



**APUNTES DEL CURSO**

**2019-2020 IMPARTIDO**

**POR CAROLINA VALLEJO**

Rafael Sánchez

Revisión del 13 de octubre de 2019 a las 23:14.

# Índice general

<b>I</b>	<b>Primer parcial</b>	<b>5</b>
<b>1.</b>	<b>Anillos, polinomios y cuerpos</b>	<b>7</b>
1.1.	Anillos . . . . .	7
1.2.	Ideales . . . . .	10
1.3.	Homomorfismos . . . . .	12
1.4.	Anillos de polinomios . . . . .	14
1.5.	Criterios de irreducibilidad . . . . .	18
1.5.1.	Raíces múltiples e irreducibilidad . . . . .	19
1.6.	Cuerpos . . . . .	20
<b>II</b>	<b>Apéndices</b>	<b>23</b>
<b>2.</b>	<b>Índices</b>	<b>25</b>



Parte I

Primer parcial



# Capítulo 1

## Anillos, polinomios y cuerpos

### 1.1. Anillos

A lo largo de este curso se supondrán conocidos los contenidos de la asignatura *Estructuras Algebraicas*, se pueden encontrar unos apuntes de los mismos en: <https://github.com/knifecake/apuntes/raw/master/ea/apuntes-ea.pdf>.

**Definición 1** (Anillo). Un **anillo** es una terna  $(A, +, \cdot)$  donde  $+: A \times A \rightarrow A$  es una operación a la que llamamos suma,  $\cdot: A \times A \rightarrow A$  es otra operación a la que llamamos producto y se verifican las siguientes propiedades

1. El par  $(A, +)$  es un grupo abeliano
2. El producto  $\cdot$  es asociativo
3. Se cumplen las propiedades distributivas:

$$\forall a, b, c \in A, \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad (1.1)$$

$$\forall a, b, c \in A, \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad (1.2)$$

Con la operación  $+$  tenemos las siguientes propiedades

1. Asociatividad:  $(a + b) + c = a + (b + c)$
2. Elemento neutro aditivo:  $\exists! \mathbf{0} \in A \mid \mathbf{0} + a = a$
3. Elemento inverso aditivo:  $\forall a \in A, \exists -a \in A \mid a + (-a) = \mathbf{0}$
4. Conmutatividad aditiva:  $\forall a, b \in A, \quad a + b = b + a$

Con la operación  $\cdot$  tenemos las siguientes propiedades

1. Asociatividad:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. No siempre existe el neutro multiplicativo:  $\mathbf{1} \in A \mid a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$
3. No siempre el producto es conmutativo.
4. No siempre existe inverso multiplicativo:  $a^{-1} \mid a \cdot a^{-1} = \mathbf{1}$
5. No siempre se da la conmutatividad multiplicativa:  $a \cdot b = b \cdot a$

**Proposición 1** (Producto con 0 en anillos).  $\forall a \in A, \quad a \cdot \mathbf{0} = \mathbf{0}$

*Demostración.*  $a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0} \implies \mathbf{0} = a \cdot \mathbf{0}$

◇

Además, a lo largo de este curso vamos a referirnos únicamente a los anillos conmutativos con unidad (o unitario), que cumplen las siguientes definiciones.

**Definición 2** (Anillo con unidad o anillo unitario). Sea  $(A, +, \cdot)$  un anillo. Decimos que es un anillo con unidad o un **anillo unitario** si tiene elemento neutro multiplicativo, es decir, si  $\exists \mathbf{1} \in A \mid \forall a \in A, \mathbf{1}a = a\mathbf{1} = a$ .

**Definición 3** (Anillo conmutativo). Sea  $(A, +, \cdot)$  un anillo. Decimos que es un **anillo conmutativo** si se cumple que:

$$r \cdot s = s \cdot r, \quad \forall r, s \in A$$

**Ejemplo 1** (*Ejemplos de anillos*)

$\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  y  $\mathbb{C}$  con la suma y producto usual verifican todas las definiciones de anillo, anillo conmutativo y anillo unitario.

Vamos a considerar además el concepto de anillo de polinomios:

**Definición 4** (Anillo de polinomios). Sea  $R$  un anillo, definimos el **anillo de polinomios**  $R[x]$  como:

$$R[x] = \left\{ \sum_{i=0}^n a_i \cdot x^i \mid a_i \in R, n \in \mathbb{N} \right\}$$

Es fácil ver que  $R[x]$  es un anillo pues la suma y el producto son transitivos y asociativos.

**Observación.** Vamos a considerar algunas definiciones y convenciones menores.

1. Sea  $p \in R[x]$ ,  $p$  es un polinomio y escribimos:

$$p(x) = a_0 + a_1x + \dots + a_nx^n$$

Donde llamamos *coeficientes* del polinomio a los  $a_i$ .

2. Sea  $p \in R[x] = \sum_{i \geq 0} a_i x^i$ , denominamos grado de  $p$  a:

$$\delta(p) = \max \{i \mid a_i \neq 0\}$$

3. Sea  $p \in R[x] = a_0 + a_1x + \dots + a_nx^n$ , llamamos *coeficiente director* al coeficiente del término de mayor grado ( $a_n$ ).
4. Sea  $p \in R[x] = a_0 + a_1x + \dots + a_nx^n$ , llamamos *término independiente* al coeficiente libre ( $a_0$ ).
5. Sea  $p \in R[x]$  con todos los coeficientes nulos, entonces  $p$  es el *polinomio cero*.

$$0 = \sum_{i \geq 0} 0 \cdot x^i$$

Por convención,  $\delta(0) = -\infty$ .

**Definición 5** (Polinomio mónico). Sea  $R[x]$  un anillo de polinomios, decimos que  $p \in R[x]$  es **mónico** si y sólo si su *término director* es 1.

**Definición 6** (Divisor de cero). Sea  $R$  un anillo, decimos que  $r \in R$  es un **divisor de cero** si satisface:

$$\exists s \in R, s \neq 0 : r \cdot s = 0$$



**Definición 7** (Unidad de un anillo). Sea  $R$  un anillo, decimos que  $r \in R$  es una **unidad** si satisface:

$$\exists s \in R : r \cdot s = \mathbf{1}$$

Decimos entonces que  $r \in \mathcal{U}(R)$ , con  $\mathcal{U}(R) = \{a \mid a \text{ es una unidad}\}$

**Definición 8** (Dominio de integridad). Sea  $R$  un anillo,  $R$  es un **dominio de integridad** si no tiene divisores de  $\mathbf{0}$ .

**Definición 9** (Cuerpo). Sea  $(A, +, \cdot)$  un anillo conmutativo con unidad. Diremos que  $A$  es un cuerpo si  $A^\times = A \setminus \{\mathbf{0}\}$  es cerrado por la segunda operación (el *producto*).

**Observación.**

- $R$  es un cuerpo si  $\mathcal{U}(R) = R$ .
- $\mathbf{1} \in \mathcal{U}(R)$ , para todo  $R$  anillo unitario.

**Proposición 2** (Cuerpo y dominio de integridad). Sea  $R$  un cuerpo, entonces  $R$  es un dominio de integridad.

*Demostración.* Vamos a ver que  $R$  no tiene divisores de  $\mathbf{0}$ . Sea  $r \in R^\times = R \setminus \{\mathbf{0}\}$ , supongamos  $\exists s \in R^\times$  tal que:

$$r \cdot s = \mathbf{0}$$

Como  $r \in \mathcal{U}(R) = R^\times$  pues  $R$  es un cuerpo, entonces,  $\exists t \in R$  tal que  $t \cdot r = r \cdot t = \mathbf{1}$ . Por tanto:

$$\mathbf{0} = t \cdot (r \cdot s) = (t \cdot r) \cdot s = \mathbf{1} \cdot s = s$$

Y  $s = \mathbf{0}$  contradice la hipótesis. Concluimos con que  $\nexists r, s \in R$  tal que  $r \cdot s = \mathbf{0}$  ◇

**Proposición 3** (Dominio de integridad en anillos de polinomios). Sea  $R$  un anillo. Si  $R$  es un dominio de integridad, entonces  $R[x]$  es un dominio de integridad.

