Tarea V

Nicholas Mc-Donnell

2do semestre 2017

Índice

Capítulo 10

10.5

1

Describe the ring obtained from $\mathbb{Z}$ by adjoining an elementα 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.

$$x \equiv 10 \quad 2(x-3) \equiv 0$$

$$\implies 10 \equiv 3 \implies 7 \equiv 0$$

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

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 $\mathbb{Z}[\alpha] \simeq \mathbb{Z}_0$ □

9

Describe the ring obtained fro $\mathbb{Z}/12\mathbb{Z}$ 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 especifico 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 $a, b \in R[x] : ab = 0$

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

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

Luego $\text{gr}(a) = n$, gr(b)=k.
Caso Base:
$n = 0, k = 0$

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

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

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

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 $\beta_0 \neq 0 \implies \forall i \leq l + 1 : \alpha_i = 0$.

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

<u>Caso Inductivo sobre k:</u>
$\underline{n = m, k = l}$

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

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

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

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 una 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. $\square$

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 $\mathbb{Z}_{10}$:

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

$$\implies \text{No hay dominio de orden } 10 \qquad \square$$

10.7 Ideales Máximos

1

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

3

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

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.

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

5

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

7

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

Capítulo 11

11.1 Factorización de Enteros y Polinomios

3

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

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

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

$$\implies a_i = kdm_i \forall i$$

$$\implies gcd(a_1, ..., a_n) = kd = d$$

$$\rightarrow\leftarrow$$

Esto finaliza la demostración. $\square$

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 and 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

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