mathbb{Z}_5$ cumple que $q(X) \in \mathbb{Z}_5[X]$. Su grado es $\deg(q(X)) = 9$.

Definición 1.4. Si el polinomio tiene la expresión $p(X) = a_0$, con $a_0 \in \mathbb{K}$, se dice que $p(X)$ es un *polinomio constante*. Si $a_0 \neq 0$, su grado es $\deg(a_0) = 0$.

Definición 1.5. También consideraremos como polinomio el elemento $0 \in \mathbb{K}$, al que llamaremos *polinomio nulo*. Por convenio se establece que el grado del polinomio 0 es $\deg(0) = -\infty$.

Ejemplo 1.6. $p(X) = 5/3 \in \mathbb{Q}[X]$ es un polinomio constante de grado $\deg(p(X)) = 0$.

$q(X) = \overline{3} \in \mathbb{Z}_5[X]$ es un polinomio constante también de grado $\deg(q(X)) = 0$.

$r(X) = 0 \in \mathbb{Q}[X]$ es un polinomio constante de grado $\deg(r(X)) = -\infty$.

Definición 1.7. Dado el polinomio $p(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0$, llamaremos:

1) *término principal* de $p(X)$ al polinomio a_nX^n,

2) *término i-ésimo* de $p(X)$ al polinomio a_iX^i,

3) *término independiente* de $p(X)$ al polinomio constante a_0,

4) *coeficiente principal* de $p(X)$ al elemento $a_n \in \mathbb{K}$,

5) *coeficiente i-ésimo* de $p(X)$ al elemento $a_i \in \mathbb{K}$.

Ejemplo 1.8. El coeficiente principal del polinomio $X^9+\overline{4}X^6+\overline{2}X \in \mathbb{Z}_5[X]$ es $\overline{1}$. Su término principal es X^9, su sexto término es $\overline{4}X^6$, mientras que su sexto coeficiente es $\overline{4}$. Su término independiente es $\overline{0}$.

Definición 1.9. Se dice que un polinomio es *mónico* si su coeficiente principal es 1.

Ejemplo 1.10. El polinomio $X^9 + \overline{4}X^6 + \overline{2}X \in \mathbb{Z}_5[X]$ es mónico.

Definición 1.11. Se dice que un polinomio es un *monomio* si tiene un único término.

Ejemplo 1.12. El polinomio $5X^3 \in \mathbb{Q}[X]$ es un monomio.

Notación 1.13. Por comodidad en la notación, cuando trabajemos con coeficientes negativos, por ejemplo $p(X) = X^2 + (-3)X + 2 \in \mathbb{Q}[X]$, escribiremos de forma abreviada $p(X) = X^2 - 3X + 2$.

Por otra parte, cuando trabajemos con polinomios de $\mathbb{Z}_n[X]$, por ejemplo $q(X) = \overline{2}X^2 + \overline{1} \in \mathbb{Z}_5[X]$, prescindiremos de los signos de clase en los coeficientes del polinomio, escribiendo $q(X) = 2X^2 + 1 \in \mathbb{Z}_5[X]$ cuando no haya confusión.

1.1. Estructura de anillo en $\mathbb{K}[X]$

Observación 1.14. En el conjunto $\mathbb{K}[X]$ se pueden definir las siguientes operaciones de suma y producto:

$$\begin{array}{rcl} +:\mathbb{K}[X]\times\mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ (p(X),q(X)) & \longmapsto & p(X)+q(X) \end{array} \qquad \begin{array}{rcl} \cdot:\mathbb{K}[X]\times\mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ (p(X),q(X)) & \longmapsto & p(X)\cdot q(X) \end{array}$$

Para cada par de polinomios

$$p(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_2X^2+a_1X+a_0,$$

$$q(X)=b_mX^m+b_{m-1}X^{m-1}+\ldots+b_2X^2+b_1X+b_0,$$

la suma $p(X)+q(X)$ tiene como término i-ésimo la suma de los términos i-ésimos de $p(X)$ y $q(X)$:

$$a_iX^i+b_iX^i=(a_i+b_i)X^i.$$

El producto de polinomios se define a partir del caso sencillo de producto de monomios, usando la regla distributiva del producto respecto a la suma: aX^j por bX^k se define como

$$aX^j\cdot bX^k:=abX^{j+k}.$$

Ejemplo 1.15. Si $p(X)=2X^2+1$ y $q(X)=X^3+X^2$ son polinomios de $\mathbb{Z}_5[X]$, entonces

$$p(X)+q(X)=X^3+(2X^2+X^2)+1=X^3+3X^2+1,$$

$$p(X)\cdot q(X)=(2X^2+1)\cdot(X^3+X^2)=2X^2\cdot X^3+2X^2\cdot X^2+1\cdot X^3+1\cdot X^2=$$
$$=2X^5+2X^4+X^3+X^2.$$

Observación 1.16. En general:

$$\deg(p(X)+q(X))\leq \text{máx}\{\deg(p(X)),\deg(q(X))\},$$

$$\deg(p(X)\cdot q(X))=\deg(p(X))+\deg(q(X)).$$

Ejemplo 1.17. Si $p(X)=2X^2+1$ y $q(X)=3X^2+X$ son polinomios de $\mathbb{Z}_5[X]$, entonces $p(X)+q(X)=X+1$, con lo que

$$\deg(p(X)+q(X))=1\leq \text{máx}\{\deg(p(X)),\deg(q(X))\}=\text{máx}\{2,2\}=2.$$

Proposición 1.18. $(\mathbb{K}[X],+,\cdot)$ *es un anillo conmutativo.*

Demostración: (Ejercicio) Los elementos neutros de suma y producto son los polinomios constantes 0 y 1 respectivamente. El elemento opuesto de un polinomio $p(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_2X^2+a_1X+a_0\in\mathbb{K}[X]$ es el *polinomio opuesto*

$$-p(X):=(-a_n)X^n+(-a_{n-1})X^{n-1}+\ldots+(-a_2)X^2+(-a_1)X+(-a_0)\in\mathbb{K}[X].$$

Ejemplo 1.19. El polinomio opuesto de $p(X)=2X^2+1\in\mathbb{Z}_5[X]$ es

$$-p(X)=-2X^2-1=3X^2+4.$$

Recuérdese que el conjunto $\mathbb{K}^*$ de unidades del cuerpo $\mathbb{K}$ es igual a $\mathbb{K} - \{0\}$.

