Álgebra I

Parcial IV

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra I
Parcial IV

Los Del DGIIM, `losdeldgiim.github.io`

Arturo Olivares Martos
Joaquín Avilés de la Fuente

Granada, 2023-2024

Asignatura Álgebra I.

Curso Académico 2022-23.

Grado Grado en Matemáticas.

Descripción Parcial I

Fecha 21 de diciembre de 2022.

Parte 1: Cuestionario

Ejercicio 1 (1 punto)**.** Selecciona la afirmación correcta relativa al número $13 \in \mathbb{Z}$.

- ☐ No es irreducible en $\mathbb{Z}[i]$ pero sí en $\mathbb{Z}[\sqrt{-3}]$.
- ■ No es irreducible en $\mathbb{Z}[i]$ ni en $\mathbb{Z}[\sqrt{-3}]$.
- ☐ Es irreducible en $\mathbb{Z}[i]$ pero no en $\mathbb{Z}[\sqrt{-3}]$.

Estudiemos la irreducibilidad de 13 en $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{-3}]$. Comencemos por $\mathbb{Z}[i]$.

Supongamos 13 reducible, entonces $13 = \beta\gamma$, $\beta, \gamma \notin \mathbb{Z}[i]$ y tenemos $N(13) = N(\beta)N(\gamma)$, de donde podemos deducir:

$$13^2 = N(\beta)N(\gamma) \Longrightarrow \left\{ \begin{array}{c} N(\beta) = 13 \Longrightarrow \beta = 2+3i \text{ y asociados} \\ \wedge \\ N(\gamma) = 13 \Longrightarrow \gamma = 3+2i \text{ y asociados} \end{array} \right. \Longrightarrow 13 = (2+3i)(3+2i)(-i)$$

Tenemos finalmente que 13 es reducible en $\mathbb{Z}[i]$. Veamos a continuación el caso para $\mathbb{Z}[\sqrt{-3}]$.

Supongamos 13 reducible, entonces $13 = \beta\gamma$, $\beta, \gamma \notin \mathbb{Z}[\sqrt{-3}]$ con $\beta = a + b\sqrt{-3}$ y $\gamma = c + d\sqrt{-3}$. Sabemos que entonces $N(13) = N(\beta)N(\gamma)$, de donde podemos deducir

$$13^2 = N(\beta)N(\gamma) \Longrightarrow \left\{ \begin{array}{c} N(\beta) = 13 \Longrightarrow a^2 + 3b^2 = 13 \Longrightarrow \beta = \pm 1 \pm 2\sqrt{-3} \text{ y asociado} \\ \wedge \\ N(\gamma) = 13 \Longrightarrow c^2 + 3d^2 = 13 \Longrightarrow \gamma = \pm 1 \pm 2\sqrt{-3} \text{ y asociado} \end{array} \right.$$

$$\overset{(*)}{\Longrightarrow} 13 = (1 - 2\sqrt{-3})(1 + 2\sqrt{-3})$$

donde en $(*)$ se ha usado lo siguiente:

$$\frac{13}{1 + 2\sqrt{-3}} = \frac{13(1 - 2\sqrt{-3})}{13} = 1 - 2\sqrt{-3}$$

Sabiendo que $\dfrac{1 - 2\sqrt{-3}}{1 + 2\sqrt{-3}} = \dfrac{(1 - 2\sqrt{-3})^2}{13} \notin \mathbb{Z}[\sqrt{-3}]$ tenemos por tanto que 13 es reducible en $\mathbb{Z}[\sqrt{-3}]$.

Ejercicio 2 (1 punto)**.** Selecciona la afirmación correcta relativa al polinomio $f = 25x^6 + 125x^3 + 5 \in \mathbb{Z}[x]$

- ☐ f es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.
- ☐ f no es irreducible en $\mathbb{Z}[x]$ ni en $\mathbb{Q}[x]$.
- ■ f no es irreducible en $\mathbb{Z}[x]$, pero sí en $\mathbb{Q}[x]$.

