Tarea 1

Nicholas Mc-Donnell

03/2018

1. Demuestre que los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$

   - $x^3 - x - 4$
   - $x^3 - \frac{3}{2}x + 1$
   - $x^4 - x^2 + 1$

Demostración.

- Por teorema de raíces racionales, y ya que es un polinomio de tercer grado, el polinomio es reducible si y solo si tiene una raíz.

$$p(x) = 0 \implies x \in \{\pm 1, \pm 2, \pm 4\}$$

$$p(\pm 1) = -4, p(2) = 2, p(-2) = -10$$

$$p(4) = 56, p(-4) = -64$$

Por lo que es un polinomio irreducible.

- De la misma forma que en el polinomio anterior.

$$p(x) = 0 \implies x \in \{\pm 1\}$$

$$p(1) = 0{,}5, p(-1) = 1{,}5$$

Por lo que es un polinomio irreducible.

- Similarmente a los polinomios anteriores, el conjunto de posibles raíces es finito, pero también hay que considerar el caso donde se puede factorizar en dos polinomios de grado dos.

$$p(x) = 0 \implies x \in \{\pm 1\}$$

$$p(\pm 1) = 1$$

Vemos que no tiene raíces, por lo que solo nos falta ver que no se puede factorizar, para eso se asume que es factorizable, luego notamos que son monicos y que por lema de

Gauss si $p(x) \in \mathbb{Z}[x]$ y es irreducible en $\mathbb{Z}[x]$ entonces es irreducible en $\mathbb{Q}[x]$.

$$p(x) = (x^2 + bx + c)(x^2 + b'x + c')$$

$$p(x) = x^4 + (b' + b)x^3 + (c' + bb' + c)x^2 + (b'c + bc')x + cc'$$

$$\implies cc' = 1,\, b' + b = b'c + bc' = 0,\, c' + bb' + c = -1$$

$$\implies b = -b',\, c = c' = 1$$

$$\implies -b^2 + 2 = -1 \iff b^2 = 3$$

Pero $b \notin \mathbb{Z}$, por lo tanto $p(x)$ es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$

$\square$

2. Sea p un numero primo. Dado un numero racional $x \in \mathbb{Q}, x \neq 0$, podemos escribir

$$x = p^r \cdot \frac{a}{b}, \quad a, b, r \in \mathbb{Z}, \quad \gcd(p, ab) = 1$$

Se define $v_p(x) := r$ y $v_p(0) := \infty$. Sea

$$O_p = \{x \in \mathbb{Q} : v_p(x) \geq 0\}, \quad m_p = \{x \in \mathbb{Q} : v_p(x) > 0\}$$

(a) Demuestre que $(O_p, +, \cdot)$ es un anillo cuyo único ideal maximal es m_p

(b) Demuestre que $O_p/m_p \cong \mathbb{Z}/p\mathbb{Z}$

(c) Sea $I \subset O_p$ un ideal propio. Muestre que existe un entero positivo n tal que

$$I = \{x \in \mathbb{Q} : v_p(x) \geq n\}$$

(d) Sea $k > 0$ un entero. Considere el ideal $I = m_p^k$. Muestre que

$$O_p/I \cong \mathbb{Z}/p^k\mathbb{Z}$$

Demostración.

(a) Hay tres partes para esta demostración, primero que O_p es un anillo, segundo que m_p es ideal y tercero que es el unico ideal maximal.

1) Sea $x, y \in O_p$, sin perdida de generalidad de asume que $r \geq r'$

$$x = p^r \cdot \frac{a}{b},\, y = p^{r'} \cdot \frac{a'}{b'}$$

$$\therefore x + y = p^{r'} \left(p^{r-r'} \frac{a}{b} + \frac{a'}{b'} \right) = p^{r'} \left(\frac{p^{r-r'} ab' + a'b}{bb'} \right)$$

Vemos que $r' \geq 0$, por lo que $x + y \in O_p$.Y claramente se ve lo siguiente

$$\gcd\left(p, bb'\left(p^{r-r'}ab' + a'b\right)\right) = 1$$

Notamos que la suma esta bien definida, y ya que es un subanillo de $\mathbb{Z}$ es conmutativa, sobre esto es fácil ver que para todo elemento del subanillo el inverso de la suma pertenece.

$$0 = p^r \cdot 0$$

$$\implies 0 \in O_p$$

Por lo que $(O_p, +)$ es grupo abeliano. Luego tomamos los mismos x, y.

$$x \cdot y = p^{rr'}\frac{aa'}{bb'}$$

$$\gcd(p, ab) = \gcd(p, a'b') = 1 \implies \gcd(p, aa'bb') = 1$$

2) Se toma $x, y \in m_p$, Similarmente a la parte anterior se nota que $x + y \in m_p$. Luego sea $x \in O_p, y \in m_p$.

$$x \cdot y = p^{r+r'}\frac{aa'}{bb'}$$

Como $r, r' \geq 0$ y $r > 0$, $r + r' > 0$. Por lo que es ideal.