Proposición 1.20. *Las unidades del anillo de polinomios $\mathbb{K}[X]$ son las constantes no nulas, es decir, $\mathbb{K}[X]^* = \mathbb{K}^*$.*

Demostración: Es consecuencia de la fórmula para el grado del producto de polinomios. □

Ejemplo 1.21. Las unidades del anillo $\mathbb{R}[X]$ son los elementos de $\mathbb{R}^*$.

Las unidades del anillo $\mathbb{Z}_5[X]$ son los elementos de $\mathbb{Z}_5^*$, que son 1, 2, 3 y 4.

2. Divisibilidad en $\mathbb{K}[X]$

En esta sección vamos a ver cómo los resultados de divisibilidad vistos para $\mathbb{Z}$ se pueden reformular en términos de polinomios.

2.1. Teorema de la división euclídea

Teorema 2.1 (**Teorema de la división euclídea en** $\mathbb{K}[X]$). *Dados dos polinomios $p(X)$ y $q(X)$ de $\mathbb{K}[X]$, con $q(X) \neq 0$, existe un único par de polinomios $c(X)$ y $r(X)$ de $\mathbb{K}[X]$ para el que se cumplan a la vez las dos condiciones siguientes:*

i) $p(X) = c(X) \cdot q(X) + r(X)$,

ii) $\deg(r(X)) < \deg(q(X))$.

Observación 2.2. En cada etapa de la división de $p(X)$ entre $q(X)$ se añade a $c(X)$ un monomio tal que al multiplicarlo por el término principal de $q(X)$ resulte el término principal de $p(X)$. En la siguiente etapa repetiremos esa operación tomando como nuevo dividendo el resto parcial, que es el resultado de restar a $p(X)$ el producto de dicho monomio por $q(X)$. Pararemos al obtener un resto parcial de grado menor que el del divisor $q(X)$.

Ejemplo 2.3. Realicemos la división euclídea del dividendo $p(X) = X^4 + 2X + 1$ entre el divisor $q(X) = 2X^2 + 1$ en $\mathbb{Z}_3[X]$:

$$\begin{array}{rl|l} X^4 + 2X + 1 & & 2X^2 + 1 \\ \cline{3-3} -(X^4 + 2X^2) & & 2X^2 + 2 \\ \cline{1-1} X^2 + 2X + 1 & & \\ -(X^2 + 2) & & \\ \cline{1-1} 2X + 2 & & \end{array}$$

El cociente es $c(X) = 2X^2 + 2$ y el resto es $r(X) = 2X + 2$.

Observación 2.4. Es habitual emplear el *algoritmo de Ruffini-Horner* cuando queremos hacer una división euclídea en la que el divisor es de la forma $X - \alpha$, con $\alpha \in \mathbb{K}$. Por ejemplo, para dividir en $\mathbb{Q}[X]$ el polinomio $p(X) = X^5 + 3X^4 - X^3 + 2X + 1$ entre $q(X) = X + 2$,

observamos que el divisor es de la forma $X-(-2)$, y de la aplicación del algoritmo de Ruffini-Horner

	1	3	−1	0	2	1
−2		−2	−2	6	−12	20
	1	1	−3	6	−10	21

deducimos que el resto es el último dato obtenido en el algoritmo $r(X)=21$ y que los valores intermedios del algoritmo son los coeficientes del cociente, que en este caso será $c(X)=X^4+X^3-3X^2+6X-10$.

Ejercicio 2.5. Realizar la división euclídea en $\mathbb{Z}_5[X]$ del polinomio X^4+X^2+2 entre $X+3$.

Definición 2.6. Dados dos polinomios $p(X)$ y $q(X)$ de $\mathbb{K}[X]$, diremos que $q(X)$ *divide* a $p(X)$ (o que $q(X)$ es *divisor* de $p(X)$, o que $p(X)$ es *múltiplo* de $q(X)$) si existe un $c(X)\in\mathbb{K}[X]$ tal que

$$p(X)=c(X)\cdot q(X).$$

Escribiremos $q(X)\mid p(X)$ si $q(X)$ divide a $p(X)$, y $q(X)\nmid p(X)$ en caso contrario.

Observación 2.7. Si $q(X)\neq 0$, esto es equivalente a que el resto $r(X)$ de la división euclídea de $p(X)$ entre $q(X)$ sea 0.

Ejemplo 2.8. En $\mathbb{R}[X]$:

$$X+2\mid X^2-4, \qquad 2X+4\mid X+2, \qquad 3\mid X+2, \qquad X+2\mid 0,$$
$$X+2\mid 2X+4, \qquad X+2\mid X+2, \qquad 0\nmid X+2, \qquad 3\mid 5.$$

Ejercicio 2.9. ¿Es cierto que $2X+1\mid 3X^2+3$ en $\mathbb{Z}_5[X]$?

A continuación enunciaremos las propiedades mas importantes de la relación de divisibilidad en $\mathbb{K}[X]$, que son similares a las vistas en el caso de los enteros, teniendo en cuenta que ahora las unidades de $\mathbb{K}[X]$ son elementos de $\mathbb{K}^*$ (en el caso de $\mathbb{Z}$ las unidades eran 1 y -1).

Propiedades 2.10. *Para todo $p(X),q(X)\in\mathbb{K}[X]$ y $k\in\mathbb{K}^*$ se cumple que:*

1) $q(X)\mid p(X)\Longrightarrow \deg(q(X))\leq\deg(p(X))$,

2) $k\mid p(X)$,

3) $k\cdot p(X)\mid p(X)$,

4) $p(X)$ *es múltiplo de un sólo polinomio mónico de su mismo grado,*

5) $p(X)\mid p(X)$,

6) $(p(X)\mid q(X))\wedge(q(X)\mid r(X))\Longrightarrow p(X)\mid r(X)$,

7) $(p(X)\mid q(X))\wedge(q(X)\mid p(X))\Longrightarrow \exists b\in\mathbb{K}^*,\ p(X)=b\cdot q(X)$.

Ejemplo 2.11. El polinomio $6X+5 \in \mathbb{Q}[X]$ es múltiplo de un sólo polinomio mónico de su mismo grado: del polinomio $X + {}^{5}\!/_{6}$.

Ejercicio 2.12. ¿De qué polinomio mónico de grado 3 es múltiplo $2X^3 + 3X^2 + 1 \in \mathbb{Z}_5$?

