

## Lectura 5: Anillos y campos

En la lectura anterior se construyeron y presentaron toda una gama de anillos conmutativos distintos de  $\mathbb{Z}$  y se vio que algunos de ellos forman dominios enteros y campos. El objetivo ahora presentar el punto clave de divergencia entre los anillos finitos y otro mejor conocidos. Para esto, comenzaremos presentando, de manera informal, dos campos con los que ya estamos muy familiarizados.

### 5.1. Los campos racional y real

El concepto de número racional no debe ser ajeno, en un primer curso de cálculo es obligatorio pasar por estos números de manera obligada y si no hemos hablado de ellos se debe a un intento de simplificar el universo de discurso. Sin embargo, ahora se hace necesario mencionarlos y clasificarlos en la terminología que hemos desarrollado. Vamos a dejar muchos detalles a la deriva, con la promesa que en una parte posterior del curso se aclarará de manera minuciosa su verdadero significado. Por esta razón su único uso, de momento, será ilustrar algunos conceptos.

Comencemos definiendo el conjunto  $\mathbb{Q}$  de los números racionales, como el menor campo de forma que  $\mathbb{Z} \subset \mathbb{Q}$ . Esto quiere decir que, como  $5 \in \mathbb{Z}$ , debe existir un elemento  $5^{-1} \in \mathbb{Q}$ , al ser este un campo, y esto se puede hacer para cualquier entero. Una de las consecuencias de ser el menor campo, resulta en poder encontrar para cualquier racional  $c$ , un par de enteros de forma que

$$c = ab^{-1},$$

La prueba de este hecho requiere de una precisa definición de los racionales, sin embargo no debe ser difícil de aceptar y de hecho será la propiedad definitoria de los racionales.

**Definición 5.1.** En un campo  $F$  cualquiera, en lugar de escribir  $ab^{-1}$  para elementos  $a$  y  $b$  del campo, se escribirá

$$\frac{a}{b}$$

Esta definición, nos permite describir el conjunto de los números racionales de la siguiente manera:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ y } b \neq 0 \right\}.$$

En contraste, el conjunto de los números reales,  $\mathbb{R}$ , es de nueva cuenta el menor campo con  $\mathbb{Q} \subset \mathbb{R}$  que además obedece axiomas análogos a 1.8 y 1.9 presentados en la lectura 1 junto al llamado *axioma del supremo*, mencionado a continuación.

**Axioma del supremo.** Para todo conjunto  $A \subset \mathbb{R}$  acotado superiormente y no vacío, existe una mínima cota superior.

Eso quiere decir que  $\mathbb{R}$  posee un orden muy particular definido de manera análoga al propuesto en  $\mathbb{Z}$ <sup>1</sup>. Este orden además tiene la peculiaridad de ser compatible con el orden sobre los naturales, enteros y racionales. Solamente basta distinguir el campo de los números reales con el campo de los racionales. Es importante recordar que la existencia de los números racionales obedece en cierta forma a la necesidad de resolver algunas ecuaciones en no tienen solución en  $\mathbb{Z}$ , por ejemplo  $2x = 3$ . Es común preguntar si existirán ecuaciones imposible de resolver en  $\mathbb{Q}$ , para lo cual no hay que buscar mucho la ecuación  $x^2 - 2 = 0$  no tiene solución en  $\mathbb{Q}$ . Es costumbre en un curso de cálculo mostrar que dicha ecuación tiene solución en  $\mathbb{R}$  lo que nos permite pensar que  $\mathbb{R}$  es a  $\mathbb{Q}$  lo mismo que  $\mathbb{Q}$  es a  $\mathbb{Z}$  y también lo que  $\mathbb{Z}$  es a  $\mathbb{N}$ . La idea de extender estructuras usando la solución de ciertas ecuaciones, es una práctica común en álgebra.

