Corso di Algebra 1 - a.a. 2022-2023
Prova scritta del 20/09/2023

1. Dati due interi positivi m e n, sia

$$G := \{\sigma \in S_n \,:\, \sigma(i) \equiv i \mod m \quad \forall\, i = 1, \dots, n\}$$

   (a) Dimostrare che G è un sottogruppo di S_n.
   (b) Dimostrare che G è contenuto in A_n se e solo se $m \geq n$.
   (c) Dimostrare che G è abeliano se e solo se $2m \geq n$.
   (d) Per $m = 2$ e $n = 5$, dimostrare che G ha ordine 12 e non è isomorfo a A_4.

2. Dato un omomorfismo di anelli commutativi $f\colon A \to B$, sia

$$S := \{a \in A \,:\, f(a) \notin B^*\}$$

   (a) Dimostrare che, se S è un sottogruppo additivo di A, allora S è anche un ideale di A.
   (b) Dimostrare che, se B è un campo, allora S è un ideale di A.
   (c) Assumendo che f sia la proiezione al quoziente $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ con $n > 1$, dimostrare che S è un ideale di $\mathbb{Z}$ se e solo se n è una potenza di un numero primo.
   (d) Assumendo che f sia la proiezione al quoziente

$$\mathbb{Q}[X] \to \mathbb{Q}[X]/(X^4 - X^3 - 2X^2 - X - 1),$$

   stabilire se S è un ideale di $\mathbb{Q}[X]$.

Soluzioni

1. (a) Chiaramente $(1) \in G$ (dato che $i \equiv i \mod m$ per ogni intero i). Essendo S_n finito, per dimostrare che G è un sottogruppo di S_n basta allora verificare che $\sigma\tau \in G$ per ogni $\sigma, \tau \in G$. In effetti questo è vero perché per ogni $i = 1, \dots, n$ si ha

$$(\sigma\tau)(i) = \sigma(\tau(i)) \equiv \tau(i) \equiv i \mod m.$$

(b) Se $m \geq n$, allora per ogni $i, j = 1, \dots, n$ si ha $|i - j| < n \leq m$, e dunque $i \equiv j \mod m$ se e solo se $i = j$. Ciò dimostra che $\sigma(i) = i$ per ogni $i = 1, \dots, n$ e per ogni $\sigma \in G$. Pertanto $G = \{(1)\} \subseteq A_n$. Se invece $m < n$, allora $(1, m+1) \in G \setminus A_n$ (dato che le trasposizioni sono permutazioni dispari).

(c) Se $2m \geq n$, allora per ogni ogni $i = 1, \dots, n$

$$C(i) := \{j = 1, \dots, n \, : \, j \equiv i \mod m\}$$

contiene al massimo 2 elementi: $C(i) = \{i\}$ se $n - m < i \leq m$, mentre $C(i) = \{i, i+m\}$ se $i \leq n-m$ e $C(i) = \{i-m, i\}$ se $i > m$. Poiché $\sigma|_{C(i)} \in S(C(i))$ per ogni $\sigma \in G$ e per ogni $i = 1, \dots, n$, dal fatto che $S(C(i))$ è abeliano (essendo isomorfo a S_1 o a S_2) segue che per ogni $\sigma, \tau \in G$ si ha

$$\sigma(\tau(i)) = \sigma|_{C(i)}(\tau|_{C(i)}(i)) = \tau|_{C(i)}(\sigma|_{C(i)}(i)) = \tau(\sigma(i))$$

per ogni $i = 1, \dots, n$. Perciò $\sigma\tau = \tau\sigma$, e dunque G è abeliano. Se invece $2m < n$, allora G non è abeliano perché $\sigma := (1, m+1), \tau := (m+1, 2m+1) \in G$ e

$$\sigma\tau = (1, m+1, 2m+1) \neq (1, 2m+1, m+1) = \tau\sigma.$$

(d) Con la notazione del punto precedente si ha $C(i) = \{1, 3, 5\}$ se i è dispari e $C(i) = \{2, 4\}$ se i è pari. Si può allora identificare G con $S(\{1, 3, 5\}) \times S(\{2, 4\}) \cong S_3 \times S_2$, e dunque $\#G = (\#S_3)(\#S_2) = 6 \cdot 2 = 12$. Inoltre $G \ncong A_4$ perché $(1, 3, 5)(2, 4) \in G$ ha ordine

$$\mathrm{mcm}(\mathrm{ord}((1, 3, 5)), \mathrm{ord}((2, 4))) = \mathrm{mcm}(3, 2) = 6$$