Notación 2.13. El conjunto de divisores de un polinomio $p(X)$ lo denotaremos por

$$\mathrm{Div}(p(X)) := \{q(X) \in \mathbb{K}[X] \ / \ q(X) \mid p(X)\}.$$

Ejemplo 2.14. Los divisores del polinomio $X + 2 \in \mathbb{R}[X]$ son los elementos de

$$\mathrm{Div}(X+2) = \{k \ / \ k \in \mathbb{R}^*\} \cup \{k(X+2) \ / \ k \in \mathbb{R}^*\}.$$

Ejercicio 2.15. Calcular los divisores del polinomio $X + 3 \in \mathbb{Z}_5[X]$.

Observación 2.16. En general, si $p(X)$ es un polinomio de grado $\deg(p(X)) = 1$ con coeficientes en un cuerpo $\mathbb{K}$, sus divisores serán obligatoriamente de grado menor o igual a 1, y por tanto son

$$\mathrm{Div}(p(X)) = \{k \ / \ k \in \mathbb{K}^*\} \cup \{k \cdot p(X) \ / \ k \in \mathbb{K}^*\}.$$

2.2. Raíces de un polinomio

Definición 2.17. Sea $p(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0$ un polinomio de $\mathbb{K}[X]$ y α un elemento de $\mathbb{K}$. Llamaremos *evaluación* de $p(X)$ en α al elemento del cuerpo $\mathbb{K}$

$$p(\alpha) := a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_2\alpha^2 + a_1\alpha + a_0.$$

Ejemplo 2.18. Si $p(X) = 2X^3 + 1 \in \mathbb{Z}_5[X]$, entonces la evaluación de $p(X)$ en el elemento $1 \in \mathbb{Z}_5$ es igual a $p(1) = 2 \cdot 1^3 + 1 = 3$.

Proposición 2.19. *$p(\alpha)$ es el resto de dividir $p(X)$ entre $X - \alpha$.*

Demostración: Realicemos la división euclídea de $p(X)$ entre $X - \alpha$:

$$p(X) = c(X) \cdot (X - \alpha) + r(X).$$

Como el divisor tiene grado 1, el resto $r(X)$ es una constante r. Ahora bien, esa constante tiene que ser $p(\alpha)$, ya que $p(\alpha) = c(\alpha) \cdot (\alpha - \alpha) + r = c(\alpha) \cdot 0 + r = 0 + r = r$.

□

Observación 2.20. Si usamos el algoritmo de Ruffini-Horner para dividir el polinomio $p(X)$ entre $X - \alpha$, el último dato obtenido en el algoritmo es el resto, luego coincidirá con $p(\alpha)$.

Ejemplo 2.21. De la Observación 2.4 deducimos que la evaluación de $p(X) = X^5 + 3X^4 - X^3 + 2X + 1 \in \mathbb{Q}[X]$ en el elemento -2 es igual a $p(-2) = 21$.

Definición 2.22. Diremos que $\alpha \in \mathbb{K}$ es una *raíz* de $p(X) \in \mathbb{K}[X]$ si $p(\alpha) = 0$.

Proposición 2.23 (Regla de Ruffini). *α es raíz de $p(X)$ si y sólo si $X - \alpha \mid p(X)$.*

Demostración: Se deduce de que $p(\alpha)$ es el resto de la división de $p(X)$ entre $X-\alpha$.

□

Ejercicio 2.24. ¿Es $2 \in \mathbb{Z}_7$ una raíz del polinomio $3X^5+3X^4+3X^3+X^2+2X+6 \in \mathbb{Z}_7[X]$?

Observación 2.25. Un polinomio $p(X) = aX + b$ de grado 1 con coeficientes en un cuerpo $\mathbb{K}$ tendrá exactamente una única raíz ya que

$$aX + b = 0 \Longleftrightarrow aX = -b \Longleftrightarrow X = a^{-1} \cdot (-b).$$

Ejemplo 2.26. El polinomio $5X + 1 \in \mathbb{Z}_7[X]$ tiene como raíz sólamente a 4 ya que

$$5X + 1 = 0 \Longleftrightarrow 5X = 6 \Longleftrightarrow X = 5^{-1} \cdot 6 = 3 \cdot 6 = 4.$$

La siguiente proposición nos permite localizar las raíces racionales de los polinomios con coeficientes enteros:

Proposición 2.27. *Si $p(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0 \in \mathbb{Q}[X]$ es un polinomio con coeficientes enteros y la fracción irreducible $r/t \in \mathbb{Q}$ es raíz suya, entonces $r|a_0$ y $t|a_n$.*

Demostración: Como $0 = p\left(r/t\right) = a_n {r^n}/{t^n} + a_{n-1} {r^{n-1}}/{t^{n-1}} + \cdots + a_1 r/t + a_0$, multiplicando por t^n se tiene que

$$0 = a_nr^n + a_{n-1}tr^{n-1} + \cdots + a_1t^{n-1}r + a_0t^n,$$

de donde $r|a_0t^n$ y $t|a_nr^n$. Aplicando el lema de Euclides obtenemos el resultado.

□

Ejemplo 2.28. Si buscamos las raíces racionales del polinomio $p(X) = 2X^3 + X^2 + 2X + 1$, podemos limitarnos a buscarlas entre las fracciones r/t tales que $r|1$ y $t|2$. Es decir, que las posibles raíces racionales de $p(X)$ serían 1, -1, $1/2$ y $-1/2$. Aplicando el algoritmo de Rufini-Horner con $-1/2$ obtenemos:

$$\begin{array}{c|cccc} & 2 & 1 & 2 & 1 \\ -1/2 & & -1 & 0 & -1 \\ \hline & 2 & 0 & 2 & \boxed{0} \end{array}.$$

De ahí que $p(X) = \left(X + 1/2\right) \cdot (2X^2+2)$. Como $2X^2+2$ no se anula para ningún X racional, y $X + 1/2$ sólo se anula en $-1/2$, deducimos que $p(X)$ sólo tiene una raíz racional, que es $-1/2$.

Ejercicio 2.29. Comprobar con la regla de Ruffini que $X^3 - 2$ no posee raíces racionales.

2.3. Polinomios irreducibles

Observación 2.30. Algunos polinomios se pueden factorizar como producto de dos polinomios de grado mayor o igual a 1. Por ejemplo $X^2-1=(X+1)\cdot(X-1)$ en $\mathbb{R}[X]$. Sin embargo otros no, como por ejemplo el polinomio $X^2+1\in\mathbb{R}[X]$, que no se puede factorizar como producto de polinomios de grado 1 porque en tal caso tendría raíces reales. A los primeros los llamaremos compuestos, y a los segundos irreducibles, y jugarán en $\mathbb{K}[X]$ un papel similar al de los números compuestos y los primos en $\mathbb{Z}$.

