Corso di Algebra 1 - a.a. 2021-2022

Prova scritta del 07/09/2022

1. Sia $G := \{(\sigma, a) \in S_4 \times D_5 \,:\, \sigma \in A_4 \iff a \in \langle R \rangle\}$.
   (a) Dimostrare che G è un sottogruppo di $S_4 \times D_5$.
   (b) Dimostrare che G non è isomorfo a S_5.
   (c) Dimostrare che esiste un omomorfismo suriettivo $G \to S_4$.
   (d) Dimostrare che esiste un omomorfismo iniettivo $S_4 \to G$.

2. Sia $f \in \mathbb{Z}[X]$ monico e sia $\overline{f} \in \mathbb{Z}/2\mathbb{Z}[X]$ la riduzione di f modulo 2. Siano inoltre $A := \mathbb{Q}[X]/(f)$ e $B := \mathbb{Z}/2\mathbb{Z}[X]/(\overline{f})$.
   (a) Dimostrare che, se B è un campo, allora A è un campo.
   (b) È vero che, se $\overline{f} = X^4 + X^3 + X^2 + X + 1$, allora A è un campo?
   (c) Dimostrare che, se $\overline{f} = X^4 + X^3 + X^2 + 1$ e f non ha radici razionali, allora A è un campo.
   (d) Fornire un esempio in cui $\overline{f} = X^4 + X^3 + X + 1$, f non ha radici razionali e A non è un campo.

Soluzioni

1. (a) Chiaramente $(1,1) \in G$, dato che $1 \in A_4$ e $1 \in \langle R \rangle$. Essendo poi $S_4 \times D_5$ finito, per concludere basta dimostrare che, se $(\sigma, a), (\tau, b) \in G$, allora anche $(\sigma, a)(\tau, b) = (\sigma\tau, ab) \in G$. Osserviamo che $\sigma\tau \in A_4$ se e solo se $\sigma, \tau \in A_4$ o $\sigma, \tau \notin A_4$ e analogamente $ab \in \langle R \rangle$ se e solo se $a, b \in \langle R \rangle$ o $a, b \notin \langle R \rangle$: ciò può essere verificato direttamente nei due casi ricordando come sono definite le operazioni in S_4 e in D_5, ma è anche molto facile vedere che è conseguenza del fatto che $[S_4 : A_4] = [D_5 : \langle R \rangle] = 2$. Poiché, per ipotesi, $\sigma \in A_4$ se e solo se $a \in \langle R \rangle$ e $\tau \in A_4$ se e solo se $b \in \langle R \rangle$, se ne deduce subito che $\sigma\tau \in A_4$ se e solo se $ab \in \langle R \rangle$, cioè $(\sigma\tau, ab) \in G$.

   (b) Basta per esempio notare che $g := ((1,2,3), R) \in G$ ha ordine $\operatorname{mcm}(\operatorname{ord}((1,2,3)), \operatorname{ord}(R)) = \operatorname{mcm}(3,5) = 15$, mentre S_5 non contiene elementi di ordine 15.

   (c) La funzione $p\colon G \to S_4$, $(\sigma, a) \mapsto \sigma$ è un omomorfismo perché

$$p((\sigma, a)(\tau, b)) = p((\sigma\tau, ab)) = \sigma\tau = p((\sigma, a))p((\tau, b))$$

   per ogni $(\sigma, a), (\tau, b) \in G$. Inoltre p è suriettivo perché per ogni $\sigma \in S_4$ si ha $\sigma = p((\sigma, 1))$ se $\sigma \in A_4$ e $\sigma = p((\sigma, S))$ se $\sigma \notin A_4$.

   (d) Basta dimostrare che esiste un omomorfismo $f\colon S_4 \to D_5$ tale che $f^{-1}(\langle R \rangle) = A_4$. Infatti, supponendo che tale f esista, la funzione $\tilde{f}\colon S_4 \to S_4 \times D_5$, $\sigma \mapsto (\sigma, f(\sigma))$è un omomorfismo perché

$$\begin{aligned}\tilde{f}(\sigma\tau) = (\sigma\tau, f(\sigma\tau)) &= (\sigma\tau, f(\sigma)f(\tau)) \\ &= (\sigma, f(\sigma))(\tau, f(\tau)) = \tilde{f}(\sigma)\tilde{f}(\tau)\end{aligned}$$

   per ogni $\sigma, \tau \in S_4$. Poiché $\sigma \in A_4 = f^{-1}(\langle R \rangle)$ se e solo se $f(\sigma) \in \langle R \rangle$, per definizione $\tilde{f}(\sigma) \in G$ per ogni $\sigma \in S_4$, e dunque $\tilde{f}$ può essere considerato un omomorfismo $S_4 \to G$. Inoltre $\tilde{f}$ è iniettivo perché $p \circ \tilde{f} = \mathrm{id}_{S_4}$ è iniettivo (p è l'omomorfismo del punto precedente). Infine è facile vedere che

$$\begin{aligned} f\colon S_4 &\to D_5 \\ \sigma &\mapsto \begin{cases} 1 & \text{se } \sigma \in A_4 \\ S & \text{se } \sigma \notin A_4 \end{cases}\end{aligned}$$

   è un omomorfismo (è composizione dell'omomorfismo segno $\epsilon\colon S_4 \to \{\pm 1\}$ con l'isomorfismo $\{\pm 1\} \to \langle S \rangle = \{1, S\}$ e con l'inclusione $\langle S \rangle \to D_5$), e chiaramente $f^{-1}(\langle R \rangle) = A_4$.

2. Osserviamo che A è un campo se e solo se l'ideale (f) è massimale in $\mathbb{Q}[x]$ se e solo se f è irriducibile in $\mathbb{Q}[X]$ (perché $\mathbb{Q}[X]$ è un dominio a ideali principali, dato che $\mathbb{Q}$ è un campo). Analogamente B è un campo se e solo se $\overline{f}$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$.

   (a) Per quanto appena detto $\overline{f}$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$, e questo implica (essendo f monico) che f è irriducibile in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$, per cui A è un campo.

   (b) Sì: per il punto precedente basta dimostrare che $\overline{f}$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$, e questo è vero perché $\overline{f}$ è di quarto grado, senza radici in $\mathbb{Z}/2\mathbb{Z}$ e non divisibile per $X^2 + X + 1$ (che è l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}/2\mathbb{Z}[X]$).

   (c) Supponiamo per assurdo che A non sia un campo, e quindi, come visto, che f sia riducibile in $\mathbb{Q}[X]$. Essendo f monico e senza radici razionali, devono allora esistere $g, h \in \mathbb{Z}[X]$ tali che $f = gh$ e $\deg(g) = \deg(h) = 2$. Poiché $\overline{f} = \overline{g}\overline{h}$, ogni fattore irriducibile di $\overline{f}$ deve dividere $\overline{g}$ o $\overline{h}$ (essendo $\mathbb{Z}/2\mathbb{Z}[X]$ un dominio a fattorizzazione unica) e pertanto ha grado al più 2. Questo porta a un assurdo perché invece $\overline{f} = (X+1)(X^3+X+1)$ e X^3+X+1 è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$ (essendo di terzo grado e senza radici in $\mathbb{Z}/2\mathbb{Z}$).

   (d) Si può prendere per esempio $f = X^4 + X^3 + 2X^2 + X + 1$, perché $f = (X^2+1)(X^2+X+1)$ non è irriducibile (e dunque A non è un campo) e non ha radici razionali (dato che non ne hanno $X^2 + 1$ e $X^2 + X + 1$).