Tarea IV

Nicholas Mc-Donnell

2do semestre 2017

Índice

1. Definiciones de un Anillo

3

Let $\alpha = \frac{1}{2}i$. Prove that the elements of $\mathbb{Z}[\alpha]$ form a dense subset of the complex plane.

Demostración. Recordemos que $a \in \mathbb{Z}[\alpha] \implies a = \sum_{i=0}^{n} a_i\alpha^i \quad a_i \in \mathbb{Z}$. Notemos que los siguientes elementos pertenecen a $\mathbb{Z}[\alpha]$

$$\frac{1}{2^n} \text{ y } \frac{1}{2^n}i$$

Estos elementos se construyen de la siguiente forma:

$$k = \left\lfloor \frac{n}{4} \right\rfloor + 1$$

$$\therefore \frac{1}{2^{4k}} = \alpha^{4k}$$

Luego $n = 4k - l, 1 \leq l \leq 4$

$$\implies \frac{1}{2^n} = \frac{1}{2^{4k}} \cdot 2^l$$

Similarmente:

$$\frac{1}{2^n}i = \frac{1}{2^{4k+1}}i \cdot 2^{l+1}$$

Por lo que:

$$\mathbb{Z}[\alpha] = \{a + bi : a, b \in \mathbb{Z}[1/2]\}$$

Recordemos que $\mathbb{Z}[\frac{1}{2}]$ es denso en $\mathbb{R}$, por lo que $\mathbb{Z}[\alpha]$ es denso en $\mathbb{C}$.

□

5

Prove that for all integers n, $\cos(2\pi/n)$ is an algebraic number.

Demostración. Consideremos el siguiente polinomio en $\mathbb{Z}[x]$:

$$x^n - 1$$

Notamos que tiene la siguiente raíz:

$$\cos(2\pi/n) + i\sin(2\pi/n)$$

Por lo que también tiene la siguiente raíz:

$$\cos(2\pi/n) - i\sin(2\pi/n)$$

Sabemos que la suma de dos números algebraicos es un número algebraico.

$$\implies 2\cos(2\pi/n) \text{ es algebraico}$$

Por lo que $\cos(2\pi/n)$ es algebraico □

11

Describe the group of units in each ring.

(a) $\mathbb{Z}/12\mathbb{Z}$

(b) $\mathbb{Z}/7\mathbb{Z}$

(c) $\mathbb{Z}/8\mathbb{Z}$

(d) $\mathbb{Z}/n\mathbb{Z}$

Demostración. Recordamos que por Intro a Algebra en $\mathbb{Z}/n\mathbb{Z}$ los únicos elementos con inverso multiplicativo son los que son coprimos a n. □

(a) $\{1, 5, 7, 11\}$

(b) $\{1, 2, 3, 4, 5, 6\}$

(c) $\{1, 3, 5, 7\}$

(d) $\{a \in \mathbb{Z} : 0 \leq a < n, \text{mcd}(a, n) = 1\}$

13

An element x of a ring R is called *nilpotent* if some power of x is zero. Prove that if x is nilpotent, then $1 + x$ is a unit in R.

Demostración. Notamos que es suficiente construir el inverso:

$$a = \sum_{i=0}^{n-1} (-1)^i x^i$$

Donde $x^n = 0$, notemos lo siguiente:

$$a \cdot (1 + x) = a + ax$$

$$a \cdot (1 + x) = \sum_{i=0}^{n-1} (-1)^i x^i + \sum_{i=0}^{n-1} (-1)^i x^{i+1} = 1 + x^n + \sum_{i=1}^{n-1} (-1)^i x^i + (-1)^{i-1} x^i$$

Por lo que:

$$a \cdot (1 + x) = 1 + x^n = 1$$ □

14

Prove that the product set $R \times R'$ of two rings is a ring with component-wise addition and multiplication:

$$(a, a') + (b, b') = (a + b, a' + b') \text{ and } (a, a')(b, b') = (ab, a'b')$$

Demostración. Primero recordemos que el producto de grupos es un grupo, por lo que $R^+ \times R'^+$ es un grupo con la suma. Luego veamos las propiedades de la multiplicación.