## 5.2. Otra aproximación a los sistemas de números

Podemos sin embargo, tomar una aproximación en otro sentido, admitiendo la existencia de los números reales de la misma manera que se hace en un curso de cálculo: Usando los axiomas de campo, orden y el axioma del supremo. Tomando  $\mathbb{R}$  como nuestro conjunto base podríamos presentar los otros conjuntos de interés de la siguiente manera.

**Definición 5.2.** Un conjunto  $A \subset \mathbb{R}$  se dirá inductivo si  $0 \in A$  y para todo real  $k$ , tenemos que  $k \in A$  implica que  $k + 1 \in A$

Con este concepto somos capaces de presentar el conjunto de los naturales  $\mathbb{N}$ , como el menor conjunto inductivo. Por otro lado los números enteros  $\mathbb{Z}$ , serán el anillo más pequeño contenido en  $\mathbb{R}$  de forma que  $\mathbb{N} \subset \mathbb{Z}$  y por último los números racionales, se presentan como el campo más pequeño contenido en  $\mathbb{R}$  de forma que  $\mathbb{Z} \subset \mathbb{Q}$ . De esta forma tenemos

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Para fines prácticos, lo anterior es lo que deseamos tener como objetos de estudio y a partir de ahora asumiremos que existe y se comporta tal cual estamos describiendo.

Quizá es pertinente preguntar por que no se ha hecho esto así con anterioridad. El cuestionamiento es justo y perfectamente válido, aunque con toda seguridad la respuesta quedará corta: Debemos notar que aunque la formulación anterior es válida, requiere del lenguaje de anillos y campos, y sin ejemplos que ilustren estos conceptos existe un falta de motivo para su existencia.

De cualquier forma, ninguna de las dos aproximaciones contesta todas las preguntas y nos piden asumir, aunque justificadamente, la existencia de algunos objetos matemáticos. Como ya se comentó, se formularán estos conjuntos de manera precisa en otra parte del curso y de momento es completamente aceptable que existan y presenten las propiedades descritas, no sólo eso, estamos tan familiarizados con estos números que son un excelente punto de partida para introducirlos en nuestro desarrollo teórico de anillos y campos.

## 5.3. Característica de un anillo

Para continuar nuestra discusión, parece importante preguntar qué hace diferentes a los anillos  $\mathbb{Z}_m$  del anillo  $\mathbb{Z}$ . Podríamos intentar responder que aunque  $\mathbb{Z}_m$  es un anillo, parece tener menos

---

<sup>1</sup>¿No te convence? Intenta formularlos cambiando cada mención de «números enteros» por «números reales», después define el orden exactamente de la misma manera, ¿no es esa la misma forma en que viste el orden de  $\mathbb{R}$ ? ¿No? Entonces consulta el primer capítulo de [Spi12].

propiedades pues de manera general no es un dominio entero mientras  $\mathbb{Z}$  lo es. Sin embargo, hemos visto que  $\mathbb{Z}_p$  no sólo es un dominio entero sino un campo por lo que excede en propiedades a  $\mathbb{Z}$ . De alguna forma, esto sugiere que son objetos que poco comparten aparte de ser anillos, pero quizá la propiedad más importante que logra diferenciarlos es su “tamaño”. Para precisar esto desde un punto de vista algebraico necesitamos algunas definiciones.

**Definición 5.3.** Sea  $R$  un anillo conmutativo  $R$  y  $a$  un elemento de este. Para cualquier natural  $n$ , definimos

$$n \cdot a = \underbrace{a + \cdots + a}_{n \text{ veces}}.$$

Además, definimos

$$(-n) \cdot a = -(n \cdot a).$$

Es importante notar que el anillo  $R$  puede ser algo muy abstracto y de alguna forma lo que se define para cada anillo  $R$ , es una función  $\mathbb{Z} \times R \rightarrow R$ . Pero esto no debe ser problemático pues al poseer el anillo una suma, es posible dar sentido a la expresión. Para ilustrar esto consideremos un par de ejemplos: En  $\mathbb{Z}_6$ , tenemos

$$3 \cdot [2]_6 = [2]_6 + [2]_6 + [2]_6 = [0]_6$$

mientras en  $\mathbb{Z}_9$ , tendríamos

$$(-4) \cdot [1]_9 = -([1]_9 + [1]_9 + [1]_9 + [1]_9) = -[4]_9 = [5]_9.$$

A falta de más ejemplos de anillos (de momento), lo anterior debe ser capaz de ilustrar el concepto a pesar que éste es absolutamente abstracto. Como nota, es importante notar que en  $\mathbb{Z}$ , la anterior definición coincide con el producto asociado a este conjunto.

