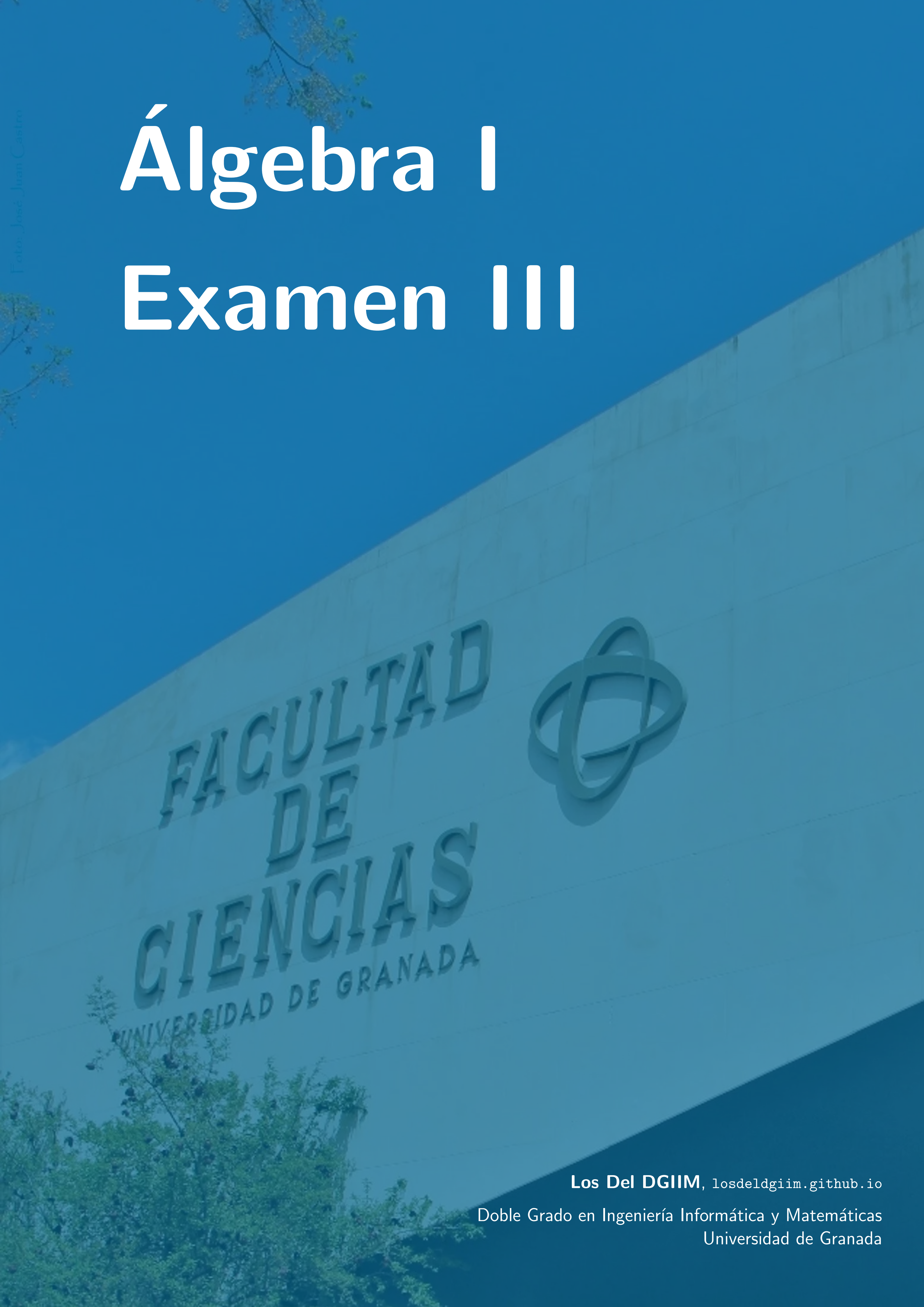

Foto: José Juan Castro

Álgebra I
Examen III

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra I
Examen III

Los Del DGIIM, losdeldgiim.github.io

José Juan Urrutia Milán
Arturo Olivares Martos

Granada, 2023-2024

Asignatura Álgebra I.

