Lectura 11: Polinomios II

11.1. Máximo común divisor

Definición 11.1. Sean f y g polinomios sobre un campo. Un polinomio d se dice un divisor común de f y g, si $d \mid f$ y $d \mid g$. Por otro lado, un polinomio d se dice *un máximo común divisor de f y g* si es un divisor común de f y g, y para todo divisor común e de f y g, satisface $e \mid d$.

No es coincidencia que se use el término *un máximo común divisor*. Es posible que exista una multitud de ellos para cada pareja de polinomios. Por ejemplo, para los polinomios $x^2 + 1$ y $x^2 - ix$ sobre el campo $\mathbb{C}$ el polinomio $ix - 1$ es un máximo común divisor, lo mismo que el polinomio $2x + 2i$. Estos polinomios no resultan arbitrarios en absoluto y guardan una fuerte relación.

Definición 11.2. Dos polinomios f y g sobre un campo se dicen *asociados*, si existe un elemento $a \neq 0$ de forma que

$$f = ag.$$

Proposición 11.1. *Sean f y g polinomios sobre un campo. Si d y e son ambos un máximo común divisor de f y g, entonces d y e están asociados.*

Demostración. Debemos notar que primero que $e \mid d$ y lo mismo $d \mid e$. Si alguno de estos polinomios fuera nulo, entonces el otro también lo sería y de esta forma $d = 0 = e$, lo que indica que estarían asociados. Si por otro lado ambos son no nulos, entonces $\operatorname{grd}(e) = \operatorname{grd}(d)$. Ahora, como $e \mid d$, existe un polinomio q de forma que $e = qd$ pero como los grados coinciden, $\operatorname{grd}(q) = 0$ y q debe ser constante. En ese caso, los polinomios d y e están asociados. ■

Proposición 11.2. *Sean f y g polinomios sobre un campo. Si d es un máximo común divisor de f y g, y e está a asociado a d, entonces e es también un máximo común divisor de f y g.*

Las proposiciones anteriores nos permiten establecer la relación que existe entre las múltiples opciones de máximo común divisor, sin embargo, debemos ahora garantizar que cada pareja de polinomios posee al menos un máximo común divisor.

Teorema 11.3. *Sean f y g polinomios sobre un campo F. Entonces, existe un máximo común divisor de f y g. Además, cualquier máximo común divisor, es una combinación lineal de f y g, i.e., existen polinomios s y t sobre F de forma que, si d es un máximo común divisor,*

$$d = sf + tg.$$

Demostración. Si f y g resultan nulos, entonces el polinomio nulo es un máximo común divisor el cual es trivialmente una combinación lineal. Supongamos sin perdida de la generalidad que $f \neq 0$ y consideremos el conjunto

$$I = \{sf + tg \mid s, t \in F[x]\}.$$

Los polinomios f y g son elementos de I por lo que el conjunto I contiene al menos un elemento no nulo y en consecuencia no será vacío el conjunto

$$N = \{\deg(p) \mid p \neq 0 \text{ y } p \in I\}.$$

En ese caso, podemos tomar $d = sf + tg$ como un polinomio en el conjunto I de forma que su grado sea el mínimo de N, para algunos polinomios s y t sobre F. Afirmamos que d es un máximo común divisor garantizando con éste, la existencia de al menos uno.

Mostraremos primero que es un divisor común de f y g, utilizando el teorema de división para expresar

$$f = qd + r$$

con $r = 0$ o $\mathrm{grd}(r) < \mathrm{grd}(d)$. Si $r \neq 0$, entonces

$$r = f - qd = f - q(sf + tg) = (1 - qs)f + (-qt)g,$$

mostrando con esto que r es una combinación lineal de f y g que tiene un grado menor que d. Esto último contradice que d sea una combinación lineal del menor grado posible y en consecuencia podemos afirmar que $r = 0$, en cuyo caso $d \mid f$. Un argumento análogo se puede proveer para g y concluir que $d \mid g$ mostrando con esto que d es un divisor común de f y g. Ahora, si e fuera un máximo común divisor, entonces éste divide a cualquier combinación lineal de f y g, en particular debemos tener que $e \mid d$. Concluimos que d es un máximo común divisor como afirmamos.