Definición 2.31. Sea $p(X)\in\mathbb{K}[X]$ un polinomio de grado $\deg(p(X))\geq 1$. Se dice que:

1) $p(X)$ es *compuesto* en $\mathbb{K}[X]$ si existen $q(X), r(X)\in\mathbb{K}[X]$ ambos de grado mayor o igual a 1 tales que $p(X)=q(X)\cdot r(X)$.

2) $p(X)$ es *irreducible* en $\mathbb{K}[X]$ en caso contrario.

Observación 2.32. $p(X)$ es irreducible si $\mathrm{Div}(p(X))=\{k\mid k\in\mathbb{K}^*\}\cup\{k\cdot p(X)\mid k\in\mathbb{K}^*\}$.

Ejemplo 2.33. En $\mathbb{R}[X]$, $2X^3+X^2+2X+1=\left(X+{}^1\!/_2\right)\cdot(2X^2+2)$ es compuesto, pero $2X+4$ es irreducible.

La siguiente es una caracterización de los polinomios irreducibles de grados 1, 2 y 3:

Propiedades 2.34. *Sea $p(X)\in\mathbb{K}[X]$.*

1) Si $\deg(p(X))=1$ entonces $p(X)$ es irreducible en $\mathbb{K}[X]$.

2) Si $\deg(p(X))$ es 2 o 3, entonces $p(X)$ es irreducible en $\mathbb{K}[X]$ si, y sólo si, no posee raíces en $\mathbb{K}$.

Demostración: Si $p(X)$ es un polinomio compuesto de grado 2 o 3, entonces $p(X)=q(X)\cdot r(X)$, donde los factores no son polinomios constantes. Pero el grado de $p(X)$ tendría que ser la suma de los grados de $q(X)$ y $r(X)$, luego alguno de estos dos polinomios ha de tener grado 1, y por tanto $p(X)$ admitiría alguna raíz en $\mathbb{K}$.

□

Ejemplo 2.35. En $\mathbb{Z}_2[X]$ el polinomio X^3+X^2+1 es irreducible, pues no tiene raíces en $\mathbb{Z}_2$. Sin embargo X^2+1 es compuesto en $\mathbb{Z}_2[X]$.

Ejemplo 2.36. En $\mathbb{Q}[X]$ el polinomio X^2-2 es irreducible, pues no tiene raíces racionales. Sin embargo en $\mathbb{R}[X]$ es compuesto, ya que $\sqrt{2}$ y $-\sqrt{2}$ son raíces suyas.

Observación 2.37. El criterio de las raíces no se cumple para polinomios de grado mayor que 3. Por ejemplo, el polinomio $(X^2+1)^2\in\mathbb{R}[X]$ no tiene raíces en $\mathbb{R}$, pero no es irreducible.

Para algunos cuerpos $\mathbb{K}$ es posible afinar un poco más este criterio de las raíces. Por ejemplo, en $\mathbb{C}[X]$ todos los polinomios no nulos poseen alguna raíz, siendo irreducibles sólamente los polinomios de grado 1:

Teorema 2.38 (Teorema fundamental del Álgebra). *Todo polinomio no constante de $\mathbb{C}[X]$ posee alguna raíz.*

Corolario 2.39. *Un polinomio $p(X) \in \mathbb{C}[X]$ es irreducible si y sólo si* $\deg(p(X)) = 1$.

Ejemplo 2.40. El polinomio $iX^2 - 7X + (4 - 2i) \in \mathbb{C}[X]$ es compuesto, pues su grado es 2.

Observación 2.41. En $\mathbb{R}[X]$, los polinomios de grado mayor o igual a 3 son todos compuestos, ya que si tienen una raíz compleja $a+bi$, también tendrán como raíz a su conjugada $a - bi$, con lo que serán divisibles por el polinomio de grado 2 con coeficientes en $\mathbb{R}[X]$

$$X^2 - 2aX + (a^2 + b^2) = (X - (a + bi)) \cdot (X - (a - bi)).$$

Como consecuencia, los polinomios irreducibles en $\mathbb{R}[X]$ son los de grado 2 con dos raíces complejas no reales, junto con todos los de grado 1.

Ejemplo 2.42. El polinomio $\sqrt[5]{2}X^3 - 4X + \ln(7) \in \mathbb{R}[X]$ es compuesto, pues su grado es 3.

2.4. Factorización única de polinomios

El siguiente teorema describe la factorización única de polinomios como producto de polinomios mónicos irreducibles, en cierto modo análoga a la factorización de enteros como producto de primos del Teorema Fundamental de la Aritmética:

Teorema 2.43. *Dado un polinomio $p(X) \in \mathbb{K}(X)$ de grado* $\deg(p(X)) \geq 1$*, existe una factorización de $p(X)$ de la forma*

$$p(X) = a_n \cdot m_1(X)^{r_1} \cdot m_2(X)^{r_2} \cdot \ldots \cdot m_k(X)^{r_k},$$

donde a_n es el coeficiente principal de $p(X)$, los polinomios $m_1(X), m_2(X), \cdots, m_k(X)$ son mónicos e irreducibles en $\mathbb{K}(X)$, y los números $r_1, \cdots, r_k$ son enteros positivos. La factorización es única salvo reordenación de los factores.

Ejemplo 2.44. La factorización única de $p(X) = 2X^3 - 4X$ en $\mathbb{R}[X]$ es

$$p(X) = 2X(X + \sqrt{2})(X - \sqrt{2}).$$

Ejercicio 2.45. Hallar la factorización única de $X^2 + 1 \in \mathbb{C}[X]$ y de $X^3 - 2 \in \mathbb{R}[X]$.

Ejercicio 2.46. Hallar las factorizaciones únicas de $6X^4 + 22X^2 - 8$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

Del teorema de factorización única de polinomios podemos extraer conclusiones acerca del número de raíces que estos pueden tener.

Definición 2.47. Sea α un elemento de $\mathbb{K}$ y $p(X) \in \mathbb{K}[X]$ un polinomio. Diremos que α es una raíz de $p(X)$ con *multiplicidad* r si

$$p(X) = (X - \alpha)^r \cdot q(X), \quad \text{con } q(\alpha) \neq 0.$$

Ejemplo 2.48. En $\mathbb{Z}_7[X]$, el 5 es una raíz de multiplicidad 4 de $2(X + 3)^3(X + 2)^4$.