Sea $f = 5g$ donde $g = 5x^6 + 25x^3 + 1 \in \mathbb{Z}[x]$, por Eisenstein para $p = 5$, g es irreducible y tenemos

$$f = 5(5x^6 + 25x^3 + 1) \in \mathbb{Z}[x]$$

Como 5 es irreducible en $\mathbb{Z}[x]$, f es reducible en $\mathbb{Z}[x]$ y como 5 es unidad en $\mathbb{Q}[x]$, f es irreducible en $\mathbb{Q}$.

Ejercicio 3 (1 punto)**.** Entre las siguientes proposiciones, seleccione las verdaderas:

- ■ El anillo $\mathbb{Z}_{441}$ tiene 252 unidades
- ■ $47^{22} \equiv 31$ mód (33)
- ■ $3^{18} \equiv 9$ en $\mathbb{Z}_{16}$

Estudiemos la veracidad de la primera afirmación

$$|\mathcal{U}(\mathbb{Z}_{441})| = \varphi(441) = \varphi(3^2 \cdot 7^2) = 3 \cdot 7 \cdot 2 \cdot 6 = 252 \Longrightarrow \textbf{afirmación cierta}$$

Estudiemos la veracidad de la segunda afirmación.

$$\left.\begin{array}{r} \text{mcd}(47, 33) = 1 \\ \varphi(33) = \varphi(3 \cdot 11) = 2 \cdot 10 = 20 \end{array}\right\} \Longrightarrow 47^{20} \equiv 1 \text{ mód } (33)$$

Tenemos entonces

$$\left.\begin{array}{r} 47^{20} \equiv 1 \text{ mód } (33) \\ 47^2 = 2209 = 66 \cdot 33 + 31 \Longrightarrow 47^2 \equiv 31 \text{ mód } (33) \end{array}\right\} \Longrightarrow 47^{20} \cdot 47^2 \equiv 1 \text{ mód } (33)$$

$$\Longrightarrow 47^{22} \equiv 31 \text{ mód } (33) \Longrightarrow \textbf{afirmación cierta}$$

Estudiemos por último la tercera afirmación. Es claro que dicha afirmación equivale a $3^{18} = 9$ mód (16), veámos entonces como podemos analizarla

$$\left.\begin{array}{r} \text{mcd}(3, 16) = 1 \\ \varphi(16) = \varphi(2^4) = 2^3 = 8 \end{array}\right\} \Longrightarrow 3^8 \equiv 1 \text{ mód } (16) \Longrightarrow 3^{16} \equiv 1 \text{ mód } (16)$$

Tenemos por tanto

$$\left.\begin{array}{r} 3^2 = 9 \equiv 9 \text{ mód } (16) \\ 3^{16} \equiv 1 \text{ mód } (16) \end{array}\right\} \Longrightarrow 3^{18} \equiv 9 \text{ mód } (16) \Longrightarrow 3^{18} = 9 \text{ en } \mathbb{Z}_{16} \Longrightarrow \textbf{afirmación cierta}$$

Ejercicio 4 (1 punto)**.** Si $n \geqslant 1$ es un entero, la afirmación **"la ecuación diofántica** $34x + 51y = 5^{2n} - 2^{3n}$ **tiene solución"** es:

- ■ siempre verdad
- □ siempre falsa
- □ verdad o falsa, depende de n

Sabemos que la ecuación tiene solución sii $\text{mcd}(34, 51) = 17 \mid 5^{2n} - 2^{3n}$, por lo que demostrémoslo por inducción.

