Lectura 10: Polinomios

10.1. Sucesiones, polinomios y funciones

El concepto de polinomio seguramente no es ajeno aunque es probable que se asocie a una discusión que involucra únicamente números. Sin embargo, podemos dar una interpretación formal de un polinomio sobre un anillo conmutativo sin mucho problema.

Definición 10.1. Sea R un anillo conmutativo. Por *una sucesión sobre* R entendemos una función $f\colon \mathbb{N} \to R$. Si para cada entero no negativo k escribimos $a_k = f(k)$, para la función f será representada como

$$f = (a_0, a_1, a_2 \dots)$$

y diremos que a_k es la *k-ésima entrada de* f.

Las sucesiones al tener entradas en un anillo, resultan susceptibles de heredar algunas operaciones del anillo donde están definidas y estás resultarán centrales en nuestra discusión.

Definición 10.2. Sean $f = (a_0, a_1, a_2, \dots)$ y $g = (b_0, b_1, b_2, \dots)$ sucesiones sobre un anillo conmutativo R. Definimos la sucesión $f + g$ como aquella con entradas,

$$(f + g)(k) = a_k + b_k.$$

Definimos también la sucesión $f \cdot g$ como aquella con entradas

$$(f \cdot g)(k) = \sum_{i=0}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0.$$

Proposición 10.1. *Sea R un anillo conmutativo y sean también f, g y h sucesiones sobre R. Entonces,*

1. $f + g = g + f$.
2. $f + (g + h) = (f + g) + h$.
3. $f \cdot g = g \cdot f$.
4. $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.
5. $f \cdot (g + h) = f \cdot g + f \cdot h$.

Demostración. Sólo se probarán los incisos 4 y 5, los demás son un ejercicio. Tomemos entonces $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots)$ y $h = (c_0, c_1, \dots)$. Para probar 4, basta con observar que para

cualquier número natural k,

$$\begin{aligned}
[f \cdot (g \cdot h)](k) &= \sum_{i=0}^{k} a_k (g \cdot h)_{k-i} \\
&= \sum_{i=0}^{k} a_k \sum_{j=0}^{k-i} b_j c_{k-i-j} \\
&= \sum_{i=0}^{k} \sum_{j=0}^{k-i} a_k b_j c_{k-i-j} \\
&= \sum_{r=0}^{k} \sum_{s=0}^{r} a_s b_{r-s} c_{k-r} \\
&= \sum_{r=0}^{k} (f \cdot g)_r \cdot c_{k-r} \\
&= [(f \cdot g) \cdot h](k),
\end{aligned}$$

por lo que podemos concluir $f \cdot (g \cdot h) = (f \cdot g) \cdot h$, como se afirma en 4. De manera similar, observamos que para cualquier natural k,

$$\begin{aligned}
[f \cdot (g + h)](k) &= \sum_{i=0}^{k} a_i (g + h)_{k-i} \\
&= \sum_{i=0}^{k} a_i (b_{k-i} + c_{k-i}) \\
&= \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i} \\
&= (f \cdot g)_k + (f \cdot h)_k \\
&= [f \cdot g + f \cdot h](k).
\end{aligned}$$

Por esta razón, $f \cdot (g + h) = f \cdot g + f \cdot h$ como se afirma en 5. ■

Hay un par de sucesiones notables: la sucesión $\mathbf{0} = (0, 0, \dots)$ que satisface $f + \mathbf{0} = \mathbf{0} + f = f$ y la sucesión $\mathbf{1} = (1, 0, \dots)$ que satisface $f \cdot \mathbf{1} = \mathbf{1} \cdot f = f$, ambas para una sucesión cualquiera f. Es un ejercicio interesante usar las definiciones para probar estas igualdades.

Definición 10.3. Una sucesión $f = (a_0, a_1, \dots)$ se dice *un polinomio sobre R*, si existe un entero no negativo n de forma que para todo $k > n$, se tenga $a_k = 0$. Si además el entero n cumple con $a_n \neq 0$ éste se denomina *el grado de f* y se denota como $\text{grd}(f)$. Por último, a las entradas de f se les denomina *coeficientes de f*, en particular la k-ésima entrada de f se denomina *el coeficiente de grado k de f*.

