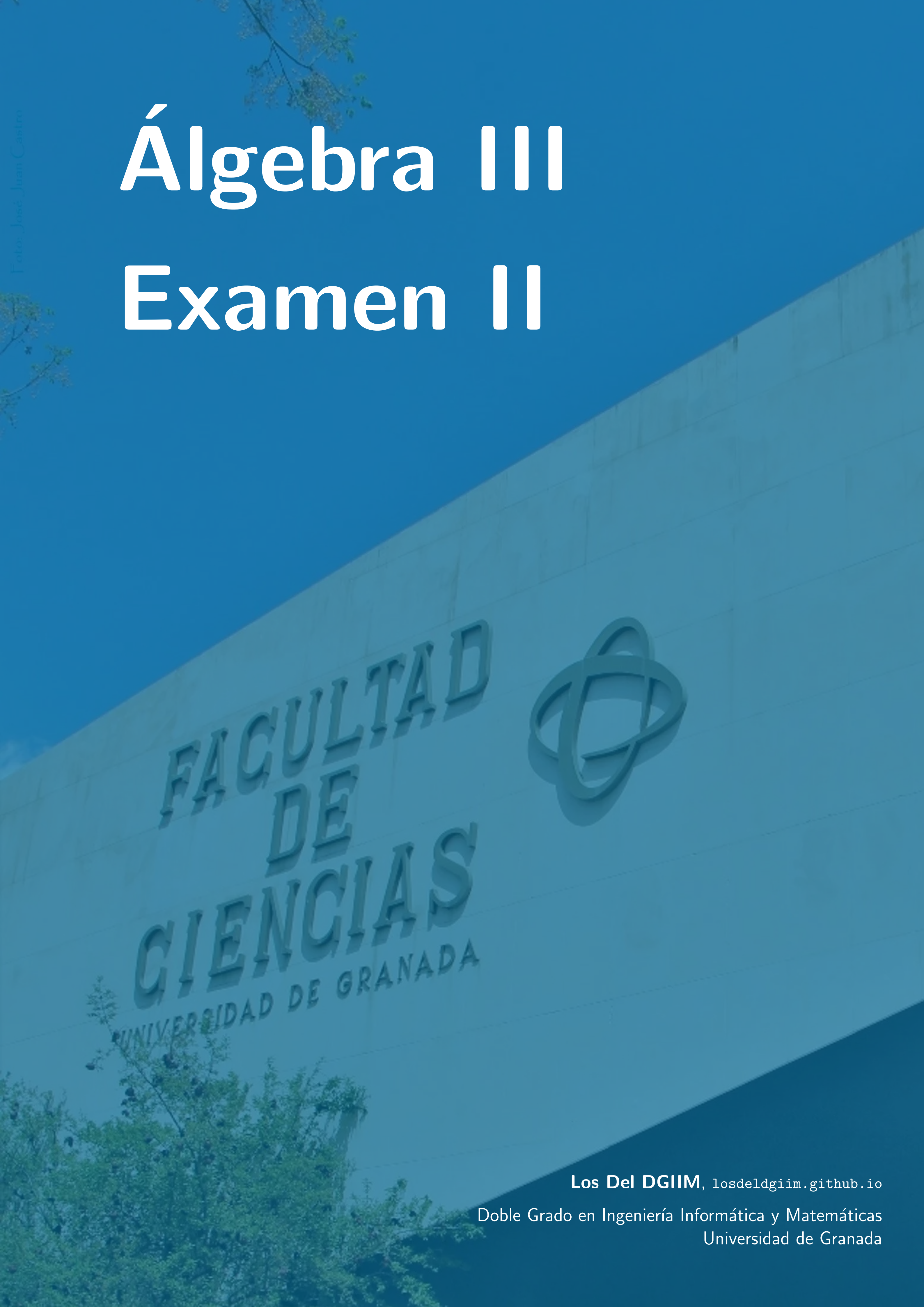

Foto: José Juan Castro

Álgebra III
Examen II

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra III
Examen II

Los Del DGIIM, `losdeldgiim.github.io`

Granada, 2025

Asignatura Álgebra III.

Curso Académico 2025/26.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor José Gómez Torrecillas.

Descripción Tercer examen sorpresa.

Duración Una hora.

Ejercicio 1. Calcular el número de polinomios mónicos irreducibles de grado menor o igual que 3 en $\mathbb{F}_5[x]$.

Ejercicio 2. ¿Cuántos subcuerpos tiene $\mathbb{F}_{256}$?

Ejercicio 3. Si alguien recuerda el enunciado de este ejercicio se ruega que lo comuniquen.