Para $n = 1$ tenemos $17 \mid 5^2 - 2^3 = 17$ que es cierto. Supuesto cierto para n, comprobémoslo para $n+1$, donde comenzaremos usando la hipótesis de inducción $17 \mid 5^{2n} - 2^{3n}$.

$$
\begin{aligned}
&5^{2n} \equiv 2^{3n} \text{ mód } (17) \Longrightarrow 5^{2n} \cdot 5^2 \equiv 2^{3n} \cdot 5^2 \text{ mód } (17)\\
&\Longrightarrow 5^{2(n+1)} - 2^{3(n+1)} \equiv 2^{3n} \cdot 5^2 - 2^{3(n+1)} \text{ mód } (17)\\
&\Longrightarrow 5^{2(n+1)} - 2^{3(n+1)} \equiv 2^{3n} \cdot (5^2 - 2^3) \text{ mód } (17)\\
&\Longrightarrow 5^{2(n+1)} - 2^{3(n+1)} \equiv 2^{3n} \cdot 17 \text{ mód } (17) \Longrightarrow 17 \mid 5^{2(n+1)} - 2^{3(n+1)}
\end{aligned}
$$

entonces $\exists$ sol $\forall n \in \mathbb{N}, n \neq 0$.

Ejercicio 5 (1 punto)**.** Dados los anillos cocientes $\mathbb{Z}_3[x]/x^3+x+1, \mathbb{Z}_3[x]/x^3-x+1$ y $\mathbb{Z}_3[x]/x^3+x^2-1$, selecciona las afirmaciones correctas.

- ☐ Sólo uno de ellos es cuerpo.
- ☐ Dos de ellos son cuerpos y uno no lo es.
- ☐ Ninguno de ellos es cuerpo.

Estudiemos si los anillos cocientes son cuerpos uno a uno.

Para $\mathbb{Z}_3[x]/x^3+x+1$ veamos si $f = x^3+x+1 \in \mathbb{Z}_3[x]$ es irreducible

$$
\begin{aligned}
&f(0) = 1 \neq 0\\
&f(1) = 3 = 0 \Longrightarrow (x-1) = (x-2) \mid f \Longrightarrow f \text{ es reducible}
\end{aligned}
$$

entonces $\mathbb{Z}_3[x]/x^3+x+1$ no es un cuerpo.

Para $\mathbb{Z}_3[x]/x^3-x+1$ veamos si $f = x^3-x+1 \in \mathbb{Z}_3[x]$ es irreducible

$$
\left.\begin{aligned}
&f(0) = 1 \neq 0\\
&f(1) = 1-1+1 = 1 \neq 0\\
&f(2) = 8-2+1 = 7 = 1 \neq 0
\end{aligned}\right\} \Longrightarrow f \text{ es irreducible por el criterio de la raíz}
$$

entonces $\mathbb{Z}_3[x]/x^3+x^2-1$ sí es un cuerpo.

Para $\mathbb{Z}_3[x]/x^3+x^2-1$ veamos si $f = x^3+x^2-1 \in \mathbb{Z}_3[x]$ es irreducible

$$
\left.\begin{aligned}
&f(0) = -1 = 2 \neq 0\\
&f(1) = 1+1-1 = 1 \neq 0\\
&f(2) = 8+4-1 = 2 \neq 0
\end{aligned}\right\} \Longrightarrow f \text{ es irreducible por el criterio de la raíz}
$$

entonces $\mathbb{Z}_3[x]/x^3+x^2-1$ sí es un cuerpo

Parte 2: Ejercicios

Ejercicio 1 (1,25 puntos)**.** Factorizar en producto de irreducibles en $\mathbb{Z}[x]$ el polinomio

$$f = 20x^5 - 10x^4 + 60x^2 - 10x - 10$$

Sea $f = 10g$ y $g = 2x^5 - x^4 + 6x^2 - x - 1 \in \mathbb{Z}[x]$. Las posibles raíces de g en $\mathbb{Q}$ son:$\{\pm 1, \pm 1/2\}$, tenemos entonces

$$\left.\begin{array}{l} g(1) = 2 - 1 + 6 - 1 - 1 = 5 \neq 0 \\ g(-1) = -2 - 1 + 6 + 1 - 1 \neq 0 \\ g(\frac{1}{2}) = 0 \Longrightarrow (x - 1/2) \mid g \text{ en } \mathbb{Q}[x] \Longrightarrow (2x-1) \mid g \text{ en } \mathbb{Z}[x] \end{array}\right\} \Longrightarrow f = 5 \cdot 2 \cdot (2x-1)h$$

