**Corso di Algebra 1 - a.a. 2023-2024**

*Prova scritta del 02/07/2024*

1. Sia $G$ un gruppo e sia $H$ un sottogruppo di $G$. Stabilire se esiste un omomorfismo suriettivo $G \to H$ in ciascuno dei seguenti casi.
   (a) $G = \mathbb{Z}$ e $H = 6\mathbb{Z}$.
   (b) $G = \mathbb{Q}$ e $H = \mathbb{Z}$.
   (c) $G = S_3$ e $H = A_3$.
   (d) $G = A_4$ e $H$ è generato da un 3-ciclo.
2. Sia $A := \mathbb{Z}[X]/(2X)$ e si indichi con $\pi\colon \mathbb{Z}[X] \to A$ la proiezione al quoziente.
   (a) Stabilire se $A$ è un dominio.
   (b) Dimostrare che $\pi(2)$ e $\pi(X)$ generano due ideali primi di $A$.
   (c) Dimostrare che $\pi(p)$ genera un ideale massimale di $A$ per ogni numero primo dispari $p$.
   (d) Stabilire se $\pi(X^4 + X + 1)$ genera un ideale massimale di $A$.

*Soluzioni*

1. (a) Sì, esiste. Infatti la funzione $f\colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 6n$ è un omomorfismo iniettivo di gruppi con immagine $6\mathbb{Z}$, e dunque induce un isomorfismo $\mathbb{Z} \to 6\mathbb{Z}$.

   (b) No, non esiste. Se per assurdo esistesse un omomorfismo suriettivo $f\colon \mathbb{Q} \to \mathbb{Z}$, esisterebbe $q \in \mathbb{Q}$ tale che $f(q) = 1$, e dunque l'intero $f(q/2)$ soddisferebbe l'equazione

$$1 = f(q) = f(q/2 + q/2) = f(q/2) + f(q/2) = 2f(q/2),$$

   il che è impossibile.

   (c) No, non esiste. Se per assurdo esistesse un omomorfismo suriettivo $f\colon S_3 \to A_3$, per il primo teorema di isomorfismo si avrebbe

$$A_3 = \operatorname{im}(f) \cong S_3/\ker(f),$$

   e quindi $\ker(f)$ sarebbe un sottogruppo normale di $S_3$ di ordine (per il teorema di Lagrange) $(\#S_3)/(\#A_3) = 6/3 = 2$. Si ottiene allora una contraddizione perché $S_3$ non contiene sottogruppi normali di ordine 2.

   (d) Sì, esiste. Infatti $V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ è un sottogruppo normale di $A_4$ e (per il teorema di Lagrange)

$$\#(A_4/V_4) = (\#A_4)/(\#V_4) = 12/4 = 3.$$

   Poiché anche $\#H = 3$ e tutti i gruppi di ordine 3 sono tra loro isomorfi, esiste un isomorfismo $g\colon A_4/V_4 \to H$. Dunque, indicando con $\pi\colon A_4 \to A_4/V_4$ l'omomorfismo (suriettivo) di proiezione al quoziente, si ottiene un omomorfismo suriettivo $g \circ \pi\colon A_4 \to H$.

2. (a) $A$ non è un dominio perché $2X$ non è irriducibile nel dominio $\mathbb{Z}[X]$ (dato che $2, X \notin \mathbb{Z}[X]^* = \mathbb{Z}^* = \{\pm 1\}$), e pertanto l'ideale $(2X)$ non è primo in $\mathbb{Z}[X]$.

   Osserviamo che, in generale, dato $f \in \mathbb{Z}[X]$, si ha

$$\big(\pi(f)\big) = \pi\big((f)\big) = \pi\big((f, 2X)\big) = (f, 2X)/(2X)$$

   come ideali di $A$. Inoltre, per il terzo teorema di isomorfismo,

$$A/\big(\pi(f)\big) = \big(\mathbb{Z}[X]/(2X)\big)/\big((f, 2X)/(2X)\big) \cong \mathbb{Z}[X]/(f, 2X).$$

   Se ne deduce che l'ideale $\big(\pi(f)\big)$ è primo/massimale in $A$ se e solo se $A/\big(\pi(f)\big) \cong \mathbb{Z}[X]/(f, 2X)$ è un dominio/campo se e solo se l'ideale $(f, 2X)$ è primo/massimale in $\mathbb{Z}[X]$.

(b) $\big(\pi(2)\big)$ e $\big(\pi(X)\big)$ sono primi in $A$ perché $(2, 2X) = (2)$ e $(X, 2X) = (X)$ sono primi in $\mathbb{Z}[X]$, dato che 2 e $X$ sono irriducibili nel dominio a fattorizzazione unica $\mathbb{Z}[X]$.

(c) Essendo $p$ dispari, $X = pX - 2X(p-1)/2 \in (p, 2X)$, da cui segue subito $(p, 2X) = (p, X)$. Dunque $\big(\pi(p)\big)$ è massimale in $A$ (cioè $(p, 2X)$ è massimale in $\mathbb{Z}[X]$) perché (grazie al terzo teorema di isomorfismo)

$$\mathbb{Z}[X]/(p, 2X) = \mathbb{Z}[X]/(p, X) \cong \mathbb{Z}/p\mathbb{Z}[X]/(X) \cong \mathbb{Z}/p\mathbb{Z}$$

è un campo (essendo $p$ primo).

(d) $\big(\pi(X^4 + X + 1)\big)$ è massimale in $A$ (cioè $(X^4 + X + 1, 2X)$ è massimale in $\mathbb{Z}[X]$). Infatti

$$2 = (X^4 + X + 1)2 - 2X(X^3 + 1) \in (X^4 + X + 1, 2X),$$

da cui segue subito $(X^4+X+1, 2X) = (X^4+X+1, 2)$. Pertanto (sempre per il terzo teorema di isomorfismo)

$$\mathbb{Z}[X]/(X^4+X+1, 2X) = \mathbb{Z}[X]/(X^4+X+1, 2) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X^4+X+1)$$

è un campo, dato che $X^4 + X + 1$ è irriducibile nel dominio a ideali principali $\mathbb{Z}/2\mathbb{Z}[X]$ (in quanto 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 $\mathbb{Z}/2\mathbb{Z}[X]$).