Para polinomios de grado mayor que 1, podría darse el caso de tener una, varias o ninguna raíz, pero el número de raíces no podrá superar nunca el grado del polinomio:

Proposición 2.49. *Si un polinomio con coeficientes en un cuerpo tiene grado n, entonces la suma de las multiplicidades de sus raíces es menor o igual a n.*

Demostración: Supongamos que $p(X)$ tiene como raíces α_1 con multiplicidad r_1, α_2 con multiplicidad r_2, $\cdots$, α_s con multiplicidad r_s. Entonces, para cada i entre 1 y s, $(X-\alpha_i)^{r_i}$ es un factor de la factorización en polinomios irreducibles de $p(X)$. Luego existe un polinomio $q(X) \in k[X]$ tal que $p(X) = (X-\alpha_1)^{r_1} \cdot \ldots \cdot (X-\alpha_s)^{r_s} \cdot q(X)$ y el grado de $p(X)$, n, es igual a la suma de los grados de los factores, luego

$$n = r_1 + \cdots + r_s + \deg(q(X)).$$

□

Ejemplo 2.50. En $\mathbb{R}[X]$, la suma de multiplicidades de las raíces del polinomio $X^4 - 1$ es dos ya que sólo posee dos raíces *simples* (de multiplicidad 1): el 1 y el -1.

Sin embargo, en $\mathbb{C}[X]$, la suma de multiplicidades de sus raíces es cuatro ya que posee cuatro raíces simples en $\mathbb{C}$: el 1, el -1, i y $-i$.

Observación 2.51. En $\mathbb{C}[X]$, la suma de multiplicidades de las raíces de cualquier polinomio coincide exactamente con su grado, ya que como consecuencia del Teorema Fundamental del Álgebra (Corolario 2.39), en su factorización como producto de irrecucibles todos los irreducibles son de grado 1.

Ejercicio 2.52. Calcular la suma de las multiplicidades de las raíces de $3X^6 + 2X^5 + 3X^3 + 3X + 4 \in \mathbb{Z}_5[X]$.

Como ocurría con los números enteros, si conocemos la factorización de un polinomio como producto de irreducibles, entonces sabremos cuáles son todos sus divisores:

Proposición 2.53. *Si la factorización de un polinomio compuesto $p(X)$ es*

$$p(X) = a_n \cdot m_1(X)^{r_1} \cdot m_2(X)^{r_2} \cdot \ldots \cdot m_k(X)^{r_k},$$

entonces los divisores de $p(X)$ son los polinomios de la forma $\lambda \cdot m_1(X)^{j_1} \cdot \ldots \cdot m_k(X)^{j_k}$, con $\lambda \in \mathbb{K}^*$, y $0 \leq j_i \leq r_i$ para cada i.

Ejemplo 2.54. Calculemos el número de divisores del polinomio $p(X) = 2 \cdot (X+1)^2 \cdot (X+2)^3$ en $\mathbb{Z}_5[X]$. En total serán $4 \cdot 3 \cdot 4 = 48$, ya que serán de la forma

$$k \cdot (X+1)^a \cdot (X+2)^b \text{ donde } k \in \mathbb{Z}_5^*,\ 0 \leq a \leq 2 \text{ y } 0 \leq b \leq 3.$$

De ellos, 12 son mónicos (aquellos en los que $k = 1$).

2.5. Máximo común divisor y algoritmo de Euclides

Dados dos polinomios $p(X)$ y $q(X)$ de $\mathbb{K}[X]$, llamamos *máximo común divisor* de $p(X)$ y $q(X)$ al polinomio mónico de mayor grado que sea divisor común de ambos. Habitualmente lo denotamos por $\text{mcd}(p(X), q(X))$.

Ejemplo 2.55. $\mathrm{mcd}(X+1,\ X^2+2X+1) = X+1$ en $\mathbb{R}[X]$.

Ejercicio 2.56. Calcular el $\mathrm{mcd}(4X+4,\ 2X^2+4X+2)$ en $\mathbb{R}[X]$.

Observación 2.57. Si conocemos las factorizaciones únicas de $p(X)$ y $q(X)$ es sencillo calcular el $\mathrm{mcd}(p(X), q(X))$: será el producto de los factores irreducibles mónicos comunes con menor exponente.

Ejemplo 2.58. En $\mathbb{R}[X]$:

$$\mathrm{mcd}(3X^4-8X^3+6X^2-1,\ 3X^4-6X^3+12X^2-18X+9) =$$

$$\mathrm{mcd}(3\cdot(X-1)^3\cdot(X+{}^1\!/_3),\ 3\cdot(X-1)^2\cdot(X^2+3)) = (X-1)^2 = X^2-2X+1.$$

Ejercicio 2.59. En $\mathbb{Z}_5[X]$ calcular el $\mathrm{mcd}(2X^2+2,\ X^2+3X+2)$ y el $\mathrm{mcd}(3X^2+1,\ X+1)$ a partir de las factorizaciones únicas de los polinomios.

Observación 2.60. En la práctica, para obtener el máximo común divisor de dos polinomios $\mathrm{mcd}(p(X), q(X))$ vamos a utilizar el *algoritmo de Euclides*, similar al que vimos en el caso de los enteros, con ligeras modificaciones:

- los r_i ahora pasarán a ser $r_i(X)$ pues denotarán polinomios,
- ordenamos $p(X)$ y $q(X)$ en grado decreciente, y los denotamos por $r_0(X)$ y $r_1(X)$, de modo que $\deg(r_0(X)) \geq \deg(r_1(X))$,
- el último resto no nulo del algoritmo en ocasiones no es un polinomio mónico, y se tomará su polinomio mónico asociado como máximo común divisor.

Ejemplo 2.61. Para calcular el $\mathrm{mcd}(2X^2+2,\ X^2+3X+2)$ en $\mathbb{Z}_5[X]$ usando el algoritmo de Euclides escribiremos:

i	división euclídea	$r_i(X)$
0		$2X^2+2$
1		X^2+3X+2
2	$2X^2+2 = (X^2+3X+2)\cdot 2 + (4X+3)$	$4X+3$
3	$X^2+3X+2 = (4X+3)\cdot(4X+4)+0$	0

.

