TEORÍA DE GALOIS

APUNTES DEL CURSO 2019-2020 IMPARTIDO POR CAROLINA VALLEJO

Rafael Sánchez

Revisión del 10 de octubre de 2019 a las 01:53.

Índice general

I Primer parcial **5**

1. Anillos, polinomios y cuerpos **7**
1.1. Anillos 7
1.2. Cuerpos 9
1.3. Ideales 10
1.4. Homomorfismos 12
1.5. Anillos de polinomios 14

II Apéndices **15**

2. Índices **17**

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 $+ : A \times A \to A$ es una operación a la que llamamos suma, $\cdot : A \times A \to A$ 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:

$$\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c \tag{1.1}$$
$$\forall a, b, c \in A,\ (a + b) \cdot c = a \cdot c + b \cdot c \tag{1.2}$$

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: $\forall a, b \in A,\ a + b = b + a$

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

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

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:

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

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 transitivas y asociativas.

Observación. Vamos a considerar algunas definiciones y convenciones menores.

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

   $$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

   Donde llamamos *coeficientes* del polinomio a los a_i.

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

   $$\delta(p) = \text{máx}\,\{i \mid a_i \neq 0\}$$

3. Sea $p \in R[x] = a_0 + a_1 x + \ldots + a_n x^n$, llamamos *coeficiente director* al coeficiente del término de mayor grado (a_n).

4. Sea $p \in R[x] = a_0 + a_1 x + \ldots + a_n x^n$, llamamos *termino independiente* al coeficiente libre (a_0).

5. Sea $p \in R[x]$ con todos los coeficientes nulos, entonces p es el *polinomio cero*.

   $$0 = \sum_{i>0} 0 \cdot x^n$$

   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:

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

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 $\mathbf{0}$.

1.2. Cuerpos

Definición 9 (Cuerpo)**.** Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Diremos que A es un cuerpo si $A^\times = A \backslash \{\mathbf{0}\}$ 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 $r \in R^\times = R \backslash \{\mathbf{0}\}$, supongamos $\exists s \in R^\times$ tal que:

$$r \cdot s = 0$$

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:

- $\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$, con $d \neq e^2, \ \forall e \in \mathbb{Z}$ es un anillo y un dominio de integridad, pero no es un cuerpo.

- $\mathbb{Q}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}$, con $d \neq e^2,\ \forall e \in \mathbb{Z}$ es un cuerpo. Decimos que $\left\{1, \sqrt{d}\right\}$ 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, $S \subseteq R$, $\mathbf{1} \in S$. Decimos que S es un **subanillo** si:
- S es cerrado por suma y producto.
- Todo elemento tiene opuesto, es decir, $\forall a \in S, \exists b \in S\ :\ a + b = \mathbf{0}$.

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, $\forall a \in S^\times, \exists b \in S^\times\ :\ a \cdot b = \mathbf{1}$

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* $\mathbb{Q}[\sqrt{d}]$

1.3. Ideales

Definición 12 (Ideal)**.** Sea R un anillo, e $I \subseteq S$. 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 $\{\mathbf{0}\}$ 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:

$$I \subsetneq R \iff \mathbf{1} \in I \iff I \cap \mathcal{U}(R) \neq \varnothing$$

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

$$I \leqslant R \iff I \cap \mathcal{U}(R) = \varnothing$$

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

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

Demostración.

- $(\implies)$

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

- $(\impliedby)$
  Sea $a \in R^\times$, $a \in \langle a \rangle \leqslant R$

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

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

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 $I \leqslant R$ un ideal.

1. Sean $I, J \leqslant R$ ideales, entonces $I + J = \{a + b \mid a \in I,\ b \in J\} \leqslant R$ es un ideal.
2. Sea $\mathbf{a} \in \mathbb{R}^n$, entonces $I = \langle \mathbf{a} \rangle = \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\} \leqslant R$ 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:

$$\begin{array}{ccc} \{J \leqslant R \mid I \subseteq J \subseteq R\} & \longrightarrow & \{{}^{J}\!/_{I} \leqslant {}^{R}\!/_{I}\} \\ J & \longmapsto & \{r + I \mid r \in J\} \end{array}$$

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

- ($\Longleftarrow$)

  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 ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.

- ($\Longrightarrow$)

  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:

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

  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 $I \leqslant R$ 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 $I \leqslant R$ un ideal, diremos que I es un **ideal maximal** si:

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

Teorema 9 (Cociente de ideales primos y maximales)**.** Sea R un anillo, $I \leqslant R$ 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 sique de los apartados anteriores junto a la proposición 2 que nos dice que un cuerpo es un dominio de integridad.

♢

1.4. Homomorfismos

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

1. φ 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.

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

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

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

Ejemplo 4 (*Proyección canónica*)

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

Observación.

$$R/_{\ker \varphi} = R/_I$$

Teorema 10 (Teorema de isomorfía)**.** Sea $\varphi : R \to S$ 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. ♢

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

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

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

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

El recíproco solo es cierto si φ es un isomorfismo, pero en general no. Como contraejemplo consideramos el homomorfismo identidad $\iota : \mathbb{Z} \to \mathbb{Q};\ a \mapsto a$. 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 $\varphi : \mathbb{Q} \to \mathbb{Z}_p$ para $p \in \mathbb{Z}$ primo.
2. No existe ningún homomorfismo de anillos $\varphi : \mathbb{R} \to \mathbb{Q}$.

Solución:

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

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

   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 $\varphi : \mathbb{R} \to \mathbb{Q};\ \sqrt{2} \mapsto a$

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

   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 $n \geqslant 2$, demuestra que el anillo cociente $\mathbb{Z}[x]/n\mathbb{Z}[x]$ es isomorfo a $\mathbb{Z}_n[x]$. Conclute 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:

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

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

- Comprobar que φ es un homomorfismo de anillos.
- Comprobar que φ 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:

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

1.5. 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 $r = \mathbf{0}$.

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 $\mathcal{E}_a(f) = f(a) = \mathbf{0}$

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.

- ($\Longleftarrow$)
$$\mathcal{E}_a(f) = \mathcal{E}_a(x - a) \cdot \mathcal{E}_a(g) = \mathbf{0}$$
- ($\Longrightarrow$)
$$f(x) = (x - a) \cdot d(x) + r(x);\ \delta(r) \leqslant \delta(x - a) \implies r \in R;\ f(a) = r = 0 \implies g(x) = d(x)$$

♢

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 $\alpha_1, \ldots, \alpha_n$ raíces distintas de f, entonces $n \leqslant \delta(f)$.

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

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 (Teorema de isomorfía) 13
11. Proposición (Algoritmo de la división) 14
12. Teorema (Raíces y dominio de integridad) 14

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

Lista de ejercicios

. Ejercicio (H1.5) 11
. Ejercicio (H1.12) 11
. Ejercicio (H1.14) 13
. Ejercicio (H1.16) 13
. Ejercicio (H1.21) 13