Curso Académico 2021-22.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor María Pilar Carrasco Carrasco.

Descripción Examen Extraordinario.

Fecha 7 de febrero de 2022.

Duración 3 horas.

Ejercicio 1 (4 puntos)**.**

1. (0.5 puntos) Sea X un conjunto y A, B y C subconjuntos de X. Suponiendo que $A \cap C = \emptyset$, probad que $(A \cup B) - C = A \cup (B - C)$.

2. (1 punto) Sea $f : \mathbb{R} \to \mathbb{R}$ la aplicación definida para cada $x \in \mathbb{R}$, por $f(x) = x^2 - 3x + 1$. Sea R_f la relación de equivalencia en $\mathbb{R}$ definida por la aplicación f. Describid el conjunto cociente. ¿Cuántos elementos tiene cada clase?

3. (0.5 puntos) En el anillo $\mathbb{Z}_8$, sea $I = 4\mathbb{Z}_8$, el ideal principal generado por 4. Describid $\mathbb{Z}_8/I$ listando todos sus elementos.

4. (1 punto) Sea A un dominio euclídeo con función euclídea $\phi : A \setminus \{0\} \to \mathbb{N}$. Demostrad que para todo $a \neq 0$, se tiene que $\phi(a) \geqslant \phi(1)$ y que se da la igualdad si, y sólo si $a \in U(A)$.

5. (0.5 puntos) Demostrad que $n^{13} - n$ es divisible por 2 y 5 para todo $n \in \mathbb{Z}$.

6. (0.5 puntos) Demostrad que en $\mathbb{Z}[i]$ se tiene que $\mathrm{mcd}(n, n + i) = 1$, para todo $n \in \mathbb{Z}$, $n \neq 0$.

Ejercicio 2 (3.5 puntos)**.**

1. (2.5 puntos) Factorizar en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ los siguientes polinomios:

   a. $48x^4 + 24x^3 - 72x + 80$
   b. $x^6 + 8x^4 + 4x^3 + 5x^2 + 4x + 1$
   c. $10x^5 + 23x^4 - 20x^3 + 5x^2 + 5x - 3$

2. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo de grado $n > 0$ y tal que existe un primo $p \in \mathbb{Z}$ verificando:

   (i) Su reducido módulo p es de la forma $R_p(f(x)) = \alpha x^n$, con $\alpha \in \mathbb{Z}$ no nulo.
   (ii) $p^2 \nmid f(p)$.

   Demostrad que $f(x)$ es irreducible.

Ejercicio 3 (2.5 puntos)**.** Dado el sistema de congruencias en $\mathbb{Z}[\sqrt{-2}]$

$$\begin{cases} \mathrm{x} \equiv 1 & \text{mód } (1 + \sqrt{-2}) \\ \mathrm{x} \equiv 2 & \text{mód } (3 + \sqrt{-2}) \\ \mathrm{x} \equiv 4 & \text{mód } (3 + 2\sqrt{-2}) \end{cases}$$

Demostrad que tiene solución sin resolverlo. Resolverlo, dando una solución óptima y la solución general.
¿Es posible encontrar una solución a $a + b\sqrt{-2}$ tal que $30 < a < 56$?

Ejercicio 1 (4 puntos)**.**

1. (0.5 puntos) Sea X un conjunto y A, B y C subconjuntos de X. Suponiendo que $A \cap C = \emptyset$, probad que $(A \cup B) - C = A \cup (B - C)$.

