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

Prova scritta del 22/01/2026

1. Dati un gruppo G e un intero positivo m, sia

$$\Gamma_m(G) := \{a \in G \,:\, \mathrm{ord}(a) \leq m\}.$$

   (a) Determinare i valori di m per cui $\Gamma_m(\mathbb{Z}/6\mathbb{Z})$ non è un sottogruppo di $\mathbb{Z}/6\mathbb{Z}$.

   (b) Dimostrare che, se G è abeliano di ordine una potenza di un numero primo, allora $\Gamma_m(G)$ è un sottogruppo di G per ogni m.

   (c) Dimostrare che, se un intero positivo n non è una potenza di un numero primo, allora $\Gamma_{n-1}(\mathbb{Z}/n\mathbb{Z})$ non è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$.

   (d) Fornire un esempio di un gruppo non abeliano G tale che $\Gamma_m(G)$ sia un sottogruppo di G per ogni m.

2. Sia A un dominio e sia $\psi\colon \mathbb{Q}[X] \to A$ un omomorfismo di anelli.

   (a) Dimostrare che $\ker(\psi)$ è un ideale primo di $\mathbb{Q}[X]$.

   (b) Dimostrare che, se ψ non è iniettivo, allora $\mathrm{im}(\psi)$ è un campo.

   (c) Dimostrare che, se $A = \mathbb{Q}$, allora $\psi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ ed esiste $q \in \mathbb{Q}$ tale che $\ker(\psi) = (X - q)$.

   (d) Dimostrare che è possibile che sia $A = \mathbb{R}$ e $\ker(\psi) = (X^5+4X+2)$.

Soluzioni

1. (a) I valori cercati sono 3, 4 e 5. Infatti in $\mathbb{Z}/6\mathbb{Z}$ si ha $\mathrm{ord}(\bar{0}) = 1$, $\mathrm{ord}(\bar{1}) = \mathrm{ord}(\bar{5}) = 6$, $\mathrm{ord}(\bar{2}) = \mathrm{ord}(\bar{4}) = 3$ e $\mathrm{ord}(\bar{3}) = 2$. Dunque

$$\Gamma_1(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0}\}, \qquad \Gamma_2(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0}, \bar{3}\} = \langle\bar{3}\rangle,$$
$$\Gamma_3(\mathbb{Z}/6\mathbb{Z}) = \Gamma_4(\mathbb{Z}/6\mathbb{Z}) = \Gamma_5(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\},$$
$$\Gamma_m(\mathbb{Z}/6\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z} \text{ per } m \geq 6,$$

e di questi sottoinsiemi di $\mathbb{Z}/6\mathbb{Z}$ l'unico che non è un sottogruppo è $\{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ (dato che, per esempio, contiene $\bar{2}$ e $\bar{3}$ ma non $\bar{2}+\bar{3} = \bar{5}$).

(b) Sia $\#G = p^l$ con p numero primo e $l \in \mathbb{N}$. Dato un intero positivo m, verifichiamo che $\Gamma_m(G)$ è un sottogruppo di G. Chiaramente $1_G \in \Gamma_m(G)$ perché $\mathrm{ord}(1_G) = 1 \leq m$. Dati $a, b \in \Gamma_m(G)$, per il teorema di Lagrange si ha $\mathrm{ord}(a) = p^i$ e $\mathrm{ord}(b) = p^j$ con $0 \leq i, j \leq l$ e $p^i, p^j \leq m$. A meno di scambiare a e b, si può supporre $i \leq j$. Allora $\mathrm{ord}(a), \mathrm{ord}(b) \mid p^j$, e dunque $a^{p^j} = b^{p^j} = 1_G$. Essendo $ab = ba$, segue che

$$(ab)^{p^j} = a^{p^j} b^{p^j} = 1_G 1_G = 1_G.$$

Pertanto $\mathrm{ord}(ab) \leq p^j \leq m$, cioè $ab \in \Gamma_m(G)$. Infine, se $a \in \Gamma_m(G)$, anche $a^{-1} \in \Gamma_m(G)$ perché $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$.

(c) Poiché n non è una potenza di un numero primo, esistono $a, b \in \mathbb{Z}$ tali che $n = ab$, $\mathrm{mcd}(a, b) = 1$ e $a, b > 1$ (da cui segue $a, b \leq n-1$). Essendo a e b coprimi, esistono $c, d \in \mathbb{Z}$ tali che $1 = ca + db$. Se ne deduce che $\Gamma_{n-1}(\mathbb{Z}/n\mathbb{Z})$ non è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ perché $\bar{a}, \bar{b} \in \Gamma_{n-1}(\mathbb{Z}/n\mathbb{Z})$ (dato che $\mathrm{ord}(\bar{a}) = b, \mathrm{ord}(\bar{b}) = a \leq n-1$), mentre

$$c\bar{a} + d\bar{b} = \overline{ca + db} = \bar{1} \notin \Gamma_{n-1}(\mathbb{Z}/n\mathbb{Z})$$

(dato che $\mathrm{ord}(\bar{1}) = n$).