Es indispensable notar que la definición anterior concluye que las sucesiones $\mathbf{0}$ y $\mathbf{1}$ son polinomios. Sin embargo, no garantiza un grado para cualquier polinomio al se imposible encontrar un entero no negativo que indique el grado de $\mathbf{0}$, también llamado el polinomio nulo, por lo que diremos tiene grado indefinido. Afortunadamente, éste es el único polinomio para lo que esto sucede y bastará con tener algo de cuidado cuando exista la posibilidad de obtenerlo.

Debemos ahora entender e interpretar la definición de polinomio, notando que éste es simplemente una sucesión f que presenta la forma

$$f = (a_0, a_1, \dots, a_n, 0, 0, \dots);$$

por esta razón se conviene escribir a un polinomio f sobre R como

$$f = a_0 + a_1 x + \cdots + a_n x^n.$$

Es importante enfatizar que la expresión de un polinomio es solamente una manera de hablar pues ni la suma dentro de esta descripción, ni el símbolo x tienen un significado riguroso[1]. A esto precisamente nos referimos cuando decimos que un polinomio es una expresión formal. Usamos símbolos sin significado para obtener *de forma* algo que reconocemos como un polinomio.

Ilustremos ahora estas ideas para lo cual tomaremos $R = \mathbb{R}$:

- $f = 1 + x + x^2$
- $f = \pi + x^2$ (aquí, $a_1 = 0$).
- $f = 1/3$ (aquí $0 = a_1 = a_2 = \dots$).
- $\mathbf{0} = 0$ (aquí todos los coeficientes son 0).

A pesar de no haber mención alguna, hay una convención en uso en los ejemplos: Si uno de los coeficientes es el elemento unitario, entonces no se escribe a menos que sea el coeficiente de grado de 0. También, si el coeficiente de algún grado no aparece se considera éste como el 0, esto resulta compatible con no escribir los coeficientes después de cierto grado, pues todos los coeficientes de grado superior serán 0.

Ahora, es interesante preguntarse sobre la igualdad de polinomios. Por la definición que hemos dado debe coincidir con la igualdad de sucesiones las cual se da elemento a elemento, i.e., para polinomios $f = a_0 + a_1 x + \cdots + a_n x^n$ y $g = b_0 + b_1 x + \cdots + b_m x^m$, tenemos $f = g$ si y sólo $a_k = b_k$ para todo número natural k. La prueba de la siguiente proposición se desprende de la discusión anterior.

Proposición 10.2. *Sean $f = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio de grado n y $g = b_0 + b_1 x + \cdots + b_n x^m$ un polinomio de grado m, ambos sobre un anillo R. Entonces, $p = q$ si y sólo si $m = n$ y $a_k = b_k$ para todo número natural k con $0 \leq k \leq n$.*

Es posible observar cierto remanente de notación funcional en la manera de expresar un polinomio en el uso de la indeterminada y es de hecho posible asociar de manera muy natural a un polinomio una función.

Definición 10.4. Sea $f = a_0 + a_1 x + \cdots + a_n x^n$, un polinomio sobre un anillo R. Definimos *la función inducida por el polinomio p* como la función $f^* \colon R \to R$ definida por

$$f^*(a) = a_0 + a_1 a + \dots a_n a^n.$$

[1]Se puede definir de una manera en extremo precisa y a pesar de ser técnicamente lo más adecuado, para una primera aproximación al tema es conveniente tratar a la indeterminada como un simple símbolo.

Es importante distinguir f de f^*, no son lo mismo. Al ser uno un objeto formal y otro una función, sus igualdades resultan distintas. Por un lado, si dos polinomios p y q resultan iguales, las funciones asociadas a ellos resultarán de igual forma iguales. Sin embargo, es posible tener dos polinomios distintos para los que sus función asociadas resultan iguales. Para ilustrar esto, considérense los polinomios sobre el anillo $\mathbb{Z}_2$ dados por $p = x + [1]$ y $q = x^3 + [1]$, en cuyo caso las funciones inducidas están dadas por $p^*([n]) = [n] + [1]$ y $q^*([n]) = [n]^3 + [1]$. En este caso, como los enteros módulo 2 tienen sólo dos elementos, es sencillo comprobar que las funciones p^* y q^* resultan iguales pues $p^*([0]) = [1] = q^*([0])$ y $p^*([1]) = [0] = q^*([1])$ y en consecuencia $p^* = q^*$. Esto comprueba que es posible tener $p \neq q$ pero $p^* = q^*$. A pesar de esto, escribiremos sin remordimiento $f(a)$ en lugar de $f^*(a)$, recalcando que es ésta la única manera sensible de interpretar dicho símbolo al considerar que los polinomios no son funciones entre anillos, pero inducen una de manera muy natural.

