Universidad Técnica Federico Santa María
Departamento de matemáticas

Ayudantía 5 MAT214

23 de abril 2024

Mateo Hidalgo

1. Ejercicios

1. Un elemento $x \in A$ es llamado nilpotente si existe un $m \in \mathbb{N}^{\geqslant 1}$ tal que $x^m = 0$

   a) Muestre que si $n = a^k b$ para algunos enteros a y b entonces $\overline{ab}$ es un elemento nilpotente de $\mathbb{Z}/n\mathbb{Z}$

   b) Si $a \in \mathbb{Z}$ es un entero, muestre que el elemento $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ es nilpotente si y solo si cada divisor primo de n es también un divisor de a. En particular, determine los elementos nilpotentes de $\mathbb{Z}/72\mathbb{Z}$ explícitamente.

   c) Sea R el anillo de funciones de un conjunto no vacío X a un cuerpo K. Pruebe que R no contiene elementos nilpotentes no nulos.

   Solución:

   a) Supongamos $n = a^k b$, donde $k \geqslant 1$. Entonces

   $$(ab)^k = a^k b^k = \left(a^k b\right) b^{k-1} = nb^{k-1} \equiv 0 \pmod{n}.$$

   b) ($\Rightarrow$) Supongamos que $\bar{a} \in \mathbb{Z}/(n)$ es nilpotente. Entonces $a^m = nk$ para algún m y k. Ahora si p es un primo dividiendo a n, entonces p divide a^m, así que divide a a. De esta forma, todo primo dividiendo a n divide a a.
   ($\Leftarrow$) Sea $n = p_1^{e_1} \cdots p_k^{e_k}$ y $a = p_1^{d_1} \cdots p_k^{d_k} m$, donde $1 \leqslant e_i, d_i$ para todo i y m es algún entero. Sea $t = \max\{e_i\}$. Entonces

   $$a^t = \left(p_1^{d_1} \cdots p_k^{d_k} m\right)^t = p_1^{d_i t} \cdots p_k^{d_i t} m^t$$

   donde $d_i t \geqslant e_i$ para cada i. Por tanto $a^t = nb$ para algún entero b, y tenemos $a^t \equiv 0 \pmod{n}$.
   Los elementos nilpotentes de $\mathbb{Z}/(72)$, donde $72 = 2^3 \cdot 3^2$, son $0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66$.

   c) Suponga que $\alpha \in R$ es nilpotente. Si $\alpha \neq 0$, entonces existe $x \in X$ tal que $\alpha(x) \neq 0$. Sea m minimal tal que $\alpha(x)^m = 0$; notar que $m \geqslant 1$. Entonces $\alpha(x)\alpha(x)^{m-1} = 0$, donde $\alpha(x)$ y $\alpha(x)^{m-1}$ no son cero. Entonces F contiene divisores del cero, una contradicción. Por tanto no hay elementos no-nulo de R nilpotentes.

2. Un anillo A se dice anillo Booleano si $a^2 = a$ para todo $a \in A$. Probar que todo anillo Booleano es conmutativo.

   Solution: Probemos primero que $(-1)^2 = 1$ y que $(-a) = (-1)(a)$. En efecto, factorizando tenemos $(-1)^2 - 1 = (-1)(-1+1) = -1(0) = 0$ así que $(-1)^2 = 1$. Además, $(-1)(a) + a = (-1+1)a = 0a = 0$ así que $-a = (-1)a$. Notar primero que para todo $a \in R$,

   $$-a = (-a)^2 = (-1)^2 a^2 = a^2 = a.$$

   Ahora si $a, b \in R$, tenemos

   $$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

Entonces $ab + ba = 0$, y tenemos $ab = -ba$. Pero entonces $ab = ba$. Por tanto R es conmutativo.

7.1.23

3. Sea D un número racional que no es un cuadrado perfecto (i.e. no existe $q \in \mathbb{Q}$ tal que $q^2 = D$), definamos

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

subconjunto de $\mathbb{C}$. Probar que cada elemento de $\mathbb{Q}(\sqrt{D})$ puede ser escrito en la forma $a + b\sqrt{D}$ de manera única y además que $\mathbb{Q}(\sqrt{D})$ es un cuerpo, llamado un cuerpo cuadrático.

Solución: Si hubiese un elemento $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ con

$$a + b\sqrt{D} = c + d\sqrt{D}$$

entonces

$$a - c = (b - d)\sqrt{D}$$

pero la única forma en que $(b - d)\sqrt{D} \in \mathbb{Z}$ es que $\sqrt{D}$ sea entero (lo cual no puede ser ya que D no es cuadrado perfecto) o que $(b - d)\sqrt{D}$ sea 0, lo cual implica que $b - d = 0$ (ya que si $D = 0$ entonces $D = 0^2$). Por tanto $a = c, b = d$ y la escritura pedida es única.

Tenemos que si $a + b\sqrt{D} \neq 0$ entonces $a^2 - Db^2 \neq 0$ (ya que sino $D = (a/b)^2$) y como $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$ sigue que si $a + b\sqrt{D} \neq 0$ entonces

$$\frac{a - d\sqrt{D}}{a^2 - Db^2}(a + b\sqrt{D}) = 1$$

es decir, $a + b\sqrt{D}$ es una unidad. Probamos así que todo elemento no nulo en $\mathbb{Q}(\sqrt{D})$ es una unidad y por tanto (como el producto es claramente conmutativo) $\mathbb{Q}(\sqrt{D})$ es un cuerpo.