*Demostración.* Sean  $f, g \in R[x]^\times$ , y  $a_m, b_k$  sus términos directores respectivamente. Como  $R$  es un dominio de integridad,  $a_m \cdot b_k \neq \mathbf{0}$ , que coincide con el término director de  $f \cdot g$  y no es nulo. Por tanto,  $R[x]$  es un dominio de integridad. ◇

**Proposición 4** (Propiedad de cuerpo en anillos de polinomios).  $R[x]$  nunca es un cuerpo.

*Demostración.* Solo hay que comprobar que aunque  $f(x) = x \in R[x]$ ,  $f(x) \notin \mathcal{U}(R[x])$ . Y por tanto  $\mathcal{U}(R[x]) \neq R[x]$ , lo que nos dice que  $R[x]$  no es un cuerpo. ◇

**Proposición 5** (Unidades en anillos de polinomios). Sea  $R$  un anillo, si  $R$  es un dominio de integridad, entonces  $\mathcal{U}(R) = \mathcal{U}(R[x])$ .

**Observación.** Podemos definir anillos como *extensión* de otros, al igual que hicimos con los anillos de polinomios:

- $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ , con  $d \neq e^2$ ,  $\forall e \in \mathbb{Z}$  es un anillo y un dominio de integridad, pero no es un cuerpo.
- $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ , con  $d \neq e^2$ ,  $\forall e \in \mathbb{Z}$  es un cuerpo. Decimos que  $\{1, \sqrt{d}\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}[\sqrt{d}]$ , pues todos los elementos de  $\mathbb{Q}[\sqrt{d}]$  se pueden expresar como combinación lineal de los elementos de la  $\mathbb{Q}$ -base.

**Definición 10** (Subanillo). Sea  $R$  un anillo,  $S \subseteq R$ ,  $1 \in S$ . Decimos que  $S$  es un **subanillo** si:

- $S$  es cerrado por suma y producto.
- Todo elemento tiene opuesto, es decir,  $\forall a \in S, \exists b \in S : a + b = 0$ .

**Definición 11** (Subcuerpo). Sean  $R$  un cuerpo,  $S \subseteq R$ . Decimos que  $S$  es un **subcuerpo** si:

- $S$  es un subanillo de  $R$
- Todo elemento no nulo tiene inverso, es decir,  $\forall a \in S^\times, \exists b \in S^\times : a \cdot b = 1$

**Ejemplo 2** (*Ejemplos de subanillos y subcuerpos*)

- $\mathbb{Z}$  es subanillo de  $\mathbb{Q}$
- $\mathbb{Q}$  es subcuerpo de  $\mathbb{R}$  y  $\mathbb{C}$
- $\mathbb{Z}[\sqrt{d}]$  es subanillo de  $\mathbb{Q}[\sqrt{d}]$

## 1.2. Ideales

**Definición 12** (Ideal). Sea  $R$  un anillo, e  $I \subseteq R$ .  $I$  es un **ideal** si:

1.  $\forall a, b \in I, a - b \in I$
2.  $\forall r \in R, \forall a \in I$  se satisface:  $r \cdot a \in I$

Los ideales triviales son  $\{0\}$  y  $R$ .

**Observación.** Sea  $R$  un anillo, denotamos al ideal generado por  $a \in R$  como:

$$\langle a \rangle$$

**Proposición 6** (Ideal propio). Sea  $R$  un anillo,  $I$  un ideal:

$$I \subsetneq R \iff 1 \notin I \iff I \cap \mathcal{U}(R) = \emptyset$$

**Observación.** Sea  $R$  un anillo,  $I \leq R$  un ideal:

$$I \leq R \iff I \cap \mathcal{U}(R) = \emptyset$$

$$I = R \iff I \cap \mathcal{U}(R) \neq \emptyset$$

**Proposición 7** (Ideales y cuerpos). Sea  $R$  un cuerpo, y sea  $I$  un ideal de  $R$  (escribimos  $I \leq R$ ), entonces  $I = \{0\}$  o  $I = R$ , ( $I$  es impropio).

El recíproco también es cierto.

*Demostración.*

- ( $\implies$ )

$$R \text{ cuerpo} \implies \mathcal{U}(R) = R^\times \implies I = \mathcal{U}(R) \cup \{0\} \text{ o trivialmente } I = \{0\}$$

- ( $\impliedby$ )

$$\text{Sea } a \in R^\times, a \in \langle a \rangle \leq R$$

$$\{0\} \neq I = \langle a \rangle, \text{ entonces } I = R \implies \exists u \in I \cap \mathcal{U}(R) \neq \emptyset \implies u \in \langle a \rangle \implies u = a \cdot r, \text{ con } r \in R$$

y por tanto:

$$1 = u \cdot u^{-1} = a \cdot r \cdot u^{-1} \implies a \in \mathcal{U}(R) \implies R \text{ es un cuerpo}$$

◇

**Ejemplo 3 (Ejemplos de ideales)**

1.  $n\mathbb{Z} \leq \mathbb{Z}$
2.  $I = \{f \in \mathbb{Z}[x] \mid \text{el termino independiente de } f \text{ es par}\}$

**Definición 13** (Ideal principal). Sea  $R$  un anillo,  $a \in R$  un elemento. El ideal generado por  $a$ :

$$\langle a \rangle = \{a \cdot r \mid r \in R\} = aR$$

se denomina **ideal principal** generado por  $a$ .

**Proposición 8** (Propiedades de ideales). Sea  $R$  un anillo e  $I \leq R$  un ideal.

1. Sean  $I, J \leq R$  ideales, entonces  $I + J = \{a + b \mid a \in I, b \in J\} \leq R$  es un ideal.
2. Sea  $\mathbf{a} \in \mathbb{R}^n$ , entonces  $I = \langle \mathbf{a} \rangle = \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\} \leq R$  es un ideal.
3.  $R/I = \{r + I \mid r \in R\}$  es un anillo.
4. (Teorema de correspondencia) Existe una biyección de la forma:

$$\begin{aligned} \{J \leq R \mid I \subseteq J \subseteq R\} &\longrightarrow \{J/I \leq R/I\} \\ J &\longmapsto \{r + I \mid r \in J\} \end{aligned}$$

**Observación.** En particular, si en  $R$  todo ideal es principal e  $I \leq R$ , en  $R/I$  todo ideal es principal.

**Ejercicio (H1.5).** Sea  $n$  un número natural. Prueba que  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$  es un cuerpo si y sólo si  $n$  es primo.

■ (  $\Leftarrow$  )

$n$  primo  $\implies \forall k : 0 < k < n$  se cumple que  $\text{mcd}(k, n) = 1$ , y por Bezout:

$$1 = ka + nb, \quad \text{con } a, b \in \mathbb{Z}$$

Donde el término  $nb \equiv 0$  en  $\mathbb{Z}/n\mathbb{Z}$  y por tanto queda  $1 = ka$ , lo que quiere decir que  $k$  es el inverso de  $a$  en  $\mathbb{Z}/n\mathbb{Z}$ .

■ (  $\implies$  )

Partimos de que  $\mathbb{Z}/n\mathbb{Z}$  es cuerpo, por la proposición 2 sabemos que  $\mathbb{Z}/n\mathbb{Z}$  es un dominio de integridad. Supongamos  $n$  no primo, entonces  $n = a \cdot b$ , entonces:

$$n \equiv \mathbf{0} \pmod{n} \implies \mathbf{0} = (a + n\mathbb{Z})(b + n\mathbb{Z})$$

Pero es imposible, ya que  $a$  y  $b$  serían divisores de  $\mathbf{0}$  pero estamos en un dominio de integridad. Por tanto,  $n$  es necesariamente primo.

