Algebra Abstracta: Tarea #6

Jonathan Andrés Niño Cortés

5 de marzo de 2015

Sección 9.5 2. Para cada uno de los cuerpos construidos en el Ejercicio 6 de la Sección 4 exhiba un generador para el grupo multiplicativo (cíclico) de elementos diferentes a cero.

Demostración. Cada uno de estos grupos es cíclico por el teorema visto en clase.

(a) 9). El anillo $F_3[x]/(x^2+1)$ es un campo de orden 9, pues por un punto de la tarea anterior el polinomio x^2+1 es irreducible (ya que -1 no es residuo cuadrático módulo 3). Ahora vamos a demostrar que el polinomio $x+1$ es un generador de $(F_3(x)/(x^2+1))^*$. Para ello vamosa demostrar que $x+1$ tiene orden 8.

$$\begin{aligned}
(x+1)^2 &= x^2+2x+1 = 2x \\
(x+1)^4 &= 4x^2 = -1 \\
(x+1)^8 &= (-1)^2 = 1
\end{aligned}$$

(b) 49). Tome el anillo $F_7[x]/(x^2+1)$, que es un campo de orden 49. x^2+1 es de nuevo irreducible porque -1 no es residuo cuadrático módulo 7. El elemento $x+2$ es el generador del grupo de unidades, pues tiene orden 48.

$$\begin{aligned}
(x+2)^2 &= x^2+4x+4 = 4x+3 \\
(x+2)^3 &= (4x+3)(x+2) = 4x^2+11x+6 = 4x+2 \\
(x+2)^4 &= (4x+3)^2 = 16x^2+24x+9 = 3x \\
(x+2)^6 &= (4x+2)^2 = 16x^2+16x+4 = 2x+2 \\
(x+2)^8 &= (3x)^2 = 9x^2 = 5 \\
(x+2)^{12} &= 5*3x = x \\
(x+2)^{16} &= 5^2 = 25 = 4 \\
(x+2)^{24} &= x^2 = -1 \\
(x+2)^{48} &= (-1)^2 = 1
\end{aligned}$$

(c) 8). Tome el anillo $F_2[x]/(x^3 + x + 1)$ que es un campo porque el polinomio no tiene raices, pues evaluar tanto en 0 como en 1 da como resultado 1.

El grupo de unidades sería de orden 7. Como 7 es primo este grupo debe ser isomorfo a $\mathbb{Z}/7\mathbb{Z}$. Por lo tanto cualquier polinomio diferente a 1 es un generador de este grupo.

(d) 81). Tome el anillo $F_3[x]/(x^4 + x + 2)$. $x^4 + x + 2$ es irreducible. En primer lugar no tiene raices pues si evaluamos en 0 da 2, si evaluamos en 1 da 1 y si evaluamos en 2 da 2. Queda la posibilidad que el polinomio sea divisible por polinomios irreducibles de grado 2. Pero es fácil ver que los únicos polinomios irreducibles de grado 2 son $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$, $2x^2 + x + 1$, $2x^2 + 2x + 1$ y $2x^2 + 2$.

El elemento $x + 1$ es el generador del grupo multiplicativo cíclico $(F_3[x]/(x^4 + x + 2))^*$, para probar esto vamos a demostrar que $x + 1$ tiene grado 80. Observese que tenemos la identidad $x^4 = -x - 2$.

$$\begin{aligned}
(x+1)^2 &= x^2 + 2x + 1 \\
(x+1)^4 &= x^4 + 4x^3 + 6x^2 + 4x + 1 = x^3 + 2 \\
(x+1)^5 &= (x^3 + 2)(x + 1) = x^3 + x \\
(x+1)^8 &= (x^3 + 2)^2 = x^6 + 4x^3 + 4 = x^2 + 1 \\
(x+1)^{10} &= (x^3 + x)^2 = x^6 + 2x^4 + x^2 = 2x^3 + 2x^2 + x + 2 \\
(x+1)^{16} &= (x^2 + 1)^2 = x^4 + 2x^2 + 1 = 2x^2 + 2x + 2 \\
(x+1)^{20} &= (2x^3 + 2x^2 + x + 2)^2 = 2x^3 + 2x^2 + x \\
(x+1)^{40} &= (2x^3 + 2x^2 + x)^2 = 2 \\
(x+1)^{80} &= (2)^2 = 4 = 1
\end{aligned}$$

□

Sección 9.5 3. Sea p un primo impar en $\mathbb{Z}$ y sea n un entero positivo. Pruebe que $x^n - p$ es irreducible sobre $\mathbb{Z}[i]$.

Demostración. Tenemos dos casos. Si $p \equiv 3 \bmod 4$, entonces p es irreducible. Por lo tanto si tomamos el ideal generado por p, este ideal es primo y por el criterio de Eisenstein concluimos que $x^n - p$ es irreducible. Ahora si $p \equiv 1 \bmod 4$ entonces existen $a, b \in \mathbb{Z}$ tales que $p = (a + bi)(a - bi)$ y estos factores son irreducibles. Si tomamos el ideal primo $(a + bi)$ vemos que p pertenece a $(a + bi)$ pero no pertenece a $(a^2 + 2abi - b^2)$ porque esto contradeciria la factorización única de p. Luego por el criterio de Eisenstein concluimos que $x^n - p$ es irreducible. □

Sección 9.5 4. Pruebe que $x^3 + 12x^2 + 18x + 6$ es irreducible sobre $\mathbb{Z}[i]$.

