Corso di laurea Matematica
Algebra 2
a.a. 2024–25
Scritto 16 settembre 2025

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

1. Sia G un gruppo con $2p$ elementi (dove p è un numero primo maggiore di 2). Quanti sottogruppi di ordine p ha G?

2. Sia A un anello (commutativo unitario) che è anche un dominio d'integrità. Quale valore può avere la caratteristica di A?

3. Nell'anello
$$A = \mathbb{Q}[x]/(x^2 - 1)$$
si considerino gli elementi $[x + a]$ con $a \in \mathbb{Q}$. Per quali valori di a tali elementi sono invertibili? E per quali valori di a sono invece divisori dello zero?

4. Si consideri l'estensione di campi $\mathbb{Q}[\sqrt{2}] : \mathbb{Q}$. Si spieghi brevemente perché $\mathbb{Q}[\sqrt{2}]$ è un'estensione algebrica di $\mathbb{Q}$ e si trovi poi il polinomio minimo su $\mathbb{Q}$ sia di $2 + \sqrt{2}$, sia del suo inverso (in $\mathbb{Q}[\sqrt{2}]$). Si riesce a trovare un legame tra questi due polinomi minimi?

5. Provare che il polinomio $x^2 + 1 \in \mathbb{Z}_3[x]$ è irriducibile. Pertanto l'anello quoziente $K = \mathbb{Z}_3[x]/(x^2+1)$ è un campo. Provare che è perfetto e trovare la radice cubica di $[x + 2]$.

Soluzioni 1. $|G| = 2p$ $p \geq 3$ primo. In quest caso un sottogruppo di G di ordine p è un p-Sylow sottogruppo. Sia N_p il loro numero. Dai teoremi di Sylow abbiamo che

$N_p \mid 2$ e $N_p \equiv 1 \mod p$

Se $N_p \mid 2$ allora N_p vale 1 o 2 ma 2 non può essere congruo a 1 modulo p per ogni p primo, quindi N_p vale 1.

Conclusione: c'è un unico sottogruppo di G con p elementi (che mancano, è normale).

2. La caratteristica di A può essere 0. Se non è zero, è il minimo $n \in \mathbb{N}$, $n>0$ t.c. $\underbrace{1_A + \dots + 1_A}_{n \text{ volte}} = 0$. Se n si spezza in un prodotto $a \cdot b$ con $a, b > 1$, $a, b < n$ allora abbiamo:

$$(a \cdot 1_A)(b \cdot 1_A) = \underbrace{(1_A + \dots + 1_A)}_{a \text{ volte}} \cdot \underbrace{(1_A + \dots + 1_A)}_{b \text{ volte}} =$$

$$= \underbrace{1_A \cdot \underbrace{(1_A + \dots + 1_A)}_{b \text{ volte}} + 1_A \cdot \underbrace{(1_A + \dots + 1_A)}_{b \text{ volte}} + \dots + 1_A \cdot \underbrace{(1_A + \dots + 1_A)}_{b \text{ volte}}}_{a \text{ volte}} =$$

$$= \underbrace{1_A + 1_A + \dots + 1_A}_{ab \text{ volte}} = (ab) 1_A = n \cdot 1_A = 0$$

Allora $(a \cdot 1_A) \cdot (b \cdot 1_A) = 0$. Essendo A dominio $a \cdot 1_A = 0$ o $b \cdot 1_A = 0$ ma questo è assurdo perché né a né b sono $< n$. Allora la caratteristica deve essere un numero primo.

3. $A = \mathbb{Q}[x]/(x^2-1)$. Gli elementi di A sono della forma $[\alpha x + \beta]$ con $\alpha, \beta \in \mathbb{Q}$. Si noti che $[\alpha x + \beta] = 0$ se e solo se $\alpha = 0$ e $\beta = 0$.

Sia $[x+a]$ è invertibile, esistono $\alpha, \beta \in \mathbb{Q}$ t.c. $[x+a][\alpha x + \beta] = 1$

Quindi $[\alpha x^2 + (\beta + a\alpha)x + a\beta - 1] = 0$. Ma $[x^2] = [1]$, quindi:

$[(\beta + a\alpha)x + \alpha + a\beta - 1] = 0$. Pertanto

$$\begin{cases} \beta + a\alpha = 0 \\ \alpha + a\beta - 1 = 0 \end{cases}$$

In questo sistema le incognite sono α, β, mentre a è un numero dato.