3) Se asume existe un ideal M tal que $m_p \subset M \subset O_p$. Recordamos la definición de O_p y de m_p, con lo que notamos que si $x \in O_p \wedge x \notin m_p \implies v_p(x) = 0$ que a su ves implica lo siguiente:

$$x = \frac{a}{b} \quad \gcd(p, ab) = 1$$

Ahora tomamos x^{-1} el cual claramente pertenece a O_p. Luego ya que M es ideal $x \cdot x^{-1} = 1 \in M$ lo que implica que $M = O_p$, lo cual es una contradicción, por ende m_p es ideal maximal. Dado esto asumimos que existe otro ideal maximal M tal que $M \neq m_p$, por lo tanto existe $x \in M \wedge x \notin m_p$, pero ya notamos que los únicos elementos que no pertenecen a m_p son los que cumplen $v_p(x) = 0$ y si estos pertenecen a un ideal, el ideal es todo el anillo. Por lo que m_p es un ideal maximal y es único.

(b) Para demostrar esto usaremos el primer teorema de isomorfismo, y tomaremos el morfismo natural $\varphi : O_p \to \mathbb{Z}/p\mathbb{Z}$ que cumple con lo siguiente:

$$x = p^r \cdot \frac{a}{b} \quad \gcd(p, ab) = 1$$

$$\varphi(p) = \bar{0}$$

$$\varphi(a) = \bar{a}$$

$$\varphi\left(\frac{1}{b}\right) = \bar{b}^{-1}$$

Este ultimo esta bien definido ya que se sabe que todo elemento no cero en $\mathbb{Z}/p\mathbb{Z}$ tiene inverso y $\gcd(b,p) = 1$ por lo que $\bar{b} \neq \bar{0}$, luego vemos que la suma esta bien definida de la siguiente forma:

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \varphi\left(\frac{ad+bc}{bd}\right)$$

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = (\bar{a}\bar{d} + \bar{b}\bar{c})(\bar{b}\bar{d})^{-1}$$

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \bar{a}\bar{b}^{-1} + \bar{c}\bar{d}^{-1}$$

Por el otro lado:

$$\varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right) = \bar{a}\bar{b}^{-1} + \bar{c}\bar{d}^{-1}$$

Por lo que la suma esta bien definida. Ahora facilmente vemos que $\ker\varphi = m_p$. Por esto $O_p/m_p \cong \mathbb{Z}/p\mathbb{Z}$.

(c) Tomamos un k tal que $(k) = I$:

$$\therefore k = p^r \cdot \frac{a}{b}$$

Luego por ser un ideal si tomamos un $x \in O_p \implies xk \in I$

$$xk = p^{r+r'} \cdot \frac{aa'}{bb'}$$

Sabemos que $r' \geq 0 \implies r + r' \geq r$, lo que nos deja que ver que $\forall a \in I : v_p(a) \geq r$, ya que x era un elemento cualquiera. Pero esto nos dice que $I \subseteq \{x \in \mathbb{Q} : v_p(x) \geq r\}$, por lo que nos falta la otra contención. Para ello notamos que

(d) Usaremos un morfismo similar al de 2. (b) y el primer teorema de isomorfismo.

$$\varphi(p^k) = 0, \varphi(p^r) \neq 0 \quad 0 \leq r < k$$

$$\varphi\left(\frac{1}{a}\right) = \bar{b}^{-1}$$

Este ultimo existe ya que $\gcd(p^k, b) = 1$, por lo que $\bar{b}$ tiene inverso en $\mathbb{Z}/p^k\mathbb{Z}$. Dado esto notamos trivialmente que $\ker\varphi = m_p^k$, por lo que podemos concluir que $O_p/m_p^k \cong \mathbb{Z}/p^k\mathbb{Z}$

$\square$

3. *Dos maneras de construir* $\mathbb{Q}[i]$. Considere el anillo de los enteros de Gauss:

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

(a) Demuestre que $\mathbb{Z}[i]$ es un dominio de integridad y que

$$Frac(\mathbb{Z}[i]) = \{a + ib : a, b \in \mathbb{Q}\}$$

A este ultimo cuerpo le denotamos $\mathbb{Q}[i]$

(b) Demuestre que $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}[i]$. Indicación: encuentre primero un morfismo apropiado $\mathbb{Q}[x] \to \mathbb{Q}[i]$

(c) Demuestre que $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i]$

(d) Demuestre que para todo ideal maximal $I \subseteq \mathbb{Z}[i]$ el cuerpo $\mathbb{Z}[i]/I$

Demostración.