**Ejercicio (H1.12).** ¿Cuántos elementos tiene el anillo  $\mathbb{Z}[i]/\langle 2i \rangle$ ? ¿Se trata de un cuerpo?

Comenzamos escribiendo los conjuntos que forman parte del cociente:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

$$\langle 2i \rangle = \langle 2 \rangle = 2\mathbb{Z}[i] = \{2(a + bi) \mid a, b \in \mathbb{Z}\} = (2\mathbb{Z})[i] = \{a + bi \mid a, b \in 2\mathbb{Z}\}$$

El conjunto cociente es por tanto:

$$\mathbb{Z}[i]/\langle 2i \rangle = \mathbb{Z}[i]/2\mathbb{Z}[i] = \{a + bi + 2\mathbb{Z}[i] \mid a, b \in \mathbb{Z}\}$$

Donde se tiene que:

$$a+bi+2\mathbb{Z}[i] = a_1+b_1i+2\mathbb{Z}[i] \iff a-a_1 \in 2\mathbb{Z} \text{ y } b-b_1 \in 2\mathbb{Z} \iff \{a+bi+2\mathbb{Z}[i] \mid a,b \in \{0,1\}\} = \{0,1,i,1+i\}$$

De esta forma vemos que el anillo tiene 4 elementos y además no es un cuerpo ya que  $i$  no tiene inverso.

**Definición 14** (Ideal primo). Sea  $R$  un anillo e  $I \leq R$  un ideal, diremos que  $I$  es un **ideal primo** si:

$$a \cdot b \in I \implies a \in I \text{ ó } b \in I$$

**Definición 15** (Ideal maximal). Sea  $R$  un anillo e  $I \leq R$  un ideal, diremos que  $I$  es un **ideal maximal** si:

$$I \subseteq J \leq R \implies J = I \text{ ó } J = R$$

**Teorema 9** (Cociente de ideales primos y maximales). Sea  $R$  un anillo,  $I \leq R$  un ideal:

1.  $I$  es primo  $\iff R/I$  es un dominio de integridad.
2.  $I$  es maximal  $\iff R/I$  es un cuerpo.
3.  $I$  ideal maximal  $\implies I$  ideal primo.

*Demostración.*

1. Se deja como ejercicio. Es directa usando definiciones.
2.  $I$  es maximal  $\iff R/I$  no tiene ideales propios (por el teorema de correspondencia 4). Y ya sabemos que  $R/I$  no tiene ideales propios  $\iff R/I$  es un cuerpo.
3. Se sigue de los apartados anteriores junto a la proposición 2 que nos dice que un cuerpo es un dominio de integridad.

◇

### 1.3. Homomorfismos

**Definición 16** (Homomorfismo de anillos). Sean  $R, S$  anillos,  $\varphi : R \rightarrow S$  es un **homomorfismo de anillos** si:

1.  $\varphi$  es homomorfismo de grupos, es decir,  $\varphi(0) = 0$  y  $\varphi(a-b) = \varphi(a) - \varphi(b)$ .
2.  $\varphi(1) = 1$ .
3.  $\varphi(ab) = \varphi(a)\varphi(b)$ .

**Observación.**

- $\ker \varphi = \{a \in R \mid \varphi(a) = 0\} \leq R$ .
- $\varphi(R) \subseteq S$  es un subanillo. (No es ideal en general).
- $\varphi$  sobreyectiva, es decir,  $\varphi$  es un epimorfismo  $\iff \varphi(R) = S$ .

**Observación.** Si  $R$  y  $S$  son cuerpos y  $\varphi : R \rightarrow S$  es un homomorfismo de anillos, llamaremos a  $\varphi$  homomorfismo de cuerpos. Además  $\varphi$  es inyectivo pues:

$$1 \notin \ker \varphi \leq R \text{ cuerpo} \implies \ker \varphi = 0$$

**Ejemplo 4** (*Proyección canónica*)

Sea  $R$  un anillo,  $I \leq R$  un ideal, es fácil ver que  $\pi : R \rightarrow R/I; r \mapsto r + I$  es un epimorfismo de anillos con  $\ker \pi = I$ .

**Observación.**

$$R/\ker \varphi = R/I$$

**Teorema 10** (Primer teorema de isomorfía). Sea  $\varphi : R \rightarrow S$  un homomorfismo de anillos, se tiene que:

$$\begin{aligned}\bar{\varphi} : R/\ker \varphi &\longrightarrow \varphi(S) \\ r + \ker \varphi &\longmapsto \bar{\varphi}(r + \ker \varphi) = \varphi(r)\end{aligned}$$

es un isomorfismo de anillos.

*Demostración.* Se deja como ejercicio.  $\diamond$

**Observación.** Sea  $\pi$  la proyección canónica,  $\bar{\pi} = id_{R/I}$

**Ejercicio** (H1.14). Demuestra que si  $\varphi : R \rightarrow S$  es un homomorfismo de anillos y  $a \in \mathcal{U}(R)$ , entonces  $\varphi(a) \in \mathcal{U}(S)$ . ¿Es cierto el recíproco?

Si  $a \in \mathcal{U}(R)$ , entonces  $\exists b \in R$  tal que  $1 = a \cdot b$ . Por tanto:

$$1 = \varphi(1) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \implies \varphi(a) \in \mathcal{U}(S)$$

El recíproco solo es cierto si  $\varphi$  es un isomorfismo, pero en general no. Como contraejemplo consideramos el homomorfismo identidad  $\iota : \mathbb{Z} \rightarrow \mathbb{Q}; a \mapsto a$ . Es fácil ver que es un homomorfismo de anillos, sin embargo:  $\iota(2) = (2)$  pero  $\iota(2) \in \mathcal{U}(\mathbb{Q})$  y  $2 \notin \mathcal{U}(\mathbb{Z})$ .

**Ejercicio** (H1.16). Demuestra que:

1. No existe ningún homomorfismo de anillos  $\varphi : \mathbb{Q} \rightarrow \mathbb{Z}_p$  para  $p \in \mathbb{Z}$  primo.
2. No existe ningún homomorfismo de anillos  $\varphi : \mathbb{R} \rightarrow \mathbb{Q}$ .

Solución:

1. Sea  $\varphi : \mathbb{Q} \rightarrow \mathbb{Z}_p; 1 \mapsto 1 + p\mathbb{Z}$ .

$$\varphi(p) = \varphi\left(\sum_1^p 1\right) = \sum_1^p (1 + p\mathbb{Z}) = p + p\mathbb{Z} = 0.$$

y como  $p \in \mathcal{U}(\mathbb{Q})$ , es imposible que la imagen de una unidad no sea otra por medio de un homomorfismo, por tanto, dicho homomorfismo no existe.

2. Sea  $\varphi : \mathbb{R} \rightarrow \mathbb{Q}; \sqrt{2} \mapsto a$

$$2 = \varphi(1 + 1) = \varphi(2) = \varphi(\sqrt{2}^2) = \varphi(\sqrt{2})^2 = a^2, a \in \mathbb{Q}$$

que es una contradicción pues no existe dicho  $a$ , con lo que no existe el homomorfismo.

**Ejercicio** (H1.21). Fijado un entero  $n \in \mathbb{Z}$  con  $n \geq 2$ , demuestra que el anillo cociente  $\mathbb{Z}[x]/n\mathbb{Z}[x]$  es isomorfo a  $\mathbb{Z}_n[x]$ . Concluye que el ideal  $n\mathbb{Z}[x]$  es primo si y sólo si  $n$  es un número primo.

