

Corso di laurea in Matematica
Algebra 2, a.a. 2025–26
Scritto 9 giugno 2026

Svolgere i seguenti esercizi. Le risposte vanno giustificate con brevità e chiarezza.

1. Sia G un gruppo finito con p elementi, dove p è un numero primo. Provare che G è un gruppo abeliano. Quanti sottogruppi normali ha G ?
2. Provare che il seguente polinomio

$$f(x) = \frac{1}{2}x^5 + ax^3 + \frac{a(a-1)}{2}x^2 + 3x + 1 \in \mathbb{Q}[x]$$

è irriducibile in $\mathbb{Q}[x]$ per ogni $a \in \mathbb{N}$.

3. Usando *solamente* i teoremi di Berlekamp, trovare la fattorizzazione in irriducibili del polinomio

$$f(x) = x^4 + 1 \in \mathbb{Z}_2[x].$$

4. Ricordare che, se $\alpha \in \mathbb{C}$, con $\mathbb{Q}[\alpha]$ si indica il più piccolo anello che contiene $\mathbb{Q}$ ed α . Sia ora $\alpha = \sqrt{3} + 1$. Provare che $\mathbb{Q}[\alpha]$ è un campo. In che modo si possono scrivere gli elementi di $\mathbb{Q}[\alpha]$?
5. Dire chi sono tutti i polinomi $f(x) \in \mathbb{Z}_3[x]$ di grado al massimo 6 tali che $D(f(x)) = 2$ (ricordare che $D(f(x))$ indica il derivato del polinomio $f(x)$).

Soluzioni:

1) Sia p primo e G un gruppo con p elem.
Se $g \in G$ $g \neq 1$, allora il gruppo ciclico $\langle g \rangle$
generato da G ha ordine $d > 1$ con d divisore
di p . Quindi $d = p$ e quindi G è ciclico
e in particolare abeliano. Per lo stesso
motivo gli unici sottogruppi di G sono $\{1\}$

e G e quando G ha 2 sottogruppi;
necessariamente normali.

2) $f(x) \in \mathbb{Q}[x]$ e' irriducibile in $\mathbb{Q}[x]$
se e solo se $2 \cdot f(x)$ e' irriducibile in $\mathbb{Q}[x]$.

$$\text{M. } 2 \cdot f(x) = x^5 + 2ax^3 + a(a-1)x^2 + 6x + 2$$

e' un polinomio a coeff in $\mathbb{Z}$ e primitivo.

Quando e' irrid in $\mathbb{Q}[x]$ se e solo se e' irrid in $\mathbb{Z}[x]$. Poiche' 2 divide il coeff di tutti i monomi, tranne quello di grado massimo e 4 non divide il termine noto, per Eisenstein il pol. e' irrid $\forall a \in \mathbb{Z}$ (il coeff di x^2 e' sempre div per 2 perche' o a e' pari, o $a-1$ e' pari).

3) $f(x) = x^4 + 1 \in \mathbb{Z}_2[x]$. $d=4, p=2$.

Calcoliamo x^{2^i} ($i=0,1,2,3$)

$$x^0 = 1, \quad x^2 \equiv x^2 \pmod{f}, \quad x^4 \equiv 1 \pmod{f}$$

$$x^6 = x^2 \cdot x^4 \equiv x^2 \pmod{f}.$$

Quindi

$$Q = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$Q - I = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$\ker Q - I = \left\{ (b_0, b_1, b_2, b_3) \mid \begin{cases} b_2 + b_3 = 0 \\ b_1 = 0 \\ b_1 + b_3 = 0 \\ b_2 + b_3 = 0 \end{cases} \right\}$$

$$= \left\{ (b_0, b_1, b_2, b_3) \mid b_1 = b_2 = b_3 = 0 \right\}$$

$$= \text{Span} \{(1, 0, 0, 0)\}.$$

Quando $\dim(\ker Q - I) = 1$. e c'è un solo fattore irriducibile. Inoltre $D(f) = 0$ Quando f è della forma g^{2^k} . Infatti $f = x^4 + 1 = (x^2 + 1)^2 = (x + 1)^4$.

4) $\alpha = \sqrt{3} + 1$. Per provare che $\mathbb{Q}[\alpha]$ è un campo possiamo mostrare che α è algebrico sul $\mathbb{Q}$. Pol. minimo dato da $(\alpha - 1)^2 = 3$ cioè $\alpha^2 - 2\alpha - 2 = 0$, cioè α è radice del polinomio $f(x) = x^2 - 2x - 2$ che è irrid. in $\mathbb{Q}[x]$. Dalla teoria si sa che

$$\mathbb{Q}[\alpha] = \frac{\mathbb{Q}[x]}{(x^2 - 2x - 2)} \quad \text{è un campo.}$$

Gli elementi di $\mathbb{Q}[\alpha]$ sono della forma

$a \cdot 1 + b \cdot \alpha$ cioè sono della forma

$a + b(\sqrt{3} + 1)$ con $a, b \in \mathbb{Q}$.

Altro modo (diretto) per vedere che $\mathbb{Q}[\alpha]$ è campo:

$$\mathbb{Q}[1+\sqrt{3}] = \{a + b(\sqrt{3}+1) \mid a, b \in \mathbb{Q}\} =$$

$$= \{u + v\sqrt{3} \mid u, v \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{3}]$$

e gli elem di $\mathbb{Q}[\sqrt{3}]$ sono invertibili, perché

$$\frac{1}{u + v\sqrt{3}} = \frac{u - v\sqrt{3}}{u^2 - 3v^2} = \frac{u}{u^2 - 3v^2} - \frac{v}{u^2 - 3v^2} \sqrt{3}$$

$$= u' + v'\sqrt{3}.$$

5). Sia $g(x) = f(x) - 2x$.

Allora $D(g(x)) = D(f(x)) - 2 = 0$

Quindi $g(x) = a_0 + a_1 x^3 + a_2 x^6$ $a_0, a_1, a_2 \in \mathbb{Z}_3$

e pertanto

$$f(x) = a_0 + 2x + a_1 x^3 + a_2 x^6, \quad a_0, a_1, a_2 \in \mathbb{Z}_3.$$