(a) Hay que demostrar dos cosas, primero que $\mathbb{Z}[i]$ es un dominio de enteros y que $Frac(\mathbb{Z}[i]) = \{a + ib : a, b \in \mathbb{Q}\}$

1) Se asume que existen dos elementos $a + ib$ y $c + id$ distintos de cero, tal que su multiplicación es igual a cero.

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc) = 0$$

$$\implies ac = bd, ad = -bc$$

$$\iff acd = bd^2, acd = -bc^2$$

$$\iff b(c^2 + d^2) = 0$$

Si $c^2 + d^2 = 0 \implies c = d = 0 \implies c + di = 0$, pero dijimos que era un elemento no cero. Por lo que $b = 0$

$$\implies ac = 0, ad = 0$$

$$\implies (a = 0 \wedge c = 0) \vee (a = 0 \wedge d = 0)$$

Si $a = 0 \implies a = b = 0 \implies a + ib = 0$, pero dijimos que era un elemento no cero. Por lo que $c = d = 0$, pero esto es la contradicción mencionada anteriormente, por lo que $\mathbb{Z}[i]$ es dominio.

2) Primero recordamos que $Frac(\mathbb{Z}[i]) = \{\frac{a}{b} : a, b \in \mathbb{Z}[i] \vee b \neq 0\}$. Primero notamos lo siguiente:

$$\frac{a + ib}{c + id} = \frac{(ac - bd)}{c^2 + d^2} + i\frac{(ad + bc)}{c^2 + d^2}$$

Ya que $c + id \neq 0$, $c^2 + d^2 \neq 0$. Lo que implica que cada termino por separado pertenece a $\mathbb{Q}$, por lo que $Frac(\mathbb{Z}[i]) \subseteq \mathbb{Q}[i]$. Luego vemos lo siguiente:

$$\frac{a}{b} + i\frac{c}{d} = \frac{ad + ibc}{bd}$$

Ya que $b \neq 0 \vee d \neq 0$, $bd \neq 0$. Y $ad + ibc, bd \in \mathbb{Z}[i]$ por lo que $Frac(\mathbb{Z}[i]) = \mathbb{Q}[i]$.

(b) Para esta demostración se puede usar el primer teorema de isomorfismo, tomando el siguiente morfismo:

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[i]$$

$$a \mapsto a$$

$$x \mapsto i$$

Notamos que $(x^2+1) \subseteq \ker\varphi$, y que $\operatorname{Im}\varphi = \mathbb{Q}[i]$, por lo que nos queda demostrar la otra contención. Luego, sea $p \in \ker\varphi \setminus \{0\}$.

$$\implies \varphi(p) = 0$$

$$p = \sum_{j=0}^{n} a_j x^j$$

$$\therefore \varphi(p) = \sum_{j=0}^{n} \varphi(a_j)\varphi(x)^j$$

$$\varphi(p) = \sum_{j=0}^{n} a_j i^j = 0$$

Si n es par (en caso de n impar es análogo):

$$\implies \sum_{j=0}^{n/2} a_{2j} i^{2j} = 0$$

$$\implies \sum_{j=1}^{n/2} a_{2j-1} i^{2j-1} = 0$$

$$\therefore p(x) = q(x) + r(x)$$

Donde q tiene los coeficientes pares y r tiene los coeficientes impares de p.

$$\implies r(i) = q(i) = 0$$

$$\implies x^2+1 \mid r, x^2+1 \mid q$$

$$\implies x^2+1 \mid p$$

$$\implies p \in (x^2+1)$$

Por lo que $(x^2+1) = \ker\varphi$, lo que implica que $\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}[i]$ por el primer teorema de isomorfismo.

(c) De la misma forma que en la demostración anterior $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$.

(d) Recordamos de Algebra Abstracta I, que $\mathbb{Z}[i]$ es un dominio Euclideano[1], por lo que ademas es DIP. Dado esto pasan dos cosas, primero $I = (a)$ para algún $a \in \mathbb{Z}[i]$, mas específicamente todo ideal maximal es un ideal primo, y segundo hay una norma definida en $\mathbb{Z}[i]$ la cual llamaremos N este también es aplicable sobre $\mathbb{Z}[i]$.

$$\therefore \mathbb{Z}[i]/I = \mathbb{Z}[i]/(p)$$

Donde p es primo de Gauss que genera el ideal I. Luego usando el algoritmo de la division notamos la norma de los restos de la division es siempre menor a la norma del divisor y que la norma de cualquier elemento siempre es mayor o igual a 0. Esto nos lleva a notar que hay cantidad finita de elementos en $\mathbb{Z}[i]$ tal que su norma sea menor a la de p, ya que el subconjunto de . Por ende $\mathbb{Z}[i]/I$ es finito.

$\square$

Referencias

[1] M. Artin. *Algebra.* Pearson Prentice Hall, 1991.