Vamos a dar una guía de como proceder con el ejercicio:

$$\text{Sea } \varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_n[x]; (a_0 + \dots + a_n x^n) \mapsto (\bar{a}_0 + \dots + \bar{a}_n x^n)$$

donde  $\bar{a}_i = a_i + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ .

- Comprobar que  $\varphi$  es un homomorfismo de anillos.
- Comprobar que  $\varphi$  es sobreyectiva.

- Ver que  $\ker \varphi = n\mathbb{Z}[x]$ .
- Aplicar el teorema de isomorfía.

**Ejemplo 5 (Homomorfismo de evaluación)**

Sea  $R$  un anillo,  $a \in R$ .

$$\begin{aligned}\mathcal{E}_a : R[x] &\longleftarrow R \\ f(x) &\longmapsto f(a)\end{aligned}$$

es un homomorfismo de anillos sobreyectivo.

**Observación.** Si  $R = K$  es un cuerpo:

$$K[x] / \ker \mathcal{E}_a \simeq K \implies \ker \mathcal{E}_a \text{ es maximal.}$$

**1.4. Anillos de polinomios**

**Proposición 11** (Algoritmo de la división). Sea  $R$  un anillo,  $f, g \in R[x]^\times$  polinomios con coeficientes en  $R$ . Si el coeficiente director de  $g$  es una unidad de  $R$ , entonces  $\exists d, r \in R[x]$  únicos tales que:

$$f = g \cdot d + r \text{ con } \delta(r) < \delta(g)$$

Diremos que  $g \mid f$  si  $r = 0$ .

**Definición 17** (Raíz de un polinomio). Sea  $R$  un anillo,  $f \in R[x]^\times$  un polinomio, decimos que  $a \in R$  es una **raíz** de  $f$  si  $\mathcal{E}_a(f) = f(a) = 0$

**Corolario 1** (Ruffini). Sea  $R$  un anillo,  $f \in R[x]^\times$  un polinomio:

$$a \text{ es raíz de } f \iff f(x) = (x - a) \cdot g(x)$$

*Demostración.*

▪ (  $\Leftarrow$  )

$$\mathcal{E}_a(f) = \mathcal{E}_a(x - a) \cdot \mathcal{E}_a(g) = 0$$

▪ (  $\Rightarrow$  )

$$f(x) = (x - a) \cdot d(x) + r(x); \delta(r) \leq \delta(x - a) \implies r \in R; f(a) = r = 0 \implies g(x) = d(x)$$

◇

**Ejemplo 6 (Uso de Ruffini)**

Sea  $f(x) = x^2 + x + 1$ ,  $f(x) \in \mathbb{Z}_3[x]$ .

Es fácil ver que  $f(1) = 0$ , según Ruffini (corolario 1)  $(x - 1) \mid f$ . Y es cierto, de hecho:  $f(x) = (x - 1)(x - 1)$ .

**Teorema 12** (Raíces y dominio de integridad). Sea  $R$  un dominio de integridad,  $f \in R[x]^\times$  un polinomio y  $\alpha_1, \dots, \alpha_n$  raíces distintas de  $f$ , entonces  $n \leq \delta(f)$ .

*Demostración.* Vamos a probarlo por inducción sobre  $\delta(f)$

- Caso base:  $\delta(f) = 1$ . Entonces  $f(x) = ax + b$ . Sea  $\alpha_1$  raíz de  $f(x)$ , entonces  $a\alpha_1 = -b$ . Si  $\alpha_2$  es raíz de  $f$ , entonces  $a\alpha_2 = -b \implies a\alpha_1 = a\alpha_2 \implies a(\alpha_1 - \alpha_2) = 0$  y como  $a \neq 0$  y  $R$  es dominio de integridad  $\alpha_1 - \alpha_2 = 0 \implies \alpha_1 = \alpha_2$

- $\delta(f) = m > 1$ . Sea  $\alpha_1$  raíz de  $f$ , por Ruffini  $f(x) = (x - \alpha_1)d(x)$ . Por hipótesis,  $\alpha_2 \dots \alpha_n$  son raíces de  $f$  distintas de  $\alpha_1$ , por lo que necesariamente  $d(\alpha_i) = 0 \forall i \in [2, n]$ . Por la hipótesis de inducción  $n - 1 \leq \delta(d) = \delta(f) - 1 \implies n \leq \delta(f)$

◇

**Observación.** La hipótesis de que  $R$  sea un dominio integridad es necesaria. Se puede comprobar que en  $\mathbb{Z}_8[x]$ , el polinomio  $f(x) = x^2 - 1$  con  $\delta(f) = 2$ , tiene 4 raíces:  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ . Sin embargo, no supondrá un problema a lo largo del curso ya que trabajaremos con cuerpos.

**Ejercicio (H1.27).** Demuestra que si  $K$  es un cuerpo finito y  $f, g \in K[x]$  tales que  $f(a) = g(a)$  para todo  $a \in K$ , entonces  $f = g$ . ¿Qué ocurre si  $K$  es finito?.

Supongamos  $h = f - g \in K[x]$ . Entonces  $h(a) = 0 \forall a \in K$  con  $K[x]$  un cuerpo infinito implica necesariamente que  $h = 0$  y por tanto  $f = g$ .

Si  $K$  es finito, por ejemplo  $K = \mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$  con  $p$  un primo, consideramos el polinomio  $f(x) = x^p - x$ . En este caso  $f(x) \neq 0$  pero se anula en todo elemento de  $\mathbb{Z}_p$  ya que  $a^p \equiv a \pmod{p}$  por el pequeño teorema de Fermat.

**Teorema 13** (Pequeño teorema de Fermat). Si  $p$  es un número primo, entonces, para cada número natural  $a$ , con  $a > 0$ ,  $a^p \equiv a \pmod{p}$ .

**Teorema 14** (Ideales principales). Sea  $K$  un cuerpo,  $I \leq K[x]$  un ideal tal que  $I \neq \{0\}$ , entonces existe un  $p \in K[x]$  tal que  $I = \langle p \rangle$ .

*Demostración.* Sea  $p \in I$  con el menor grado finito posible, es decir, sea  $0 \neq g \in I \implies \delta(g) \geq \delta(p) \forall g \in I$ . Entonces por el algoritmo de la división, para  $f \in I$ ,  $f = pd + r$ , con  $d, r \in K[x]$  y  $\delta(r) < \delta(p) \implies r \in I$ . Por la elección de  $p$ , la única opción es que  $r = 0$  entonces  $f = pd \implies f \in \langle p \rangle$ . ◇

**Ejercicio (H1.25).** Hallar un generador de  $I = \langle x^3 + 1, x^2 + 1 \rangle$  en  $\mathbb{Z}_2[x]$ .

Basta observar que en  $\mathbb{Z}_2[x]$ ,  $(x^2 + 1) = (x + 1)^2$  y  $(x^3 + 1) = (x + 1) \cdot (x^2 + x + 1)$ , por tanto,  $I = \langle x + 1 \rangle$ .

**Definición 18** (Dominio de ideales principales). Un anillo  $R$  en el que todo ideal es principal y es un dominio de integridad se llama **dominio de ideales principales** (o DIP para abreviar).

**Definición 19** (Elemento irreducible). Sea  $R$  un anillo y  $a \neq 0 \in \mathcal{U}(R)$ , decimos que  $a$  es **irreducible** si  $a = b \cdot c \implies$  tiene que ocurrir que  $b \in \mathcal{U}(R)$  o que  $c \in \mathcal{U}(R)$

**Teorema 15** (Irreducibilidad en DIP). Sea  $R$  un dominio de ideales principales, entonces:

$$a \in R \text{ irreducible} \iff \langle a \rangle \text{ es maximal.}$$

*Demostración.*

$\implies$  Sea  $\langle a \rangle \subseteq J \leq R$ , con  $J = \langle b \rangle$ . Si  $J \neq R$  entonces  $b \notin \mathcal{U}(R)$ . Falta ver que  $\langle a \rangle = \langle b \rangle$ . Como  $\langle a \rangle \subseteq \langle b \rangle$ ,  $a = b \cdot c$  con  $c \in R$ . Además como  $b \notin \mathcal{U}(R)$  y  $a$  es irreducible, entonces  $c \in \mathcal{U}(R)$  y con ello  $\langle a \rangle = \langle bc \rangle = \langle b \rangle$ .