¿Cuál es entonces la diferencia que buscamos entre  $\mathbb{Z}_m$  y  $\mathbb{Z}$ ? Usando esta notación debemos observar que en  $\mathbb{Z}_m$ ,

$$m \cdot [1]_m = [m \cdot 1]_m = [0]_m$$

mientras en  $\mathbb{Z}$ , la única posibilidad para tener

$$m \cdot 1 = 0$$

es  $m = 0$ . De alguna forma esto indica que la “finitud” de  $\mathbb{Z}_m$  le entrega cierto ciclo respecto a la suma de unos (por esto el nombre de anillo: regresa donde comenzó) en contraste con  $\mathbb{Z}$  que se incrementa sin cota alguna. Esto debe ser suficiente razón para considerar la siguiente definición.

**Definición 5.4.** Sea  $R$  un anillo conmutativo en donde  $1_R \neq 0_R$ . Decimos que  $R$  tiene característica  $m$ , si  $m$  es el entero positivo más pequeño tal que  $m \cdot 1_R = 0_R$ . Si dicho entero no existe, decimos que el anillo tiene característica 0.

No es difícil ver que  $\mathbb{Z}_m$  tiene característica  $m$  y que  $\mathbb{Z}$  tiene característica 0. Esto nos puede llevar a pensar erróneamente que la característica es una forma extraña de referirse al tamaño del conjunto en cuestión, a continuación probaremos que este no es el caso usando un contraejemplo. Consideraremos las parejas con elementos en el anillo  $\mathbb{Z}_3$ , en el cual es no posible resolver la ecuación

$$([x]_3)^2 = -[1]_3.$$

Precisando, tomaremos el conjunto

$$\mathbb{F}_9 = \{(a, b) \mid a, b \in \mathbb{Z}_3\}$$

en el cual definiremos las operaciones de suma y producto de la siguiente manera:

$$(a, b) +_{\mathbb{F}_9} (c, d) = (a + c, b + d)$$

y

$$(a, b) \cdot_{\mathbb{F}_9} (c, d) = (ac - bd, ad + bc).$$

No debe existir problema en admitir que  $\mathbb{F}_9$  es un anillo conmutativo de exactamente 9 elementos y que los neutros aditivo y multiplicativo resultan los elementos  $([0]_3, [0]_3)$  y  $([1]_3, [0]_3)$ , respectivamente. De esta forma podemos observar que

$$1 \cdot ([1]_3, [0]_3) \neq ([0]_3, [0]_3)$$

$$2 \cdot ([1]_3, [0]_3) = ([2]_3, [0]_3) \neq ([0]_3, [0]_3)$$

y

$$3 \cdot ([1]_3, [0]_3) = ([3]_3, [0]_3) = ([0]_3, [0]_3)$$

de esta forma debemos concluir que  $\mathbb{F}_9$  tiene característica 3 aunque tiene 9 elementos. Esto muestra que la característica de un anillo y su número de elementos no son necesariamente idénticos.

Ahora, como todo campo es un anillo, toda esta discusión acerca de la característica se puede extender sin problemas. Sabemos por ejemplo que existen campos finitos  $(\mathbb{Z}_p)$  y que tienen característica distinta de 0, de hecho esto es una generalidad.