Si tomamos ahora e como un máximo común divisor, por el la proposición 11.1, los polinomios e y d están asociados y como d es una combinación lineal de f y g, e debe resultar de igual manera una combinación lineal de f y g. Esto termina la prueba. ■

Definición 11.3. Un polinomio se dice *mónico* si su coeficiente principal es 1.

Proposición 11.4. *Para cada par de polinomios no ambos nulos sobre un campo, existe un único polinomio mónico que es un máximo común divisor de éstos.*

Demostración. Tomemos f y g polinomios sobre un campo. Por el teorema 11.3 sabemos que existe un máximo común divisor d de estos polinomios el cual debe ser no nulo al ser al menos uno de ellos no nulo. Como el coeficiente principal de cualquier polinomio es distinto de 0, podemos tomar a^{-1} como el inverso del coeficiente principal de d para formar el polinomio mónico

$$m = a^{-1}d.$$

Por la proposición 11.2, el polinomio m debe ser un máximo común divisor al estar asociado d.

Supongamos ahora que p fuera un polinomio mónico que además resulta un máximo común divisor de f y g. Por definición $p \mid m$ y además $m \mid p$ por lo que $\mathrm{grd}(p) = \mathrm{grd}(m)$; esto implica que al expresar $m = qp$, podemos concluir $\mathrm{grd}(q) = 0$. Si expresamos $q = a$, donde $a \neq 0$ es un elemento del campo, entonces el coeficiente principal de qp entonces resulta a y este debe coincidir con el coeficiente principal de m que es 1 al ser mónico. En ese caso $a = 1$ y consecuencia $m = p$. ■

Definición 11.4. Para polinomios f y g sobre un campo, definimos *el máximo común divisor de f y g* como sigue: Si f y g son ambos nulos, entonces el máximo común divisor es el polinomio nulo. En caso contrario, el máximo común divisor es el único polinomio mónico que resulta un máximo común divisor de f y g. Al máximo común divisor se le denota usando (f, g).

En el ejemplo que hemos dado al principio con los polinomios $x^2 + 1$ y $x^2 - ix$, resultaba que los polinomios $ix - 1$ y $2x + 2i$ eran ejemplos de un máximo común divisor. En sencillo ver que éstos están asociados, además permiten calcular el polinomio mónico que resulta el máximo común divisor, simplemente multiplicando por el inverso de su coeficiente principal, resultado entonces

$$(x^2 + 1, x^2 - ix) = x - i.$$

11.2. Algoritmo de Euclides

Como en el caso de enteros, en los polinomios podemos describir un análogo al algoritmo de Euclides aplicando el teorema de la división suficientes veces. Así, para polinomios f y g, obtenemos

$$\begin{aligned}
f &= q_1 g + r_1 \\
g &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

Sabemos que esto sucede al tener $\operatorname{grd}(r_{k+1}) < \operatorname{grd}(r_k)$ o $r_{k+1} = 0$ para cada k donde pueda ejecutarse la división. De la misma manera en que se realiza en los enteros, el algoritmo Euclides nos provee de un método para calcular el máximo común divisor de manera mecánica y también permite expresar cualquier máximo común divisor como una combinación lineal. Esto se debe a que el polinomio r_n debe cumplir

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \cdots = (g, r_1) = (f, g)$$

por lo que resulta en máximo común divisor de f y g. Para ilustrar esto, consideremos los polinomios $f = x^3 - x - x + 1$ y $g = x^2 + x - 2$ en ese caso

$$\begin{aligned}
x^3 - x^2 - x + 1 &= (x-2)(x^2 + x - 2) + 3x - 3 \\
x^2 + x - 2 &= \left(\frac{1}{3}x + \frac{2}{3}\right)(3x - 3).
\end{aligned}$$

Por lo que podemos concluir que $3x - 3$ es un máximo común divisor el cual está asociado al polinomio mónico $x - 1$ y al ser este el único con esa propiedad podemos concluir que se trata del máximo común divisor de f y g. La expresión también nos muestra como expresar un máximo común divisor como una combinación lineal:

$$3x - 3 = (1)(x^3 - x^2 - x + 1) + (-x + 2)(x^2 + x - 2).$$

Debe recordarse que el proceso se explicó para enteros con mucho más detalle y parecería ocioso repetirlo de nueva cuenta al ser idéntico. Lo mejor será que ante la duda, se revisen los conceptos en enteros y se cambien todas las apariciones de enteros por polinomios, lo que será suficiente para describir el proceso con absoluto detalle.