$\Leftarrow$  Sabemos que  $\langle a \rangle \leq R$  es maximal. Sea  $a = bc$  con  $b, c \in R$ , entonces:

$$\langle a \rangle \subseteq \langle b \rangle \leq R \implies \text{ o bien } (\langle a \rangle = \langle b \rangle \implies c \in \mathcal{U}(R)) \text{ o bien } (\langle b \rangle = R \implies b \in \mathcal{U}(R))$$

y por tanto  $a$  es irreducible.

◇

**Corolario 2.** Sea  $0 \neq f \in K[x]$ , con  $K$  un cuerpo.

$$f \text{ es irreducible} \iff K[x]/\langle f \rangle \text{ es un cuerpo.}$$

*Demostración.* La prueba es directa sabiendo que  $K[x]$  es un DIP, el teorema anterior y el teorema 9. ◇

**Observación.**  $f \in K[x]$  es irreducible si  $\delta(f) > 1$  y  $f \neq gh$  con  $g, h \in K[x]$ ,  $\delta(g) < \delta(f)$  y  $\delta(h) < \delta(f)$ .

**Observación.** En  $K[x]$  los polinomios de grado 1 son irreducibles por definición. Los de grado 2 y grado 3 son irreducibles  $\iff$  no tienen raíces en  $K$  (por Ruffini).

**Corolario 3** (Euclides). Sea  $0 \neq f \in K[x]$  irreducible, si  $f \mid gh$  entonces  $f \mid g$  o  $f \mid h$ .

*Demostración.*

$$f \text{ irreducible} \implies \langle f \rangle \text{ es maximal} \implies \langle f \rangle \text{ es primo.}$$

Por definición de ideal primo:

$$f \mid gh \iff gh \in \langle f \rangle \iff g \in \langle f \rangle \vee h \in \langle f \rangle$$

◇

### Ejemplo 7

Este corolario nos permite construir cuerpos finitos distintos a los  $\mathbb{F}_p$ .

$E = \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$  es un cuerpo. Veamos su caracterización.

- Primero comprobamos que  $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$  es irreducible. Como es un polinomio de grado 2, es irreducible si no tiene raíces en  $\mathbb{F}_2$ , y es cierto ya que  $f(0) = f(1) = 1$ .
- Los elementos de  $E$  son de la forma:  $g + \langle f \rangle$ , y además  $g + \langle f \rangle \neq 0$  en  $E \iff g \notin \langle f \rangle$ .  
 $g = fq + r$ ,  $\delta(r) < \delta(f) = 2$  y como  $g$  no es múltiplo,  $0 \leq \delta(r) \leq 1$ .  
 $g + \langle f \rangle = r + fq + \langle f \rangle = r + \langle f \rangle$ . Por tanto, todo elemento en  $E$  tiene un representante con grado menor a 2.

Y por tanto:

$$E = \{a + bx + \langle f \rangle \mid a, b \in \mathbb{F}_2\} \implies E = \{0, 1, x, x + 1\}$$

**Teorema 16** (Máximo común divisor). Sean  $K$  cuerpo,  $0 \neq f, g \in K[x]$  polinomios, existe un único polinomio mónico  $d \in K[x]$  tal que:

$$\langle f \rangle + \langle g \rangle = \langle d \rangle \text{ es decir, } \exists a, b \in K[x] : d = af + bg$$

Además,  $d \mid f$  y  $d \mid g$  y si  $\exists e \mid f$  y  $e \mid g \implies e \mid d$  en  $K[x]$ . Denotamos al polinomio  $d$  por  $\text{mcd}_K(f, g)$ .

*Demostración.* Se deja como ejercicio. ◇

**Proposición 17** (Máximo común divisor en subcuerpos). Sean  $E, K \subseteq E$  cuerpos, y  $0 \neq f, g \in K[x]$  polinomios.

$$\text{mcd}_K(f, g) = \text{mcd}_E(f, g)$$



*Demostración.* Sea  $d = \text{mcd}_K(f, g)$ ,  $e = \text{mcd}_E(f, g)$ . Entonces,  $d = af + bg$  en  $K[x] \subseteq E[x] \implies e \mid d$  en  $E[x]$ . Como  $d \mid f$  y  $d \mid g$  en  $K[x]$  (y en particular también en  $E[x]$ ), entonces  $d \mid e$  en  $E[x]$ . Por tanto:

$$(d \mid e) \wedge (e \mid d) \wedge e, d \text{ mónicos} \implies e = d \in K[x]$$

◇

**Corolario 4.** Sea  $0 \neq f, g \in K[x]$  con  $f$  irreducible.

1.  $\text{mcd}(f, g) = 1$  o  $f \mid g$ .
2. Si tenemos  $K \subseteq E$ , y  $f, g$  tienen una raíz común en  $E$ , entonces  $f \mid g$  en  $K[x]$ .

*Demostración.*

1. Si  $d = \text{mcd}(f, g) \neq 1 \implies \delta(d) > 1 \implies f = ad \implies d = a \cdot f$ ,  $a \in K^\times$ . Sea  $b \in K[x]$ ,  $g = b \cdot d = baf \implies f \mid g$ .
2. Sea  $a \in E$  la raíz común, por Ruffini  $(x - a) \mid f, g$  en  $E[x] \implies \text{mcd}_E(f, g) = \text{mcd}_K(f, g) > 1 \implies f \mid g$ .

◇

**Corolario 5** (Descripción de  $\mathcal{U}(K[x]/\langle f \rangle)$ ). Sea  $0 \neq f \in K[x]$ ,  $R = K[x]/\langle f \rangle$ . Entonces:

$$\bar{g} = g + \langle f \rangle \in \mathcal{U}(R) \iff \text{mcd}(f, g) = 1$$

Es decir,  $\exists a, b \in K[x]$  tal que  $1 = af + bg$  y por tanto  $(g + \langle f \rangle)^{-1} = b + \langle g \rangle$ .

**Ejercicio (H1.24).** Sea  $p \in \mathbb{Q}[x]$  dado por  $p(x) = (x^2 + 1)(x^4 + 2x + 2)$ . Escribimos  $R = \mathbb{Q}[x]/\langle p \rangle$  y  $\bar{f} = f + \langle p \rangle$ .

1. Describe los ideales en  $R$ . ¿Es  $R$  un cuerpo?
2. Decide justificadamente si  $\bar{x}$  y  $\overline{x+1}$  son divisores de cero en  $R$ .
3. Decide si  $\bar{x}$  y  $\overline{x+1}$  son elementos invertibles en  $R$  y, en caso afirmativo, encuentra sus inversos.

El primer apartado se resuelve por el teorema de correspondencia.

En el segundo apartado tenemos que ver que  $\text{mcd}(x, p) = 1 = \text{mcd}(x + 1, p)$ . Con ello vemos que  $\bar{x}$  y  $\overline{x+1} \in \mathcal{U}(R)$  y por tanto no pueden ser divisores de cero.

En el tercer apartado faltaría calcular los inversos con la identidad de Bezout.

**Proposición 18** (Cociente de cuerpo e ideal de polinomio irreducible). Sea  $K$  un cuerpo,  $f \in K[x]$  irreducible,  $K[x]/\langle f \rangle$  es un cuerpo.

*Demostración.* Ver el corolario 2.