El $\mathrm{mcd}(2X^2+2,\ X^2+3X+2)$ será el polinomio mónico asociado al último resto no nulo. Esto es, el polinomio mónico asociado a $4X+3$. Lo calculamos multiplicando este polinomio por el inverso en $\mathbb{Z}_5$ de su coeficiente principal, que es $4^{-1}=4$:

$$\mathrm{mcd}(2X^2+2,\ X^2+3X+2) = 4^{-1}\cdot(4X+3) = 4\cdot(4X+3) = X+2.$$

Como en el caso de $\mathbb{Z}$, este algoritmo se puede extender al *algoritmo de Euclides extendido* con el que calcular coeficientes $\lambda_i(X)$ y $\mu_i(X)$ que nos permiten expresar cada resto $r_i(X)$ como combinación lineal de los polinomios iniciales $p(X)$ y $q(X)$. Este algoritmo nos ayudará a obtener la *identidad de Bézout* enunciada en el siguiente teorema:

Teorema 2.62 (**Identidad de Bézout**). *Dados dos polinomios $p(X)$ y $q(X)$ de $\mathbb{K}[X]$ no simultáneamente nulos, existen dos polinomios $\lambda(X)$ y $\mu(X)$ en $\mathbb{K}[X]$ tales que*

$$\lambda(X) \cdot p(X) + \mu(X) \cdot q(X) = \text{mcd}(p(X), q(X)).$$

Ejemplo 2.63. Hallemos polinomios $\lambda(X)$ y $\mu(X)$ en $\mathbb{Z}_5[X]$ para los que $\lambda(X) \cdot (3X^2 + 1) + \mu(X) \cdot (X + 1) = \text{mcd}(3X^2 + 1,\ X + 1)$, esto es, una Identidad de Bézout para el $\text{mcd}(3X^2 + 1,\ X + 1)$. Usaremos para ello el algoritmo de Euclides extendido, introduciendo dos columnas para ir calculando polinomios $\lambda_i(X)$ y $\mu_i(X)$ con valores iniciales 1, 0, 0, 1:

i	división euclídea	$r_i(X)$	$\lambda_i(X)$	$\mu_i(X)$
0		$3X^2 + 1$	1	0
1		$X + 1$	0	1
2	$3X^2 + 1 = (X + 1) \cdot (3X + 2) + 4$	4	1	$2X + 3$
3	$X + 1 = 4 \cdot (4X + 4) + 0$	0		

.

El $\text{mcd}(3X^2 + 1,\ X + 1)$ será el polinomio mónico asociado al último resto no nulo. Esto es, el polinomio mónico asociado a 4. Lo calculamos multiplicando este polinomio por el inverso en $\mathbb{Z}_5$ de su coeficiente principal. El coeficiente principal de un polinomio constante es esa misma constante. Por tanto multiplicamos por $4^{-1} = 4$:

$$\text{mcd}(2X^2 + 2,\ X^2 + 3X + 2) = 4^{-1} \cdot 4 = 1.$$

La igualdad obtenida para el último resto no nulo del algoritmo es

$$4 = 1 \cdot (3X^2 + 1) + (2X + 3) \cdot (X + 1).$$

Multiplicándola por el inverso del coeficiente principal del mcd obtenemos una identidad de Bézout:

$$1 = 4 \cdot (3X^2 + 1) + (3X + 2) \cdot (X + 1).$$

Los polinomios $\lambda(X) = 4$ y $\mu(X) = 3X + 2$ cumplen con lo buscado.

Definición 2.64. Dos polinomios son *primos entre sí* si su máximo común divisor es 1.

Ejemplo 2.65. Los polinomios del ejemplo anterior $3X^2 + 1$ y $X + 1$ de $\mathbb{Z}_5[X]$ son primos entre sí. Al ser primos entre sí, no tendrán ningún divisor irreducible en común.

3. El conjunto cociente $\mathbb{K}[X]/(f(X))$

3.1. Congruencias en $\mathbb{K}[X]$

En el tema anterior definimos sobre $\mathbb{Z}$ la relación de congruencia módulo un entero $m \geq 2$. En esta sección definiremos una relación análoga con polinomios de $\mathbb{K}[X]$: la relación de congruencia módulo un polinomio $f(X)$. A lo largo de esta sección $f(X)$ denotará un polinomio de $\mathbb{K}[X]$ fijado, de grado $\deg(f(X)) \geq 1$.

Definición 3.1. Dados $p(X), q(X) \in \mathbb{K}[X]$, diremos que $p(X)$ *es congruente con* $q(X)$ *módulo* $f(X)$ si $f(X) \mid p(X) - q(X)$.

Notación 3.2. Si $p(X)$ es congruente con $q(X)$ módulo $f(X)$ escribiremos

$$p(X) \equiv q(X) \,(\text{mod } f(X)).$$

Ejemplo 3.3. En $\mathbb{Q}[X]$:

$$X^2 - 3 \equiv X - 3 \,(\text{mod } X),$$

pues $(X^2 - 3) - (X - 3) = X^2 - X = X \cdot (X - 1)$ es múltiplo de X.

Ejercicio 3.4. ¿Es cierto que $5X^3 + 16X + 2 \equiv X + 2 \,(\text{mod } X^2 + 3)$ en $\mathbb{Q}[X]$?

La relación de congruencia módulo $f(X)$ cumple propiedades similares a las de la de congruencia para enteros. Por ejemplo las propiedades reflexiva, simétrica y transitiva:

Proposición 3.5. *La relación de congruencia módulo $f(X)$ es una relación de equivalencia sobre el conjunto $\mathbb{K}[X]$.*

Denotaremos por $\mathbb{K}[X]/(f(X))$ el conjunto cociente de esta relación. Recordemos que dos elementos están en la misma clase de equivalencia cuando están relacionados, en nuestro caso, dos polinomios están en la misma clase cuando son congruentes módulo $f(X)$.

Ejemplo 3.6. En $\mathbb{Q}[X]/(X)$ se tiene que $\overline{X^2 - 3} = \overline{X - 3}$.

Dada una clase de equivalencia $\overline{p(X)} \in \mathbb{K}[X]/(f(X))$, el siguiente resultado nos proporciona un método sencillo para encontrar el representante $r(X)$ de menor grado de la clase $\overline{p(X)}$. Consiste simplemente en calcular el resto de la división euclídea de $p(X)$ entre $f(X)$.

