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 7

4. Factorización explicita de polinomios **7**

1 7

3 9

7 10

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 $\sigma : R \setminus \{0\} \to \mathbb{Z}$.

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

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 $\forall x \in R : \sigma(r) \neq 2$. 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. □

(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. □

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 $\sigma : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{Z}$ 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. $\square$

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.

Demostración. Se demostrará que $f(x)$ no es irreducible, si solo si $f(ax+b)$ no es irreducible.
$\implies$
Sea $f(x) = g(x)h(x)$ con $g, h \in F[x]$. Luego:

$$f(ax+b) = g(ax+b)h(ax+b)$$

Por clausura multiplicativa y aditiva. Y ya que $a \neq 0$.

$$g(ax+b), h(ax+b) \in F[x]$$

Entonces $f(ax+b)$ no es irreducible en $F(x)$
$\impliedby$
Sea $f(ax+b) = g(x)h(x)$ con $g, h \in F[x]$

$$u = ax+b, \quad x = \frac{u-b}{a}$$

$$\therefore f(u) = g\left(\frac{u-b}{a}\right) h\left(\frac{u-b}{a}\right)$$

Renombrando variables:

$$f(x) = g\left(\frac{x-b}{a}\right) h\left(\frac{x-b}{a}\right)$$

Sabemos que por clausura $g\left(\frac{x-b}{a}\right), h\left(\frac{x-b}{a}\right) \in F[x]$, por lo que $f(x)$ no es irreducible. $\square$

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 $\mathbb{Z}[x] \to \mathbb{R}$ sending $x \mapsto 1 + \sqrt{2}$ is a principal ideal, and find a generator for this ideal.

Demostración. Sea φ este homomorfismo.

$$\ker \varphi = \{p \in \mathbb{Z}[x] : \varphi(p) = 0\}$$

Luego tomamos el siguiente elemento:

$$-x^2 + 2x + 1$$

Notamos que $\varphi(-x^2 + 2x + 1) = 0$, por lo que este elemento pertenece al kernel de φ. Sea I el ideal generado por este elemento. Asumamos que existe un ideal tal que $J = \ker \varphi$ y $J \neq I$. Luego, sabemos que $I \subset J$.

$$p \in J \implies p(1 + \sqrt{2}) = 0$$

$$\therefore p(x) = \sum_{i=0}^{gr(p)} \alpha_i x^i$$

$$\implies \sum_{i=0}^{gr(p)} \alpha_i (1 + \sqrt{2})^i = 0$$

$$p(1 + \sqrt{2}) = \sum_{2i \leq gr(p)} \alpha_{2i} (3 + 2\sqrt{2})^i + (1 + \sqrt{2}) \cdot \sum_{2i+1 \leq gr(p)} \alpha_{2i+1} (3 + 2\sqrt{2})^i$$

□

4. Factorización explicita 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) $x^5 - 3x^4 + 3$

Por comodidad, se denotaran los polinomios como p.

(a) *Demostración.* Si p no es irreducible, entonces $p = qr$ con $q, r \in \mathbb{Q}[x]$ y $gr(q) = gr(r) = 1$, estos polinomios solo tienen una raíz cada uno. Ahora por Teo de raíces racionales, las raíces de p, q, son de la forma b/a con $gcd(a, b) = 1$ y $a \mid 1, b \mid 213$.

$$\implies a = \pm 1 \wedge (b = \pm 1 \vee b = \pm 3 \vee b = \pm 71 \vee b = \pm 213)$$

Notamos que si $x > 0$, $p(x) > 0$. Y que si $x_1 < x_2 < 0$ tal que $p(x_1) > p(x_2) \implies \forall x < x_1 : p(x) > p(x_1)$

$$p(-1) = 187$$

$$p(-3) = 141$$

$$p(-71) = 3337$$

Por lo que p es irreducible. □

(b) *Demostración.* Similarmente al ejercicio anterior, si p no es irreducible, entonces tiene un factor de grado 1. Sea b/a una posible raíz.

$$\implies a = \pm 1 \wedge (b = \pm 1 \vee b = \pm 2 \vee b = \pm 3 \vee b = \pm 4 \vee b = \pm 6 \vee b = \pm 8)$$

También similarmente al ejercicio anterior, si $x > 0 \implies p(x) > 0$. Y que si $x_1 < x_2 < 0$ tal que $p(x_1) > p(x_2) \implies \forall x < x_1 : p(x) > p(x_1)$. Ya que p es estrictamente creciente. $(3x^2 + 6 > 0 \quad \forall x)$.

$$p(-1) = 5$$

$$p(-2) = -8$$

$$p(-3) = -33$$

Por lo que p es irreducible. □

(c) *Demostración.* Al igual que el ejercicio anterior por Teorema de las raíces racionales, tomamos una raíz b/a.

$$\implies (a = \pm 1 \vee a = \pm 2 \vee a = \pm 4 \vee a = \pm 8) \wedge b = \pm 1$$

Notamos que p es estrictamente creciente para $x \in (-\infty, -\frac{1}{2}) \cup (\frac{1}{2}, \infty)$ y estrictamente decreciente en $(-\frac{1}{2}, \frac{1}{2})$

$$p\left(-\frac{1}{2}\right) = 3$$

$$p\left(\frac{1}{2}\right) = -1$$

$$p(1) = 3$$

$$p(-1) = -1$$

$$p\left(\frac{1}{4}\right) = -0{,}375$$

$$p\left(\frac{1}{8}\right) = 0{,}265625$$

Por lo que p es irreducible. $\square$

(d) *Demostración.* Continuando con lo que hemos hecho en los otros ejercicios, sea b/a una posible raíz racional de p.

$$a = \pm 1 \wedge (b = \pm 1 \vee b = \pm 7)$$

Notamos que p es estrictamente creciente en $(-\infty, -4) \cup (0, \infty)$, y estrictamente decreciente en $(-4, 0)$.

$$p(-1) = 12$$

$$p(-7) = -42$$

Por lo que p es irreducible. $\square$

(e) *Demostración.* Usando el criterio de Eisenstein, con $q = 3$.

$$3 \nmid 1$$

$$3 \mid 0$$

$$3 \mid 6$$

$$3 \mid 3$$

$$9 \nmid 3$$

Luego p es irreducible en $\mathbb{Q}[x]$ $\square$

3

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

Demostración. Sea $q(x) = x^3 + x + 1$

- $p = 2$

$$q(0) = 1$$

$$q(1) = 1$$

Por lo que q es irreducible.

- $p = 3$

$$q(x) = (x + 2)(x^2 + x + 2)$$

Sea $t(x) = x^2 + x + 2$

$$t(1) = 1$$

$$t(2) = 2$$

Por lo que q se factoriza como $t(x+2)$

- $p = 5$

$$q(1) = 3$$

$$q(2) = 1$$

$$q(3) = 1$$

$$q(4) = 4$$

Por lo que q es irreducible.

$\square$

7

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

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

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

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

Respuesta:

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

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

(c) Tomamos $p = 3$, y notamos que por el criterio de Eisenstein, $x^9 - 6x^6 + 9x^3 - 3$ es irreducible.