11.3. Polinomios irreducibles

Vamos a definir ahora una generalización de número primo y enseguida mostraremos que su comportamiento es muy similar al de estos números.

Definición 11.5. Un polinomio no constante p sobre un campo se dice *irreducible* cuando, $p = fg$ implica que alguno de los polinomios f o g es constante.

Proposición 11.5. *Si p es un polinomio irreducible y f un polinomio tal que $p \nmid f$, ambos sobre un campo, entonces $(p, f) = 1$.*

Demostración. Como $p \nmid f$, el residuo de la división $f = qp + r$ es no nulo con $\text{grd}(r) < \text{grd}(p)$. Si elegimos d como un máximo común divisor de f y q, entonces d divide a r al ser el residuo una combinación lineal de f y p; en ese caso

$$\text{grd}(d) \leq \text{grd}(r) < \text{grd}(p).$$

Ahora, por definición $d \mid p$, por lo que existe un polinomio e de forma que $p = ed$ y en consecuencia

$$\text{grd}(p) = \text{grd}(e) + \text{grd}(d),$$

pero al ser p irreducible, alguno de estos polinomios debe ser constante. Si $\text{grd}(e) = 0$, entonces $\text{grd}(p) = \text{grd}(d)$ lo cual es contradictorio. Obtenemos con esto que d es constante y el único polinomio mónico constante es 1 por lo que $(p, f) = 1$ como afirmamos. ■

Teorema 11.6 (Euclides)**.** *Sean f, g y p polinomios sobre un campo de forma que p sea irreducible. Entonces, si $p \mid fg$ se tiene $p \mid f$ o $p \mid g$.*

Demostración. Ejercicio 11.7 ■

El concepto de irreducible puede no ser tan sencillo como el de número primo y depende en gran medida de la estructura base:

- El polinomio $x^2 + 1$ es irreducible en $\mathbb{R}[x]$.
- El polinomio $x^3 - 2$ es irreducible en $\mathbb{Q}[x]$.
- El polinomio $x^2 + [1]$ es irreducible en $\mathbb{Z}_3[x]$.
- Los polinomios $x - a$ son irreducibles en $F[x]$ para cualquier campo F.

Proposición 11.7. *Sea f un polinomio de grado 2 o 3 sobre un campo F. Entonces, f es irreducible si y sólo si f no tiene una raíz en el campo.*

Demostración. Si f tiene una raíz entonces admite un divisor de grado 1, resultando éste no irreducible. Con esto se prueba que, si f es irreducible, entonces f no tiene una raíz.

Si ahora asumimos que f no es irreducible, entonces existen polinomios p y q que permiten expresar $f = pq$, con $0 < \text{grd}(p) < \text{grd}(f)$ y $0 < \text{grd}(q) < \text{grd}(f)$. Ahora, como $\text{grd}(f) = 2$ o 3 la suma $\text{grd}(p) + \text{grd}(q)$ lo será de igual forma. Eso quiere decir que por lo menos uno de estos grados debe ser 1, por lo que f admite un divisor de grado 1 y en consecuencia una raíz. Con esto hemos probado que, si f no tiene una raíz en el campo, entonces es irreducible. ■

En particular, el ejercicio 11.9 muestra bajo qué condiciones un polinomio de grado 2 es irreducible en $\mathbb{R}$. Además, según el teorema de valor intermedio, todo polinomio de grado impar en $\mathbb{R}[x]$ tiene una raíz real lo que implica tiene al menos un divisor de grado 1 resultando no irreducible. En general, un polinomio con grado mayor que 2 en $\mathbb{R}[x]$ no puede ser irreducible. Este resultado se creyó cierto por un largo tiempo antes de conseguir ser probado. Leonhard Euler consiguió desarrollar un método que garantizaba esto para polinomios de grado 4 y 6, pero fue incapaz de encontrar un método general. Fue Carl Friedrich Gauss quien en 1800 encontró un método que conseguía mostrar lo a Euler buscaba. El resultado derivado de las indagaciones de Gauss es tan importante que lleva por nombre *El teorema fundamental del álgebra*. Mencionamos ahora sólo su postulado, lamentablemente la prueba escapa, de momento, nuestro alcance.