10.2. El anillo de los polinomios

Como hemos realizado en un número nada pequeño de ocasiones, intentaremos construir un anillo con nuestros objetos de interés. En particular, nos enfocaremos en crear una estructura con los polinomios.

Teorema 10.3. *Sean f y g polinomios no nulos sobre un anillo R. Entonces, $f + g$ es también un polinomio sobre R y en particular $f + g = 0$ o $\operatorname{grd}(f + g) \leq \text{máx}\{\operatorname{grd}(f), \operatorname{grd}(g)\}$.*

Demostración. Sean $f = (a_0, a_1, \dots)$ y $g = (b_0, b_1, \dots)$ con grados n y m respectivamente. Entonces, para cualquier $k > \text{máx}\{m, n\}$, se tiene

$$(f + g)(k) = a_k + b_k = 0.$$

Lo anterior indica que $f + g$ es en verdad un polinomio y que en el caso de ser éste distinto de 0, su grado no puede exceder al máximo indicado, como afirma el teorema. ■

Teorema 10.4. *Sean f y g polinomios no nulos sobre un anillo R. Entonces, $f \cdot g$ es un polinomio sobre R; en particular $f \cdot g = 0$ o $\operatorname{grd}(f \cdot g) \leq \operatorname{grd}(f) + \operatorname{grd}(g)$.*

Demostración. Tomando $f = (a_0, a_1, \dots)$ y $g = (b_0, b_1, \dots)$ con grados n y m respectivamente, basta probar que $(f \cdot g)(k) = 0$ para cada $k > m + n$. Supongamos entonces $k > m + n$. Sabemos que

$$(f \cdot g)(k) = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{n} a_i b_{k-i} + \sum_{i=n+1}^{k} a_i b_{k-i}.$$

Entonces para todo $i \leq n$, tenemos $k - i \geq m$ por lo que $b_{k-i} = 0$ y en consecuencia

$$\sum_{i=0}^{n} a_i b_{k-i} = 0.$$

Además sabemos que $a_i = 0$ si $i \leq n + 1$ por lo que

$$\sum_{i=n+1}^{k} a_i b_{k-i} = 0$$

con lo que es posible concluir que $(f \cdot g)(k) = 0$ siempre que $k > m + n$, concluyendo el resultado deseado. ■

Corolario 10.5. *Si R es un dominio entero, entonces $f \cdot g \neq 0$ y $\operatorname{grd}(f \cdot g) = \operatorname{grd}(f) + \operatorname{grd}(g)$*

Demostración. Tomando $f = (a_0, a_1, \dots)$ y $g = (b_0, b_1, \dots)$ de nueva cuenta, nos interesa calcular el coeficiente de grado $m + n$ del producto, si éste resulta distinto de cero, entonces podemos garantizar el resultado. Por un lado tenemos que, si $i > n$, entonces $a_i = 0$ y si $i < n$, entonces $m < m + n - i$ por lo que $b_{m+n-i} = 0$. Podemos entonces concluir que $a_i b_{m+n-i} \neq 0$ si y sólo si $i = n$. Esta conclusión, se traduce en tener

$$(f \cdot g)(m + n) = \sum_{i=0}^{m+n} a_i b_{m+n-i} = a_n b_m,$$

pero por hipótesis $a_n \neq 0$ y $b_n \neq 0$ y como R es un dominio entero, entonces $a_n b_m \neq 0$ lo que nos permite concluir $(f \cdot g)(m + n) \neq 0$ y por tanto $\operatorname{grd}(f \cdot g) = m + n$ como afirma en enunciado. ■

Definición 10.5. Al conjunto de todos los polinomios sobre R, se le denota como $R[x]$.

Una vez establecido, que entre polinomios es posible definir operaciones derivadas del anillo conmutativo, podemos construir una estructura nueva.

Teorema 10.6. *Sea R un anillo conmutativo. Entonces $R[x]$ junto a las operaciones definidas en las sucesiones, forma un anillo conmutativo.*

Demostración. Los teoremas 10.3 y 10.4 muestran que las operaciones sobre sucesiones, resultan en operaciones sobre el conjunto $R[x]$. Además, la proposición 10.1 muestra que las operaciones son tanto conmutativas como asociativas además de satisfacer la ley distributiva. Basta entonces probar la existencia de los neutros e inversos.

