Corso di laurea Matematica
Algebra 2
a.a. 2025–26
Scritto 10 febbraio 2026

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

1. Provare che per ogni $n \in \mathbb{Z}$ il numero
$$A(n) = 4n^{18} + n^{15} + 2n^7 + 3n^6 - n^3 + 5n + 21$$
è divisibile per 7. Per quali valori di n, $A(n)$ risulta divisibile per 3?

2. Sia G un gruppo di 91 elementi. Dire quanti sottogruppi normali ha G.

3. Sia A un anello finito. Provare che gli elementi di A o sono invertibili o sono divisori dello zero. Dare l'esempio di un anello in cui un elemento non è invertibile e non è divisore dello zero.

4. Sia $F : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ l'omomorfismo di anelli dato da $F(a) = a$ per ogni $a \in \mathbb{Q}$ e $F(x) = \sqrt{2}$ e poi esteso su tutto $\mathbb{Q}[x]$ nell'unico modo possibile. Trovare il nucleo di F.

5. Sia $K = \mathbb{Z}_3[x]/(x^2 + 1)$. Spiegare perché K è un campo perfetto. Trovare un elemento $a \in K$ tale che $a^3 = [2x + 1]$.

1) Da Fermat abbiamo: $n^7 \equiv n \mod 7 \quad \forall n$

Quindi $n^{18} \equiv (n^7)^2 \cdot n^4 \equiv n^6 \mod 7 \qquad n^{15} \equiv (n^7)^2 \cdot n \equiv n^3 \mod 7$

Allora, $\forall n \in \mathbb{Z}$:

$$A(n) \equiv 4n^6 + n^3 + 2n + 3n^6 - n^3 + 5n + 0 \equiv 7n^6 + 7n \equiv 0 \mod 7$$

Quindi $7 \mid A(n)$ per ogni n.

Analogamente $n^{18} \equiv (n^3)^6 \equiv n^6 \equiv n^2 \mod 3 \qquad n^{15} \equiv (n^3)^5 \equiv n^5 \equiv n \mod 3$

$n^7 \equiv (n^3)^2 \cdot n \equiv n^3 \equiv n \mod 3 \qquad n^6 \equiv n^2 \mod 3$

Allora, $\forall n$

$$A(n) \equiv 4n^2 + n + 2n + 0 \cdot n^6 - n + 5n + 0 \equiv n^2 + n \mod 3$$

Quindi 3 divide $A(n)$ se e solo se 3 divide $n(n+1)$.

Ma 3 divide $n(n+1)$ se e solo se 3 divide n o 3 divide $n+1$ (poiché 3 è primo).

In conclusione, 3 divide $A(n) \iff n = 3k$ o $n = 3k+2$.

2) $|G| = 91 = 13 \cdot 7$. Per il III teor di Sylow, se N_{13} indica il numero dei 13-Sylow sottogruppi, $N_{13} \equiv 1 \mod 13$ e $N_{13} \mid 7$. Quindi $N_{13} = 1$. Analogamente, $N_7 = 1$. Quindi G ha un solo 13-Sylow sottogruppo che è normale perché coincide con ogni suo coniugato e G ha un solo 7-Sylow sottogruppo anch'esso normale.

In conclusione G ha 4 sottogruppi normali che sono: $\{1\}$, G e il 13-Sylow sottogruppo e il 7-Sylow sottogruppo.

3) Sia $a \in A$. Supponiamo che a non sia div. dello zero. Quindi $a \neq 0$.

Allora, $\forall b \quad ab = 0 \Rightarrow b = 0$.

Consideriamo $a \neq 0$, la successione $a, a^2, a^3,$ è infinita ma A è finito, quindi $\exists\, m, n \in \mathbb{N}$ $m < n$ t.c. $a^m = a^n$. Pertanto

$a^m(1 - a^{n-m}) = 0$. Quindi $a \cdot (a^{m-1}(1 - a^{n-m})) = 0$

e allora $a^{m-1}(1-a^{n-m})=0$. Procedendo in questo modo, si vede che $1-a^{n-m}=0$ cioè $a(a^{n-m-1})=1$, quindo a è invertibile.

4) Sicuramente il polinomio x^2-2 sta in ker F, infatti

$$F(x^2-2)= F(x^2)-F(2)= 2-2=0.$$

Scegliere ~~F~~ Dividiamo g per x^2-2. Quindi

$$g = h\cdot(x^2-2)+r \quad \text{dove } r \text{ ha grado} \leq 1.$$

Inoltre $F(g)= F(h\cdot(x^2-2)+r)$ da cui $F(r)=0$.

Se $r=\alpha x+\beta$ con $\alpha\neq 0$ abbiamo allora che $F(\alpha x+\beta)=0=\alpha\sqrt{2}+\beta$ $\alpha,\beta\in\mathbb{Q}$ da cui $\sqrt{2}=-\frac{\beta}{\alpha}$ assurdo, perché $\sqrt{2}$ è irrazionale. L'unica possibilità allora è che $r=0$ cioè $g=h(x^2-2)$.

Quindi $\ker F=(x^2-2)$.

5). Il polinomio $x^2+1\in\mathbb{Z}_3[x]$ è irriducibile (né 0, né 1 né 2 sono radici di x^2+1). Quindi $K=\mathbb{Z}_3[x]/_{(x^2+1)}$ è un campo finito con $3^2=9$ elementi. In particolare è un campo perfetto (in quanto ogni campo finito è perfetto). Gli elem. di K sono della forma $[\alpha+\beta x]$ con $\alpha,\beta\in\mathbb{Z}_3$. Cerchiamo allora $\alpha,\beta\in\mathbb{Z}_3$ t.c. $[\alpha+\beta x]^3=[2x+1]$.

Ma $[\alpha+\beta x]^3=[\alpha^3+\beta^3x^3]$ perché K ha caratt. 3. Inoltre $\alpha^3=\alpha$ e $\beta^3=\beta$ (piccolo teorema Fermat), allora

$[\alpha^3+\beta^3x^3]=[\alpha+\beta x^3]=[\alpha+\beta(-x)]$ perché $[x^3]=[-x]$.

Quindi si tratta di trovare $\alpha,\beta\in\mathbb{Z}_3$: $[\alpha-\beta x]=[2x+1]$

e pertanto $\alpha=1$ $-\beta=2$ cioè $\alpha=1$, $\beta=1$.