◇

**Teorema 19** (Factorización única). Sea  $K[x]$  un dominio de factorización única (DFU), sea  $0 \neq f \in K[x]$ , de la forma:

$$f(x) = ap_1(x) \cdots p_r(x), \quad a \in K^\times, \quad p_i \text{ irreducibles mónicos no necesariamente distintos}$$

entonces la expresión es única (salvo el orden de los factores).

*Demostración.* Se deja como ejercicio.

◇

## 1.5. Criterios de irreducibilidad

**Lema 20** (de Gauss). Sea  $f(x) \in \mathbb{Z}[x]$  un polinomio con  $\delta(f) \leq 2$ , entonces:

$$f(x) \text{ irreducible en } \mathbb{Z}[x] \implies f(x) \text{ irreducible en } \mathbb{Q}(x)$$

*Demostración.* Se deja como ejercicio. ◇

**Lema 21** (Reducción módulo  $p$ ). Sea  $f$  un polinomio entero mónico, y  $\varphi_p : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ ;  $\sum a_j x^j \mapsto \sum \bar{a}_j x^j$ . Si existe algún primo  $p$  de forma que  $\varphi_p(f)$  es irreducible en  $\mathbb{Z}_p[x]$ , entonces  $f$  es irreducible en  $\mathbb{Z}[x]$ .

*Demostración.* Se deja como ejercicio. ◇

**Ejercicio** (H1.34 (c)). Demuestra que  $f(x) = x^3 + x + 1$  es irreducible en  $\mathbb{Q}[x]$ .

Usamos reducción módulo  $p$  con  $p = 2$ .

$$f(0) = 1, f(1) = 1$$

Como es un polinomio de grado 3 sin raíces, es irreducible en  $\mathbb{Z}_2[x]$  y por tanto es irreducible en  $\mathbb{Q}[x]$ .

**Teorema 22** (Criterio de Einsestein). Sea  $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ . Si existe un primo  $p$  tal que:

1.  $p \nmid a_n$ .
2.  $p^2 \nmid a_0$ .
3.  $p \mid a_i, \forall i \in \{0, \dots, n-1\}$ .

Entonces  $f$  es irreducible en  $\mathbb{Q}[x]$ .

*Demostración.* Se deja como ejercicio. ◇

**Proposición 23** (Raíces racionales de un polinomio). Sea  $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ . Si  $\frac{r}{s} \in \mathbb{Q}$  con  $\text{mcd}(r, s) = 1$  es una raíz de  $f$ , entonces:  $s \mid a_n$  y  $r \mid a_0$ . En particular, si  $f \in \mathbb{Z}[x]$  es mónico, las raíces racionales están contenidas en los enteros.

*Demostración.*

$$\begin{aligned} 0 &= f\left(\frac{r}{s}\right) = a_0 + a_1 \frac{r}{s} + \dots + a_n \frac{r^n}{s^n} \\ 0 &= a_0 s^n + a_1 r s^{n-1} + \dots + a_n r^n \\ -a_0 s^n &= a_1 r s^{n-1} + \dots + a_n r^n = r(s^{n-1} a_1 + \dots + a_n r^{n-1}) \implies r \mid a_0 s^n \implies r \mid a_0 \\ -a_n r^n &= s(a_0 s^{n-1} + \dots + a_{n-1} r^{n-1}) \implies s \mid a_n r^n \implies s \mid a_n \end{aligned}$$

◇

### Ejemplo 8 (Irreducibilidad cuando fallan otros criterios)

¿Es  $x^3 + x + 6$  irreducible en  $\mathbb{Q}[x]$ ?

Si intentamos comprobarlo con el criterio de Einsestein o por reducción módulo  $p$  no llegamos a nada. Podemos utilizar la proposición 23 para hallar que las únicas raíces racionales del polinomio son los divisores de 6, es decir,  $\{\pm 1, \pm 2, \pm 3, \pm 6\}$  y si evaluamos el polinomio en los posibles valores ninguno resulta 0. Por tanto, es un polinomio de grado 3 sin raíces y entonces es irreducible en  $\mathbb{Q}[x]$ .

**Lema 24** (Irreducibilidad evaluando en  $x + a$ ). Sea  $f \in K[x]$  ( $K$  cuerpo),  $a \in K$ .

$$f(x) \text{ irreducible} \iff f(x + a) \text{ irreducible}$$

*Demostración.* La demostración se sigue de demostrar que  $\varphi_a : K[x] \rightarrow K[x]; f(x) \mapsto f(x+a)$  es un isomorfismo de anillos (cuerpos).  $\diamond$

**Teorema 25** (Irreducibilidad de polinomios ciclotómicos). Sea  $p$  primo,  $\Phi_p(x) = x^{p-1} + \dots + x + 1$  es irreducible en  $\mathbb{Q}[x]$ .

*Demostración.* Partimos de  $(x-1)\Phi_p(x) = x^p - 1$ . Aplicamos el lema 24 con  $a = 1$ . Tenemos por tanto:  $x\Phi(x+1) = (x+1)^p - 1$ . Desarrollando con el binomio de Newton llegamos a la expresión:

$$\Phi(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}$$

Ahora aplicamos Einsestein para el primo  $p$ , donde vemos que  $p \mid \binom{p}{i}$  y  $p^2 \nmid \binom{p}{p-1} = p$ , por lo que  $\Phi_p(x+1)$  es irreducible y también lo es  $\Phi_p(x)$ .  $\diamond$

### 1.5.1. Raíces múltiples e irreducibilidad

**Definición 20** (Raíz múltiple). Sea  $0 \neq f(x) \in K[x]$  un polinomio,  $a \in K$  un raíz de  $f$ , existe un  $m \in \mathbb{N} > 0$  tal que  $f(x) = (x-a)^m g(x)$  con  $g(a) \neq 0$  aplicando Ruffini y siendo  $K[x]$  un DFU. Decimos que  $a$  es **raíz múltiple** si  $m > 1$ .

**Definición 21** (Derivada formal). Sea  $f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x] \setminus K$ . Se define  $f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1} \in K[x]$  como **derivada formal**. Si  $f \in K$ ,  $f'(x) = 0$ .

**Proposición 26** (Propiedades de derivada formal). Sean  $f, g \in K[x]$

1.  $(f+g)' = f' + g'$ ;  $(af)' = a \cdot f'$ ,  $\forall a \in K$ .
2.  $(fg)' = f' \cdot g + f \cdot g'$ .
3. Si  $f(x) = (x-a)^m$ ,  $m \geq 1$  entonces  $f'(x) = m(x-a)^{m-1}$ .

**Proposición 27** (Raíz de derivadas). Sean  $K \subseteq E$  un subcuerpo,  $f(x), f'(x) \in K[x]$  polinomios,  $a \in E$  una raíz múltiple (con multiplicidad  $m$ ) de  $f$ , entonces:

$$f(a) = f'(a) = 0 \iff m > 1$$

*Demostración.* En ambos supuestos:  $f(x) = (x-a)^m g(x)$ , con  $m \geq 1$ ,  $g(a) = 0$  y  $f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m \cdot g'(x)$ .

$\implies m > 1 \implies m-1 \geq 1$  y  $(f(a) = f'(a) = 0)$ .

$\Leftarrow 0 = f'(a) = m \cdot 0^{m-1} \cdot g(a) \implies m > 1$ . ( $g(a) \neq 0$ ). Si tuvieramos  $m = 1$  entonces  $f'(x) = g(x) + (x-a)g'(x)$ , con lo que llegaríamos a  $0 = f'(a) = g(a) \neq 0$  lo que es imposible y la desigualdad es necesariamente estricta.

$\diamond$

**Teorema 28** (Irreducibilidad y raíces múltiples). Sea  $K \subseteq E$  un subcuerpo,  $f(x) \in K[x]$  un polinomio con  $f'(x) \neq 0$ .

