Corso di Algebra 1 - a.a. 2015-2016

Prova scritta del 22.1.2016

1. Sia G il gruppo $D_4 \times \mathbb{Z}/8\mathbb{Z}$.
   (a) Quanti elementi di ordine 8 ci sono in G?
   (b) Stabilire se G è isomorfo a $D_8 \times \mathbb{Z}/4\mathbb{Z}$.
   (c) Trovare un sottogruppo non normale di G di ordine 16.

2. Dato un intero positivo n, sia
$$f\colon S_n \to S_{n+2}$$
$$\sigma \mapsto (n+1, n+2)^{\frac{1-\varepsilon(\sigma)}{2}} \widetilde{\sigma},$$
dove $\varepsilon(\sigma) \in \{\pm 1\}$ indica il segno di σ, e $\widetilde{\sigma} \in S_{n+2}$ è la permutazione definita come σ su $\{1, \dots, n\}$ e tale che $\widetilde{\sigma}(n+i) = n+i$ per $i = 1, 2$.
   (a) Dimostrare che f è un omomorfismo di gruppi.
   (b) Dimostrare che f è iniettivo e che l'immagine di f è contenuta in A_{n+2}.
   (c) Dimostrare che per ogni gruppo finito G esiste un intero positivo m tale che G è isomorfo a un sottogruppo di A_m.

3. Sia K un campo e si consideri
$$A := \{\sum_{i \geq 0} a_i X^i \in K[X] \,:\, a_1 = 0\}.$$
   (a) Dimostrare che A è un sottoanello di $K[X]$ e che $A^* = K \setminus \{0\}$.
   (b) Dimostrare che X^2 è irriducibile in A.
   (c) L'ideale generato da X^2 è primo in A?

4. Stabilire se ciascuno dei seguenti polinomi
$$p_1(X) = X^3 + 4X^2 + 6X + 4$$
$$p_2(X) = 25X^3 + 5X + 15$$
$$p_3(X) = X^5 + 5X + 1$$
è irriducibile in $A[X]$ in ciascuno dei seguenti casi:
   (a) $A = \mathbb{Z}$;
   (b) $A = \mathbb{Q}$;
   (c) $A = \mathbb{Z}/2\mathbb{Z}$.

Soluzioni

1. (a) Per un elemento $g = (g_1, g_2) \in G$ vale

$$\mathrm{ord}(g) = \mathrm{mcm}(\mathrm{ord}(g_1), \mathrm{ord}(g_2)).$$

I possibili valori di $\mathrm{ord}(g_1)$ sono $1, 2, 4$, mentre quelli di $\mathrm{ord}(g_2)$ sono $1, 2, 4, 8$. Dunque $\mathrm{ord}(g) = 8$ se e solo se $\mathrm{ord}(g_2) = 8$. È allora chiaro che g_1 può essere uno qualunque degli 8 elementi di D_4, mentre g_2 può essere uno dei 4 elementi di ordine 8 di $\mathbb{Z}/8\mathbb{Z}$ (cioè $\overline{1}, \overline{3}, \overline{5}, \overline{7}$). Gli elementi cercati sono quindi $8 \cdot 4 = 32$.

(b) Dato $g = (g_1, g_2) \in D_8 \times \mathbb{Z}/4\mathbb{Z}$, i possibili valori di $\mathrm{ord}(g_1)$ sono $1, 2, 4, 8$, mentre quelli di $\mathrm{ord}(g_2)$ sono $1, 2, 4$. Ragionando come nel punto precedente, questa volta si ha $\mathrm{ord}(g) = 8$ se e solo se $\mathrm{ord}(g_1) = 8$. Allora ci sono 4 possibilità sia per g_1 (cioè R, R^3, R^5, R^7) che per g_2 (qualunque elemento di $\mathbb{Z}/4\mathbb{Z}$), per cui $D_8 \times \mathbb{Z}/4\mathbb{Z}$ ha $4 \cdot 4 = 16$ elementi di ordine 8. Se ne deduce che G non è isomorfo a $D_8 \times \mathbb{Z}/4\mathbb{Z}$.

(c) Sia $H := \{1, S\} \times \mathbb{Z}/8\mathbb{Z} \subset G$. Chiaramente $H \neq \emptyset$ e, dati $a, b \in H$ (con $a = (a_1, a_2)$ e $b = (b_1, b_2)$), si ha

$$ab = (a_1 b_1, a_2 b_2) \in H,$$

essendo $\{1, S\} = \langle S \rangle$ un sottogruppo di D_4. Ciò basta a concludere che H è un sottogruppo di G, visto che H è finito. D'altra parte, presi $g = (R, \overline{0}) \in G$ e $h = (S, \overline{0}) \in H$, si ha

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

il che mostra che H non è normale in G.

