**Corso di Algebra 1 - a.a. 2022-2023**

*Prova scritta del 13/06/2023*

1. Indicando con $G$ il gruppo $S(\mathbb{N})$ delle permutazioni di $\mathbb{N}$, sia

$$H := \{\sigma \in G \,:\, \exists n \in \mathbb{N} \text{ tale che } \sigma(i) = i \ \forall i > n\}.$$

   (a) Dimostrare che $H$ è un sottogruppo di $G$.

   (b) Dimostrare che $H$ è normale in $G$.

   (c) Dimostrare che, se $\sigma \in G$ ha ordine infinito, allora anche $\sigma H \in G/H$ ha ordine infinito.

   (d) Dimostrare che in $G/H$ esiste un elemento di ordine $n$ per ogni intero positivo $n$.

2. Sia $f\colon A \to B$ un omomorfismo di anelli. Indicando con $\mathcal{I}(A)$ e $\mathcal{I}(B)$ gli insiemi degli ideali rispettivamente di $A$ e di $B$, si consideri la funzione

$$\begin{aligned} \varphi\colon \mathcal{I}(B) &\to \mathcal{I}(A) \\ I &\mapsto f^{-1}(I) \end{aligned}$$

   (a) Dimostrare che, se $f$ è suriettivo, allora $\varphi$ è iniettiva.

   (b) Dimostrare che, se $\varphi$ è suriettiva, allora $f$ è iniettivo.

   (c) Nel caso in cui $B$ sia un campo, dimostrare che $\varphi$ è biunivoca se e solo se anche $A$ è un campo.

   (d) Nel caso in cui $A = \mathbb{Z}$ e $B = \mathbb{Q}[X]$, dimostrare che $\varphi$ non è né iniettiva né suriettiva.

*Soluzioni*

1. (a) Chiaramente $\mathrm{id}_{\mathbb{N}} \in H$. Dati $\sigma, \tau \in H$, per ipotesi esistono $l, m \in \mathbb{N}$ tali che $\sigma(i) = i$ per ogni $i > l$ e $\tau(i) = i$ (quindi anche $\tau^{-1}(i) = i$) per ogni $i > m$. Ponendo $n := \max\{l, m\}$ risulta allora

$$(\sigma\tau^{-1})(i) = \sigma(\tau^{-1}(i)) = \sigma(i) = i$$

per ogni $i > n$, il che dimostra che $\sigma\tau^{-1} \in H$.

(b) Dati $\sigma \in H$ e $\tau \in G$, va dimostrato che $\sigma' := \tau\sigma\tau^{-1} \in H$. Per ipotesi esiste $n \in \mathbb{N}$ tale che $\sigma(i) = i$ per ogni $i > n$. Ponendo $n' := \max\{\tau(0), \dots, \tau(n)\} \in \mathbb{N}$, per ogni $i > n'$ si ha $\tau^{-1}(i) > n$, quindi

$$\sigma'(i) = \tau(\sigma(\tau^{-1}(i))) = \tau(\tau^{-1}(i)) = i,$$

e pertanto $\sigma' \in H$.

(c) Dato $k \in \mathbb{N}$ tale che $(\sigma H)^k = H$ in $G/H$, va dimostrato che $k = 0$. Poiché $(\sigma H)^k = \sigma^k H$, si ha $\sigma^k \in H$. Dunque esiste $n \in \mathbb{N}$ tale che $\sigma^k(i) = i$ per ogni $i > n$. Da questo segue subito che $\sigma^k$ (che può essere identificato con $\sigma^k|_{\{0,\dots,n\}}$ nel gruppo finito $S(\{0, \dots, n\}) \cong S_{n+1}$) ha ordine finito, cioè esiste $m > 0$ tale che $\mathrm{id}_{\mathbb{N}} = (\sigma^k)^m = \sigma^{km}$. Avendo $\sigma$ ordine infinito, da ciò segue $km = 0$ e quindi $k = 0$.