(essendo $(1, 3, 5)$ e $(2, 4)$ cicli disgiunti), mentre A_4 non contiene elementi di ordine 6 (gli elementi non banali di A_4 sono i 3-cicli, di ordine 3, e le coppie di trasposizioni disgiunte, di ordine 2).

2. (a) Basta dimostrare che, se $a \in A$ e $s \in S$, allora $as \in S$. Se per assurdo $as \notin S$, per definizione $b := f(as) \in B^*$, e dunque

$$b^{-1}f(a)f(s) = b^{-1}f(as) = b^{-1}b = 1.$$

Essendo B commutativo, questo dimostra $f(s) \in B^*$ (con $f(s)^{-1} = b^{-1}f(a)$), cioè $s \notin S$, contro l'ipotesi.

(b) Per definizione di campo si ha $B^* = B \setminus \{0\}$, e quindi

$$S = \{a \in A \,:\, f(a) = 0\} = \ker(f)$$

è un ideale perché nucleo di un omomorfismo di anelli.

(c) Ricordando che, per ogni intero a, $f(a) = a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}^*$ se e solo se $\operatorname{mcd}(a, n) = 1$, otteniamo che in ogni caso

$$S = \{a \in \mathbb{Z} \,:\, \operatorname{mcd}(a, n) \neq 1\}.$$

Se $n = p^k$ con p primo e $k > 0$, allora $\operatorname{mcd}(a, n) \neq 1$ se e solo se $p \mid a$, e dunque in questo caso $S = p\mathbb{Z}$ è un ideale di $\mathbb{Z}$. Se invece n non è potenza di un primo, esistono due primi distinti p_1 e p_2 tali che $p_1, p_2 \mid n$. Poiché $\operatorname{mcd}(p_1, p_2) = 1$, esistono $m_1, m_2 \in \mathbb{Z}$ tali che $m_1p_1 + m_2p_2 = 1$. Dato che $m_ip_i \in S$ (perché $p_i \mid \operatorname{mcd}(n, m_ip_i)$) per $i = 1, 2$, mentre $1 \notin S$ (perché $f(1) = 1 + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}^*$), se ne deduce che S non è un ideale di $\mathbb{Z}$.

(d) In questo caso S non è un ideale di $\mathbb{Q}[X]$. Osserviamo infatti che $g := X^4 - X^3 - 2X^2 - X - 1 = g_1g_2$ con $g_1 := X + 1$ e $g_2 := X^3 - 2X^2 - 1$ irriducibili in $\mathbb{Q}[X]$ (g_2 lo è perché di terzo grado e senza radici razionali, dato che le eventuali radici vanno cercate in $\{\pm 1\}$ e $g_2(1) \neq 0 \neq g_2(-1)$). Essendo g_1 e g_2 irriducibili e non associati in $\mathbb{Q}[X]$ che è un dominio a ideali principali (perché $\mathbb{Q}$ è un campo), in modo analogo al punto precedente esistono $h_1, h_2 \in \mathbb{Q}[X]$ tali che $1 = h_1g_1 + h_2g_2$. Per concludere che S non è un ideale basta allora mostrare che $h_ig_i \in S$ per $i = 1, 2$, dato che invece $1 \notin S$ (perché $f(1) = 1 + (g) \in \mathbb{Q}[X]/(g)^*$). In effetti $f(h_ig_i) = h_ig_i + (g) \notin \mathbb{Q}[X]/(g)^*$ (cioè $h_ig_i \in S$) perché $h_ig_i + (g) \in (g_i)/(g)$ e $(g_i)/(g)$ è un ideale proprio (dunque non contenente elementi invertibili) di $\mathbb{Q}[X]/(g)$.