

Tarea VI

Nicholas Mc-Donnell

2do semestre 2017

Índice

2. Dominios de factorización única, Dominios de Ideales Principales y Dominios Euclidianos	3
1	3
3	3
9	3
13	5
3. Lema de Gauss	6
1	6
3	6
9	6
4. Factorización explícita de polinomios	6
1	6
3	6
7	6

2. Dominios de factorización única, Dominios de Ideales Principales y Dominios Euclidianos

1

Prove or disprove the following.

- (a) The polynomial ring $\mathbb{R}[x, y]$ in two variables is a Euclidean domain.
- (b) The ring $\mathbb{Z}[x]$ is a principal ideal domain.

Demostración.

- (a) Tomamos el ideal (x, y) y notamos que no es un ideal principal, por lo que concluimos que $\mathbb{R}[x, y]$ no es un dominio Euclidiano.
- (b) Recordamos que si un anillo R es DIP, entonces $R/(a)$ es un cuerpo, si tomamos $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ vemos que no es cuerpo, por lo que $\mathbb{Z}[x]$ no es DIP.

□

3

Give an example showing that division with remainder need not be unique in a Euclidean domain.

Demostración. Tomamos los enteros de Gauss con los siguientes elementos: $b/a = x, b = 1 + i, a = 2$

$$2 * 0 + 1 + i = 1 + i$$

$$2 * 1 - 1 + i = 1 + i$$

$$\sigma(1 + i) = \sigma(1 - i)$$

Por lo que no necesariamente es única.

□

9

- (a) Prove that $2, 3, 1 \pm \sqrt{-5}$ are irreducible elements of the ring $R = \mathbb{Z}[\sqrt{-5}]$ and that the units of this ring are ± 1 .
- (b) Prove that the existence of factorization is true for this ring.
- (a) *Demostración.* Comenzamos por demostrar que las únicas unidades de este anillo son ± 1 . Asumiremos que existe alguna unidad u .

$$\therefore (u) = (1)$$

$$\implies \exists r \in R : ur = 1$$

Notamos que $\bar{u}\bar{r} = 1$. ($\overline{a + b\sqrt{-5}} = a - b\sqrt{-5}$)

$$\implies (u\bar{u}) = (1)$$

$$u\bar{u} \in \mathbb{Z}^+$$

$$\therefore u\bar{u} = 1 \vee u\bar{u} > 1$$

Si $u\bar{u} > 1$

$$(u\bar{u})^2 > u\bar{u}$$

$$\implies (u\bar{u}) \neq (1)$$

$$\implies (u) \neq (1)$$

$$\rightarrow \leftarrow$$

Si $u\bar{u} = 1$, con $u = a + b\sqrt{-5}$.

$$u\bar{u} = a^2 + 5b^2 = 1$$

$$\implies b = 0 \quad a^2 = 1$$

$$\implies u = \pm 1$$

Que es lo que queríamos demostrar. Para demostrar la irreductibilidad de $2, 3, 1 \pm \sqrt{-5}$ definiremos una función $\sigma : R \setminus \{0\} \rightarrow \mathbb{Z}$.

$$\sigma(a + b\sqrt{-5}) = a^2 + 5b^2$$

Sean $u, v \in R$

$$\sigma(uv) = \sigma((a + b\sqrt{-5})(c + d\sqrt{-5})) = \sigma(ac - 5bd + (ad + bc)\sqrt{-5}) = (ac - 5bd)^2 + 5(ad + bc)^2$$

$$\sigma(u)\sigma(v) = (a^2 + 5b^2)(c^2 + 5d^2) = a^2c^2 + 25b^2d^2 + 5b^2c^2 + 5a^2d^2$$

$$\sigma(u)\sigma(v) = a^2c^2 + 25b^2d^2 + 5b^2c^2 + 5a^2d^2 + 10abcd - 10abcd = (ac - 5bd)^2 + 5(ad + bc)^2$$

$$\implies \sigma(uv) = \sigma(u)\sigma(v)$$

Notamos que $u \in R$ unidad $\iff \sigma(u) = 1$, sean $a, b \in R : a \mid b$.