1.  $\text{mcd}(f, f') = 1 \implies f$  no tiene raíces múltiples en  $E$ .
2. Si  $f$  es irreducible, entonces  $f$  no tiene raíces múltiples en  $E$ .

*Demostración.*

1.  $\text{mcd}(f, f') = 1 \implies \exists g, h \in K[x] : 1 = fg + hf'$ . Por reducción al absurdo, si supones que un cierto  $a \in E$  es raíz múltiple de  $f$ , entonces  $f(a) = f'(a) = 0$  y llegaríamos a  $1 = 0$ .

2. Como  $f, f' \neq 0$  y  $f$  es irreducible, por el lema de Euclides o bien son coprimos o bien  $f \mid f'$ . Si  $f \mid f'$ , entonces  $\delta(f) < \delta(f')$  pero  $\delta(f') = \delta(f) - 1$  y llegamos a una contradicción, por tanto  $\text{mcd}(f, f') = 1$  ya que son coprimos.

◇

**Ejercicio (H1.30 (parte)).** Enumera los polinomios irreducibles en  $\mathbb{F}_2$  de grado 1, 2, y 3.

$$\delta(f) = 1 \quad f(x) = x, \quad f(x) = x + 1.$$

$$\delta(f) = 2 \quad f(x) = x^2 + x + 1.$$

$$\delta(f) = 3 \quad f(x) = x^3 + x^2 + 1, \quad f(x) = x^3 + x + 1.$$

**Ejercicio (H1.35).** Discute la irreducibilidad de  $f(x) = x^5 + 11x^2 + 15$  en  $\mathbb{Q}[x]$ .

Vamos a ver que es irreducible por medio de reducción módulo  $p$  con  $p = 2$ .  $\varphi_2(f) = f_2(x) = x^5 + x^2 + 1$ .

1. Vemos que no tiene raíces:  $f_2(0) = 1$ ,  $f_2(1) = 1$ . Por tanto, no existe una forma de factorizarlo en un producto de dos polinomios de grado 1 y grado 4.
2. Faltaría ver que no se puede factorizar en un producto de polinomios de grado 2 y grado 3. Si fuera posible:  $f_2(x) = g(x) \cdot h(x)$ . Además,  $g$  y  $h$  han de ser irreducibles ya que no existe un polinomio de grado 1 en sus factores. Con el ejercicio anterior, basta ver que  $f_2(x)$  no es el resultado de multiplicar los posibles polinomios irreducibles de grados 2 y 3.

$$(x^2 + x + 1)(x^3 + x^2 + 1) \neq f_2(x) \neq (x^2 + x + 1)(x^3 + x + 1)$$

**Ejercicio (H1.39).** Factoriza  $x^4 - 1$  como producto de irreducibles mónicos en:  $\mathbb{Q}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{C}[x]$ ,  $\mathbb{F}_2[x]$  y  $\mathbb{F}_3[x]$ .

- $\mathbb{R}[x]$  y  $\mathbb{Q}[x]$ :  $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$ .
- $\mathbb{C}[x]$ :  $x^4 - 1 = (x - 1)(x + 1)(x - i)(x + i)$ .
- $\mathbb{F}_2[x]$ : Como  $f'(x) = 0$ , 1 es una raíz con multiplicidad 4, y por tanto  $x^4 - 1 = (x - 1)^4$ .
- $\mathbb{F}_3[x]$ :  $f'(x) = 4x = x \in \mathbb{F}_3[x] \implies$  las raíces son simples. Se pueden comprobar a mano y obtenemos  $x^4 - 1 = (x - 1)(x - 2)(x^2 + 1)$ .

## 1.6. Cuerpos

**Definición 22** (Cuerpo primo). Sea  $K$  un cuerpo,  $\mathcal{A} = \{L \subseteq K \text{ subcuerpos}\}$ . Sea  $F = \bigcap_{L \in \mathcal{A}} L$ , es un subcuerpo de  $K$  (se puede comprobar). Llamamos a  $F$  el **cuerpo primo** de  $K$ , y tiene la característica de ser el menor subcuerpo contenido en  $K$ , es decir, si  $E \subseteq K$  y  $E \subseteq F$ , entonces  $E = F$ .

**Teorema 29** (Isomorfías del cuerpo primo). Sea  $K$  un cuerpo y  $F$  su cuerpo primo, entonces  $F$  es isomorfo a:

- $\mathbb{Q} \iff \sum_1^n \mathbf{1} \neq 0 \forall n \in \mathbb{Z}^\times$
- $\mathbb{F}_p \iff \sum_1^n \mathbf{1} = \mathbf{0} \iff p \mid n$  para algún primo  $p$ .

**Observación.** Vamos a abreviar  $\sum_1^n \mathbf{1}$  por  $n\mathbf{1}$ , donde  $\mathbf{1} \in F$  y  $n \in \mathbb{Z}^\times$ .

*Demostración.* Consideramos el homomorfismo  $\alpha : \mathbb{Z} \rightarrow F; n \mapsto n\mathbf{1}$ . Si  $I = \ker(\alpha) = \{0\} \iff n\mathbf{1} \neq \mathbf{0} \forall n \in \mathbb{Z}^\times$ ,  $\alpha$  se puede extender a  $\tilde{\alpha} : \mathbb{Q} \rightarrow F; \frac{n}{m} \mapsto (n\mathbf{1}) \cdot (m\mathbf{1})^{-1}$ .

Tenemos que comprobar que  $\tilde{\alpha}$  está bien definida. Partimos de  $\frac{n}{m} = \frac{a}{b} \in \mathbb{Q}$ :

$$\begin{aligned} nb = ma &\implies \alpha(nb) = \alpha(ma) \implies (n\mathbf{1})(b\mathbf{1}) = (m\mathbf{1})(a\mathbf{1}) \implies (*) \\ (*) &\implies (n\mathbf{1})(m\mathbf{1})^{-1} = (a\mathbf{1})(b\mathbf{1})^{-1} \implies \tilde{\alpha}\left(\frac{n}{m}\right) = \tilde{\alpha}\left(\frac{a}{b}\right) \end{aligned}$$

Concluimos con que  $\tilde{\alpha}$  está bien definida y es un homomorfismo de grupos inyectivo. Por el primer teorema de isomorfía (teorema 10):

$$\tilde{\alpha}(\mathbb{Q}) \subseteq F \subseteq K \text{ donde además } \tilde{\alpha}(\mathbb{Q}) \simeq \mathbb{Q}$$

y por la definición de cuerpo primo:  $\mathbb{Q} \simeq \tilde{\alpha}(\mathbb{Q}) = F$ .

Consideremos ahora el caso en que  $I = \ker(\alpha) \neq \{0\} \iff (\alpha(n) = 0 \iff p \mid n)$ . Entonces, existe  $p$  primo tal que  $I = \langle p \rangle$ .

Como  $\mathbb{Z}$  es un dominio de ideales principales, e  $I \leq \mathbb{Z}$ , existe  $0 \neq m \in \mathbb{Z}$  que cumple  $I = \langle m \rangle = m\mathbb{Z}$ . Supongamos  $m = a \cdot b$ , entonces  $0 = \alpha(m) = \alpha(a)\alpha(b) \implies \alpha(a) = 0$  ó  $\alpha(b) = 0 \implies a$  ó  $b \in \langle m \rangle \implies m \mid a$  ó  $m \mid b \implies m = p$  primo.

Entonces, de nuevo por el primer teorema de isomorfía:

$$\mathbb{Z}/\ker(\alpha) = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \simeq \alpha(\mathbb{Z}) \subseteq F \subseteq K$$

y por la definición de cuerpo primo:  $\mathbb{F}_p \simeq \alpha(\mathbb{Z}) = F$  ◇

**Definición 23** (Característica de un cuerpo). Sea  $K$  un cuerpo y  $F$  su cuerpo primo, decimos que su **característica**  $\text{car}(K)$ , es  $\text{car}(K) = 0$  si  $F \simeq \mathbb{Q}$  y  $\text{car}(K) = p$  si  $F \simeq \mathbb{F}_p$ .