**Lema 5.1.** *La característica de un campo finito, es diferente de 0.*

*Demostración.* Sea  $F$  un campo finito cualquiera y sea  $G \subset F$  el conjunto definido por

$$G = \{n \cdot 1_F \mid n \in \mathbb{N}\}.$$

Como  $F$  es finito,  $G$  debe ser de igual forma finito. Eso quiere decir la secuencia de elementos indicada se debe repetir en algún momento, en otras palabras existen naturales  $m$  y  $n$  de forma que  $m \neq n$  y  $m \cdot 1 = n \cdot 1$ , sin pérdida de la generalidad, podemos suponer que  $m > n$ , en ese caso

$$(m - n) \cdot 1 = m \cdot 1 - n \cdot 1 = 0_F.$$

por lo que la característica de  $F$  es cuando más  $m - n$  pero no 0. Esto es lo que queríamos probar. ■

Ahora, en el caso de los enteros módulo, la única forma de obtener un campo era tener un módulo primo y ésta resultaba una condición tanto suficiente como necesaria. Sin embargo, el anillo  $\mathbb{F}_9$  resulta también un campo (ejercicio 5.4), lo que quiere decir que existen campos que no tienen un tamaño primo. A pesar de las apariencias, esto no es lo realmente importante acerca de un módulo primo, pues en este su tamaño coincide con su característica, sino que su característica es un número primo y esto no es un caso particular sino una sorprendente generalidad.

**Teorema 5.2.** *La característica de un campo finito es un número primo.*

*Demostración.* Supongamos que  $F$  es un campo finito, de acuerdo al lema anterior  $F$  tiene característica diferente de cero, supongamos que su característica es  $m$ , i.e.,  $m$  es el entero positivo más pequeño tal que  $m \cdot 1_F = 0_F$ .

Si  $m$  fuera un número compuesto, podríamos encontrar enteros  $a$  y  $b$  de forma que  $m = ab$  donde  $1 < a, b < m$ . En ese caso, los elementos del campo  $x = a \cdot 1_F$  y  $y = b \cdot 1_F$ , satisfacen

$$xy = (a \cdot b) \cdot 1_F = m \cdot 1_F = 0_F$$

y como  $F$  es un campo, y por tanto un dominio entero, debemos tener que  $a \cdot 1_F = 0_F$  o  $b \cdot 1_F = 0_F$  y de cualquiera de estas posibilidades se obtiene una contradicción con el hecho de ser  $m$  el mínimo con esta propiedad. En ese caso  $m$  resulta primo como afirma el resultado. ■

Los campos  $\mathbb{Z}_p$  se pueden comparar con los números racionales de la misma forma en que comparar los anillos  $\mathbb{Z}_m$  con  $\mathbb{Z}$ : Usando su característica. Hasta el momento, no sabemos si existen campos que tengan característica cero, pero es fácil de revertir pues no es difícil probar que  $\mathbb{Q}$  tiene esa característica (ejercicio 5.5), lo que nos permite apreciar que los fenómenos de anillos y campos presentan una bellísima diversidad.

## 5.4. Homomorfismos de anillo

Existe un concepto ubicuo en matemáticas del que es imposible librarse: Las funciones. En cálculo toman las propiedades de continuidad y diferenciabilidad, en geometría de rigidez y simetría, y en álgebra de *homomorfismo*. La diferencia crucial de las otras áreas en matemáticas es que en álgebra no tenemos un punto de referencia visual sino operativo. Mientras en cálculo la continuidad tiene una interpretación visual y en geometría es imposible remover el espacio al hablar de simetría, en álgebra el trabajo es distinto y poderosamente abstracto, ¿qué se propiedades deben guardar las funciones entonces? Como se ha visto lo peculiar en una estructura algebraica son las operaciones, de ahí que las funciones que buscamos sean aquellas que respeten las operaciones.