$$(a, a'), (b, b'), (c, c') \in R \times R'$$

$$\therefore ((a, a')(b, b'))(c, c') = (ab, a'b')(c, c')$$

$$((a, a')(b, b'))(c, c') = (abc, a'b'c')$$

$$((a, a')(b, b'))(c, c') = (a, a')(bc, b'c')$$

$$\implies ((a, a')(b, b'))(c, c') = (a, a')((b, b')(c, c'))$$

Por lo que es asociativa.

$$(1_R, 1_{R'}) \in R \times R'$$

$$(1_R, 1_{R'})(a, a') = (1_R a, 1_{R'} a') = (a, a')$$

$$(a, a')(1_R, 1_{R'}) = (a 1_R, a' 1_{R'}) = (a, a')$$

$$\implies (1_R, 1_{R'}) = 1_{R \times R'}$$

Por lo tiene una identidad. Ahora, veamos la distributividad.

$$(a, a'), (b, b'), (c, c') \in R \times R'$$

$$\big((a, a') + (b, b')\big)(c, c') = (a + b, a' + b')(c, c')$$

$$\big((a, a') + (b, b')\big)(c, c') = (ac + bc, a'c' + b'c')$$

$$\big((a, a') + (b, b')\big)(c, c') = (ac, a'c') + (bc, b'c')$$

Similarmente:

$$(c, c')\big((a, a') + (b, b')\big) = (ca, c'a') + (cb, c'b')$$

Por lo que se cumple la distributividad. Lo que concluye esta demostración. □

2. Construcción formal de los enteros y los polinomios

7

Prove that the units of the polynomial ring $\mathbb{R}[x]$ are the nonzero constant polynomials.

Demostración. Recordemos que una unidad es un elemento a de un anillo R, tal que existe b que cumple $ab = ba = 1_R$. Para el caso de $\mathbb{R}[x]$ estos elementos serian:

$$a, b \in \mathbb{R}[x] : ab = ba = 1_{\mathbb{R}[x]}$$

Sabemos que para todo elemento en $\mathbb{R}[x]$ su grado es mayor igual a 0, y específicamente las constantes son de grado 0.

$$\implies gr(a) + gr(b) = 0$$

Por lo mencionado anteriormente

$$gr(a) = gr(b) = 0$$

Luego notamos que:

$$\{a \in \mathbb{R}[x] : gr(a) = o\} = \mathbb{R}$$

Sabemos que todos los números reales, excepto el cero, tienen inverso. Por lo que los únicas unidades de $\mathbb{R}[x]$ son las constantes no cero. □

3. Homomorfismos e Ideales

1

Show that the inverse of a ring isomorphism $\varphi : R \to R'$ is an isomorphism.

Demostración. Sean $\varphi(a) = a', \varphi(b) = b'$ donde $a, b \in R$

$$a' + b' = \varphi(a) + \varphi(b) = \varphi(a + b)$$

$$\therefore \varphi^{-1}(a' + b') = a + b = \varphi^{-1}(a') + \varphi^{-1}(b')$$

También:

$$a' \cdot b' = \varphi(a) \cdot \varphi(b) = \varphi(a \cdot b)$$

$$\therefore \varphi^{-1}(a' \cdot b') = a \cdot b = \varphi^{-1}(a') \cdot \varphi^{-1}(b')$$

Y por último:

$$\varphi(1_R) = 1_{R'} \implies \varphi^{-1}(1_{R'}) = 1_R$$

Por lo que φ^{-1} es un isomorfismo. □

7

Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.

Demostración. Sea $n = a + bi$ con $a, b \in \mathbb{Z}$ y $n \in I$

$$\therefore \bar{n} = a - bi$$

Entonces tomamos lo siguiente:

$$\bar{n}n = (a - bi)(a + bi) = a^2 + b^2 \in \mathbb{Z} \wedge a^2 + b^2 \in I$$

Por lo que todo ideal no cero contiene un entero no cero. $\square$

10

Describe the kernel of the homomorphism $\varphi : \mathbb{C}[x, y, z] \to \mathbb{C}[t]$ defined by $\varphi(x) = t, \varphi(y) = t^2, \varphi(z) = t^3$.