donde $h = x^4 + 3x + 1 \in \mathbb{Z}[x]$ viene dado del siguiente cálculo:

$$\begin{array}{llllll}
\big(& 2x^5 - x^4 + 6x^2 & - x - 1\big) \div \big(2x - 1\big) = x^4 + 3x + 1 \\
& -2x^5 + x^4 & \\ \hline
& & 6x^2 - x \\
& & -6x^2 + 3x \\ \hline
& & \quad 2x - 1 \\
& & -2x + 1 \\ \hline
& & \quad\quad 0
\end{array}$$

Como las posibles raíces de h en $\mathbb{Q}$ son: $\{\pm 1\}$, tenemos

$$\left.\begin{array}{l} h(1) = 1 + 3 + 1 \neq 0 \\ h(-1) = 1 - 3 + 1 = -1 \neq 0 \end{array}\right\} \Longrightarrow h \text{ no tiene factores de grado 1 ni 3}$$

Reduciendo módulo 2 obtenemos $R_2(h) = x^4 + x + 1 \in \mathbb{Z}_2[x]$, entonces

$$\left.\begin{array}{l} R_2(h)(0) = 1 \neq 0 \\ R_2(h)(1) = 3 = 1 \neq 0 \end{array}\right\} \Longrightarrow R_2(h) \text{ no tiene factores de grado 1 ni 3}$$

Veamos ahora si es que $R_2(h)$ tiene factores de grado 2 mediante la siguiente división

$$\begin{array}{cccccc|l}
x^4 & & & +x & +1 & & x^2 + x + 1 \\ \cline{7-7}
-x^4 & -x^3 & -x^2 & & & & x^2 + x \\ \cline{1-3}
& x^3 & +x^2 & +x & +1 & & \\
& -x^3 & -x^2 & -x & & & \\ \cline{2-4}
& & & & +1 & &
\end{array}$$

Como el resto es $1 \neq 0$ tenemos que $x^2 + x + 1 \nmid R_2(h)$, por lo que $R_2(h)$ no tiene factores de grado 2. Tenemos por tanto que $R_2(h)$ es irreducible y por consecuencia h también es irreducible, obteniendo así la factorización del polinomio pedido como

$$f = 5 \cdot 2 \cdot (2x - 1)(x^4 + 3x + 1)$$

Ejercicio 2 (1,25 puntos)**.** Encuentra una solución al siguiente sistema de congruencia en $\mathbb{Z}$ que esté entre 4000 y 6000.

$$\begin{cases} 4x \equiv 4 \text{ mód } (8) \\ x \equiv 86 \text{ mód } (121) \\ x \equiv 2 \text{ mód } (7) \end{cases}$$

Resolvemos primero el siguiente sistema

$$\begin{cases} x \equiv 1 \text{ mód } 2 \Longrightarrow x = 1 + 2k, \quad k \in \mathbb{Z} \\ x \equiv 86 \text{ mód } 121 \end{cases} \Longrightarrow x = 1 + 2k \equiv 86 \text{ mód } 121 \Longrightarrow 2k \equiv 85 \text{ mód } 121$$

Como $\text{mcd}(2, 121) = 1 = 61 \cdot 2 + 121 \cdot (-1)$, entonces tenemos

$$61 \cdot 2 \equiv 1 \text{ mód } (121) \Longrightarrow 61 \cdot 2 \cdot 85 \equiv 85 \text{ mód } (121) \Longrightarrow k_0' = 61 \cdot 85 \text{ es solución particular}$$
$$\Longrightarrow k_0' = 61 \cdot 85 = 5185 = 42 \cdot 121 + 103 \Longrightarrow k_0 = 103 \text{ es solución óptima}$$
$$\Longrightarrow k = 103 + 121t, t \in \mathbb{Z}$$