**Definición 5.5.** Sea  $R$  y  $S$  anillos cualquiera y sea también  $f: R \rightarrow S$  una función. A  $f$  se le llama un *homomorfismo de anillo* si para cualesquiera elementos  $a$  y  $b$  de  $R$ , satisface las siguientes condiciones:

- $f(1_R) = 1_S$ .
- $f(a +_R b) = f(a) +_S f(b)$ .
- $f(a \cdot_R b) = f(a) \cdot_S f(b)$

Es importante aclarar que las expresiones  $1_R$  son indeseables por voluminosas, muchas veces el contexto explica que  $1$  es el elemento neutro de un anillo sin tratarse este necesariamente de  $\mathbb{Z}$ . Cuando afirmamos que  $f: R \rightarrow S$  es una función, lo que decimos es que cualquier elemento  $r$  de  $R$  se transforma en el elemento  $f(r)$  de  $S$ , por lo que al afirmar simplemente que  $f(0) = 0$  debe quedar perfectamente claro que el elemento  $0_R$  se envía al elemento  $0_S$  usando la función  $f$  y eso se logra explicar en el contexto a la perfección. Esto nos permite simplificar la manera en nos referimos a los homomorfismos, por ejemplo, las propiedades que los definen pueden simplemente escribirse como  $f(1) = 1$ ,  $f(a + b) = f(a) + f(b)$  y  $f(ab) = f(a)f(b)$ . Entonces, la notación de subíndices se reserva para caso en los que sea estrictamente necesaria.

Los homomorfismos presentan una serie de propiedades básicas sin necesidad tener un caso concreto, por ejemplo preservan más de lo que la definición afirma.

**Teorema 5.3.** Sea  $f: R \rightarrow S$  un homomorfismo de anillos. Entonces, satisface las siguientes propiedades:

1.  $f(0) = 0$ .
2. Para todo  $a \in R$ ,  $f(-a) = -f(a)$ .
3. Si  $a \in R$  tiene inverso, entonces  $f(a^{-1}) = f(a)^{-1}$ .

*Demostración.* Como ningún anillo no es vacío, sea  $a \in R$  un elemento cualquiera del anillo. Entonces

$$f(a) = f(a + 0) = f(a) + f(0)$$

y por la ley de cancelación para la suma,  $f(0) = 0$ . Esto prueba 1.

Para probar 2., debemos tomar  $a + (-a) = 0$  y por 1., tenemos

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a);$$

como los inversos son únicos,  $f(-a) = -f(a)$ .

Por último, si  $a$  tiene inverso, entonces  $aa^{-1} = 1$ . En ese caso

$$1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1})$$

y como los inversos son únicos, entonces  $f(a^{-1}) = f(a)^{-1}$ . Lo que prueba 3. ■

Parte del interés de estudiar homomorfismos es la toda información que pueden entregarnos acerca de los anillos respecto a las propiedades de la función, por ejemplo, cuándo ésta es inyectiva.

**Teorema 5.4.** Sea  $f: R \rightarrow S$  un homomorfismo de anillos. Entonces  $f$  es inyectiva si y sólo si  $f(a) = 0$  implica que  $a = 0$ .

*Demostración.* Supongamos que  $f(a) = 0$  implica que  $a = 0$ , entonces al asumir que  $f(b) = f(c)$  para  $b$  y  $c$  elementos de  $R$ , debemos tener qu

$$f(b - c) = f(b) - f(c) = 0$$

por lo que  $b - c = 0$  y en consecuencia  $b = c$ , de lo que podemos concluir que la función es inyectiva.

Si ahora suponemos que  $f$  es inyectiva y tomamos  $f(a) = 0$ , tenemos que  $f(a) = f(0)$  pues  $f(0) = 0$ . En ese caso debemos tener que  $a = 0$  por se la función inyectiva. Esto termina la prueba. ■

Es quizá importante ilustrar esto con ejemplos. El primero y más sencillo es por supuesto la función identidad sobre un anillo  $R$ , ésta transforma elementos usando la regla  $a \mapsto a$  y es en automático un homomorfismo. Quizá un ejemplo más interesante resulta al tener dos anillos, por ejemplo  $\mathbb{Z} \subset \mathbb{Q}$ , en ese caso podemos proponer la función inclusión  $i: \mathbb{Z} \rightarrow \mathbb{Q}$  de forma que  $i(m) = m$ , la cual no es difícil exhibir como un homomorfismo.