Hemos probador ya (ejercicio 10.2) que las sucesiones $\mathbf{0}$ y $\mathbf{1}$ cumplen con las propiedades de neutro aditivo y multiplicativo además de ser polinomios. Ahora, si tomamos un polinomio cualquiera $f = a_0 + a_1 x + \cdots + a_n x^n$, el polinomio

$$g = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$$

satisface $f + g = \mathbf{0}$, mostrando que los inversos para la suma existen para cada polinomio y son también polinomios. Con esto $R[x]$ resulta un anillo conmutativo como se afirma. ■

Un resultado que nos permitirá dar una descripción del anillo de polinomios a condición que R tenga un poco más de estructura se menciona en el siguiente corolario, el cual es una consecuencia inmediata del corolario 10.5.

Corolario 10.7. *Si R es un dominio entero, entonces $R[x]$ es también un dominio entero.*

Una vez establecido $R[x]$ como un anillo conmutativo, podemos usar este hecho para conseguir el anillo de polinomios sobre $R[x]$ con indeterminada y, $R[x][y]$, el cual se acostumbra escribir como $R[x, y]$; por ejemplo la expresión

$$p = 5 + (x + 1)y + (5 + x + x^2)y^2$$

pertenece al conjunto $\mathbb{Z}[x, y]$. Es común denotar el polinomio p como

$$p = 5 + x + xy + 5y^2 + xy^2 + x^2y^2.$$

El proceso anterior puede continuar de manera indefinida y obtener un anillo de polinomios en varias indeterminadas formando otra vez un anillo: $R[x_1, \dots x_m]$. Aunque interesante, este procedimiento se menciona simplemente como curiosidad, de momento tenemos amplio interés en los polinomios en una variable, con especial énfasis en los polinomios sobre un campo, en particular sobre los campos real y complejo.

10.3. Un teorema de división

Queremos estudiar y dar resultados acerca de polinomios que tomen valores en los campos real y complejo, por lo que en esta sección nos restringiremos a tomar polinomios sobre un campo F. Si esta razón no parece suficiente, considérese también que muchos de los anillos que hemos estudiado y que nos interesan en el desarrollo de la teoría de polinomios, están contenidos en algún campo.

Definición 10.6. Sean f y g polinomios sobre un campo F. Se dice que *g divide a f* o que *f es un múltiplo de g*, en símbolos $g \mid f$, siempre que exista un polinomio q de forma que

$$f = qg$$

Esta definición es análoga a la que dimos enteros, no debe parecer sorprendente entonces que podamos efectuar una división entre polinomios.

Teorema 10.8. *Sea F un campo y sean f y g polinomios sobre F. Entonces existen un par de polinomios únicos q y r tales que $r = 0$ o $\operatorname{grd}(r) < \operatorname{grd}(g)$ y además*

$$f = qg + r.$$

Demostración. Supongamos primero que $g \mid f$, en ese caso de existir un polinomio q de forma que $f = qg$ por lo que basta tomar $r = 0$. Si por otro lado $g \nmid f$, el conjunto de polinomios

$$S = \{f - qg \mid q \in F[x]\}$$

contiene debe contener al menos un elemento distinto del polinomio nulo, resultando con esto que el conjunto

$$P = \{\operatorname{grd}(p) \mid p \in S \text{ y } p \neq 0\}$$

es de igual forma no vacío y por esta razón debe poseer un mínimo. Sea m el mínimo de P y sea $r = f - qg$ el polinomio en S de forma que $\operatorname{grd}(r) = m$. Como $f = qg + r$, resta mostrar la desigualdad $\operatorname{grd}(r) < \operatorname{grd}(g)$. Si elegimos $\operatorname{grd}(g) = n$ y expresamos $g = b_0 + b_1 x + \cdots + b_n x^n$ y $r = c_0 + c_1 x + \cdots + c_m x^m$, debemos tener $b_n \neq 0$ y, al ser un elemento de un campo, este debe tener inverso. Mostraremos ahora que $m < n$ al obtener una contradicción al tomar como cierto $n \leq m$. Haciendo esa suposición y definiendo los polinomios