Allora $\beta + a(1 - a\beta) = 0$ cioè $\beta(1-a^2) + a = 0$ cioè, se $1 - a^2 \neq 0$

$\beta = \frac{a}{a^2-1}$ e $\alpha = 1 - a\beta = \frac{1}{1-a^2}$.

Quindi se $a^2 - 1 \neq 0$ cioè $a \neq \pm 1$, allora α e β esistono e $[x+a]$ è invertibile.

Se $a = \pm 1$ allora abbiamo che $\beta(1-a^2) + a = 0 \Rightarrow a = 0$, contraddizione.

Quindi $[x \pm 1]$ non è invertibile.

Per vedere quando $[x+a]$ è div. dell'1, si deve prendere solo $a=\pm 1$ perché per gli altri valori di a, come visto, $[x+a]$ è invertibile.

Vediamo se $[x+1]$ è div. dell'1:

deve esistere $[\alpha x+\beta] \neq 0$ t.c. $[x+1][\alpha x+\beta]=0$. Quindi compatta $\alpha+\beta=0$ e quindi si vede che $[x+1]$ è divisore dell'1. Analogam. si vede che anche $[x-1]$ è divisore dell'1.

Conclusione: $[x+a]$ è invertibile se e solo se $a \neq \pm 1$, mentre se $a=\pm 1$ è divisore dell'1.

4. $\mathbb{Q}[\sqrt{2}]:\mathbb{Q}$. $\sqrt{2}$ è algebrico su $\mathbb{Q}$ di grado 2, quindi $[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]=2$, allora $\mathbb{Q}[\sqrt{2}]$ è estensione finita di $\mathbb{Q}$, quindi algebrica

Pol. minimo di $2+\sqrt{2}$. Sia $a=2+\sqrt{2}$ allora $(a-2)^2=2$ cioè $a^2-4a+2=0$. Quindi a è soluzione del polinomio $f(x)=x^2-4x+2$. $f(x)$ è monico e irriducibile (p.es per Eisenstein) Quindi $f(x)$ è il polinomio minimo di $2+\sqrt{2}$ su $\mathbb{Q}$

L'inverso di $2+\sqrt{2}$ è dato da $\frac{1}{2+\sqrt{2}} = \frac{1\cdot(2-\sqrt{2})}{(2+\sqrt{2})(2-\sqrt{2})} = 1-\frac{\sqrt{2}}{2}$

Se $b=1-\frac{\sqrt{2}}{2}$, $b-1=-\frac{\sqrt{2}}{2}$ e quindi il polinomio $g(x)=x^2-2+\frac{1}{2}$ è monico, irriducibile (p.es. perché il suo discriminante vale 2 e $\sqrt{2}$ non è razionale), quindi $g(x)$ è il polinomio minimo di b.

Legame tra f e g $\quad f(a)=a^2-4a+2=0$ dividendo per a^2:

$1-\frac{4}{a}+\frac{2}{a^2}=0$ cioè $2\left(\frac{1}{a^2}\right)-4\left(\frac{1}{a}\right)+1=0$ Quindi $h(x)=2x^2-4x+1$ è t.c. $h\left(\frac{1}{a}\right)=0$. $h(x)$ non è monico.

Dividendo per 2 diventa $g(x)$

Quindi $g(x)=\frac{1}{2}h(x)$ Si noti che $h(x)=f\left(\frac{1}{x}\right)\cdot x^2$

Quindi legame tra $g(x)$ e $f(x)$: $\quad g(x)=\frac{1}{2}x^2 f\left(\frac{1}{x}\right)$

5. x^2+1 irriducibile perché $0,1,2 \in \mathbb{Z}_3$ non sono suoi zeri.

Quindi K è campo. Il monomorfismo di Frobenius è $\varphi : K \to K$ dato da $\varphi(a) = a^3$ (3 è la caratteristica di K)

K è finito, quindi φ è isomorfismo.

Per fare $\sqrt[3]{[x+2]}$ si tratta di trovare $[\alpha x+\beta]$ t.c.

$[\alpha x+\beta]^3 = [x+2]$. Cioè $[(\alpha x+\beta)^3] = [x+2]$ cioè

$[\alpha^3 x^3+\beta^3] = [x+2]$, da cui $[\alpha x^3+\beta] = [x+2]$. Ma $[x^3] =$

$= [x^2 \cdot x] = [-1 \cdot x] = [2x]$, allora

$[2\alpha x+\beta] = [x+2]$ cioè $2\alpha = 1$, $\beta = 2$ da cui $\alpha = 2$, $\beta = 2$ ($\in \mathbb{Z}_3$)

Quindi $\sqrt[3]{[x+2]} = [2x+2]$.