Lema 3.7. *Si $p(X) = f(X) \cdot c(X) + r(X)$ entonces $p(X) \equiv r(X) \,(\text{mod } f(X))$. Por tanto $\overline{p(X)} = \overline{r(X)}$ en $\mathbb{K}[X]/(f(X))$.*

Ejemplo 3.8. Si queremos hallar el representante de menor grado de $\overline{5X^3 + 16X + 2} \in \mathbb{Q}[X]/(X^2 + 3)$, habremos de calcular el resto de dividir $5X^3 + 16X + 2$ entre $X^2 + 3$:

$$5X^3 + 16X + 2 = (X^2 + 3) \cdot 5X + (X + 2).$$

Concluimos que al ser $5X^3 + 16X + 2 \equiv X + 2 \,(\text{mod } X^2 + 3)$, se cumple que $\overline{5X^3 + 16X + 2} = \overline{X + 2}$ en $\mathbb{Q}[X]/(X^2 + 3)$ y por tanto ese representante buscado de $\overline{5X^3 + 16X + 2}$ es $X + 2$.

Observación 3.9. El Lema anterior nos dice que cada clase $\overline{p(X)} \in \mathbb{K}[X]/(f(X))$ viene caracterizada por el resto de $p(X)$ módulo $f(X)$. Dicho resto es siempre un polinomio de grado menor que el del divisor $f(X)$. Por lo tanto, si $f(X)$ es de grado $\deg(f(X)) = n$,

$$\mathbb{K}[X]/(f(X)) = \{\overline{a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0} \ / \text{ cada } a_i \in \mathbb{K}\},$$

es decir, cada clase admite como representante a uno de los polinomios de grado menor que n y hay tantas clases distintas como polinomios de $\mathbb{K}[X]$ de grado menor que n.

Ejemplo 3.10. $\mathbb{Z}_3[X]/(X^2 + 1) = \{\overline{0}, \overline{1}, \overline{2}, \overline{X}, \overline{X+1}, \overline{X+2}, \overline{2X}, \overline{2X+1}, \overline{2X+2}\}$.

Observación 3.11. El cardinal de $\mathbb{Z}_p[X]/(f(X))$ es igual a $p^{\deg(f(X))}$.

Ejercicio 3.12. Calcular $\mathbb{Z}_2[X]/(X^3 + X)$ y $\mathbb{Q}[X]/(X^2 + 3)$.

3.2. Estructura de anillo

Observación 3.13. En el conjunto $\mathbb{K}[X]/(f(X))$ se pueden definir las siguientes operaciones

$$\begin{array}{rccc} + : \mathbb{K}[X]/(f(X)) \times \mathbb{K}[X]/(f(X)) & \longrightarrow & \mathbb{K}[X]/(f(X)) \\ (\overline{p(X)}, \quad \overline{q(X)}) & \longmapsto & \overline{p(X)+q(X)} \end{array}$$

$$\begin{array}{rccc} \cdot : \mathbb{K}[X]/(f(X)) \times \mathbb{K}[X]/(f(X)) & \longrightarrow & \mathbb{K}[X]/(f(X)) \\ (\overline{p(X)}, \quad \overline{q(X)}) & \longmapsto & \overline{p(X)\cdot q(X)} \end{array}$$

Al igual que ocurría con las operaciones de suma y producto en $\mathbb{Z}_m$, la suma y producto de clases de $\mathbb{K}[X]/(f(X))$ no dependen de los representantes de las clases escogidos.

Ejemplo 3.14. Calculemos $(\overline{X^2+1}\cdot\overline{X+1})+\overline{X+1}$ en $\mathbb{Z}_2[X]/(X^3+1)$. En $\mathbb{Z}_2[X]$ el polinomio $(X^2+1)\cdot(X+1)+(X+1) = X^3+X^2$, y el resto de la división de X^3+X^2 entre X^3+1 es X^2+1, luego el resultado es $\overline{X^2+1}$.

Ejercicio 3.15. Calcular $(\overline{X^2+1}+\overline{X+1})\cdot\overline{X^2}+\overline{1}$ en $\mathbb{Z}_2[X]/(X^3+X+1)$.

Proposición 3.16. *$(\mathbb{K}[X]/(f(X)), +, \cdot)$ es un anillo conmutativo.*

Demostración: (Ejercicio) Los neutros de suma y producto son el $\overline{0}$ y el $\overline{1}$ respectivamente. El opuesto de un elemento $\overline{p(X)} \in \mathbb{K}[X]/(f(X))$ es el elemento $\overline{-p(X)} \in \mathbb{K}[X]/(f(X))$.

Ejemplo 3.17. Las tablas de sumar y multiplicar en $\mathbb{Z}_2[X]/(X^2+X+1) = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}\}$ son:

$+$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\overline{0}$	$\overline{1}$
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{X+1}$	$\overline{1}$
$\overline{X+1}$	$\overline{0}$	$\overline{X+1}$	$\overline{1}$	$\overline{X}$

Obsérvese que los elementos neutros de suma y producto son el $\overline{0}$ y el $\overline{1}$ respectivamente, y que los opuestos de $\overline{0}$, $\overline{1}$, $\overline{X}$ y $\overline{X+1}$ son respectivamente $\overline{-0} = \overline{0}$, $\overline{-1} = \overline{1}$, $\overline{-X} = \overline{X}$ y $\overline{-(X+1)} = \overline{X+1}$.

3.3. Estructura de cuerpo

El siguiente resultado nos permite comprobar si un elemento es unidad de $\mathbb{K}[X]/(f(X))$.

Proposición 3.18. *Para un $\overline{p(X)} \in \mathbb{K}[X]/(f(X))$ se cumple:*

$$\overline{p(X)} \text{ es una unidad } \iff \operatorname{mcd}(p(X), f(X)) = 1.$$

Además, en este caso, si $\lambda(X)p(X)+\mu(X)f(X) = 1$ entonces $\overline{p(X)}^{-1} = \overline{\lambda(X)}$.

