

Corso di Algebra 1 - a.a. 2024-2025

Prova scritta del 10/02/2026

1. Dati due gruppi G e G' , scriviamo $G \prec G'$ se G' contiene un sottogruppo isomorfo a G ; altrimenti scriviamo $G \not\prec G'$.
 - (a) Dimostrare che, se $G \prec G'$ e $G' \prec G''$, allora $G \prec G''$.
 - (b) Dimostrare che, se $f: G \rightarrow G'$ è un omomorfismo suriettivo con G finito e $\mathbb{Z}/n\mathbb{Z} \prec G'$ (dove n è un intero positivo), allora $\mathbb{Z}/n\mathbb{Z} \prec G$.
 - (c) Dimostrare che, se $G \prec A_4$ e G è abeliano, allora $G \prec D_6$.
 - (d) Fornire un esempio di un omomorfismo suriettivo $f: G \rightarrow G'$ tale che $\#G = 8$, $V_4 \prec G'$ e $V_4 \not\prec G$.
2. Si consideri il polinomio $f = 3X^3 - 3X + 6 \in \mathbb{Z}[X]$.
 - (a) Trovare tutti gli ideali principali di $\mathbb{Z}[X]$ che contengono (f) .
 - (b) Trovare $y \in \mathbb{Z}[X]/(2, f)$ tale che $y \neq 0$ e $y^2 = 0$.
 - (c) Determinare il più piccolo numero primo p tale che $\mathbb{Z}[X]/(p, f)$ sia un campo.
 - (d) Dimostrare che, se $p > 3$ è un numero primo, allora $X - 2 + (p, f)$ è invertibile in $\mathbb{Z}[X]/(p, f)$.

Soluzioni

1. (a) Per ipotesi esistono $H < G'$ e $H' < G''$ tali che $G \cong H$ e $G' \cong H'$. Indicando con $f: G' \rightarrow H'$ un isomorfismo, si ha $f(H) < H' < G''$ e $H \cong f(H)$. Dunque $G \cong f(H)$ e $f(H) < G''$, cioè $G \prec G''$.
- (b) Per ipotesi esiste $H' < G'$ tale che $H' \cong \mathbb{Z}/n\mathbb{Z}$. In particolare H' è ciclico, per cui esiste $a' \in H'$ tale che $H' = \langle a' \rangle$ e $\text{ord}(a') = \#H' = n$. Essendo f suriettivo, esiste $a \in G$ tale che $f(a) = a'$. Poiché $\text{ord}(a) < \infty$ (dato che G è finito), si ha $n = \text{ord}(a') \mid \text{ord}(a)$, cioè esiste un intero positivo k tale che $\text{ord}(a) = nk$. Allora $\text{ord}(a^k) = n$ e $H := \langle a^k \rangle < G$ è tale che $H \cong \mathbb{Z}/n\mathbb{Z}$, per cui $\mathbb{Z}/n\mathbb{Z} \prec G$.
- (c) Se $G \prec A_4$, per il teorema di Lagrange $\#G \mid \#A_4 = 12$. Assumendo G abeliano si ha anche $\#G < 12$ (altrimenti $G \cong A_4$, che non è abeliano). Dunque a priori potrebbe essere $G \cong \mathbb{Z}/n\mathbb{Z}$ con $n \in \{1, 2, 3, 4, 6\}$ o $G \cong V_4$. D'altra parte A_4 non contiene elementi di ordine 4 o 6, quindi deve essere $G \cong \mathbb{Z}/n\mathbb{Z}$ con $n \in \{1, 2, 3\}$ o $G \cong V_4$ (ed effettivamente A_4 contiene sottogruppi appartenenti a ognuna di queste classi di isomorfismo). Per concludere basta osservare che $\mathbb{Z}/n\mathbb{Z} \cong \langle R^{6/n} \rangle < D_6$ (per cui $\mathbb{Z}/n\mathbb{Z} \prec D_6$) per $n \in \{1, 2, 3\}$ e

$$V_4 \cong \langle R^3, S \rangle = \{1, R^3, S, R^3S\} < D_6$$

(per cui $V_4 \prec D_6$).