Teorema 11.8 (Teorema fundamental del álgebra)**.** *Todo polinomio no constante con coeficientes en los complejos, tiene una raíz en los complejos.*

Corolario 11.9. *Sea f un polinomio en $\mathbb{R}[x]$. Si f es irreducible, entonces* $\operatorname{grd}(f) \leq 2$*.*

Demostración. Probaremos el resultado de manera contrapositiva, suponiendo que un polinomio f con $\operatorname{grd}(f) > 2$, no puede ser irreducible. Si por un lado, el polinomio f tiene un raíz real, entonces admite un divisor de grado 1 y en consecuencia no será irreducible. Supongamos entonces que f no tiene raíces reales. Según el teorema fundamental del álgebra, debe existir una raíz $\alpha \in \mathbb{C}$ de f de forma que $\alpha \notin \mathbb{R}$; además el ejercicio 11.10 garantiza que su conjugado, $\bar{\alpha}$, también es una raíz y cumple que $\alpha \neq \bar{\alpha}$. Ahora, si definimos el polinomio $p = (x - \alpha)(x - \bar{\alpha})$, éste resulta un polinomio con coeficientes reales; en otras palabras es un elemento e $\mathbb{R}[x]$. Dividimos f por este polinomio para obtener los polinomios q y r, ambos en $\mathbb{R}[x]$, de forma que

$$f = qp + r$$

donde $r = 0$ o $\operatorname{grd}(r) \leq 1$. En ese caso podemos tomar $r = ax + b$, con a y b reales. Como α y $\bar{\alpha}$ son raíces de f y de p, se satisface

$$a\alpha + b = r(\alpha) = 0 = r(\bar{\alpha}) = a\bar{\alpha} + b$$

lo cual sólo es posible si $a = b = 0$. Por tanto $f = qp$ y como ni q ni p son polinomios constantes, concluimos que f no puede ser irreducible. Esto prueba el resultado. ■

Con estos resultados, hemos conseguido dar condiciones para clasificar polinomios irreducibles en $\mathbb{R}[x]$ y $\mathbb{C}[x]$. Aunque estos métodos son limitados (y los polinomios que resultan no muy interesantes) nos permiten observar cuan completos son estos campos, éstos contienen una buena cantidad de soluciones para ecuaciones que no resultan nada triviales. Por supuesto, mientras menos propiedades algebraicas tenga un campo, menos ecuaciones se resuelven él y más variedad de polinomios irreducibles tendrá. Sin embargo, esto no repercute para considerar a estos polinomios como nuestro bloque fundamental para construir a los polinomios.

11.4. Factorizacion única

Como en el caso de los enteros, probaremos primero que es posible realizar dichas factorizaciones, sin embargo, dejaremos cierta terminología sin aclarar guardando la ilusión que ésta se explique por si misma.

Lema 11.10. *Sea un polinomio no constante f sobre un campo. Entonces, existen polinomios mónicos irreducibles $p_1, p_2, \ldots, p_{k-1}$ y p_k, y un elemento c del campo de forma que*

$$f = cp_1 \ldots p_k.$$

Demostración. Probaremos el resultado por inducción sobre el grado f. Para $\mathrm{grd}(f) = 1$, $f = ax + b$ para algunos $a \neq 0$ y b elementos del campo, en ese caso $f = a(x - a^{-1}b)$ y como todo polinomio lineal es irreducible, el resultado sigue. Supongamos ahora el resultado para n, i.e., todo polinomio de grado n o menor se puede expresar como un producto de polinomios mónicos irreducibles. Tomemos entonces f de grado $n + 1$. Si f es irreducible, entonces el resultado sigue como en el caso lineal. Supongamos entonces que no es irreducible; en ese caso, existen polinomios p y q con $\mathrm{grd}(p) < n + 1$ y $\mathrm{grd}(q) < n + 1$, que satisfacen $f = pq$. Por hipótesis de inducción, esto implica que existen polinomios mónicos irreducibles $p_1, \ldots, p_l, \ldots, p_{k-1}$ y p_k de forma que

$$p = c_1 p_1 \ldots p_l$$

y

$$q = c_2 q_{l+1} \ldots q_k.$$

En ese caso,

$$f = c_1 c_2 p_1 \ldots p_k$$

y el resultado es válido para $n + 1$. Por inducción fuerte, el enunciado del lema sigue. ■

Al conjunto de polinomios mónicos irreducibles que aparecen en el lema 11.10 se llama *una factorización en mónico irreducibles*. Como el caso de los enteros, el orden no importará cuando establecemos la igualdad entre factorizaciones.