$$s = c_m b_n^{-1} x^{m-n}$$

y

$$h = r - sg,$$

debemos notar que h debe cumplir una de dos posibilidades: $h = 0$ o $\operatorname{grd}(h) < m$. Si por un lado $h = 0$, entonces $r = sg$ y

$$f = qg + r = (q + s)g,$$

lo que implica, de manera contradictoria, que $g \mid f$. Si por otro lado $h \neq 0$ y $\text{grd}(h) < m$, entonces

$$f - qg = r = h + sg$$

y por tanto $h = f - (q + s)g$ lo que contradice que m sea el mínimo de P, como afirmamos anteriormente. Debemos entonces concluir que $n \leq m$ es imposible, y obtener en consecuencia $\text{grd}(r) < \text{grd}(g)$. Afirmando con esto, la existencia de los polinomios q y r con las propiedades deseadas.

Supongamos que existe otro par de polinomios q' y r' de forma que $\text{grd}(r') < \text{grd}(g)$ y también $f = q'g + r'$. En ese caso,

$$(q - q')g = r' - r.$$

Si $r \neq r'$, entonces

$$\begin{aligned} \text{grd}(g) &\leq \text{grd}(q - q') + \text{grd}(f) \\ &= \text{grd}(r' - r) \\ &< \text{grd}(g), \end{aligned}$$

lo cual es por supuesto contradictorio; por tanto $r' = r$ y obtenemos $g(q - q') = 0$. Al ser $F[x]$ un dominio entero y $g \neq 0$, concluimos también $q = q'$. Lo anterior afirma que los polinomios q y r no sólo existen sino son los únicos con las propiedades que buscamos. ■

Definición 10.7. Los polinomios q y r que ocurren en el teorema 10.8, llevan el nombre *cociente y residuo de dividir p por q*, respectivamente.

Un caso muy sencillo de división entre polinomios, se da precisamente cuanto dividimos entre un polinomio de grado 1.

Lema 10.9. *Sea f un polinomio sobre un campo F y sea a en dicho campo. Entonces, existe un polinomio q de forma que*

$$f = q(x - a) + f(a).$$

Demostración. Por el teorema de división existen polinomios q y r de forma que

$$f = q(x - a) + r$$

con $\text{grd}(r) < 1$. En el ejercicio 10.5 se muestra que la función de evaluación e_a, es un homomorfismo entre anillos, en ese caso

$$f(a) = e_a(f) = e_a(q(x - a)) + e_a(r) = e_a(r) = r(a)$$

pero como el grado de r es 0, entonces $r = f(a)$. En ese caso, el resultado sigue. ■

La ecuación en el lema sugiere una condición sugiere una relación con un tipo de ecuaciones asociadas a la función que induce un polinomio. Las cuales estudiaremos con detalle más adelante, de momento podemos ver cual es la relación que guardan con la divisibilidad.

Definición 10.8. Sea f un polinomio sobre un campo F y sea a un elemento de ese mismo campo. Decimos que *a es una raíz de f* si $f(a) = 0$.

Proposición 10.10. *Sea f es un polinomio sobre un campo F. Entonces un elemento a del campo es una raíz de p si y sólo si $x - a$ divide a f.*

Demostración. Es inmediato del lema 10.9. ■

Vamos por último a citar un importante teorema que nos deja estimar el número de raíces de un polinomio.

Teorema 10.11. *Sea F un campo. Cualquier polinomio sobre el campo F con grado n tiene a lo más n raíces.*

Demostración. Procederemos por inducción sobre $n \geq 0$. Si $n = 0$ y f es un polinomio con ese grado, entonces f debe ser no nulo y constante, por lo que su número de raíces es cero. Supongamos ahora el resultado para n, i.e., todo polinomio de grado n tiene a lo más n raíces y supongamos también que f sea de grado $n+1$. Si f no tiene raíces entonces el resultado sigue al tener $0 \leq n+1$; si por el contrario, f tiene al menos una raíz, digamos a, entonces $(x-a) \mid f$ según el lema 10.10. En otras palabras, existe un polinomio q de forma que $f = q(x-a)$ lo que nos permite calcular el grado de q directamente como $\text{grd}(q) = n$ y en ese caso, la hipótesis de inducción garantiza que q tiene a lo más n raíces. Además, si b es una raíz de f distinta de a, entonces

$$q(b)(b-a) = f(b) = 0$$

y como $b - a \neq 0$, podemos concluir $q(b) = 0$ por ser elementos de un campo. En conclusión, cualquier raíz de f distinta de a, es una raíz de q. En ese caso, las raíces f distintas de a no pueden ser más de n, agregando a a esa lista, se deben tener a lo más $n+1$ raíces de f. De esto se concluye el resultado. ■

Como precaución, los polinomios que no están sobre dominios enteros pueden no poseen la propiedad mencionada. Por ejemplo, el polinomio

$$x^2 - [1] \in \mathbb{Z}_8[x]$$

tiene cuatro raíces distintas, a decir $[1]$, $[3]$, $[5]$ y $[7]$.