(d) Si può prendere come G il gruppo $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ delle unità dei quaternioni. Infatti in Q si ha $\mathrm{ord}(1) = 1$, $\mathrm{ord}(-1) = 2$, e $\mathrm{ord}(a) = 4$ per $a \in Q \setminus \{\pm 1\}$. Dunque

$$\Gamma_1(Q) = \{1\}, \qquad \Gamma_2(Q) = \Gamma_3(Q) = \{\pm 1\} = \langle -1\rangle,$$
$$\Gamma_m(Q) = Q \text{ per } m \geq 4,$$

e questi sottoinsiemi di Q sono tutti sottogruppi.

2. (a) Poiché il nucleo di un omomorfismo di anelli è sempre un ideale, resta da dimostrare che $\ker(\psi)$ è primo. In effetti $1 \notin \ker(\psi)$ perché $\psi(1) = 1_A \neq 0_A$ (un dominio è in particolare un anello non banale). Inoltre, dati $f, g \in \mathbb{Q}[X]$ tali che $fg \in \ker(\psi)$, si ha $0_A = \psi(fg) = \psi(f)\psi(g)$, da cui segue (essendo A un dominio) $\psi(f) = 0_A$ o $\psi(g) = 0_A$, cioè $f \in \ker(\psi)$ o $g \in \ker(\psi)$.

   (b) Poiché ψ non è iniettivo, $\ker(\psi) \neq \{0\}$. D'altra parte $\ker(\psi)$ è un ideale primo per il punto precedente. Tenendo conto che $\mathbb{Q}[X]$ è un dominio a ideali principali (essendo $\mathbb{Q}$ un campo), questo implica che $\ker(\psi)$ è un ideale massimale. Per il primo teorema di isomorfismo per anelli si conclude allora che $\mathrm{im}(\psi) \cong \mathbb{Q}[X]/\ker(\psi)$ è un campo, dato che il quoziente di un anello commutativo per un ideale massimale è un campo.

   (c) $\psi|_{\mathbb{Z}} \colon \mathbb{Z} \to \mathbb{Q}$ è necessariamente l'inclusione (per ogni anello B esiste un unico omomorfismo di anelli $\mathbb{Z} \to B$). Dunque per ogni $ab^{-1} \in \mathbb{Q}$ (con $a, b \in \mathbb{Z}$ e $b \neq 0$) si ha

$$\psi(ab^{-1}) = \psi(a)\psi(b)^{-1} = ab^{-1},$$

   cioè $\psi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Posto $q := \psi(X) \in \mathbb{Q}$, si ha inoltre

$$\psi(X - q) = \psi(X) - \psi(q) = q - q = 0,$$

   cioè $X - q \in \ker(\psi)$. Essendo $\ker(\psi)$ un ideale, questo implica $(X - q) \subseteq \ker(\psi)$. Poiché $(X - q)$ è un ideale massimale (dato che $\mathbb{Q}[X]/(X - q) \cong \mathbb{Q}$ è un campo) e $\ker(\psi) \neq \mathbb{Q}[X]$ (per il primo punto), si conclude che $(X - q) = \ker(\psi)$.

   (d) Sia $r \in \mathbb{R}$ una radice di $g := X^5 + 4X + 2$ (si noti che una tale radice esiste perché $g \in \mathbb{R}[X]$ e $\deg(g) = 5$ è dispari). Allora la valutazione in r

$$\begin{aligned} \psi \colon \mathbb{Q}[X] &\to \mathbb{R} \\ f &\mapsto f(r) \end{aligned}$$

   è un omomorfismo di anelli, e resta da dimostrare che $\ker(\psi) = (g)$. Poiché $\psi(g) = g(r) = 0$, si ha $g \in \ker(\psi)$, e quindi $(g) \subseteq \ker(\psi)$. Come nel punto precedente, per concludere che tale inclusione è un'uguaglianza basta dimostrare che (g) è un ideale massimale di $\mathbb{Q}[X]$. Questo è vero perché $\mathbb{Q}[X]$ è un dominio a ideali principali e g è irriducibile in $\mathbb{Q}[X]$, dato che lo è in $\mathbb{Z}[X]$ per il criterio di Eisenstein relativo al primo 2.