Ejemplo 3.19. El elemento $\overline{4X+3}$ de ${}^{\mathbb{Z}_5[X]}\!/_{(X^2+3X+2)}$ no es unidad del anillo pues

$$\mathrm{mcd}(4X+3,\ X^2+3X+2) = \mathrm{mcd}(4(X+2),\ (X+1)(X+2)) = X+2 \neq 1.$$

Ejemplo 3.20. El elemento $\overline{X+1}$ de ${}^{\mathbb{Z}_5[X]}\!/_{(3X^2+1)}$ sí que es unidad del anillo, pues $\mathrm{mcd}(X+1,\ 3X^2+1) = 1$ (ver Ejemplo 2.63). La identidad de Bézout calculada era

$$1 = 4 \cdot (3X^2+1) + (3X+2) \cdot (X+1).$$

Tomamos clases en ${}^{\mathbb{Z}_5[X]}\!/_{(3X^2+1)}$ y teniendo en cuenta que $\overline{3X^2+1} = \overline{0}$, se tiene que

$$\overline{1} = \overline{3X+2} \cdot \overline{X+1},$$

luego $\overline{X+1}^{-1} = \overline{3X+2}$.

Ejercicio 3.21. Comprobar que el elemento $\overline{2X+1}$ de ${}^{\mathbb{Z}_5[X]}\!/_{(X^2+3X+2)}$ es una unidad, y calcular su elemento inverso.

Observación 3.22. En algunos casos, el anillo ${}^{\mathbb{K}[X]}\!/_{(f(X))}$ es además un cuerpo, como por ejemplo ${}^{\mathbb{Z}_2[X]}\!/_{(X^2+X+1)}$ (ver Ejemplo 3.17). De su tabla de multiplicar deducimos que $\left({}^{\mathbb{Z}_2[X]}\!/_{(X^2+X+1)}\right)^* = \{\overline{1}, \overline{X}, \overline{X+1}\}$. Los inversos de las unidades serían en este caso $\overline{1}^{-1} = \overline{1}$, $\overline{X}^{-1} = \overline{X+1}$ y $\overline{X+1}^{-1} = \overline{X}$.

La siguiente es una caracterización de los anillos ${}^{\mathbb{K}[X]}\!/_{(f(X))}$ que son cuerpos.

Proposición 3.23. ${}^{\mathbb{K}[X]}\!/_{(f(X))}$ *es un cuerpo, si y sólo si,* $f(X)$ *es irreducible en* $\mathbb{K}[X]$.

Ejemplo 3.24. ${}^{\mathbb{Z}_5[X]}\!/_{(X^2+3X+2)}$ no es un cuerpo ya que $X^2+3X+2 = (X+1)(X+2)$ es compuesto en $\mathbb{Z}_5[X]$.

Ejercicio 3.25. ¿Es ${}^{\mathbb{Z}_2[X]}\!/_{(X^3+X+1)}$ un cuerpo?

Observación 3.26. Con lo visto hasta ahora hemos construido dos tipos de cuerpos finitos. En el tema anterior construimos cuerpos de cardinal un número primo p; estos son

$$(\mathbb{Z}_p, +, \cdot).$$

También podemos construir cuerpos con cardinal una potencia p^r de un número primo, con tal de buscar un polinomio irreducible $f(X) \in \mathbb{Z}_p[X]$, de grado r, y considerar el cuerpo

$$\left({}^{\mathbb{Z}_p[X]}\!/_{(f(X))}, +, \cdot\right).$$

Se puede demostrar que estos son los únicos cuerpos finitos que existen, es decir, sólo hay cuerpos finitos de cardinal p^r, con p primo y $r \geq 1$. Es más, para cada potencia p^r existe en esencia un único cuerpo de cardinal p^r salvo renombramiento de sus elementos.

3.4. El grupo de unidades

El conjunto de unidades de un anillo con la operación producto tiene estructura de grupo.

Definición 3.27. Un *grupo* $(G, *)$ es un conjunto G con al menos un elemento $e \in G$, junto con una operación $* : G \times G \Rightarrow G$, cumpliendo para cada $x, y, z \in G$ las propiedades:

G1) *Asociativa*: $(x * y) * z = x * (y * z)$.

G2) e es el *elemento neutro*: $x * e = x, \quad e * x = x$.

G3) Cada $x \in G$ posee un *elemento inverso* x^{-1}: $x * x^{-1} = e, \quad x^{-1} * x = e$.

Propiedades 3.28. *Si* $(A, +, \cdot)$ *es un anillo entonces* $(A^*, \cdot)$ *es un grupo.*

Observación 3.29. En el caso en que $\mathbb{K}$ es un cuerpo finito de p^r elementos, el grupo $(\mathbb{K}^*, \cdot)$ tiene una característica especial: es un grupo *cíclico*. Esto significa que existe un elemento $\beta \in \mathbb{K}^*$, que se llama *generador del grupo*, tal que

$$\mathbb{K}^* = \{\beta^n \ / \ 1 \leq n \leq p^r - 1\}.$$

La posibilidad de poder expresar los elementos no nulos como potencias de un elemento generador, es muy útil en la práctica, por ejemplo para multiplicar elementos o hallar inversos.

Ejemplo 3.30. El 3 es generador del grupo $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ ya que sus potencias generan todas las unidades:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

El 5 también sería generador de $\mathbb{Z}_7^*$ pues

$$5^1 = 5, \quad 5^2 = 4, \quad 5^3 = 6, \quad 5^4 = 2, \quad 5^5 = 3, \quad 5^6 = 1.$$

Sin embargo, ni el 1, ni el 2, ni el 4, ni el 6 son generadores de $\mathbb{Z}_7^*$.

Ejemplo 3.31. $\overline{X}$ es generador del grupo de unidades del cuerpo $\mathbb{Z}_2[X]/(X^3 + X + 1) = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}, \overline{X^2}, \overline{X^2+1}, \overline{X^2+X}, \overline{X^2+X+1}\}$. Si denotamos $g := \overline{X}$, se tiene que

$$\begin{array}{ll} g = \overline{X}, & g^5 = \overline{X^2+X+1}, \\ g^2 = \overline{X^2}, & g^6 = \overline{X^2+1}, \\ g^3 = \overline{X+1}, & g^7 = \overline{1}. \\ g^4 = \overline{X^2+X}, & \end{array}$$

Como $g^7 = \overline{1}$, deducimos cuál es el inverso de cada elemento: $\overline{X}^{-1} = \overline{X^2+1}$, $\overline{X^2}^{-1} = \overline{X^2+X+1}$ y $\overline{X+1}^{-1} = \overline{X^2+X}$, ya que $g^{-1} = g^6$, $(g^2)^{-1} = g^5$ y $(g^3)^{-1} = g^4$.

Ejercicio 3.32. Comprobar que el único generador del grupo $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ es el 2.

Ejercicio 3.33. Encontrar un generador del grupo de unidades de $\mathbb{Z}_3[X]/(X^2+1)$.