Corso di Algebra 1 - a.a. 2018-2019

Prova scritta del 19/02/2019

1. Sia G il gruppo $D_3 \times \mathbb{Z}/3\mathbb{Z}$.
   (a) Quanti sottogruppi ciclici di ordine 6 ci sono in G?
   (b) Dimostrare che nessun sottogruppo ciclico di ordine 6 è normale in G.
   (c) Esiste un sottogruppo non normale di ordine 3 in G?

2. Sia G un gruppo non banale e sia T l'unione di tutti i sottogruppi propri di G (cioè diversi da G).
   (a) Dimostrare che, se G non è ciclico, allora $T = G$.
   (b) Dimostrare che, se G è ciclico, allora T è un sottogruppo di G se e solo se l'ordine di G è una potenza di un numero primo.

3. Indicando con $M_2(\mathbb{R})$ l'anello delle matrici 2×2 a coefficienti reali, sia
$$A := \left\{ \begin{pmatrix} n & a \\ 0 & b \end{pmatrix} \in M_2(\mathbb{R}) \,:\, n \in \mathbb{Z},\ a, b \in \mathbb{R} \right\}.$$
   Per ogni sottogruppo H di $\mathbb{R}$ sia inoltre
$$I_H := \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \,:\, a \in H \right\}.$$
   (a) Dimostrare che A è un sottoanello di $M_2(\mathbb{R})$.
   (b) Dimostrare che I_H è sempre un ideale sinistro di A e che I_H è un ideale destro di A se e solo se $H = \{0\}$ o $H = \mathbb{R}$.
   (c) Dimostrare che l'anello quoziente $A/I_{\mathbb{R}}$ è isomorfo a $\mathbb{Z} \times \mathbb{R}$.

4. Sia I l'ideale di $\mathbb{Z}[X]$ generato da $X^5 - 4X^3 + 5X^2 + 4X - 10$ e da $X^4 + X^3 - 2X^2 + 3X + 5$.
   (a) Dimostrare che $I = (X^3 - 2X + 5)$.
   (b) I è un ideale primo?
   (c) Dimostrare che, se $n > 1$ è un intero, allora $n + I$ non è nullo e non è invertibile nell'anello quoziente $\mathbb{Z}[X]/I$.

Soluzioni

1. (a) Un sottogruppo ciclico di ordine 6 è generato da un elemento di ordine 6. Vediamo quindi intanto quanti (e quali) sono gli elementi di ordine 6 di G. Se $g = (a, b) \in G$ (con $a \in D_3$ e $b \in \mathbb{Z}/3\mathbb{Z}$), $\mathrm{ord}(g) = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. Tenendo conto che $\mathrm{ord}(a)$ può essere 1, 2 o 3 e $\mathrm{ord}(b)$ 1 o 3, si ha $\mathrm{ord}(g) = 6$ se e solo se $\mathrm{ord}(a) = 2$ (cioè $a = R^i S$ con $i = 0, 1, 2$) e $\mathrm{ord}(b) = 3$ (cioè $b = \overline{j}$ con $j = 1, 2$). Ci sono dunque $3 \cdot 2 = 6$ elementi di ordine 6. Ciascun elemento di ordine 6 appartiene a un unico sottogruppo ciclico di ordine 6 (quello da lui generato) e d'altra parte ogni sottogruppo ciclico di ordine 6 contiene due elementi di ordine 6 (è isomorfo a $\mathbb{Z}/6\mathbb{Z}$, in cui gli elementi di ordine 6 sono $\overline{1}$ e $\overline{5}$). Se ne deduce che in G ci sono $6/2 = 3$ sottogruppi ciclici di ordine 6.