**Ejercicio** (H1.40). Sean  $K$  y  $E$  dos cuerpos de distinta característica, demuestra que no existe  $\varphi : K \rightarrow E$  tal que  $\varphi$  sea un homomorfismo de cuerpos.

Supongamos  $\text{car}(E) = 0$  y  $\text{car}(K) = p > 0$ . Entonces:

$$\mathbf{0} = \varphi(p\mathbf{1}) = p\varphi(\mathbf{1}) = p\mathbf{1} \neq \mathbf{0}(\text{en } E)$$

Faltaría ver el caso en que  $\text{car}(E) = p \neq q = \text{car}(K)$  con  $p, q$  primos:

$$\mathbf{0} = \varphi(q\mathbf{1}) = q\varphi(\mathbf{1}) = q\mathbf{1} \neq \mathbf{0}(\text{en } E)$$

Con lo que llegamos a una contradicción en ambos casos, y no existe dicho homomorfismo.

**Observación.** En un cuerpo de característica  $p$ ,  $(a \pm b)^p = a^p \pm b^p$ .

**Definición 24** (Cuerpo perfecto). Sea  $K$  un cuerpo de característica  $p$ , y el monomorfismo  $Frob : K \rightarrow K; a \mapsto a^p$ . Decimos que  $K$  es **perfecto** si  $Frob$  es sobreyectivo, es decir,  $Frob$  es un isomorfismo de cuerpos.

**Proposición 30** (Endomorfismo y cuerpo primo). Sea  $K$  un cuerpo,  $F$  su cuerpo primo y  $\sigma : K \rightarrow K$  un endomorfismo de cuerpos, entonces;

$$\sigma(a) = a, \forall a \in F$$

*Demostración.* Se deja como ejercicio. ◇

**Ejercicio** (H1.42 (parte)). Si  $n > 0$  no es un cuadrado, demuestra que:

1.  $\mathbb{F}_3[\xi] = \{a + b\xi \mid a, b \in \mathbb{F}_3, \xi^2 = -1\}$  es un cuerpo.
2. No existe un homomorfismo de anillos  $\varphi : \mathbb{Q}[i] \rightarrow \mathbb{Q}[\sqrt{2}]$ .

1. Sea el polinomio  $f(x) = x^2 + 1$ , de forma que  $f(\xi) = 0$ . Otra forma de describir  $\mathbb{F}_3[\xi]$  es:

$$\mathbb{F}_3[\xi] = \{a + b\xi \mid a, b \in \mathbb{F}_3, f(\xi) = 0\} \simeq \mathbb{F}_3[x] / \langle f(x) \rangle$$

por lo que es un cuerpo ya que  $x^2 + 1$  es irreducible en  $\mathbb{F}_3[x]$  al no tener raíces.

2. El problema surge de la imagen de  $i$ .  $\varphi(i)$  será de la forma:  $a + b\sqrt{2}$ , y entonces:

$$-1 = \varphi(-1) = \varphi(i^2) = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

de donde podría deducirse que  $\sqrt{2} \in \mathbb{Q}$  y es imposible. Por tanto no existe dicho homomorfismo.

## Parte II

# Apéndices





## Capítulo 2

## Índices



# Lista de definiciones

1.	Definición (Anillo)	7
2.	Definición (Anillo con unidad o anillo unitario)	8
3.	Definición (Anillo conmutativo)	8
4.	Definición (Anillo de polinomios)	8
5.	Definición (Polinomio mónico)	8
6.	Definición (Divisor de cero)	8
7.	Definición (Unidad de un anillo)	9
8.	Definición (Dominio de integridad)	9
9.	Definición (Cuerpo)	9
10.	Definición (Subanillo)	10
11.	Definición (Subcuerpo)	10
12.	Definición (Ideal)	10
13.	Definición (Ideal principal)	11
14.	Definición (Ideal primo)	12
15.	Definición (Ideal maximal)	12
16.	Definición (Homomorfismo de anillos)	12
17.	Definición (Raíz de un polinomio)	14
18.	Definición (Dominio de ideales principales)	15
19.	Definición (Elemento irreducible)	15
20.	Definición (Raíz múltiple)	19
21.	Definición (Derivada formal)	19
22.	Definición (Cuerpo primo)	20
23.	Definición (Característica de un cuerpo)	21
24.	Definición (Cuerpo perfecto)	21



# Lista de teoremas

1.	Proposición (Producto con 0 en anillos)	7
2.	Proposición (Cuerpo y dominio de integridad)	9
3.	Proposición (Dominio de integridad en anillos de polinomios)	9
4.	Proposición (Propiedad de cuerpo en anillos de polinomios)	9
5.	Proposición (Unidades en anillos de polinomios)	9
6.	Proposición (Ideal propio)	10
7.	Proposición (Ideales y cuerpos)	10
8.	Proposición (Propiedades de ideales)	11
9.	Teorema (Cociente de ideales primos y maximales)	12
10.	Teorema (Primer teorema de isomorfía)	13
11.	Proposición (Algoritmo de la división)	14
12.	Teorema (Raíces y dominio de integridad)	14
13.	Teorema (Pequeño teorema de Fermat)	15
14.	Teorema (Ideales principales)	15
15.	Teorema (Irreducibilidad en DIP)	15
16.	Teorema (Máximo común divisor)	16
17.	Proposición (Máximo común divisor en subcuerpos)	16
18.	Proposición (Cociente de cuerpo e ideal de polinomio irreducible)	17
19.	Teorema (Factorización única)	17
20.	Lema (de Gauss)	18
21.	Lema (Reducción módulo $p$ )	18
22.	Teorema (Criterio de Einsestein)	18
23.	Proposición (Raíces racionales de un polinomio)	18
24.	Lema (Irreducibilidad evaluando en $x + a$ )	18
25.	Teorema (Irreducibilidad de polinomios ciclotómicos)	19
26.	Proposición (Propiedades de derivada formal)	19
27.	Proposición (Raíz de derivadas)	19
28.	Teorema (Irreducibilidad y raíces múltiples)	19
29.	Teorema (Isomorfías del cuerpo primo)	20
30.	Proposición (Endomorfismo y cuerpo primo)	21



# Lista de ejemplos

1.	Ejemplo (Ejemplos de anillos) . . . . .	8
2.	Ejemplo (Ejemplos de subanillos y subcuerpos) . . . . .	10
3.	Ejemplo (Ejemplos de ideales) . . . . .	11
4.	Ejemplo (Proyección canónica) . . . . .	12
5.	Ejemplo (Homomorfismo de evaluación) . . . . .	14
6.	Ejemplo (Uso de Ruffini) . . . . .	14
8.	Ejemplo (Irreducibilidad cuando fallan otros criterios) . . . . .	18





# Lista de ejercicios

. Ejercicio (H1.5) . . . . .	11
. Ejercicio (H1.12) . . . . .	11
. Ejercicio (H1.14) . . . . .	13
. Ejercicio (H1.16) . . . . .	13
. Ejercicio (H1.21) . . . . .	13
. Ejercicio (H1.27) . . . . .	15
. Ejercicio (H1.25) . . . . .	15
. Ejercicio (H1.24) . . . . .	17
. Ejercicio (H1.34 (c)) . . . . .	18
. Ejercicio (H1.30 (parte)) . . . . .	20
. Ejercicio (H1.35) . . . . .	20
. Ejercicio (H1.39) . . . . .	20
. Ejercicio (H1.40) . . . . .	21
. Ejercicio (H1.42 (parte)) . . . . .	22