Vamos ahora a describir un ejemplo algo más general y de gran importancia. Supongamos que  $R$  es un anillo conmutativo, entonces podemos definir una función  $f: \mathbb{Z} \rightarrow R$  como  $f(m) = m \cdot 1_R$ . No es difícil notar que este es un homomorfismo, lo notable es que resulta el único.

**Teorema 5.5.** Sea  $R$  un anillo conmutativo. Entonces existe un único homomorfismo  $f: \mathbb{Z} \rightarrow R$ .

*Demostración.* En el párrafo anterior a este teorema, se describe una función definida por

$$f(m) = m \cdot 1_R.$$

Afirmamos que ésta es un homomorfismo. Para probar nuestra afirmación vemos que por definición  $f(1) = 1_R$ , por lo que debemos sólo probar que preserva suma y producto; para esto tomamos dos enteros cualquiera  $m$  y  $n$ , entonces

$$f(m) + f(n) = m \cdot 1_R + n \cdot 1_R = (m + n) \cdot 1_R = f(m + n).$$

y también

$$f(m) \cdot f(n) = (m \cdot 1_R)(n \cdot 1_R) = (mn) \cdot 1_R = f(mn).$$

Concluimos entonces que se trata de un homomorfismo como afirmamos.

Supongamos ahora que  $g: \mathbb{Z} \rightarrow R$  es un homomorfismo. Afirmamos que  $g(m) = m \cdot 1_R$  para todo  $m \geq 0$ . En efecto, si  $a = 0$ , entonces  $g(0) = 0_R = 0 \cdot 1_R$ . Supongamos ahora que  $g(m) = m \cdot 1_R$ , en ese caso

$$g(m + 1) = g(m) + g(1) = m \cdot 1_R + 1_R = (m + 1) \cdot 1_R.$$

Por inducción, la afirmación que hicimos sigue. También, para cualquier natural  $m$ , tenemos

$$\begin{aligned} g(-m) &= -(g(m)) \\ &= -(m \cdot 1_R) \\ &= (-m) \cdot 1_R \end{aligned}$$

De esto podemos concluir que para cualquier entero  $a$ , tenemos que  $g(a) = a \cdot 1_R$ , en ese caso

$$g(a) = a \cdot 1_R = f(a),$$

para todo entero  $a$ , lo que nos lleva a concluir que  $g = f$  y mostrando que  $f$  es el único homomorfismo posible. ■

**Definición 5.6.** Al único homomorfismo de  $\mathbb{Z} \rightarrow R$  se le denomina *el homomorfismo inicial en  $R$* .

Por ejemplo, podemos preguntar como son los homomorfismos iniciales de los anillos  $\mathbb{Z}_m$ . Definamos la función  $\pi_m: \mathbb{Z} \rightarrow \mathbb{Z}_m$  como  $\pi_m(a) = [a]_m$ . No es difícil verificar que esta función es en verdad un homomorfismo y como sólo puede existir uno, entonces ¡ $\pi_m$  es el homomorfismo inicial en  $\mathbb{Z}_m$ ! No sólo eso, quien recuerde el tema de clases de equivalencia, no debería dudar que  $\pi_m$  es la función canónica de la relación  $\cdot \text{ mód } m$ . En este pequeño párrafo, podemos observar cuanta información pueden guardar los homomorfismos acerca de un anillo, siendo además capaces de capturarla en un modo muy particular.

Terminaremos esta sección introduciendo algo de terminología que usa el concepto de homomorfismos.

**Definición 5.7.** Sea  $f: R \rightarrow S$  un homomorfismo de anillos. Entonces,  $f$  se dice:

- Una *inmersión de anillos* si  $f$  es inyectiva.
- Un *isomorfismo de anillos* si  $f$  es biyectiva.