Dada k_0 la solución óptima veamos ahora sustituyendo en x la solución obtenida del sistema

$$x = 1 + 2k = 1 + 2(103 + 121t) = 1 + 206 + 242t \Longrightarrow x = 207 + 242t, t \in \mathbb{Z}$$

Por tanto el sistema a resolver es

$$\begin{cases} x \equiv 207 \text{ mód } (242) \\ x \equiv 2 \text{ mód } (7) \Longrightarrow x = 2 + 7k, k \in \mathbb{Z} \end{cases} \Longrightarrow x = 2 + 7k \equiv 207 \text{ mód } (242)$$
$$\Longrightarrow 7k \equiv 205 \text{ mód } (242)$$

Por el algoritmo extendido de Euclídes, desarrollado a continuación, tenemos que mcd(7,242) $= 1 = 2 \cdot 242 - 69 \cdot 7$

r_i	u_i	v_i
242	1	0
7	0	1
4	1	-34
3	-1	35
1	2	-69
0	0	0

Por tanto usando el mcd dado y mediante el siguiente desarrollo tenemos la solución del sistema pedido

$$-69 \cdot 7 \equiv 1 \text{ mód } (242) \Longrightarrow -205 \cdot 69 \cdot 7 \equiv 205 \text{ mód } (242)$$
$$\Longrightarrow k_0' = -205 \cdot 69 \text{ es solución particular} \Longrightarrow k_0 = 133 \text{ es solución óptima}$$
$$\Longrightarrow k = 133 + 242t, t \in \mathbb{Z} \Longrightarrow x = 2 + 7k = 2 + 7(133 + 242t), t \in \mathbb{Z}$$
$$\Longrightarrow x = 933 + 1694t, t \in \mathbb{Z}$$

Ejercicio 3 (1,25 puntos)**.** Factoriza en irreducibles $11+3i$ en productos irreducibles en $\mathbb{Z}[i]$

Supongamos $\alpha = 11+3i = \beta\gamma$, entonces tenemos

$$N(\alpha) = N(\beta)N(\gamma) \Longrightarrow 11^2+3^2 = 13\cdot 5\cdot 2 = N(\beta)N(\gamma)$$

Buscamos irreducibles de norma 2

$$N(\beta) = a^2+b^2 \Longrightarrow a=\pm 1 \wedge b = \pm 1 \Longrightarrow (1+i) \text{ y asociados}$$
$$\overset{(*)}{\Longrightarrow} \alpha = (1+i)\beta, \beta = 7-4i$$

donde en (*) se ha usado que

$$\frac{11+3i}{1+i} = \frac{(11+3i)(1-(1-i))}{2} = \frac{11+3i-11i+3}{2} = 7-4i$$

Busquemos ahora irreducibles de norma 5

$$N(\gamma) = a^2+b^2 \Longrightarrow \begin{cases} a=\pm 2 \wedge b=\pm 1 \Longrightarrow (2+i) \text{ y asociados} \\ \vee \\ a=\pm 1 \wedge b = \pm 2 \Longrightarrow (1+2i) \text{ y asociados} \end{cases} \Longrightarrow$$

$$\overset{(*)}{\Longrightarrow} \alpha = (1+i)(2+i)(2-3i)$$

donde en (*) se ha usado que

$$\frac{7-4i}{2+i} = \frac{(2-i)(7-4i)}{5} = \frac{4-8i-7i-4}{5} = 2-3i$$

Como $N(2-3i) = 4+9 = 13$ y 13 es primo, entonces $2-3i$ es primo. Además, como sus normas son distintas y no son asociados, tenemos finalmente la factorización pedida

$$11+3i = \alpha = (1+i)(2+i)(2-3i)$$

Ejercicio 4 (1,25 puntos)**.** Encuentra todos los polinomios (si los hay) $f, g \in \mathbb{R}[x]$, con f mónico y de grado 2, tales que:

$$(x^5+x^4+2x^3+2x^2+x+1)\cdot f + (x^4+x^3+2x^2+x+1)\cdot g = x^3+2x^2+x+2$$

Desarrolando el algoritmo extendido de Euclídes tenemos:

r_i	u_i	v_i	
$x^5+x^4+2x^3+2x^2+x+1$	1	0	
$x^4+x^3+2x^2+x+1$	1	1	
x^2+1	1	$-x$	$(*)$
0	0	0	

donde $(*)$ viene dado por

$$
\begin{array}{rrrrrr|l}
x^5 & +x^4 & +2x^3 & +2x^2 & +x & +1 & x^4+x^3+2x^2+x+1 \\ \cline{7-7}
-x^5 & -x^4 & -2x^3 & -x^2 & -x & & x \\ \cline{1-5}
 & & & x^2 & & +1 &
\end{array}
$$

Se tiene entonces que $\text{mcd}(x^5+x^4+2x^3+2x^2+x+1, x^4+x^3+2x^2+x+1) = x^2+1$, comprobemos a continuación si x^2+1 divide a x^3+2x^2+x+2

$$
\begin{array}{rrrr|l}
x^3 & +2x^2 & +x & +2 & x^2+1 \\ \cline{5-5}
-x^3 & & -x & & x+2 \\ \cline{1-3}
 & 2x^2 & & +2 & \\
 & -2x^2 & & -2 & \\ \cline{2-4}
 & & & 0 &
\end{array}
$$

Como efectivamente hemos demostrado que $x^2+1 \mid x^3+2x^2+x+2$, tenemos a continuación la ecuación diofántica reducida al dividir entre x^2+1

$$(x^3+x^2+x+1)\cdot f + (x^2+x+1)\cdot g = x+2$$

ecuación obtenida a partir de estas divisiones rutinarias de polinomios

$$
\begin{array}{rrrrrr|l}
x^5 & +x^4 & +2x^3 & +2x^2 & +x & +1 & x^2+1 \\ \cline{7-7}
-x^5 & & -x^3 & & & & x^3+x^2+x+1 \\ \cline{1-3}
 & x^4 & +x^3 & +2x^2 & +x & +1 & \\
 & -x^4 & & -x^2 & & & \\ \cline{2-4}
 & & x^3 & +x^2 & +x & +1 & \\
 & & -x^3 & & -x & & \\ \cline{3-5}
 & & & x^2 & & +1 & \\
 & & & -x^2 & & -1 & \\ \cline{4-6}
 & & & & & 0 &
\end{array}
\qquad
\begin{array}{rrrrr|l}
x^4 & +x^3 & +2x^2 & +x & +1 & x^2+1 \\ \cline{6-6}
-x^4 & & -x^2 & & & x^2+x+1 \\ \cline{1-3}
 & x^3 & +x^2 & +x & +1 & \\
 & -x^3 & & -x & & \\ \cline{2-4}
 & & x^2 & & +1 & \\
 & & -x^2 & & -1 & \\ \cline{3-5}
 & & & & 0 &
\end{array}
$$

Como sabemos que $\text{mcd}(x^3+x^2+x+1, x^2+x+1) = 1 = 1\cdot(x^3+x^2+x+1) - x(x^2+x+1)$, tenemos entonces que

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

$$\Longrightarrow \begin{cases} f_0 = x+2 \\ g_0 = -x(x+2) = -x^2-2x \end{cases} \text{solución particular} \Longrightarrow$$

$$\Longrightarrow \begin{cases} f = (x+2) + k(x^2+x+1) \\ g = -x^2-2x+k(x^3+x^2+x+1) \end{cases} k \in \mathbb{R}[x]$$

Como se pide $grd(f) = 2 \Longrightarrow grd(k) = 1 \Longrightarrow k \in \mathbb{R}$ y se pide f mónico entonces tenemos $k = 1$. Obtenemos finalmente los dos polinomios requeridos

$$\begin{cases} f = x+2+x^2+x+1 \\ g = -x^2-2x-x^3-x^2-1 \end{cases} \Longrightarrow \begin{cases} f = x^2+2x+3 \\ g = -x^2-2x^2-3x-1 \end{cases}$$