

Tarea V

Nicholas Mc-Donnell

2do semestre 2017

Índice

Capítulo 10	3
10.5	3
1	3
7	3
9	3
10.6 Dominio de Enteros y Cuerpos Fraccionarios	4
1	4
3	4
5	5
10.7 Ideales Máximos	6
1	6
3	6
7	7
10.8 Geometría Algebraica	7
1	7
5	8
7	9
Capítulo 11	9
11.1 Factorización de Enteros y Polinomios	9
3	9
5	10
8	11

Capítulo 10

10.5

1

Describe the ring obtained from \mathbb{Z} by adjoining an element α satisfying the two relations $2\alpha - 6 = 0$ and $\alpha - 10 = 0$

Demostración. Primero recordemos que $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(x - 10, 2x - 6)$, y con esto veremos algunas propiedades del anillo.

$$\begin{aligned}x &\equiv 10 & 2(x - 3) &\equiv 0 \\ \implies 10 &\equiv 3 & \implies 7 &\equiv 0\end{aligned}$$

Por lo que podemos ver que usando el primer teorema de isomorfismos, se concluye que $\mathbb{Z}[\alpha] \simeq \mathbb{Z}_7$ \square

7

Analyze the ring obtained from \mathbb{Z} by adjoining an element α which satisfies the pair of relations $\alpha^3 + \alpha^2 + 1 = 0$ and $\alpha^2 + \alpha = 0$

Demostración. Lo primero que notamos es que $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(x^3 + x^2 + 1, x^2 + x)$. Notamos que el ideal $(x^3 + x^2 + 1, x^2 + x)$ contiene el 1. Esto implica que $\mathbb{Z}[\alpha] \simeq \mathbb{Z}_0$ \square

9

Describe the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2

Demostración. Se sabe que adjuntar un inverso a un anillo es equivalente a cocientar de la siguiente forma:

$$R[a] = R[x]/(2x - 1)$$

Donde a es el inverso del elemento en cuestión. Para este caso en específico es el inverso de 2.

$$\implies \mathbb{Z}_{12}[a] = \mathbb{Z}_{12}[x]/(2x - 1)$$

Usando las propiedades del anillo:

$$12x \equiv 0$$

$$x \equiv a$$

$$\therefore 12a \equiv 0$$

Pero notamos lo siguiente:

$$12 = 6 \cdot 2 \implies 6 \equiv 0$$

Mas aun:

$$3 \equiv 0$$

Observamos que $2 \cdot 2 = 4 = 3 + 1 \equiv 1$

$$\implies 2 \equiv a$$

Esto nos lleva a que concluir $\mathbb{Z}_{12}[a] \simeq \mathbb{Z}_3$, usando el primer teorema de isomorfismos. \square

10.6 Dominio de Enteros y Cuerpos Fraccionarios

1

Prove that the subring of an integral domain is an integral domain.

Demostración. Sea $R' \subset R$ anillo, y R dominio.

$$a, b \in R' : ab = 0$$

$$\therefore a, b \in R \implies (a = 0 \vee b = 0)$$

Lo que implica que R' es dominio. \square

3

Let R be an integral domain. Prove that the polynomial ring $R[x]$ is an integral domain.

Demostración. Demostraremos esto por medio de inducción.

Sean $a, b \in R[x] : ab = 0$

$$\therefore a = \sum_{i=0}^n \alpha_i x^i \quad \forall i : \alpha_i \in R$$

$$\therefore b = \sum_{j=0}^k \beta_j x^j \quad \forall j : \beta_j \in R$$

Luego $\text{gr}(a) = n$, $\text{gr}(b) = k$.

Caso Base:

$$\underline{n = 0, k = 0}$$

$$a = \alpha_0, b = \beta_0$$

$$\implies \alpha_0 \beta_0 = 0$$

$$\alpha_0, \beta_0 \in R \implies \alpha_0 = 0 \vee \beta_0 = 0$$

Caso Inductivo sobre n :

$$\underline{n = l, k = 0}$$

$$\sum_{i=0}^l \alpha_i \beta_0 x^i = 0 \implies (\forall i \leq l : \alpha_i = 0 \vee \beta_0 = 0) \iff (a = 0 \vee b = 0)$$

$$\underline{n = l + 1, k = 0}$$

$$\sum_{i=0}^{l+1} \alpha_i \beta_0 x^i = \sum_{i=0}^l \alpha_i \beta_0 x^i + \alpha_{l+1} \beta_0 x^{l+1} = 0$$