   (b) Da quanto visto nel punto precedente segue facilmente che i 3 sottogruppi ciclici di ordine 6 di G sono

$$H_i := \langle (R^i S, \overline{1}) \rangle = \langle (R^i S, \overline{2}) \rangle = \langle R^i S \rangle \times \mathbb{Z}/3\mathbb{Z}$$

   per $i = 0, 1, 2$. Nessuno di essi è normale, perché per esempio

$$(R, \overline{0})(R^i S, \overline{1})(R, \overline{0})^{-1} = (RR^i S R^{-1}, \overline{1}) = (R^{i+2} S, \overline{1}) \notin H_i.$$

   (c) Sì, esiste. Per esempio il sottogruppo H di G generato da $(R, \overline{1})$ ha ordine $\mathrm{mcm}(\mathrm{ord}(R), \mathrm{ord}(\overline{1})) = \mathrm{mcm}(3, 3) = 3$ e non è normale perché $H = \{(1, \overline{0}), (R, \overline{1}), (R^2, \overline{2})\}$ e

$$(S, \overline{0})(R, \overline{1})(S, \overline{0})^{-1} = (SRS^{-1}, \overline{1}) = (R^2, \overline{1}) \notin H.$$

2. (a) Per ogni $g \in G$ si ha $g \in \langle g \rangle$ (che è un sottogruppo di G) e $\langle g \rangle \neq G$ (perché G non è ciclico), dunque $g \in T$ per definizione di T.

   (b) Osserviamo che in generale $T = \{g \in G : \langle g \rangle \neq G\}$: ragionando come nel punto precedente si vede che ques'ultimo insieme è contenuto in T; viceversa, se $g \in T$, esiste un sottogruppo proprio H di G tale che $g \in H$, e quindi $\langle g \rangle \neq G$, dato che $\langle g \rangle \subseteq H$ (ricordiamo che $\langle g \rangle$ è il più piccolo sottogruppo di G contenente g). Supponiamo ora che G sia ciclico. Se G è infinito, G è isomorfo a $\mathbb{Z}$ e per tale gruppo si ha $T = \{a \in \mathbb{Z} : a \neq \pm 1\}$, che non è un sottogruppo di $\mathbb{Z}$ ($3, 2 \in T$ ma $3 - 2 = 1 \notin T$). Se G è finito, G è isomorfo a $\mathbb{Z}/n\mathbb{Z}$ per qualche intero $n > 1$, e

per tale gruppo si ha $T = \mathbb{Z}/n\mathbb{Z} \setminus \mathbb{Z}/n\mathbb{Z}^*$. Se $n = p^k$ con p primo e $k > 0$, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$ se e solo se $p \nmid a$, e quindi $T = \langle \overline{p} \rangle$ è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$. Altrimenti esistono $a, b > 1$ tali che $n = ab$ e $\mathrm{mcd}(a, b) = 1$. Dato che $\mathrm{mcd}(a, n) = a > 1$, $\mathrm{mcd}(b, n) = b > 1$, mentre $\mathrm{mcd}(a + b, n) = 1$ (ciò segue dal fatto che $\mathrm{mcd}(a + b, a) = \mathrm{mcd}(a + b - a, a) = \mathrm{mcd}(b, a) = 1$ e analogamente $\mathrm{mcd}(a + b, b) = 1$), si ottiene $\overline{a}, \overline{b} \in T$ e $\overline{a} + \overline{b} = \overline{a + b} \notin T$, il che dimostra che T non è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$.

3. (a) La matrice identità appartiene evidentemente ad A. Siano

$$\begin{pmatrix} n & a \\ 0 & b \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} n' & a' \\ 0 & b' \end{pmatrix}$$

due elementi di A. Allora

$$\begin{pmatrix} n & a \\ 0 & b \end{pmatrix} + \begin{pmatrix} n' & a' \\ 0 & b' \end{pmatrix} = \begin{pmatrix} n + n' & a + a' \\ 0 & b + b' \end{pmatrix} \in A,$$

$$- \begin{pmatrix} n & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} -n & -a \\ 0 & -b \end{pmatrix} \in A,$$

$$\begin{pmatrix} n & a \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} n' & a' \\ 0 & b' \end{pmatrix} = \begin{pmatrix} nn' & na' + ab' \\ 0 & bb' \end{pmatrix} \in A.$$

Questo dimostra che A è un sottoanello di $M_2(\mathbb{R})$.