Teorema 11.11. *Sea un polinomio no constante f sobre un campo. Entonces, existe una única factorización de f en polinomios mónicos irreducibles.*

Demostración. El lema 11.10 garantiza la existencia de al menos una factorización. Supongamos entonces que $f = c_1 p_1 \ldots p_k$ y $f = c_2 q_1 \ldots q_l$ son factorizaciones de f. Queremos probar que $c_1 = c_2$, $k = l$ y ambas factorizaciones están formadas por los mismos polinomios. Primero, como los polinomios involucrados en ambas son mónicos, podemos concluir que c_1 y c_2 son iguales y distintos de 0. Lo anterior implica que la siguiente igualdad debe ser cierta

$$p_1 \ldots p_k = q_1 \ldots q_l.$$

Debemos entonces probar que los polinomios a cada lado de la igualdad son los mismos, lo cual se conseguirá usando un argumento inductivo sobre k.

Para $k = 1$, debemos suponer $p_1 = q_1 \ldots q_l$. En ese caso, $k = l = 1$ y $p_1 = q_1$, pues en otro caso p_1 sería el producto de mónicos irreducibles y por tanto no sería irreducible.

Supongamos para un natural k, que las factorizaciones coinciden siempre que su producto coincida. Si $p_1 \ldots p_k p_{k+1} = q_1 \ldots q_l$, entonces $p_1 \mid q_1 \ldots q_l$ y, por el lema de Euclides para polinomios, p_1 debe dividir alguno de los factores q_j. Pero q_j siendo mónico e irreducible, no puede tener más divisores mónicos que 1 y si mismo. En otras palabras o $p_1 = 1$ o $p_1 = q_j$. Pero p_1 es también irreducible, así $p_1 \neq 1$, por lo que nos vemos obligados a concluir que $p_1 = q_j$ para algún $1 \leq j \leq l$. Esto nos permite, usando la ley de cancelación del producto en el anillo de polinomios, dar por válida la igualdad:

$$p_2 \cdots p_{k+1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_l.$$

Con lo anterior, la hipótesis de inducción garantiza que los conjuntos

$$\{p_2, \dots, p_{k+1}\} = \{q_1, \dots, q_{j-1} q_{j+1} \dots q_l\}$$

lo cual implica a su vez que

$$\{p_1, \dots, p_{k+1}\} = \{q_1, \dots, q_l\}\,;$$

i.e., las factorizaciones en mónicos irreducibles coinciden. El resultado, entonces, es cierto por inducción. ■

Como en el caso entero, el teorema tiene una implicación sobre la expresión del máximo común divisor. Además, el concepto de mínimo común múltiplo se puede definir de manera análoga al de máximo común divisor. Y siguiendo este camino, denotamos al único polinomio mónico que sea un mínimo común múltiplo de los polinomios f y g por $[f, g]$.

Teorema 11.12. *Sean $p_1, \dots, p_{k-1}$ y p_k polinomios mónicos irreducibles distintos, $m_1, \dots m_k, n_1, \dots n_{k-1}$ y n_k números naturales cualquiera, y sean por último $f = a p_1^{m_1} \dots p_k^{m_k}$ y $g = b p_1^{n_1} \dots p_k^{n_k}$. Entonces, si se elige $l_i = \text{mín}\{m_i, n_i\}$ y $L_i = \text{máx}\{m_i, n_i\}$, se tiene*

$$(f, g) = p_1^{l_1} \dots p_k^{l_k}$$

y

$$[f, g] = p_1^{L_1} \dots p_k^{L_k}.$$

El enunciado debe parecer familiar pues resultar idéntico al propuesto en el caso de enteros. La prueba, por consiguiente, es una recreación a calca de la prueba del resultado para enteros y es un ejercicio interesante mostrar que las manipulaciones necesarias son las mismas en ambos casos.