2. (a) Posto $\rho := (n+1, n+2) \in S_{n+2}$ e $\varepsilon'(\sigma) := \frac{1-\varepsilon(\sigma)}{2} \in \{0, 1\}$, per ogni $\sigma, \tau \in S_n$ si ha

$$f(\sigma) f(\tau) = \rho^{\varepsilon'(\sigma)} \widetilde{\sigma} \rho^{\varepsilon'(\tau)} \widetilde{\tau} = \rho^{\varepsilon'(\sigma)} \rho^{\varepsilon'(\tau)} \widetilde{\sigma}\widetilde{\tau} = \rho^{\varepsilon'(\sigma)+\varepsilon'(\tau)} \widetilde{\sigma\tau},$$

considerando che $\widetilde{\sigma}$ e ρ commutano (perché $\widetilde{\sigma}$ lascia fissi $n+1$ e $n+2$) e che chiaramente $\widetilde{\sigma}\widetilde{\tau} = \widetilde{\sigma\tau}$. D'altra parte,

$$f(\sigma\tau) = \rho^{\varepsilon'(\sigma\tau)} \widetilde{\sigma\tau},$$

per cui $f(\sigma\tau) = f(\sigma)f(\tau)$ se e solo se $\rho^{\varepsilon'(\sigma\tau)} = \rho^{\varepsilon'(\sigma)+\varepsilon'(\tau)}$. Avendo ρ ordine 2, quest'ultima uguaglianza vale se e solo se

$$\varepsilon'(\sigma\tau) \equiv \varepsilon'(\sigma) + \varepsilon'(\tau) \mod 2,$$

cioè se l'intero

$$\varepsilon'(\sigma) + \varepsilon'(\tau) - \varepsilon'(\sigma\tau) = \frac{1 - \varepsilon(\sigma) + 1 - \varepsilon(\tau) - 1 + \varepsilon(\sigma\tau)}{2}$$

è pari. Ciò in effetti è vero perché il numeratore di questa frazione si può riscrivere (tenendo conto che $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$) come

$$(1 - \varepsilon(\sigma))(1 - \varepsilon(\tau)),$$

e quindi è un multiplo di 4 (dato che ciascuno dei due fattori può valere 0 o 2). Questo dimostra che f è un omomorfismo.

(b) Dato $\sigma \in \ker(f)$, per definizione si ha $f(\sigma)(i) = i$ per ogni $1 \leq i \leq n+2$. In particolare, per $1 \leq i \leq n$ vale

$$i = f(\sigma)(i) = \widetilde{\sigma}(i) = \sigma(i),$$

cioè σ è l'elemento neutro di S_n, e pertanto f è iniettivo.
Ricordando che $\varepsilon(\rho) = -1$, per ogni $\sigma \in S_n$ si ha

$$\varepsilon(f(\sigma)) = \varepsilon(\rho^{\varepsilon'(\sigma)}\widetilde{\sigma}) = \varepsilon(\rho^{\varepsilon'(\sigma)})\varepsilon(\widetilde{\sigma}) = (-1)^{\varepsilon'(\sigma)}\varepsilon(\sigma)$$

(ovviamente $\varepsilon(\widetilde{\sigma}) = \varepsilon(\sigma)$). Osservando che $(-1)^{\varepsilon'(\sigma)} = \varepsilon(\sigma)$, si ottiene allora $\varepsilon(f(\sigma)) = 1$, cioè $f(\sigma) \in A_{n+2}$.

(c) Per il teorema di Cayley esiste un intero positivo n tale che G è isomorfo a un sottogruppo H di S_n (in particolare, si può prendere $n = \#G$). Allora $H' := f(H)$ è un sottogruppo di A_{n+2} (perché f è un omomorfismo la cui immagine è contenuta in A_{n+2}) e $H' \cong H$ (perché f è un omomorfismo iniettivo). Si ottiene quindi $G \cong H'$, come richiesto.