(b) Se $H \subset \mathbb{R}$ è un sottogruppo, I_H è un sottogruppo di A perché

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & a' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a - a' \\ 0 & 0 \end{pmatrix} \in I_H$$

per ogni $a, a' \in H$ (e contiene la matrice nulla). Inoltre, se $a' \in H$,

$$\begin{pmatrix} n & a \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & a' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & na' \\ 0 & 0 \end{pmatrix} \in I_H.$$

Dunque I_H è un ideale sinistro. D'altra parte

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} n' & a' \\ 0 & b' \end{pmatrix} = \begin{pmatrix} 0 & ab' \\ 0 & 0 \end{pmatrix} \in I_{\mathbb{R}}.$$

Quindi $I_{\mathbb{R}}$ è anche un ideale destro. $I_{\{0\}}$ contiene solo la matrice nulla ed è chiaramente un ideale destro. Invece se $\{0\} \subsetneq H \subsetneq \mathbb{R}$, allora esiste $a \in H$, $a \neq 0$ ed esiste $c \in \mathbb{R} \setminus H$. Posto $b' := c/a \in \mathbb{R}$, dalla formula sopra otteniamo

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & b' \end{pmatrix} = \begin{pmatrix} 0 & ab' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \notin I_H.$$

Dunque in questo caso I_H non è un ideale destro.

(c) Consideriamo l'applicazione $f : A \to \mathbb{Z} \times \mathbb{R}$,

$$f\begin{pmatrix} n & a \\ 0 & b \end{pmatrix} := (n, b).$$

Segue immediatamente dalle formule sopra che f è un omomorfismo di anelli. Inoltre è chiaramente suriettivo, mentre $\operatorname{Ker} f = I_{\mathbb{R}}$. Dal primo teorema di isomorfismo per anelli otteniamo $A/I_{\mathbb{R}} \cong \mathbb{Z} \times \mathbb{R}$.

4. (a) Poniamo

$$f(X) = X^5 - 4X^3 + 5X^2 + 4X - 10,$$
$$g(X) = X^4 + X^3 - 2X^2 + 3X + 5,$$
$$h(X) = X^3 - 2X + 5.$$

Dividendo f per h otteniamo $f = (X^2 - 2)h$. Dividendo g per h otteniamo $g = (X + 1)h$. Quindi $I = (f, g) \subset (h)$. D'altro canto $1 = (X-1)(X+1)-(X^2-2)$. Dunque $h = (X-1)g-f$ e quindi $(h) \subset I$.

(b) Siccome $\mathbb{Z}[X]$ è un dominio a fattorizzazione unica, basta verificare che h è un elemento irriducibile di $\mathbb{Z}[X]$. Ogni radice di h in $\mathbb{Q}$ è intera, perché h è monico, e deve dividere 5. Si verifica che ± 1 e ± 5 non sono radici di h. Dunque h non ha radici in $\mathbb{Q}$. Siccome è di grado 3, h è irriducibile in $\mathbb{Q}[X]$. Essendo un polinomio primitivo è irriducibile anche in $\mathbb{Z}[X]$.

(c) Sia $n \in \mathbb{Z}$, $n > 1$. Gli elementi di I sono i multipli di h. Quindi (a parte il polinomio nullo) essi sono polinomi di grado almeno 3. Pertanto $n \notin I$ e di conseguenza $n + I \neq 0$ in $\mathbb{Z}[X]/I$. Proviamo che $n+I$ non è invertibile. Se fosse invertibile esisterebbe $p \in \mathbb{Z}[X]$ tale che $(p + I)(n + I) = 1 + I$, ossia $np - 1 \in I$, ossia

$$1 - np = qh.$$

per un certo $q \in \mathbb{Z}[X]$. Considerando l'equazione sopra modulo n, otteniamo $\overline{1} = \overline{q}\overline{h}$ in $\mathbb{Z}/n\mathbb{Z}[X]$. Ma siccome $\overline{h}$ è monico e $\deg(\overline{h}) = 3$, $\deg(\overline{q}\overline{h}) = \deg(\overline{q}) + 3 \geq 3$ se $\overline{q} \neq \overline{0}$. Dunque $\overline{1} \neq \overline{q}\overline{h}$ per ogni $q \in \mathbb{Z}[X]$. Abbiamo dimostrato che l'equazione sopra non può valere. Pertanto n non è invertibile in $\mathbb{Z}[X]/I$.