- (d) Si può prendere come f la proiezione al quoziente

$$G := Q \rightarrow G' := Q/\{\pm 1\}$$

(dove $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ è il gruppo delle unità dei quaternioni), che è un omomorfismo suriettivo con $\#G = 8$. Infatti

$$\#G' = \frac{\#Q}{\#\{\pm 1\}} = \frac{8}{2} = 4$$

e ogni elemento di G' ha ordine 1 o 2 (perché $a^2 \in \{\pm 1\}$ per ogni $a \in Q$), il che implica $G' \cong V_4$. Pertanto $V_4 \prec G'$, mentre $V_4 \not\prec G$, dato che V_4 contiene 3 elementi di ordine 2, ma Q ha un solo elemento di ordine 2 (cioè -1).

2. (a) Gli ideali principali di $\mathbb{Z}[X]$ che contengono (f) sono della forma (g) con $g \mid f$; inoltre $g, g' \in \mathbb{Z}[X]$ sono tali che $(g) = (g')$ se e solo se g e g' sono associati in $\mathbb{Z}[X]$. Tenendo conto che $\mathbb{Z}[X]$ è un dominio a fattorizzazione unica (perché $\mathbb{Z}$ lo è), per trovare i divisori di f basta conoscere la fattorizzazione di f come prodotto di irriducibili. In effetti si ha $f = 3(X^3 - X + 2)$, e in $\mathbb{Z}[X]$ sono irriducibili sia 3 (perché irriducibile in $\mathbb{Z}$) che $X^3 - X + 2$ (perché primitivo in $\mathbb{Z}[X]$, di terzo grado e senza radici razionali, come si può verificare con il criterio della radice razionale). Dunque, a meno di associati, i divisori di f in $\mathbb{Z}[X]$ sono 1, 3, $X^3 - X + 2$ e f . Pertanto gli ideali principali di $\mathbb{Z}[X]$ che contengono (f) sono $(1) = \mathbb{Z}[X]$, (3) , $(X^3 - X + 2)$ e (f) .

Osserviamo che, per il terzo teorema di isomorfismo per anelli, per ogni numero primo p si ha $\mathbb{Z}[X]/(p, f) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\bar{f})$, dove $\bar{f}$ indica l'immagine di f in $\mathbb{Z}/p\mathbb{Z}[X]$.

- (b) Per $p = 2$ si ha $\bar{f} = X^3 + X = X(X + \bar{1})^2$. Poiché $\bar{f} \nmid X(X + \bar{1})$ e $\bar{f} \mid (X(X + \bar{1}))^2$ in $\mathbb{Z}/p\mathbb{Z}[X]$, l'elemento $y := X(X + 1) + (2, f)$ è tale che $y \neq 0$ e $y^2 = 0$ in $\mathbb{Z}[X]/(2, f)$.
- (c) Il valore cercato di p è 5. Infatti $\mathbb{Z}[X]/(p, f) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\bar{f})$ è un campo se e solo se $\bar{f}$ è irriducibile (essendo $\mathbb{Z}/p\mathbb{Z}[X]$ un dominio a ideali principali, dato che $\mathbb{Z}/p\mathbb{Z}$ è un campo). Inoltre $\bar{f}$ non è irriducibile per $p = 2$ (per il punto precedente) e per $p = 3$ (in tal caso $\bar{f} = \bar{0}$), mentre lo è per $p = 5$ (perché di terzo grado e senza radici in $\mathbb{Z}/5\mathbb{Z}$, come è immediato verificare).
- (d) Per il teorema di Ruffini $f = (X - 2)q + f(2)$ per qualche $q \in \mathbb{Z}[X]$. Poiché $f(2) = 24$, in $\mathbb{Z}/p\mathbb{Z}[X]/(\bar{f})$ si ha $\overline{X - 2} \bar{q} = \overline{-24}$ e $\overline{-24}$ è invertibile (dato che $\overline{-24}$ è invertibile anche nel campo $\mathbb{Z}/p\mathbb{Z}$ per $p > 3$ numero primo). Ciò implica che anche $\overline{X - 2}$ è invertibile in $\mathbb{Z}/p\mathbb{Z}[X]/(\bar{f})$, il che equivale a dire che $X - 2 + (p, f)$ è invertibile in $\mathbb{Z}[X]/(p, f) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\bar{f})$.