2. (1 punto) Sea $f : \mathbb{R} \to \mathbb{R}$ la aplicación definida para cada $x \in \mathbb{R}$, por $f(x) = x^2 - 3x + 1$. Sea R_f la relación de equivalencia en $\mathbb{R}$ definida por la aplicación f. Describid el conjunto cociente. ¿Cuántos elementos tiene cada clase?

3. (0.5 puntos) En el anillo $\mathbb{Z}_8$, sea $I = 4\mathbb{Z}_8$, el ideal principal generado por 4. Describid $\mathbb{Z}_8/I$ listando todos sus elementos.

$$\mathbb{Z}_8/I = \{[a] \mid a \in \mathbb{Z}_8\} = \{a + I \mid a \in \mathbb{Z}_8\}$$

$$[0] = \{b \in \mathbb{Z}_8 \mid b \equiv 0 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 0 \text{ en } \mathbb{Z}_4\} = \{0, 4\}$$

$$[1] = \{b \in \mathbb{Z}_8 \mid b \equiv 1 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 1 \text{ en } \mathbb{Z}_4\} = \{1, 5\}$$

$$[2] = \{b \in \mathbb{Z}_8 \mid b \equiv 2 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 2 \text{ en } \mathbb{Z}_4\} = \{2, 6\}$$

$$[3] = \{b \in \mathbb{Z}_8 \mid b \equiv 3 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 3 \text{ en } \mathbb{Z}_4\} = \{3, 7\}$$

Luego:

$$\mathbb{Z}_8/I = \{0 + I, 1 + I, 2 + I, 3 + I\}$$

4. (1 punto) Sea A un dominio euclídeo con función euclídea $\phi : A \setminus \{0\} \to \mathbb{N}$. Demostrad que para todo $a \neq 0$, se tiene que $\phi(a) \geqslant \phi(1)$ y que se da la igualdad si, y sólo si $a \in U(A)$.

$$\phi(a) = \phi(a \cdot 1) \geqslant \phi(1) \quad \forall a \in A \setminus \{0\}$$

$\Rightarrow$) Supongamos que $\phi(a) = \phi(1)$:
Dividimos 1 entre a, $1 = qa + r$ con:

$$\begin{cases} \text{r} = 0 \\ \vee \\ \phi(r) < \phi(a) = \phi(1) \end{cases}$$

- Supongamos que $r \neq 0$, luego $\phi(r) < \phi(1)$, pero:

$$\phi(b) \geqslant \phi(1) \quad \forall b \in A \setminus \{0\} \Rightarrow \phi(r) \geqslant \phi(1)$$

<u>Contradicción</u>. Luego $r = 0$.
Por tanto: $1 = qa \Rightarrow a \in U(A)$.

$\Leftarrow$) Supongamos que $a \in U(A) \Rightarrow \exists a^{-1} \in A \mid aa^{-1} = 1 \Rightarrow \phi(aa^{-1}) = \phi(1)$

$$\left.\begin{array}{r} \phi(1) = \phi(aa^{-1}) \geqslant \phi(a) \\ \phi(a) \geqslant \phi(1) \quad \forall a \in A \setminus \{0\} \end{array}\right\} \Rightarrow \phi(a) = \phi(1)$$

5. (0.5 puntos) Demostrad que $n^{13} - n$ es divisible por 2 y 5 para todo $n \in \mathbb{Z}$.

Demostremos primero que $2 \mid n^{13} - n \quad \forall n \in \mathbb{Z}$:
• Supongamos que $2 \mid n \Rightarrow \exists k \in \mathbb{Z}$ tal que $n = 2k$.

$$n^{13} - n = n(n^{12} - 1) = 2k(n^{12} - 1) = 2k'$$

Con $k' = k(n^{12} - 1) \Rightarrow 2 \mid n^{13} - n$.