Por último, debemos observar que la existencia de las raíces, garantiza una forma muy simple de expresar un polinomio como una descomposición. La prueba del teorema es relativamente sencilla y se deja como ejercicio (10.9).

Teorema 10.12. *Sea f un polinomio de grado n sobre un campo F y sean $c_1, c_2, \ldots, c_n$ raíces distintas de f, entonces existe un elemento c en el campo de forma que*

$$f = c(x - c_1)(x - c_2)\ldots(x - c_n).$$

Ejercicios

Ejercicio 10.1. Termina la prueba de la proposición 10.1

Ejercicio 10.2. Demuestra que las sucesiones $\mathbf{0}$ y $\mathbf{1}$ satisfacen $f + \mathbf{0} = \mathbf{0} + f = f$ y $f \cdot \mathbf{1} = \mathbf{1} \cdot f = f$.

Ejercicio 10.3. Sean f y g polinomios no nulos sobre un campo F. Si $g \mid f$, demuestra que

$$\text{grd}(g) \leq \text{grd}(f).$$

Ejercicio 10.4. Considera los polinomios no nulos f y g sobre un campo F, expresados como $f = a_0 + a_1x + \cdots + a_mx^m$ y $g = b_0 + b_1x + \cdots + b_nx^n$, tomando m y n como sus grados, respectivamente, y $n \leq m$. Si definimos el polinomio $s = a_m b_n^{-1} x^{m-n}$ y $f - sg$ es no nulo, demuestra que

$$\text{grd}(f - sg) < \text{grd}(f).$$

Ejercicio 10.5. Sea F un campo. Para un elemento a del campo F, definimos la función $e_a \colon F[x] \to F$ usando la siguiente regla:

$$e_a(f) = f(a).$$

Demuestra que e_a es un homomorfismo de anillos.

Ejercicio 10.6. Demuestra el teorema 10.12 Sugerencia: Usa inducción sobre $n \geq 1$.

Ejercicio 10.7. Sea $\alpha \in \mathbb{C}$ y sea

$$\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[x]\}.$$

Muestra que $\mathbb{Z}[\alpha]$ es cerrado con las operaciones en los complejos y que junto a éstas resulta un anillo conmutativo.

Ejercicio 10.8. Demuestra la siguiente igualdad de conjuntos

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

Ejercicio 10.9. Demuestra el teorema 10.12.

Hasta ahora, no hemos hablado de subanillos a pesar que hemos ya tocado el tema de subgrupos, motivados únicamente por la falta de ejemplos. Ahora, con mucha más teoría desarrollada, podemos proveer una gran diversidad de ejemplos.

Definición 10.9. Sea R un anillo conmutativo. Decimos que un conjunto $S \subset R$ es *un subanillo de* R, si

- $1_R \in S$.
- Para cualesquiera a y b en S, $a - b$ es también un elemento de S.
- S es cerrado bajo el producto del anillo.

Ejercicio 10.10. Prueba que $\mathbb{Z}$ es el subanillo más pequeño contenido en $\mathbb{C}$.

Ejercicio 10.11. Sea $\alpha \in \mathbb{C}$. Demuestra que $\mathbb{Z}[\alpha]$ es el subanillo más pequeño en $\mathbb{C}$ que contiene a α, i.e., si $R \subset \mathbb{C}$ es un subanillo de forma que $\alpha \in R$, entonces $\mathbb{Z}[\alpha] \subset R$.

Ejercicio 10.12. Un complejo α se dice un *entero algebraico* si existe un polinomio $f \in \mathbb{Z}[x]$ de forma que $f(\alpha) = 0$. Demuestra que el conjunto de enteros algebraicos es un subanillo de $\mathbb{C}$.

Referencias

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

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

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 aumentalo. El único objectivo 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.