4. Sea D un entero libre de cuadrados, y definamos

$$\omega = \begin{cases} \sqrt{D}, \text{ si } D \equiv 2, 3 \text{ mód } 4 \\ \frac{1+\sqrt{D}}{2}, \text{ si } D \equiv 1 \text{ mód } 4 \end{cases}$$

y

$$\mathscr{O} = \mathscr{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

llamado el anillo de enteros en el cuerpo cuadrático $\mathbb{Q}(\sqrt{D})$. Defina la norma del cuerpo como

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q}$$

Pruebe que N es multiplicativa, es decir, que $N(\alpha\beta) = N(\alpha)N(\beta)$ para todo $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$. Pruebe que $N(\alpha) \in \mathbb{Z}$ para todo $\alpha \in \mathscr{O}$. Pruebe que $\alpha \in \mathscr{O}$ es una unidad si y solo si $N(\alpha) = \pm 1$

Solución: En efecto tenemos por una lado

$$N(a + b\sqrt{D})N(c + d\sqrt{D}) = (a^2 - b^2D)(c^2 - d^2D) = a^2c^2 - a^2d^2D - b^2c^2D + b^2d^2D^2$$

y por otro lado

$$N((a + b\sqrt{D})(c + d\sqrt{D})) = N(ac + bdD + (ad + bc)\sqrt{D}) = (ac + bdD)^2 - (ad + bc)^2D$$

Ahora, notemos que en el anillo de enteros $\mathscr{O}$ la norma viene dada por

$$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) = \begin{cases} a^2 - Db^2, \text{ si } D \equiv 2,3 \text{ mód } 4 \\ a^2 + ab + \frac{1-D}{4}b^2, \text{ si } D \equiv 1 \text{ mód } 4 \end{cases}$$

donde

$$\bar{\omega} = \begin{cases} -\sqrt{D}, \text{ si } D \equiv 2,3 \text{ mód } 4 \\ \frac{1-\sqrt{D}}{2}, \text{ si } D \equiv 1 \text{ mód } 4 \end{cases}$$

Por tanto $N(\alpha)$ es un entero para cada $\alpha \in \mathscr{O}$. Notamos así que si $\alpha \in \mathscr{O}$ es una unidad de inverso $\alpha^{-1} \in \mathscr{O}$ entonces

$$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$$

pero como $N(\alpha), N(\alpha^{-1}) \in \mathbb{Z}$ tenemos entonces $N(\alpha) = \pm 1$ por ser una unidad de $\mathbb{Z}$. Por otro lado si $\alpha \in \mathscr{O}$ con $N(\alpha) = \pm 1$ entonces la fórmula anterior da $(a+b\omega)^{-1} = \pm(a+b\bar{\omega})$, como $(a+b\bar{\omega}) = a+1-b\omega \in \mathscr{O}$ entonces α es una unidad de $\mathscr{O}$.

5. Sea D un entero libre de cuadrados. Sea $\mathscr{O}$ el anillo de enteros en el cuerpo cuadrático $\mathbb{Q}(\sqrt{D})$. (i.e. $O = \mathbb{Z}[\omega]$.) Para todo entero positivo f pruebe que el conjunto

$$\mathscr{O}_f = \mathbb{Z}[f\omega] = \{a + bf\omega \mid a, b \in \mathbb{Z}\}$$

es un subanillo de $\mathscr{O}$ conteniendo la identidad. Probar que $[\mathscr{O} : \mathscr{O}_f] = f$. (El índice como grupo abeliano). Probar conversamente que un subanillo de $\mathscr{O}$ conteniendo la identidad y teniendo (como subgrupo) índice finito f es igual a $\mathscr{O}_f$.

Solución: Claramente es un subgrupo. Si $\omega^2 = D$ entonces

$$(a+bf\omega)(c+df\omega) = (ac + bdf^2D) + f\omega(bc+ad)$$

y si $\omega = (1+\sqrt{D})/2$ entonces $\omega^2 = \omega + (D-1)/4$ así que

$$(a+bf\omega)(c+df\omega) = (ac + bdf^2(D-1)/4) + f\omega(bc+ad+bd)$$

Como además claramente $1 \in \mathscr{O}_f$ tenemos que $\mathscr{O}_f$ es un subanillo de $\mathscr{O}$. Notemos que $\Phi : \mathbb{Z}[\omega] \to \mathbb{Z}/f\mathbb{Z}$, $a + b\omega \mapsto [b]_f$ es un morfismo de grupos que tiene kernel $\mathbb{Z}[f\omega]$ y es sobreyectiva así que $[\mathscr{O} : \mathscr{O}_f] = f$.

Ahora si $S \subset \mathbb{Z}[\omega]$ subanillo con $1 \in S$ y $[\mathscr{O} : S] = f$. Tenemos en las clases de equivalencia $f(xS) = S$ así que $S = fxS = f(a+b\omega)S = (fa-a)S + (a+fb\omega)S = (a+fb\omega)S$ (esto último ya que $a(f-1) \in S$ pues $\mathbb{Z} \subset S$), por tanto $a + fb\omega \in S$ así que $\mathbb{Z}[f\omega]$ es un subanillo de S y por tanto

$$[\mathscr{O} : \mathscr{O}_f] = f = [\mathscr{O} : S][S : \mathscr{O}_f] = f[S : \mathscr{O}_f] \implies [S : \mathscr{O}_f] = 1 \implies S = \mathscr{O}_f$$