Respuestas a los problemas impares del capítulo 10

Anillos

10.1 Para ver que $\oplus$ es asociativa observemos que

$$(a \oplus b) \oplus c = a + b + c - 2 = a \oplus (b \oplus c).$$

Por otra parte $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$. Por lo tanto $\oplus$ es conmutativa. $a \oplus 1 = a + 1 - 1 = a$. Por lo tanto 1 es neutro aditivo. Si $a \oplus b = 1$ entonces $a + b - 1 = 1$, por lo tanto $b = 2 - a$ es el inverso aditivo de a. Para ver que $\odot$ es asociativa observemos que

$$(a \odot b) \odot c = (a + b + c) - (ab + ac + bc) + abc = a \odot (b \odot c).$$

Por otra parte $a \oplus b = a + b - ab = b + a - ba = b \oplus a$, por lo tanto $\odot$ es conmutativa. Además $a \odot 0 = a + 0 - a \cdot 0 = a$. Por lo tanto 0 es elemento unitario. La propiedad distributiva se cumple porque

$$a \odot (b \oplus c) = 2a + b + c - ab - ac - 1 = (a \odot b) \oplus (a \odot c).$$

Por lo tanto $(\mathbb{Z}, \oplus, \odot)$ es anillo conmutativo con elemento unitario. Por último, $a \odot b = 1$ implica que $a+b-ab = 1$ y de ahí que $b(1-a) = 1-a$. De modo que si $a \neq 1$ (es decir, si a no es el neutro aditivo) entonces $b = 1$ (es decir, b es el neutro aditivo). Por lo tanto $(\mathbb{Z}, \oplus, \odot)$ es dominio entero.

10.3 No es anillo porque no se cumple la propiedad distributiva, por ejemplo, $1 \odot (2 \odot 3) = 1 \odot (-2) = 1 - 2 + 3 = 2$, pero $(1 \odot 2) \oplus (1 \odot 3) = (-3) \oplus (-5) = -15$.

10.5 Por inducción. El paso inductivo es: $(ab)^{n+1} = (ab)^n(ab) = a^n b^b ab = (a^n a)(b^n b) = a^{n+1} b^{n+1}$.

10.7 Si $f : \mathbb{Z} \to A$ es un homomorfismo se debe cumplir que $f(1) = 0$, orque 0 es el neutro aditivo de A. También se debe cumplir que $f(2) = f(1 + 1) = f(1) \oplus f(1) = 0 \oplus 0 = 0 + 0 - 1 = -1$, $f(3) = f(2 + 1) = f(2) \oplus f(1) = -1 \oplus 0 = -1 + 0 - 1 = -2$. Esto sugiere definir $f(a) = -(a - 1) = 1 - a$. Observemos ahora que

$$f(a) \oplus f(b) = (1-a) \oplus (1-b) = (1-a)+(1-b)-1 = 1-a-b = f(a+b),$$

$f(a)\odot f(b) = (1-a)\odot(1-b) = (1-a)+(1-b)-(1-a)(1-b) = 1-ab = f(ab)$.

Por lo tanto f es un homomorfismo. Además

$$f(a) = f(b) \;\Rightarrow\; 1-a = 1-b \;\Rightarrow\; a = b,$$

por lo tanto f es inyectiva. Por último, si $c \in \mathbb{Z}$ entonces

$$f(1-c) = 1-(1-c) = c,$$

por lo tanto f es suprayectiva.

Campos

10.9 [13].

10.11 $ax = b \;\Rightarrow\; a^{-1}(ax) = a^{-1}b \;\Rightarrow\; x = a^{-1}b$.

10.13 $(a/b)/(c/d) = (ab^{-1})(cd^{-1})^{-1} = (ab^{-1})(c^{-1}d) = (ad)(bc)^{-1} = ad/bc$.

10.15 Para ver que $\oplus$ es asociativa obsérvese que

$$(a \oplus b) \oplus c = a+b+c+6 = a \oplus (b \oplus c).$$

Por otra parte $a \oplus b = a+b+3 = b+a+3 = b \oplus a$. Por lo tanto $\oplus$ es conmutativa. $a \oplus -3 = a+(-3)+3 = a$. Por lo tanto -3 es neutro aditivo. Si $a \oplus b = -3$ entonces $a+b+3 = -3$, por lo tanto $b = -a-6$ es el inverso aditivo de a. Para ver que $\odot$ es asociativa obsérvese que

$$(a \odot b) \odot c = (a+b+c) + (ab+ac+bc)/3 + abc/9 = a \odot (b \odot c).$$

Por otra parte $a \oplus b = a+b+ab/3 = b+a+ba/3 = b \oplus a$, por lo tanto $\odot$ es conmutativa. Además $a \odot 0 = a+0+a\cdot 0/3 = a$. Por lo tanto 0 es elemento unitario. La propiedad distributiva se cumple porque