Pero sabemos que lo primero implica $\forall i \leq l : \alpha_i = 0 \vee \beta_0 = 0$. Lo que nos deja con lo siguiente:

$$\alpha_{l+1} \beta_0 x^{l+1} = 0$$

$$\implies \alpha_{l+1} \beta_0 = 0$$

Recordamos que ambos coeficientes pertenecen a R , por lo que $\alpha_{l+1} = 0 \vee \beta_0 = 0$. Vemos que si $\beta_0 \neq 0 \implies \forall i \leq l + 1 : \alpha_i = 0$.

$$\implies \forall n : a \beta_0 = 0 \iff a = 0 \vee \beta_0 = 0$$

Caso Inductivo sobre k:

$$\underline{n = m, k = l}$$

$$ab = 0 \implies (\forall i \leq n : \alpha_i = 0 \vee \forall j \leq k : \beta_j = 0) \iff (a = 0 \vee b = 0)$$

$$\underline{n = m, k = l + 1}$$

$$\left(\sum_{i=0}^n \alpha_i x^i \right) \cdot \left(\sum_{j=0}^{l+1} \beta_j x^j \right) = \left(\sum_{i=0}^n \alpha_i x^i \right) \cdot \left(\sum_{j=0}^l \beta_j x^j \right) + \sum_{i=0}^n \alpha_i \beta_{l+1} x^{i+l+1} = 0$$

Sabemos que lo primero implica que $\forall i \leq n : \alpha_i = 0 \vee \forall j \leq l : \beta_j = 0$. Y notamos que lo segundo es un caso similar y equivalente a la inducción sobre n . También vemos que si $\beta_{l+1} \neq 0 \implies \forall i \leq n : \alpha_i = 0$.

$$\implies (\forall i \leq n : \alpha_i = 0 \vee \forall j \leq k : \beta_j = 0) \iff a = 0 \vee b = 0$$

Que es lo que queríamos demostrar. □

5

Is there an integral domain containing exactly 10 elements?

Demostración. Hay dos grupos de orden 10, el dihedral y \mathbb{Z}_{10} , notamos que solo \mathbb{Z}_{10} es un grupo

abeliano. Vemos los siguientes elementos de \mathbb{Z}_{10} :

$$2 \cdot 5 = 10 = 0$$

\implies No hay dominio de orden 10

□

10.7 Ideales Máximos

1

Prove that the maximal ideals of the ring of integers are the principal ideals generated by prime integers.

Demostración. Recordamos la definición de un ideal máximo: M es ideal máximo de $R \iff \nexists I \neq R : M \subset I$ con $M \neq R$.

Asumamos que existe un ideal máximo (I) que no es generado por un primo. Se sabe que todo ideal de \mathbb{Z} es principal:

$$a \in \mathbb{Z} : (a) = I$$

Pero, sabemos que a no es primo.

$$\therefore a = p_1^{\lambda_1} \cdot \dots \cdot p_n^{\lambda_n}$$

$$\therefore a \in (p_1)$$

$$\implies I \subset (p_1)$$

$$\rightarrow \leftarrow$$

Lo que concluye esta demostración.

□

3

Prove that the ideal $(x + y^2, y + x^2 + 2xy^2 + y^4)$ in $\mathbb{C}[x, y]$ is a maximal ideal

Demostración. En esta demostración primero se va a mostrar que el ideal dado es igual al ideal de (x, y) , después se usara el primer teorema de isomorfismo para ver que al cocientar por el ideal se genera un cuerpo.

\subseteq :

$$(x + y^2)(1 + y(x + y^2)) - y(y + x^2 + 2xy^2 + y^4) = x$$

$$(y + x^2 + 2xy^2 + y^4) - (x + y^2)^2 = y$$

$$\implies (x, y) \subseteq (x + y^2, y + x^2 + 2xy^2 + y^4)$$

La otra contención se puede ver trivialmente.

$$\implies (x + y^2, y + x^2 + 2xy^2 + y^4) = (x, y)$$

$$\therefore \mathbb{C}[x, y]/(x + y^2, y + x^2 + 2xy^2 + y^4) = \mathbb{C}[x, y]/(x, y)$$

Fácilmente se puede ver que $\mathbb{C}[x, y]/(x, y) \simeq \mathbb{C}$, por el primer teorema de isomorfismo. Por lo que $(x + y^2, y + x^2 + 2xy^2 + y^4)$ es un ideal máximo. \square

7

Prove that the ring $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a field, but that $\mathbb{F}_3[x]/(x^3 + x + 1)$ is not a field.