Demostración. 3 es irreducible en $\mathbb{Z}[i]$ y por lo tanto su ideal es primo. Vemos que los coeficientes 12, 18 y 6 pertenecen a (3). Pero además, 6 no pertenece a (9) porque 6 tiene una norma más pequeña que 9. Luego por el criterio de Eisenstein concluimos que $x^3 + 12x^2 + 18x + 6$ es irreducible. □

Sección 9.5 7. Pruebe que los grupos aditivos y multiplicativos de un campo nunca son isomórficos.

Demostración. Considere 3 casos. Cuando el campo es finito claramente no son isomorfos porque si el orden del campo en n, el orden del grupo aditivo es n mientras que el orden del grupo multiplicativo es $n - 1$.

Ahora, si el campo es infinito y $-1 \neq 1$, entonces tenemos que -1 es de orden 2 en el grupo multiplicativo, pero en el grupo aditivo no hay ningun elemento de orden 2. Si lo hubiera este deberia ser tal que $x + x = 0$, ahora si multiplicamos por x^{-1} a lado y lado obtenemos que 1+1=0. Luego $1 = -1$ lo que contradice nuestra hipótesis.

Por otro lado, si $-1 = 1$ entonces eso quiere decir que 1 es su propio inverso aditivo. Si tomamos cualquier homomorfismo ϕ entre el grupo aditivo y el multiplicativo entonces $\phi(0) = 1$, pero además $\phi(1 + 1) = \phi(0) = 1$, por lo tanto $\phi(1)\phi(1) = 1$. Ahora las únicas soluciones de la ecuación $x^2 = 1$ son 1 o -1 pero como $-1 = 1$ concluimos que $\phi(1) = 1$ por lo que ningun homomorfismo puede ser inyectivo. □

Sección 10.1 8. Un elemento m de un R-módulo M se llama un elemento de torsión si $rm = 0$ para algún elemento no cero $r \in R$. El conjunto de los elementos de torsión se denota

$$\text{Tor}(M) = \{m \in M \mid rm = 0 \text{ para algún elemento no cero } r \in R\}.$$

(a) Pruebe que si R es un dominio integral entonces $\text{Tor}(M)$ es un submódulo de M (llamado el submódulo de torsión de M).

Demostración. Vamos a utilizar el criterio de submódulo. En primer lugar $\text{Tor}(M)$ no es vacío pues para cualquier $r \in R$ tenemos que $r * 0 = 0$, por lo que 0 es un elemento de torsión.

En segundo lugar tomemos $x + ry$ para cualquier $r \in R$ y cualesquiera $x, y \in N$ y veamos que pertenece a N. Por definición tenemos que existen $s, t \in R$ tales que $sx = 0$ y $ty = 0$, luego si multiplicamos por st tenemos que $(st)(x + ry) = stx + stry = t(sx) + sr(ty) = t0 + sr0 = 0$. Por lo que $x + ry \in N$. □

(b) De un ejemplo de un anillo R y un R-módulo M tal que $\text{Tor}(M)$ no es un submódulo.

Demostración. Tome por ejemplo el anillo que no es un dominio integral $\mathbb{Z}/6\mathbb{Z}$, si tomamos a R como un R-m'odulo entonces $\text{Tor}(M)$ sería igual a los divisores de 0 junto con el 0 de R. Estos son $\overline{0}$, $\overline{2}$ y $\overline{3}$. Pero esto no es un submódulo de R, pues si tomamos la suma $\overline{2} + \overline{3} = \overline{5}$, esta no pertenece a los elementos de torsión. □

(c) Si R tiene divisores de cero muestre que cualquier R-módulo no cero tiene elementos de torsión no cero.

Demostración. Sea M un R-módulo. Tome $a, b \in R$ diferentes de 0 tales que $ab = 0$. Ahora tome cualquier elemento $m \in M$ distinto de 0. Si $bm = 0$ ya tendriamos que m es un elemento de torsión, si no entonces $a(bm) = abm = 0m = 0$, por lo que bm sería un elemento de torsión. $\square$

Sección 10.1 18. Sea $F = \mathbb{R}$, sea $V = \mathbb{R}^2$ y sea T la transformación lineal de V a V que es rotación horaria alrededor del origen por $\pi/2$ radianes. Muestre que V y 0 son los únicos $F[x]$-submódulos para este T.

Demostración. Una forma de demostrarlo es calculando el polinomio caracteristico de la transformación. La matriz asociada a esta transformación es

$$\begin{pmatrix} \cos(\pi/2) & -\sin(\pi/2) \\ \sin(\pi/2) & cos(\pi/2) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

El polinomio caracteristico lo calculamos como

$$\begin{vmatrix} t & -1 \\ 1 & t \end{vmatrix} = t^2 + 1$$

Pero vemos que este polinomio es irreducible en $\mathbb{R}$ por lo que esta transformación no tiene asociado ningun valor propio. Esto significa que no hay espacios invariantes de dimensión 1 por lo que los únicos $F[x]$-módulos posibles son V y 0. $\square$