• Supongamos que $2 \nmid n$:
Como 2 es primo, $\operatorname{mcd}(2, n) = 1$. Por el Teorema de Fermat:

$$n^{\varphi(2)} = n \equiv 1 \mod (2) \Rightarrow n^{12} \equiv 1 \mod (2) \Rightarrow n^{13} \equiv n \mod (2) \Rightarrow$$

$$\Rightarrow n^{13} - n \equiv 0 \mod (2) \Rightarrow 2 \mid n^{13} - n$$

Veamos que $5 \mid n^{13} - n \quad \forall n \in \mathbb{Z}$:
• Supongamos que $5 \mid n \Rightarrow \exists k \in \mathbb{Z}$ tal que $n = 5k$.

$$n^{13} - n = n(n^{12} - 1) = 5k(n^{12} - 1) = 5k'$$

Con $k' = k(n^{12} - 1) \Rightarrow 5 \mid n^{13} - n$.

• Supongamos que $5 \nmid n$:
Como 5 es primo, $\operatorname{mcd}(5, n) = 1$. Por el Teorema de Fermat:

$$n^{\varphi(5)} = n^4 \equiv 1 \mod (5) \Rightarrow n^{12} \equiv 1 \mod (5) \Rightarrow n^{13} \equiv n \mod (5) \Rightarrow$$

$$\Rightarrow n^{13} - n \equiv 0 \mod (5) \Rightarrow 5 \mid n^{13} - n$$

6. (0.5 puntos) Demostrad que en $\mathbb{Z}[i]$ se tiene que $\operatorname{mcd}(n, n+i) = 1$, para todo $n \in \mathbb{Z}$, $n \neq 0$.

Supongamos que $\exists n \in \mathbb{Z}^+ \mid \operatorname{mcd}(n, n+i) \neq 1$.
Como el máximo común divisor es único salvo asociados y:
$1 \sim a$ con $a \in U(\mathbb{Z}[i])$:

$$\operatorname{mcd}(n, n+i) = \alpha \mid \alpha \notin U(A)$$

$$\begin{cases} \alpha \mid n & \Rightarrow \quad \mathrm{N}(\alpha) \mid N(n) & \Rightarrow \quad \mathrm{N}(\alpha) \mid n^2 \\ \wedge & & \\ \alpha \mid n+i & \Rightarrow \quad \mathrm{N}(\alpha) \mid N(n+i) & \Rightarrow \quad \mathrm{N}(\alpha) \mid n^2+1 \end{cases}$$

Veamos ahora el siguiente resultado:
Sean a, $b \in \mathbb{Z}^+$: $a \mid b \wedge a \mid b+1 \Leftrightarrow a = \pm 1$

$\Leftarrow$) Supongamos que $a = \pm 1 \Rightarrow a \in U(A) \Rightarrow a \mid b \wedge a \mid b+1$
$\Rightarrow$) Supongamos que $a \mid b \wedge a \mid b+1$:

$$\left.\begin{array}{lcr} \mathrm{a} \mid b & \Rightarrow & \exists k \in \mathbb{Z} \mid b = ka \\ \mathrm{a} \mid b+1 & \Rightarrow & \exists k' \in \mathbb{Z} \mid b+1 = k'a \end{array}\right\} \Rightarrow ka + 1 = k'a \Rightarrow$$

$$\Rightarrow 1 = a(k' - k) \Rightarrow a \mid 1 \Rightarrow a \in U(\mathbb{Z}) \Rightarrow a = \pm 1$$

$$\left.\begin{array}{l} \mathrm{N}(\alpha) \mid n^2 \\ \wedge \\ \mathrm{N}(\alpha) \mid n^2+1 \end{array}\right\} \Rightarrow N(\alpha) = \pm 1 \Rightarrow \alpha \in U(A)$$

Lo que es una contradicción.

Luego $mcd(n, n+i) = 1 \quad \forall n \in \mathbb{Z}^+$.