Demostración. Recordamos que R/I es un cuerpo ssi I es ideal máximo. Además que si F es cuerpo entonces, todo ideal en $F[x]$ es principal. Notamos que todo ideal $(g(x))$ es máximo ssi $g(x)$ es irreducible en $F[x]$.

$$p(x) = x^3 + x + 1$$

$$\therefore p(0) = 1, p(1) = 1$$

Por lo que $p(x)$ es irreducible en $\mathbb{F}_2[x]$.

Notamos que $x^3 + x + 1 \equiv (x + 2)(x^2 + x + 2)$ en \mathbb{F}_3 , por lo que $(x^3 + x + 1) \subset (x + 2)$. Lo que implica que $\mathbb{F}_3[x]/(x^3 + x + 1)$ no es cuerpo. \square

10.8 Geometría Algebraica

1

Determine the following points of intersection of two complex plane curves in each of the following:

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

(b) $x^2 + xy + y^2 = 1, x^2 + 2y^2 = 1$

(c) $y^2 = x^3, xy = 1$

(d) $x + y + y^2 = 0, x - y + y^2 = 0$

(e) $x + y^2 = 0, y + x^2 + 2xy^2 + y^4 = 0$

Demostración. (a) Tomamos $y = 1 - x$:

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

$$\implies 1 - 2x + x^2 - x^3 + x^2 = 1$$

$$-2x + 2x^2 - x^3 = 0$$

$$\therefore x(2 - 2x + x^2) = 0$$

Notamos que $x^2 - 2x + 2 = (x - (1 + i))(x - (1 - i))$

$$\implies x = 1 + i, x = 1 - i, x = 0$$

$$\implies \{(1 + i, -i), (1 - i, i), (0, 1)\} = \{(x, y) \in \mathbb{C}[x, y] : y^2 - x^3 + x^2 = 1, x + y = 1\}$$

(b) Restamos $x^2 + 2y^2 = 1$ de $x^2 + xy + y^2 = 1$

$$\therefore xy - y^2 = 0$$

$$\implies y(x - y) = 0$$

Notamos que no todo punto que cumple $x = y$ cumple $x^2 + 2y^2 = 1$, por lo que reemplazamos:

$$3y^2 = 1$$

$$\implies \{(\pm\sqrt{3}/3, \pm\sqrt{3}/3), (\pm 1, 0)\} = \{(x, y) \in \mathbb{C}[x, y] : x^2 + xy + y^2 = 1, x^2 + 2y^2 = 1\}$$

(c) Tomamos $y = 1/x$:

$$\therefore (1/x)^2 = x^3$$

$$\implies x^5 = 1$$

Por lo que los x son las raíces quintas de la unidad, y los y son sus inversos.

(d) Restamos $x - y + y^2 = 0$ de $x + y + y^2$:

$$\therefore 2y = 0$$

$$\implies y = 0$$

$$\implies \{(0, 0)\} = \{(x, y) \in \mathbb{C}[x, y] : x + y + y^2 = 0, x - y + y^2 = 0\}$$

(e) Tomamos $x = -y^2$:

$$\therefore y + (-y^2)^2 + 2(-y^2)y^2 + y^4 = 0$$

$$\implies y = 0$$

$$\implies \{(0, 0)\} = \{(x, y) \in \mathbb{C}[x, y] : x + y^2 = 0, y + x^2 + 2xy^2 + y^4 = 0\}$$

□

5

Let $f_1, \dots, f_r; g_1, \dots, g_r \in \mathbb{C}[x_1, \dots, x_n]$, and let U, V be the zeros of $\{f_1, \dots, f_r\}, \{g_1, \dots, g_s\}$ respectively. Prove that if U and V do not meet, then $(f_1, \dots, f_r; g_1, \dots, g_s)$ is the unit ideal.

Demostración. Si U y V no se encuentran, esto implica que $U \cap V = \emptyset$. Por lo que el sistema de ecuaciones $f_1 = \dots = f_r = g_1 = \dots = g_s = 0$ no tiene solución, por el corolario (8.5), existe una combinación lineal de estos polinomios que genera el 1, por lo que $1 \in (f_1, \dots, f_r; g_1, \dots, g_s) \implies (f_1, \dots, f_r; g_1, \dots, g_s) = (1)$ \square

7

Prove that the variety defined by a set $\{f_1, \dots, f_r\}$ of polynomials depends only on the ideal (f_1, \dots, f_r) that they generate.