(d) Sia per esempio $\sigma \in G$ definita da

$$\sigma(i) := \begin{cases} i + 1 - n & \text{se } i \equiv n - 1 \mod n \\ i + 1 & \text{altrimenti.} \end{cases}$$

È molto facile vedere che $\sigma^n = \mathrm{id}_{\mathbb{N}}$, mentre per $0 < k < n$ si ha $\sigma^k(i) \neq i$ per ogni $i \in \mathbb{N}$. Questo chiaramente implica che $\sigma^n \in H$ mentre $\sigma^k \notin H$ per $0 < k < n$. Si conclude allora che $(\sigma H)^n = \sigma^n H = H$, mentre $(\sigma H)^k = \sigma^k H \neq H$ per $0 < k < n$, cioè $\sigma H$ ha ordine $n$.

2. (a) Essendo $f$ suriettivo, $f(f^{-1}(S)) = S$ per ogni sottoinsieme $S$ di $B$. Dunque, se $I$ e $I'$ sono ideali di $B$ tali che $\varphi(I) = \varphi(I')$ (cioè $f^{-1}(I) = f^{-1}(I')$), allora

$$I = f(f^{-1}(I)) = f(f^{-1}(I')) = I'.$$

Pertanto $\varphi$ è iniettiva.

(b) Essendo $\varphi$ suriettiva, esiste un ideale $I$ di $B$ tale che $\varphi(I) = \{0\}$. Dato che ogni ideale contiene 0, si ottiene

$$\{0\} = f^{-1}(I) \supseteq f^{-1}(\{0\}) = \ker(f),$$

e quindi $\ker(f) = \{0\}$, cioè $f$ è iniettivo.

(c) Poiché un campo ha solo gli ideali banali, $\mathcal{I}(B) = \{\{0\}, B\}$. Se anche $A$ è un campo, allora $\mathcal{I}(A) = \{\{0\}, A\}$ e $f$ è iniettivo (in quanto omomorfismo da un campo verso un anello non banale). Dunque $\varphi$ è biunivoca perché

$$\varphi(\{0\}) = f^{-1}(\{0\}) = \ker(f) = \{0\},$$
$$\varphi(B) = f^{-1}(B) = A.$$

Viceversa, se $\varphi$ è biunivoca, allora $\#\mathcal{I}(A) = \#\mathcal{I}(B) = 2$, il che implica che $A$ è un anello non banale i cui unici ideali sono quelli banali. Inoltre, essendo in particolare $\varphi$ suriettiva, $f$ è iniettivo per il punto precedente, da cui segue che $A$ è commutativo (perché $A$ è isomorfo al sottoanello $\mathrm{im}(f)$ dell'anello commutativo $B$). Per concludere basta ricordare che un anello commutativo non banale con solo gli ideali banali è un campo.

(d) Ricordando che esiste un unico omomorfismo di anelli da $\mathbb{Z}$ verso ogni anello, $f$ deve essere l'inclusione di $\mathbb{Z}$ in $\mathbb{Q}[X]$. Allora $\varphi$ non è iniettiva perché per esempio $(X) \neq \{0\}$ in $\mathcal{I}(\mathbb{Q}[X])$, ma

$$\varphi((X)) = f^{-1}((X)) = \mathbb{Z} \cap (X) = \{0\} = f^{-1}(\{0\}) = \varphi(\{0\}).$$

D'altra parte $f = g \circ h$, con $h\colon \mathbb{Z} \to \mathbb{Q}$ e $g\colon \mathbb{Q} \to \mathbb{Q}[X]$ gli omomorfismi di inclusione. Allora per ogni ideale $I$ di $\mathbb{Q}[X]$ si ha

$$\varphi(I) = f^{-1}(I) = (g \circ h)^{-1}(I) = h^{-1}(g^{-1}(I)).$$

D'altra parte $g^{-1}(I)$ (essendo un ideale del campo $\mathbb{Q}$) può essere solo $\{0\}$ o $\mathbb{Q}$. Poichè $h^{-1}(\{0\}) = \{0\}$ e $h^{-1}(\mathbb{Q}) = \mathbb{Z}$, da ciò segue che $\varphi(I)$ può essere solo $\{0\}$ o $\mathbb{Z}$. Dunque per $n > 1$ gli ideali $n\mathbb{Z}$ di $\mathbb{Z}$ non sono nell'immagine di $\varphi$, che quindi non è suriettiva.