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

Prova scritta del 25/01/2022

1. Dato un omomorfismo di gruppi $f\colon G \to G$, sia $\tilde{f}\colon G \to G$ la funzione definita da $\tilde{f}(a) := af(a)$.

   (a) Dimostrare che $\tilde{f}$ è un omomorfismo se e solo se $\mathrm{im}(f) \subseteq Z(G)$.

   (b) Dimostrare che, se $\tilde{f}$ è un omomorfismo, allora $\ker(\tilde{f}) \subseteq Z(G)$.

   (c) Dimostrare che, se $\tilde{f}$ è un omomorfismo, allora $[G,G] \subseteq \ker(f) \subseteq \mathrm{im}(\tilde{f})$.

   (d) Dimostrare che, se $\tilde{f}$ è un omomorfismo e $G = D_4$, allora $\tilde{f}$ è un isomorfismo.

2. Siano $f := 2X^4 + 2X^3 - 2X^2 + 2$ e $g := X^5 + X^3 + X^2 - 2X + 2$.

   (a) Fattorizzare f come prodotto di irriducibili in $\mathbb{Z}[X]$.

   (b) Trovare $h \in \mathbb{Z}[X]$ monico tale che $(f,g) = (h)$ in $\mathbb{Q}[X]$.

   (c) È vero che $(f,g) = (h)$ in $\mathbb{Z}[X]$?

   (d) Trovare un numero primo p tale che esista un omomorfismo di anelli $\mathbb{Z}[X]/(h) \to \mathbb{Z}/p\mathbb{Z}$.

Soluzioni

1. (a) Per definizione $\tilde{f}$ è un omomorfismo se e solo se $\tilde{f}(ab) = \tilde{f}(a)\tilde{f}(b)$ per ogni $a, b \in G$. Poiché

$$\tilde{f}(ab) = abf(ab) = abf(a)f(b),$$
$$\tilde{f}(a)\tilde{f}(b) = af(a)bf(b),$$

per le leggi di cancellazione $\tilde{f}(ab) = \tilde{f}(a)\tilde{f}(b)$ se e solo se $bf(a) = f(a)b$. Dunque $\tilde{f}$ è un omomorfismo se e solo se

$$f(a) \in Z(G) = \{g \in G \,:\, bg = gb \;\forall\, b \in G\}$$

per ogni $a \in G$, se e solo se $\mathrm{im}(f) \subseteq Z(G)$.

(b) Se $a \in \ker(\tilde{f})$, allora $1 = \tilde{f}(a) = af(a)$, da cui segue

$$a = f(a)^{-1} = f(a^{-1}) \in \mathrm{im}(f).$$

Poiché $\mathrm{im}(f) \subseteq Z(G)$ per il punto (a), si conclude che $a \in Z(G)$.

(c) Essendo $\ker(f)$ un sottogruppo normale di G, si ha $[G, G] \subseteq \ker(f)$ se e solo se $G/\ker(f)$ è abeliano. In effetti $G/\ker(f)$ è abeliano perché, per il primo teorema di isomorfismo, è isomorfo a $\mathrm{im}(f)$, che è abeliano in quanto sottogruppo del gruppo abeliano $Z(G)$ (sempre per il punto (a)).
Si ha inoltre $\ker(f) \subseteq \mathrm{im}(\tilde{f})$ perché, se $a \in \ker(f)$, allora

$$\tilde{f}(a) = af(a) = a1 = a,$$

il che dimostra $a \in \mathrm{im}(\tilde{f})$.

(d) Essendo D_4 finito, basta dimostrare che $\tilde{f}$ è iniettivo, cioè $\ker(\tilde{f}) = \{1\}$. Supponiamo quindi per assurdo che sia $\ker(\tilde{f}) \neq \{1\}$. Per il punto (b) $\ker(\tilde{f}) \subseteq Z(D_4)$, quindi, tenendo conto che $Z(D_4) = \{1, R^2\}$, deve essere $R^2 \in \ker(\tilde{f})$. Come nella dimostrazione del punto (b) da ciò segue

$$R^2 = f((R^2)^{-1}) = f(R^2) = f(R)^2.$$

Ma questo è impossibile perché $f(R)^2 = 1$, dato che $f(R) \in Z(D_4) = \{1, R^2\}$ per il punto (a).

2. (a) Chiaramente $f = 2f_1$ con $f_1 := X^4 + X^3 - X^2 + 1$ e 2 è irriducibile in $\mathbb{Z}$, quindi anche in $\mathbb{Z}[X]$. Le eventuali radici razionali di f_1 possono essere solo 1 o -1; si verifica che in effetti $f_1(-1) = 0$, e risulta $f_1 = (X+1)(X^3 - X + 1)$. Analogamente si vede che $X^3 - X + 1$ non ha radici razionali, dunque (avendo grado 3) è irriducibile in $\mathbb{Q}[X]$, come pure ovviamente $X + 1$. Inoltre questi due fattori di f_1 sono irriducibili anche in $\mathbb{Z}[X]$ (perché primitivi), quindi la fattorizzazione cercata è

$$f = 2(X+1)(X^3 - X + 1).$$

(b) Risulta $h = X^3 - X + 1$: si verifica infatti facilmente che, dei due fattori irriducibili di f in $\mathbb{Q}[X]$ (cioè $X + 1$ e h), solo h divide $g = (X^2 + 2)h$. Essendo $\mathbb{Q}[X]$ un dominio a ideali principali, se ne deduce che $\mathrm{mcd}(f, g) = h$, quindi $(f, g) = (h)$ in $\mathbb{Q}[X]$.

(c) No, non è vero. Se lo fosse, esisterebbero $s, t \in \mathbb{Z}[X]$ tali che

$$h = fs + gt = 2(X+1)hs + (X^2+2)ht = [(2X+2)s + (X^2+2)t]h,$$

e dunque (essendo $\mathbb{Z}[X]$ un dominio e $h \neq 0$)

$$1 = (2X + 2)s + (X^2 + 2)t.$$

Ma quest'ultima uguaglianza è impossibile perché nel polinomio a secondo membro il coefficiente del termine di grado 0 è pari.

(d) Basta prendere un numero primo p tale che $h(a)$ sia divisibile per p per qualche intero a (cioè tale che h abbia una radice in $\mathbb{Z}/p\mathbb{Z}$), per esempio $p = 5$ con $a = 3$. Infatti, indicando con $\alpha\colon \mathbb{Z}[X] \to \mathbb{Z}$ l'omomorfismo dato dalla valutazione in a (cioè $\alpha(u) = u(a)$ per ogni $u \in \mathbb{Z}[X]$) e con $\pi\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la proiezione al quoziente, si ottiene un omomorfismo di anelli

$$\beta = \pi \circ \alpha\colon \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}.$$

Per ipotesi $\beta(h) = \pi(\alpha(h)) = \pi(h(a)) = \overline{0}$, cioè $h \in \ker(\beta)$, e quindi $(h) \subseteq \ker(\beta)$. Per il teorema di omomorfismo si ottiene allora un omomorfismo di anelli $\gamma\colon \mathbb{Z}[X]/(h) \to \mathbb{Z}/p\mathbb{Z}$ (tale che $\gamma(u + (h)) = \beta(u)$ per ogni $u \in \mathbb{Z}[X]$).