3. (a) Chiaramente $1 \in A$ e, dati $p = \sum_{i\geq 0} a_i X^i$, $q = \sum_{i\geq 0} b_i X^i \in A$ (quindi con $a_1 = b_1 = 0$), si ha

$$p - q = \sum_{i\geq 0} c_i X^i, \qquad pq = \sum_{i\geq 0} d_i X^i$$

con $c_1 = a_1 - b_1 = 0$ e $d_1 = a_0 b_1 + a_1 b_0 = 0$. Dunque $p-q$, $pq \in A$ e A risulta un sottoanello di $K[X]$. Questo implica che $A^* \subseteq K[X]^*$

(un elemento invertibile in A è ovviamente invertibile anche in $K[X]$). D'altra parte K è un sottoanello di A (dato che K è un sottoanello di $K[X]$ e $K \subset A$), quindi anche $K^* \subseteq A^*$. Poiché

$$K[X]^* = K^* = K \setminus \{0\}$$

(essendo K un campo) si conclude che $A^* = K \setminus \{0\}$.

(b) $X^2 \neq 0$ e, per il punto precedente, $X^2 \notin A^*$. Resta allora da dimostrare che, dati $p, q \in A$ tali che $pq = X^2$, vale $p \in A^*$ o $q \in A^*$. Ricordando che $K[X]$ è un dominio a fattorizzazione unica e che X è irriducibile in $K[X]$, l'unicità della fattorizzazione di X^2 implica che uno tra p e q è invertibile, oppure che entrambi sono associati a X in $K[X]$. Quest'ultima possibilità è però esclusa, dato che gli elementi associati a X in $K[X]$ sono quelli della forma aX con $a \in K \setminus \{0\}$, e dunque non appartengono ad A. Deve essere allora $p \in A^*$ o $q \in A^*$, tenendo conto che $A^* = K[X]^*$.

(c) L'ideale X^2A non è primo in A. Ciò si può verificare osservando che $X^3 \notin X^2A$ (perché l'unico elemento $p \in K[X]$ tale che $X^3 = X^2p$ è $p = X$ e $X \notin A$), ma

$$X^3X^3 = X^6 = X^2X^4 \in X^2A.$$

4. (a) Essendo primitivo, p_1 è irriducibile in $\mathbb{Z}[X]$ se e solo se lo è in $\mathbb{Q}[X]$. Poiché inoltre è di terzo grado, è irriducibile se e solo se non ha radici in $\mathbb{Q}$. Le eventuali radici di p_1 possono essere solo $\pm 1, \pm 2, \pm 4$. È immediato verificare che -2 è una radice, per cui p_1 non è irriducibile (in effetti la sua fattorizzazione è $p_1 = (X+2)(X^2+2X+2)$).
p_2 non è irriducibile perché non è primitivo (il suo contenuto è infatti $\mathrm{mcd}(25, 5, 15) = 5$).
Posto $q_3(X) := p_3(X-1)$, si ha

$$q_3 = (X-1)^5 + 5(X-1) + 1 = X^5 - 5X^4 + 10X^3 - 10X^2 + 10X - 5.$$

Allora q_3 è irriducibile per il criterio di Eisenstein relativo al primo 5, e questo implica che anche p_3 è irriducibile.

(b) Si è già visto nel punto precedente che p_1 non è irriducibile.
Chiaramente p_2 è irriducibile se e solo se lo è

$$q_2 := \frac{p_2}{5} = 5X^3 + X + 3.$$

Si verifica facilmente che nessuno dei numeri $\pm 1, \pm 3, \pm\frac{1}{5}, \pm\frac{3}{5}$ è radice di q_2. Essendo di terzo grado, ciò implica che q_2 (e quindi p_2) è irriducibile. In alternativa si può osservare che q_2 (che è primitivo in $\mathbb{Z}[X]$) è irriducibile in $\mathbb{Z}[X]$ (e dunque anche in $\mathbb{Q}[X]$) perché lo è la sua riduzione modulo 2 (che coincide con quella di p_2).
p_3 è irriducibile in $\mathbb{Q}[X]$ perché è primitivo e irriducibile in $\mathbb{Z}[X]$, come visto nel punto precedente.

(c) Ovviamente $p_1 = X^3$ non è irriducibile.
$p_2 = X^3 + X + 1$ è irriducibile perché è di terzo grado e non ha radici.
$p_3 = X^5 + X + 1$ non ha radici, ma non è irriducibile perché è divisibile per l'unico polinomio irriducibile di secondo grado (cioè $X^2 + X + 1$). Risulta infatti $p_3 = (X^2 + X + 1)(X^3 + X^2 + 1)$.