

Corso di laurea Matematica
Algebra 2
a.a. 2024–25
Scritto 15 giugno 2025

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

1. Sia G un gruppo con 77 elementi. Quanti sono i sottogruppi di G ? Quanti di questi sono normali?
2. Dare la definizione di ideale massimale di un anello A commutativo unitario. Provare poi che se I è un ideale proprio di A tale che ogni elemento di A che non sta in I è invertibile, allora I è massimale.
3. Sia $P = \{x^3 + 5x^2 + ax + b \mid a, b \in \mathbb{N}\} \subseteq \mathbb{Z}[x]$ un insieme di polinomi. Provare che nell'insieme P ci sono infiniti polinomi riducibili e infiniti polinomi irriducibili in $\mathbb{Z}[x]$.
4. Sia $a \in \mathbb{C}$ algebrico su $\mathbb{Q}[\sqrt{3}]$. Provare che allora a è algebrico anche su $\mathbb{Q}$.
5. Usando i teoremi di Berlekamp, provare che il polinomio $x^5 - 1 \in \mathbb{Z}_3[x]$ è il prodotto di due fattori irriducibili distinti.

Soluzioni.

1) Sia H sottogruppo di G . Per il teorema di Lagrange, l'ordine di H divide 77, quindi un sottogruppo di G può avere ordine 1, 7, 11, 77.

Se $|H| = 1$ H è il sottogruppo banale $\{1_G\}$

Se $|H| = 77$, $H = G$, e questi sono due sottogruppi normali di G .

Perché $77 = 7 \cdot 11$ ma N_7 il numero dei

7 - sottogruppi di Sylow. Allora

$$N_7 \equiv 1 \pmod{7}$$

$$N_7 \mid 11$$

Quindi $N_7 = 1$. Pertanto in G c'è uno ed un solo sottogruppo H di ordine 7. I suoi coniugati devono coincidere con H (o perché ogni coniugato di H è un sottogruppo di ordine 7 o per il II teorema di Sylow), quindi H è normale.

Analogamente, se N_{11} è il numero dei sottogr. di G di ordine 11, $N_{11} \equiv 1 \pmod{11}$ e $N_{11} \mid 7$, quindi $N_{11} = 1$ e c'è un solo sottogruppo di G di ordine 11.

Conclusione: G ha 4 sottogruppi che sono tutti normali e sono i due banali, un sottogruppo di ordine 7 e un sottogruppo di ordine 11.

2. Un ideale $\mathcal{M} \subseteq A$ si dice massimale se è un ideale proprio e se inoltre vale:

se $J \subseteq A$ è un ideale t. ch. $\mathcal{M} \subsetneq I$, allora $I = A$.

Sia $I \subseteq A$ un ideale proprio e sia J un ideale di A t. ch. $I \subsetneq J$. Allora esiste un elemento $a \in J$, $a \notin I$ quindi a è invertibile, allora esiste $b \in A$ t. ch. $ab = 1$.

Per annullamento $ab \in J$, quindi $1 \in J$. Pertanto $J = A$ e questo prova che I è massimale.

3. Se prendiamo $b=5$ $a=5b$, il polinomio

$x^3 + 5x^2 + 5bx + 5$ è irriducibile in $\mathbb{Z}[x]$ per ogni $b \in \mathbb{N}$ (per il criterio di Eisenstein).

Se prendiamo $b=0$ $a \in \mathbb{N}$ il polinomio

$x^3 + 5x^2 + ax$ è riducibile (avendo x a fattore).

4. Si consideri il campo $L = (\mathbb{Q}[\sqrt{3}])(a)$.

Sia n il grado di a nel campo $\mathbb{Q}[\sqrt{3}]$ (cioè n è il grado del polinomio minimo di a nel campo $\mathbb{Q}[\sqrt{3}]$). Il campo $\mathbb{Q}[\sqrt{3}]$ è un'estensione algebrica di $\mathbb{Q}$ di grado 2.

Consideriamo i seguenti campi:

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] \subseteq L = (\mathbb{Q}[\sqrt{3}])(a)$$

$$\text{Vale: } [\mathbb{Q}[\sqrt{3}]:\mathbb{Q}] = 2, \quad [L:\mathbb{Q}[\sqrt{3}]] = n$$

allora, dal teorema della torre:

$$[L:\mathbb{Q}] = 2 \cdot n.$$

Pertanto L è un'estensione finita di $\mathbb{Q}$ e quindi algebrica, allora a è algebrico su $\mathbb{Q}$.

5. Consideriamo $x^5 - 1 \in \mathbb{Z}_3[x]$.

Procedendo con Berlekamp:

$$x^5 \equiv 1 \pmod{(x^5 - 1)}$$

dobbiamo calcolare il resto della divisione di x^{2^i} per $x^5 - 1$

con $p=3$ $i=0, 1, 2, 3, 4$.

$$X^0 = 1$$

$$X^{1 \cdot 3} = X^3$$

$$X^{2 \cdot 3} = X^6 = X \cdot X^5 \equiv X \pmod{(X^5-1)}$$

$$X^{3 \cdot 3} = X^9 = X^3 \cdot X^6 \equiv X^4 \pmod{(X^5-1)}$$

$$X^{4 \cdot 3} = X^{12} = X^6 \cdot X^6 \equiv X^2 \pmod{(X^5-1)}$$

Quindi la matrice Q le cui colonne sono i coefficienti dei 5 polinomi scritti sopra, vale:

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{quindi } Q-I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Se $\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} \in \ker(Q-I)$, allora deve essere:

$$\begin{cases} 2b_1 + b_2 = 0 \\ 2b_2 + b_4 = 0 \\ b_1 + 2b_3 = 0 \\ b_3 + 2b_4 = 0 \end{cases} \Rightarrow \begin{cases} b_2 = b_1 \\ b_4 = b_2 \\ b_3 = b_1 \\ b_4 = b_3 \end{cases} \Rightarrow \begin{cases} b_2 = b_1 \\ b_3 = b_1 \\ b_4 = b_1 \end{cases}$$

Quando b_0 e b_1 sono parametri liberi, il nucleo di $Q-I$ è generato dai vettori $(1, 0, 0, 0, 0)^t$ e $(0, 1, 1, 1, 1)^t$ e $\dim(Q-I) = 2$. Pertanto X^5-1 ha 2 fattori irriducibili.