$$a \odot (b \oplus c) = 2a+b+c+(ab+ac)/3+3 = (a \odot b) \oplus (a \odot c).$$

Por lo tanto $(\mathbb{Z}, \oplus, \odot)$ es anillo conmutativo con elemento unitario. Por último, $a \odot b = 0$ implica que $a+b+ab/3 = 0$ y de ahí que $(3+a)b = -3a$. De modo que si $a \neq -3$ (es decir, si a no es el neutro aditivo) entonces $b = -3a/(3+a)$ es el inverso multiplicativo de a. Por lo tanto $(\mathbb{Z}, \oplus, \odot)$ es un campo.

El anillo de polinomios

10.17 $a(x)+b(x)=1+5x+3x^2+6x^3,\ \ a(x)b(x)=1+5x+2x^2+5x^3+x^5.$

10.19 $-a(x)=6+9x+2x^2+4x^3+x^5.$

10.21 Sean $d(x)=a(x)b(x)$ y $e(x)=b(x)c(x)$. Por lo tanto el coeficiente de x^k en $[a(x)b(x)]c(x)$ es:

$$\sum_{j=0}^{k} d_j c_{k-j} = \sum_{j=0}^{k} \left(\sum_{i=0}^{j} a_i b_{j-i} \right) c_{k-j}.$$

Por otra parte, el coeficente de x^k en $a(x)[b(x)c(x)]$ es:

$$\sum_{j=0}^{k} a_j e_{k-j} = \sum_{j=0}^{k} e_j a_{k-j} = \sum_{j=0}^{k} \left(\sum_{i=0}^{j} b_i c_{j-i} \right) a_{k-j}.$$

Por lo tanto $[a(x)b(x)]c(x)=a(x)[b(x)c(x)]$.

10.23 Sea $f: D \to D[x]$ definida por $f(a)=a$, donde a es interpretado como un polinomio constante. Por lo tanto $f(a+b)=a+b=f(a)+f(b)$ y $f(ab)=ab=f(a)f(b)$, es decir, f es un homomorfismo del anillo D en el anillo $D[x]$. Además si $f(a)=f(b)$ entonces $a=b$. Por lo tanto f es inyectivo. De ahí que D está inmerso en $D[x]$.

10.25 Basta observar que si $1<k<p$ entonces $p|\binom{p}{k}$.

Divisibilidad

10.27 El cociente es $2x^2+x+1$ y el residuo es x^2-3x+1.

10.29

3	-1	2	5	3	4	$\underline{3}$
	9	24	78	249	756	
3	8	26	83	252	760	

Por lo tanto $q(x)=3x^4+8x^3+26x^2+83x+252$ y $r=760$.

10.31 $a(1)=3,\ a(2)=1,\ a(3)=4,\ a(4)=3$. Por lo tanto el polinomio no tiene raíces.

10.33 Si $n = 1$ entonces $a(x) = a_1x + a_0$ tiene exactamente una raíz: $x = -a_0a_1^{-1}$. Supongamos el resultado cierto para n. Sea $a(x)$ un polinomio de grado $n + 1$. Si $a(x)$ no tiene raíces el resultado se cumple. En otro caso sea r una raíz. Por lo tanto $a(x) = (x - r)q(x)$, donde el grado de $q(x)$ es n. Por hipótesis de inducción $q(x)$ tiene a lo más n raíces, por lo tanto $a(x)$ tiene a los más $n + 1$ raíces.

Máximo común divisor

10.35 El máximo común divisor es x^2+1, además $x^2+1 = a(x)-(x^2+1)b(x)$.

Polinomios irreducibles

10.37 Los polinomios irreducibles de grado menor o igual a 2 son:

$$x,\ x+1,\ x+2,\ x^2+x+2,\ x^2+2x+2,\ x^2+1.$$

10.39 La única raíz es 1, la cual es simple. Dividiendo $x^7 + x^6 + x^4 + 1$ entre $x + 1$ obtenemos:

$$x^7 + x^6 + x^4 + 1 = (x + 1)(x^6 + x^3 + x^2 + x + 1)$$

en $\mathbb{Z}_2[x]$.

Campos finitos

10.41 Basta ver que si $a(x) \equiv b(x) \pmod{p(x)}$ y $c(x) \equiv d(x) \pmod{p(x)}$, entonces $a(x) + c(x) \equiv b(x) + d(x) \pmod{p(x)}$ y $a(x)c(x) \equiv b(x)d(x) \pmod{p(x)}$.