Demostración.

$$\ker \varphi = \{\alpha \in \mathbb{C}[x, y, z] : \varphi(\alpha) = 0\}$$

Luego

$$\varphi(x^2 - y) = \varphi(x)^2 - \varphi(y) = t^2 - t^2 = 0$$

$$\varphi(x^3 - z) = \varphi(x)^3 - \varphi(z) = t^3 - t^3 = 0$$

$$\varphi(y^3 - z^2) = \varphi(y)^3 - \varphi(z)^2 = t^6 - t^6 = 0$$

Mas generalmente, $\forall a, b, c \in \mathbb{C}[x, y, z]$ y $n, k, m \in \mathbb{N}$

$$\varphi(a(x^{2n} - y^n) + b(x^{3k} - z^k) + c(y^{3m} - z^{2m})) = 0$$

Ya que:

$$\varphi(a(x^{2n}-y^n)+b(x^{3k}-z^k)+c(y^{3m}-z^{2m})) = \varphi(a)(\varphi(x^2)^n-\varphi(y)^n)+\varphi(b)(\varphi(x^3)^k-\varphi(z)^k)+\varphi(c)(\varphi(y^3)^m-\varphi(z^2)^m)$$

$$\varphi(a(x^{2n} - y^n) + b(x^{3k} - z^k) + c(y^{3m} - z^{2m})) = \varphi(a)(t^{2n} - t^{2n}) + \varphi(b)(t^{3k} - t^{3k}) + \varphi(t^{6m} - t^{6m})$$

$$\implies \varphi(a(x^{2n} - y^n) + b(x^{3k} - z^k) + c(y^{3m} - z^{2m})) = 0$$

Por lo que el kernel de φ son los elementos de la siguiente forma:

$$a(x^{2n} - y^n) + b(x^{3k} - z^k) + c(y^{3m} - z^{2m}) \quad a, b, c \in \mathbb{C}[x, y, z] \quad k, m, n \in \mathbb{N}$$ $\square$

19

Let R be a ring of characteristic p. Prove that the map $R \to R$ defined by $x \mapsto x^p$ is a ring homomorphism. This map is called the *Frobenius homomorphism.*

Demostración. Denotaremos φ a la función.

$$\varphi(1_R) = 1_R^p = 1_R$$

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

$$\varphi(a+b) = (a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n}$$

Notamos que p primo $\implies \forall 1 < n < p : n \nmid p$. Por lo que

$$(a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$$

Por lo que es un homomorfismo. $\square$

23

Let R be a ring of characteristic p. Prove that if a is nilpotent then $1+a$ is *unipotent*, that is, some power of $1+a$ is equal to 1.

Demostración. Sea $a^k = 0$, tomamos N tal que es múltiplo de $(k-1)!p$.

$$\implies (1+a)^N = \sum_{i=0}^{N} \binom{N}{i} a^i = \sum_{i=0}^{k-1} \binom{N}{i} a^i$$

$$\therefore \binom{N}{i} = \frac{N!}{(N-i)!i!} = \frac{N(N-1)(N-2)...(N-i-1)}{i!}$$

Sabemos que $p \mid N$, y que $\forall i < k-1 : i! \mid (k-1)!$

$$\implies (1+a)^N = 1$$

$\square$

33

Prove or disprove. If $a^2 = a$ for all a in a ring R, then R has characteristic 2

Demostración. Sea $a \in R \setminus \{0\}$ (Se asume que R tiene mas de un elemento), y se toma el homomorfismo de $\mathbb{Z}$ a R.

$$\therefore a^2 = a$$

$$a^2 - a = 0$$

$$a(a-1) = 0$$

$$\varphi(n(n-1)) = 0$$

Tomamos $n-1$

$$\varphi((n-1)(n-2)) = 0$$

$$\therefore \varphi(n^2-n) - \varphi(n^2-3n+2) = 0$$

$$\varphi(2n-2) = 0$$

$$\varphi(2)\varphi(n-1) = 0$$

Tomamos $n = 2$

$$\varphi(2)\varphi(1) = 0 \implies \varphi(2) = 0$$

Esto implica que R tiene característica 2. $\square$

4. Anillos cocientes y relaciones en Anillos

3

Describe each of the following rings

(a) $\mathbb{Z}[x]/(x^2-3, 2x+4)$

(b) $\mathbb{Z}[i]/(2+i)$

(a) *Demostración.* Queremos probar que $\mathbb{Z}[x]/(x^2-3, 2x+4) \simeq \mathbb{F}_2[\sqrt{3}]$. Para esto vamos a operar dentro del anillo:

$$2x+4 \equiv 0$$

$$2(x+2) \equiv 0$$

$$2(x+2)(x-2) \equiv 0$$

$$2(x^2-4) \equiv 0$$

$$\therefore -2 \equiv 0$$

Lo que es equivalente a: $2 \equiv 0$. También vemos lo siguiente:

$$x^2 - 3 \equiv 0$$

$$\therefore x \equiv \sqrt{3}$$

Por lo visto

$$\implies \mathbb{Z}[x]/(x^2-3, 2x+4) \simeq \mathbb{F}_2[\sqrt{3}]$$

Que es lo que queríamos. $\square$

(b) *Demostración.* Queremos probar que $\mathbb{Z}[i]/(2+i) \simeq \mathbb{Z}/5\mathbb{Z}$, para esto usaremos el primer teorema de isomorfismo.

$$\varphi : \mathbb{Z} \to \bar{R}$$

Queremos que:

$$\ker \varphi = 5\mathbb{Z}$$

Y que:

$$\operatorname{Im} \varphi = \bar{R}$$

Primero notamos que en $\bar{R}$:

$$-2 = i$$

Por lo que el resto de $a + bi$ es el mismo que el de $a - 2b$. Lo que implica que $\operatorname{Im} \varphi = \bar{R}$. Tomemos un elemento $n \in \ker \varphi$.

$$n = (a + bi)(2 + i)$$

$$n = (2a - b) + i(2b + a)$$

Como n es un entero $-2b = a$

$$n = -5b$$

O sea:

$$n \in 5\mathbb{Z}$$

Ahora notamos que $5 = (2 + i)(2 - i)$, por lo que $5 \in \ker \varphi$

$$\implies \ker \varphi = 5\mathbb{Z}$$

Por lo que $\mathbb{Z}[i]/(2 + i) \simeq \mathbb{Z}/5\mathbb{Z}$. $\square$

7

Let I, J be ideals of a ring R such that $I + J = R$

(a) Prove that $IJ = I \cap J$.

(b) Prove the *Chinese Remainder Theorem:* for any pair a, b of elements of R, there is an element x such that $x \equiv a \pmod{I}$ and $x \equiv b \pmod{J}$. [The notation $x \equiv a \pmod{I}$ means that $x - a \in I$]

(a) *Demostración.* $\underline{\subseteq |}$

$$a \in IJ \implies a = rsn = srn \quad r \in I, s \in J, n \in R$$

$$\therefore a \in I \cap J$$

$\underline{\supseteq |}$ Para esto necesitamos ver que la suma de elementos en IJ esta en IJ.

$$n \in IJ \iff n = \sum_i \lambda_i I_i J_i \quad I_i \in I, J_i \in J$$

Luego sean $a, b \in IJ$

$$a = \sum_i \lambda_i I_i J_i$$

$$b = \sum_j \lambda'_j I_j J_j$$

$$a + b = \sum_i \lambda_i I_i J_i + \sum_j \lambda'_j I_j J_j = \sum_k \lambda''_k I_k J_k$$

$$\implies a + b \in IJ$$

Ahora, sea $x \in I \cap J$ y sea $1_R = r + s$ tal que $r \in I, s \in J$

$$\therefore x = x \cdot 1_R = x \cdot (r + s) = xr + xs$$

$$xr, xs \in IJ$$

$$\implies xr + xs \in IJ \implies x \in IJ$$

Por lo que $IJ = I \cap J$ $\square$

(b) *Demostración.* Sean $r + s = 1_R$ y $r \in I, s \in J$, definimos x de la siguiente manera:

$$x = ar + bs$$

$$\therefore x = ar + b - br$$

$$x - b = (a - b)r \in I$$

Similarmente:

$$x - a = (b - a)s \in J$$

$$\implies x \equiv b \mod I \wedge x \equiv a \mod J$$

Por lo que existe un x que cumple lo pedidos $\square$