No estamos aún en posición de dar un ejemplo de isomorfismo, pero en la lectura siguiente lo estaremos. De momento sólo podemos proveer un interesante ejemplo de inmersión dado por la función de inclusión  $\mathbb{Z} \rightarrow \mathbb{Q}$  que es un homomorfismo. No es difícil notar que ésta es también inyectiva por lo que podemos decir que los enteros no sólo son un subconjunto de los racionales sino que de alguna forma están “sumergidos” pues sus estructuras son compatibles. Esto nos lleva a una terminología que esperamos que parezca justificada y si no lo ésta, con algo de tiempo y paciencia seguro lo estará.

**Definición 5.8.** Para anillos  $R$  y  $S$ , decimos que  $R$  se puede sumergir en  $S$ , si existe una inmersión de  $R$  en  $S$ . Se dice también que  $R$  es isomorfo a  $S$  si existe un isomorfismo entre los anillos.

## Ejercicios

*Ejercicio 5.1.* Muestra que todo campo es un dominio entero y usando  $\mathbb{Z}$  muestra que no todo dominio entero es un campo.

Una manera mucho más precisa de definir el producto de un natural con un elemento de un anillo es la siguiente definición recursiva:

- $0 \cdot a = 0$ .
- $(n + 1) \cdot a = n \cdot a + a$ .

Esta definición se puede usar para dar pruebas por inducción muy sencillas.

*Ejercicio 5.2.* Demuestra que para todo elemento  $a$  de un anillo conmutativo y cualesquiera naturales  $m$  y  $n$  se tiene:

1.  $n \cdot a + m \cdot a = (n + m) \cdot a$ .
2.  $(n \cdot a)(m \cdot b) = (nm) \cdot ab$ .

*Ejercicio 5.3.* Muestra que para todo natural  $n$  y entero  $a$ , se cumple

$$n \cdot [a]_m = [n \cdot a]_m$$

*Ejercicio 5.4.* Muestra que  $\mathbb{F}_9$  es un campo y encuentra todos sus elementos.

*Ejercicio 5.5.* Sea  $F$  un campo de característica 0. Si  $Q$  es un campo tal que  $F \subset Q$ , muestra que  $Q$  también tiene característica 0.

*Ejercicio 5.6.* Muestra que función  $\pi_m: \mathbb{Z} \rightarrow \mathbb{Z}_m$  definida como  $\pi_m(a) = [a]_m$ , es en verdad un homomorfismo.

*Ejercicio 5.7.* Sea  $C(\mathbb{R})$  el conjunto que contiene todas las funciones continuas de  $\mathbb{R}$  en  $\mathbb{R}$ , i.e.,

$$C(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ es continua}\}.$$

En cualquier curso de cálculo se definen operaciones de suma y producto de funciones siguiendo las siguientes reglas:

- $(f + g)(x) = f(x) + g(x)$ , para todo  $x \in \text{dom}(f) \cap \text{dom}(g)$ .
- $(f \cdot g)(x) = f(x)g(x)$ , para todo  $x \in \text{dom}(f) \cap \text{dom}(g)$ .

Muestra que  $C(\mathbb{R})$  con estas operaciones forman un anillo conmutativo usando el hecho que la suma y el producto de funciones continuas resultan en funciones continuas. Muestra además que, la función  $\varphi: C(\mathbb{R}) \rightarrow \mathbb{R}$  definida como  $\varphi(f) = f(2)$  es un homomorfismo.



## Referencias

[Chi95] Childs, Lindsay N.: *A concrete introduction to higher algebra*. Springer, 2ª edición, 1995.

[Spi12] Spivak, Michael: *Cálculo Infinitesimal*. Editorial Reverté, 3ª edición, 2012.

Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentarlo. El único objetivo real al que sirven, es preparar el curso de Álgebra Superior II impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.

El contenido original que aparezca en estas notas (si es que lo hay), se distribuye bajo la Licencia Creative Commons Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0). ©Eduardo Antonio Gomezcaña Alanis.