Terminaremos con una discusión mínima acerca de las formas que presentan los factores primos en algunos anillos:

- Es importante notar qué sucede con las factorizaciones sobre un anillo cualquiera. Por ejemplo, en el anillo de polinomios $\mathbb{Z}_4[x]$ es posible expresar

  $$x^2 - [1] = (x - [1])\,(x + [1]) = (x - [3])\,(x + [3])\,.$$

  Parecería que esto contradice la existencia de una única factorización, el problema se encuentra en no ser $\mathbb{Z}_4$ un campo. Si se estudia con detenimiento la prueba del teorema, se encontrarán al menos dos instancias en donde las propiedades de campo se ponen en juego.

- Por el teorema fundamental del álgebra, todo polinomio f de grado n en $\mathbb{C}[x]$ se puede expresar como

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

  siendo ésta su factorización en irreducibles mónicos. Por supuesto, los complejos $c_1, \dots, c_{n-1}$ y c_n son las raíces del polinomio que el teorema fundamental del álgebra garantiza.

- El teorema fundamental del álgebra también nos dice la forma que presenta la descomposición en irreducibles de un elemento en $\mathbb{R}[x]$: Supongamos que f es un polinomio mónico de grado n en $\mathbb{R}[x]$. Como éste es también un polinomio en $\mathbb{C}[x]$, entonces podemos encontrar complejos $c_1, \dots, c_{n-1}$ y c_n tales que

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

Al ser estos complejos las raíces de f sabemos que, si el complejo c_i no es real, entonces $\bar{c}_i$ debe también aparecer en la lista y ser distinto de c_i. Entonces, el conjunto de raíces de f presenta la forma

$$\{r_1, \ldots, r_k, c_1, \bar{c}_1, \ldots, c_l \bar{c}_l\}$$

donde $r_1, \ldots, r_{k-1}$ y r_k son números reales y $c_1, \ldots, c_{l-1}$ y c_l son complejos no reales. Bajo esta descripción, podemos descomponer el polinomio f como

$$f = (x - r_1)(x - r_2) \cdots (x - r_k) q_1 \cdots q_r$$

donde q_i es el polinomio cuadrático con coeficientes reales dado por

$$q_i = (x - c_i)(x - \bar{c}_i).$$

Por supuesto, la hipótesis de tener f como mónico es realmente innecesaria y se impone sólo para evitar la constante al inicio de la factorización.

Ejercicios

Ejercicio 11.1. Sean f y g polinomios sobre un campo no ambos nulos. Si d es un máximo común divisor de f y g entonces d es no nulo.

Ejercicio 11.2. Sean f y g polinomios sobre un campo. Entonces, f y g están asociados si y sólo si $g \mid f$ y $f \mid g$.

Ejercicio 11.3. Demuestra la proposición 11.2.

Ejercicio 11.4. Sean m, n y d enteros positivos de forma que $d = (m, n)$. Demuestra que

$$(x^n - 1, x^m - 1) = x^d - 1.$$

Ejercicio 11.5. Sea f un polinomio no nulo sobre un campo F. Demuestra que f es una unidad si y sólo si $\operatorname{grd}(f) = 0$.

Ejercicio 11.6. Muestra que los polinomios de la forma $x - a$ sobre un campo cualquiera son irreducibles.

Ejercicio 11.7. Prueba el lema de Euclides para polinomios.

Ejercicio 11.8. Sean $f_1, f_2, \ldots, f_n$ y p polinomios sobre un campo de forma que p sea irreducible. Si $p \mid f_1 \ldots f_n$, demuestra que $p \mid f_k$ para algún entero k entre 1 y n.

Ejercicio 11.9. Demuestra que un polinomio $f = x^2 + bx + c$ es irreducible en $\mathbb{R}[x]$ si y sólo si $b^2 - 4c < 0$.

Ejercicio 11.10. Sea f un polinomio sobre $\mathbb{R}$ y sea α un número complejo. Si $f(\alpha) = 0$, entonces $f(\bar{\alpha}) = 0$ también.

Ejercicio 11.11. Sea α un número complejo cualquiera. Muestra que el polinomio $q = (x - \alpha)(x - \bar{\alpha})$ es un elemento del anillo $\mathbb{R}[x]$.

Ejercicio 11.12. Sea F un campo cualquiera. Muestra que las leyes de cancelación de la suma y producto, son válidas en $F[x]$.

Ejercicio 11.13. Define el concepto de mínimo común múltiplo y prueba el teorema 11.12.

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.