$$\therefore b = ar \quad r \in R$$

$$\implies \sigma(b) = \sigma(a)\sigma(r)$$

$$\implies \sigma(a) \mid \sigma(b)$$

Asumamos que $2, 3, 1 \pm \sqrt{-5}$ no son irreducibles.

$$\therefore \exists a \in R : a \mid 2$$

$$\implies \sigma(a) \mid \sigma(2)$$

$$\sigma(a) \mid 4$$

Pero notamos que el único divisor no trivial es 2, pero $\forall x \in R : \sigma(x) \neq 2$. Similarmente $\forall x \in R : \sigma(x) \neq 3$, vemos que $\sigma(3) = 9, \sigma(1 \pm \sqrt{-5}) = -4$, por lo que $\nexists x \in R \setminus \{1, 2\} : \sigma(x) \mid \sigma(2)$, y análogamente se ven los otros casos, pero esto es una contradicción. Por lo que $2, 3, 1 \pm \sqrt{-5}$ son irreducibles. \square

(b) *Demostración.* Para simplificar la demostración, sin perder generalidad, no se tomara los asociados en cuenta.

Sean $a, b \in R : a \mid b$, y sea σ la función definida anteriormente.

$$\therefore \sigma(a) \mid \sigma(b)$$

Sabemos que $1 < \sigma(a) < \sigma(b)$ o $\sigma(a) = \sigma(b)$, lo segundo implica que son elementos asociados, por lo que no es un caso a considerar. El primero se divide en dos casos, a irreducible, o $\exists c \in R : c \mid a$, por lo mismo que antes:

$$1 < \sigma(c) < \sigma(a)$$

Entonces notamos que b solo puede tener finitos divisores (sin considerar unidades y elementos asociados), ya que la secuencia de divisores $\sigma(a_n)$ es estrictamente decreciente, pero es mayor a 1. \square

13

If a, b are integers and if a divides b in the ring of Gauss integers, then a divides b in \mathbb{Z}

Demostración. Usando $\sigma : \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{Z}$ tal que:

$$\sigma(a + bi) = a^2 + b^2$$

La cual sabemos que cumple lo mismo que la función denotada en el ejercicio anterior. Ahora, sean $a, b \in R : a \mid b$ enteros.

$$\therefore \sigma(a) \mid \sigma(b)$$

$$\sigma(a) = a^2, \sigma(b) = b^2$$

$$\implies a^2 \mid b^2$$

$$\implies a \mid b$$

Que es lo que queríamos demostrar. □

3. Lema de Gauss

1

Let a, b be elements of a field F , with $a \neq 0$. Prove that the polynomial $f(x) \in F[x]$ is irreducible if and only if $f(ax + b)$ is irreducible.

3

Let f be an irreducible polynomial in $\mathbb{C}[x, y]$, and let g be another polynomial. Prove that if the variety of zeros of g in \mathbb{C}^2 contains the variety of zeros of f , then f divides g .

9

Prove that the kernel of the homomorphism $\mathbb{Z}[x] \rightarrow \mathbb{R}$ sending $x \mapsto 1 + \sqrt{2}$ is a principal ideal, and find a generator for this ideal.

4. Factorización explícita de polinomios

1

Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$.

(a) $x^2 + 27x + 213$

(b) $x^3 + 6x + 12$

(c) $8x^3 - 6x + 1$

(d) $x^3 + 6x^2 + 7$

(e) $x^5 - 3x^4 + 3$

3

Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$, when $p = 2, 3, 5$.

7

Factor the following polynomials into irreducible factors in $\mathbb{Q}[x]$.

(a) $x^3 - 3x - 2$

(b) $x^3 - 3x + 2$

(c) $x^9 - 6x^6 + 9x^3 - 3$