Demostración. Sea $\{g_1, \dots, g_s\}$ un conjunto de polinomios tal que $(g_1, \dots, g_s) = (f_1, \dots, f_r)$. Sea V la variedad del conjunto $\{f_1, \dots, f_r\}$.

$$a \in V \implies f_1(a) = \dots = f_r(a) = 0$$

$$\therefore t \in (f_1, \dots, f_r) \implies t(a) = 0$$

Notamos que $\forall i : g_i \in (f_1, \dots, f_r)$

$$\implies g_i(a) = 0$$

$$\implies a \in U$$

Donde U es la variedad del conjunto $\{g_1, \dots, g_s\}$.

$$\implies V \subseteq U$$

Se puede hacer el mismo argumento en reversa, por lo que:

$$U = V$$

Esto implica que la variedad depende del ideal, no del conjunto de polinomios. \square

Capítulo 11

11.1 Factorización de Enteros y Polinomios

3

Prove that if d is the greatest common divisor of a_1, \dots, a_n then the greatest common divisor of $a_1/d, \dots, a_n/d$ is 1.

Demostración. Asumamos que el gcd de $a_1/d, \dots, a_n/d$ es k , donde $k \neq 1$

$$\therefore a_i/d = km_i \forall i$$

$$\begin{aligned} &\implies a_i = kdm_i \forall i \\ &\implies \gcd(a_1, \dots, a_n) = kd = d \\ &\rightarrow \leftarrow \end{aligned}$$

Esto finaliza la demostración. □

5

- (a) Let a, b be integers with $a \neq 0$, and write $b = aq + r$, where $0 \leq r \leq |a|$. Prove that the two greatest common divisors (a, b) and (a, r) are equal.
- (b) Describe an algorithm, based on (a), for computing the greatest common divisor.
- (c) Use your algorithm to compute the greatest common divisor of the following:
- (a) 1456, 235
- (b) 123456789, 135792468

- (a) *Demostración.* Sean e, f el gcd de a, b y de a, r respectivamente:

$$\begin{aligned} \therefore f \mid aq + r &\implies f \mid b \\ &\implies f \mid e \end{aligned}$$

Similarmente:

$$\begin{aligned} e \mid b - aq &\implies e \mid r \\ &\implies e \mid f \\ &\implies e = f \end{aligned} \quad \square$$

- (b) En base a lo visto uno puede ver que $\gcd(r_i, r_{i+1}) = \gcd(a, b)$ donde r_i es el resto de la division de r_{i-2} y r_{i-1} , $\forall i < q$, con $r_q = 0$. Por esto podemos ver un algoritmo donde se dividen repetidamente los restos, hasta que uno sea 0, y el resto anterior a ese es el gcd.

- (c) (a)

$$1456 : 235 = 6$$

Resto: 46

$$235 : 46 = 5$$

Resto: 5

$$46 : 5 = 9$$

Resto: 1

$$5 : 1 = 5$$

Resto: 0

$$\gcd(1456, 235) = 1$$

(b)

$$135792468 : 123456789 = 1$$

Resto: 12335679

$$123456789 : 12335679 = 10$$

Resto: 99999

$$12335679 : 99999 = 123$$

Resto: 35802

$$99999 : 35802 = 2$$

Resto: 28395

$$35802 : 28395 = 1$$

Resto: 7407

$$28395 : 7407 = 3$$

Resto: 6174

$$7407 : 6174 = 1$$

Resto: 1233

$$6174 : 1233 = 5$$

Resto: 9

$$1233 : 9 = 137$$

Resto: 0

$$\gcd(123456789, 135792468) = 9$$

8

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

(a) $x^3 + x + 1, p = 2$

(b) $x^2 - 3x - 3, p = 5$

(c) $x^2 + 1, p = 7$

(a) Sea $p(x) = x^3 + x + 1$

$$p(0) = 1, p(1) = 1$$

Por lo que $p(x)$ no tiene ceros, sabemos que x no divide a $p(x)$. Veamos si $x + 1$ divide a $p(x)$.

$$x^3 + x + 1 : x + 1 = x^2 - x + 2$$

Con resto -1

$$\implies x^3 + x + 1 = (x + 1)(x^2 - x + 2) - 1$$

En \mathbb{F}_2

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

Por lo que $x^3 + x + 1$ es irreducible.

(b) Sea $p(x) = x^2 - 3x - 3$

$$p(1) = -5$$

$$\implies p(1) \equiv 0$$

Vemos lo siguiente:

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

$$\therefore (x - 1)(x + 2) \equiv x^2 - 3x - 3$$

Los cuales claramente son irreducibles.

(c) Sea $p(x) = x^2 + 1$

$$p(7k) \equiv 1, p(7k + 1) \equiv 2, p(7k + 2) \equiv 5$$

$$p(7k + 3) \equiv 3, p(7k + 4) \equiv 3, p(7k + 5) \equiv 5$$

$$p(7k + 6) \equiv 2$$

Por lo que vemos que no tiene ceros, lo que nos lleva a concluir que $p(x)$ es irreducible.