Solución.

Ejercicio 1. Calcular el número de polinomios mónicos irreducibles de grado menor o igual que 3 en $\mathbb{F}_5[x]$.

Calculamos el número de polinomios mónicos irreducibles de grados 1, 2 y 3 en $\mathbb{F}_5$:

Polinomios de grado 1. Los únicos polinomios mónicos de grado 1 en $\mathbb{F}_5[x]$ son:

$$x \qquad x-1 \qquad x-2 \qquad x-3 \qquad x-4 \qquad x-5$$

y todos ellos son irreducibles. Vemos que hay 5.

Polinomios de grado 2. Sabemos por lo visto en teoría que todos los polinomios mónicos irreducibles de grado 2 de $\mathbb{F}_5[x]$ han de ser divisores del polinomio:

$$x^{5^2} - x = x^{25} - x \in \mathbb{F}_5[x]$$

Además, los únicos divisores de este polinomio son los polinomios mónicos irreducibles en $\mathbb{F}_5[x]$ de grados 1 y 2 (divisores de 2). Así:

- Tenemos que todos los polinomios mónicos irreducibles de grado 1 dividen a $x^{25} - x$, y había 5 de estos, por lo que la factorización de $x^{25} - x$ ya ha alcanzado grado 5.
- Tenemos por tanto que sumar 20 grados al producto para alcanzar grado 25 con polinomios de grado 2, es decir, tenemos que añadir $^{20}/_2 = 10$ polinomios mónicos irreducibles de grado 2 en $\mathbb{F}_5[x]$, por lo que solo hay 10 polinomios irreducibles mónicos de grado 2 en $\mathbb{F}_5[x]$.

Polinomios de grado 3. De forma análoga al apartado anterior, sabemos que la factorización de:

$$x^{5^3} - x = x^{125} - x \in \mathbb{F}_5[x]$$

nos da todos los polinomios mónicos irreducibles en $\mathbb{F}_5[x]$ de grados 1 y 3 (divisores de 3), por lo que:

- Hay 5 de grado 1.
- Debemos sumar hasta grado 125, nos faltan 120 grados, por lo que debe haber $^{120}/_3 = 40$ polinomios mónicos irreducibles de grado 3 en $\mathbb{F}_5[x]$.

En total, tenemos:

$$5 + 10 + 40 = 55$$

polinomios mónicos irreducibles de grado menor o igual que 3 en $\mathbb{F}_5[x]$.

Ejercicio 2. ¿Cuántos subcuerpos tiene $\mathbb{F}_{256}$?

Vemos que $\mathbb{F}_{256} = \mathbb{F}_{2^6}$, con lo que tenemos que $\mathbb{F}_2 \leqslant \mathbb{F}_{256}$ y además esta extensión es de Galois, por ser una extensión de cuerpo finitos. Sabemos además que:

$$\mathrm{Aut}(\mathbb{F}_{256}) = [\mathbb{F}_{256} : \mathbb{F}_2] = [\mathbb{F}_{2^6} : \mathbb{F}_2] = 6$$

Por lo que $\mathrm{Aut}(\mathbb{F}_{256})$ es un grupo cíclico[1] de orden 6. Sabemos que los grupos cíclicos tienen un único subgrupo por cada divisor del orden del grupo, por lo que $\mathrm{Aut}(\mathbb{F}_{256})$ tiene:

$$|Div(6)| = |\{1, 2, 3, 6\}| = 4$$

subgrupos. La conexión de Galois nos dice que $\mathrm{Subgr}(\mathrm{Aut}(\mathbb{F}_{256}))$ está en correspondencia biyectiva con $\mathrm{Subex}(\mathbb{F}_2 \leqslant \mathbb{F}_{256})$, por lo que $\mathbb{F}_{256}$ tiene 4 subcuerpos.

Más aún, los subgrupos de $\mathrm{Aut}(\mathbb{F}_{256})$ tienen órdenes 1, 2, 3 y 6, por lo que los respectivos subcuerpos de $\mathbb{F}_{256}$ tendran grados (usando la conexión de Galois) 6, 3, 2 y 1 sobre $\mathbb{F}_2$, con lo que en definitiva estos son isomorfos de forma respectiva a:

$$\mathbb{F}_{256}, \qquad \mathbb{F}_8, \qquad \mathbb{F}_4, \qquad \mathbb{F}_2$$

Ejercicio 3. Si alguien recuerda el enunciado de este ejercicio se ruega que lo comuniquen.

[1]Esto lo sabemos por ser $\mathbb{F}_{256}$ un cuerpo finito.