Ejercicio 2 (3.5 puntos)**.**

1. (2.5 puntos) Factorizar en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ los siguientes polinomios:

   a. $48x^4 + 24x^3 - 72x + 80$

   Sea $f = 48x^4+24x^3-72x+80$, $f = 8g$ con $g = 6x^4+3x^3-9x+10 \in \mathbb{Z}[x]$. g es irreducible en $\mathbb{Z}[x]$ por Eisenstein para $p = 3$. Por la misma razón, también lo es en $\mathbb{Q}[x]$.

   $$f = 2^3(6x^4 + 3x^3 - 9x + 10) \text{ en } \mathbb{Z}[x]$$

   $$f = 8(6x^4 + 3x^3 - 9x + 10) \text{ en } \mathbb{Q}[x]$$

   b. $x^6 + 8x^4 + 4x^3 + 5x^2 + 4x + 1$

   Sea $f = x^6 + 8x^4 + 4x^3 + 5x^2 + 4x + 1$.
   Las posibles raíces de f en $\mathbb{Q}$ son $\{\pm 1\}$:

   $$\left.\begin{array}{l} f(1) = 1+8+4+5+4+1 = 23 \neq 0 \\ f(-1) = 1+8-4+5-4+1 = 7 \neq 0 \end{array}\right\} \Rightarrow \begin{array}{l} f \text{ no tiene factores} \\ \text{de grado 1 ni 5} \end{array}$$

   • Reducimos módulo 2:

   $R_2(f) = x^6+x^2+1 = (x^3+x+1)^3 \Rightarrow R_2(f)$ no tiene factores de grado 2 ni 4

   Luego f tampoco tiene factores de grado 2 ni 4.

   • Reducimos módulo 3:

   $$R_3(f) = x^6 + 2x^4 + x^3 + 2x^2 + x + 1 \in \mathbb{Z}_3[x]$$

   $$\left.\begin{array}{l} R_3(f)(0) = 1 \neq 0 \\ R_3(f)(1) = 8 \neq 0 \\ R_3(f)(2) = 115 = 1 \neq 0 \end{array}\right\} \Rightarrow \begin{array}{l} R_3(f) \text{ no tiene factores} \\ \text{de grado 1 ni 5} \end{array}$$

   Al dividir $R_3(f)$ entre $x^2 + 1$ obtenemos que:

   $$x^6+2x^4+x^3+2x^2+x+1 = (x^2+1)(x^4+x^2+x+1) \Rightarrow (x^2+1) \mid R_3(f)$$

   $$R_3(f) = (x^2 + 1)g \text{ con } g = x^4 + x^2 + x + 1 \in \mathbb{Z}_3[x]$$

   Como $R_3(f)$ no tiene factores de grado 1 $\Rightarrow g$ no tiene de grado 1 ni 3.
   $R_3(f)$ no tiene factores de grado 3 $\Rightarrow f$ tampoco.

   Concluimos que f es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

c. $10x^5 + 23x^4 - 20x^3 + 5x^2 + 5x - 3$

2. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo de grado $n > 0$ y tal que existe un primo $p \in \mathbb{Z}$ verificando:

   (i) Su reducido módulo p es de la forma $R_p(f(x)) = \alpha x^n$, con $\alpha \in \mathbb{Z}$ no nulo.

   (ii) $p^2 \nmid f(p)$.

   Demostrad que $f(x)$ es irreducible.

Ejercicio 3 (2.5 puntos)**.** Dado el sistema de congruencias en $\mathbb{Z}[\sqrt{-2}]$

$$\begin{cases} \text{x} \equiv 1 \quad \text{mód } (1+\sqrt{-2}) \\ \text{x} \equiv 2 \quad \text{mód } (3+\sqrt{-2}) \\ \text{x} \equiv 4 \quad \text{mód } (3+2\sqrt{-2}) \end{cases}$$

Demostrad que tiene solución sin resolverlo. Resolverlo, dando una solución óptima y la solución general.
¿Es posible encontrar una solución a $a + b\sqrt{-2}$ tal que $30 < a < 56$?