Corso di Algebra 1 - a.a. 2018-2019

Prova scritta del 23/01/2019

1. Sia k un intero positivo.

   (a) Se G è un gruppo abeliano finito di ordine n e $\mathrm{mcd}(k, n) = 1$, dimostrare che la funzione $f\colon G \to G$ definita da $f(a) := a^k$ è un automorfismo di G.

   (b) Se k è dispari, dimostrare che la congruenza

   $$x^k \equiv a \mod 17$$

   ha un'unica soluzione modulo 17 per ogni $a \in \mathbb{Z}$.

2. Sia $n \geq 3$ un intero e sia

   $$H := \{\sigma \in S_n \,:\, \sigma(i) \equiv i \mod 2 \text{ per ogni } i = 1, \ldots, n\}.$$

   (a) Dimostrare che H è un sottogruppo di S_n.

   (b) Dimostrare che H non è normale in S_n.

   (c) Stabilire se H è abeliano nel caso in cui $n = 5$.

3. Dati due ideali (bilateri) I e J di un anello A, sia

   $$(I : J) := \{a \in A \,:\, ab \in I \text{ per ogni } b \in J\}.$$

   (a) Dimostrare che $(I : J)$ è un ideale (bilatero) di A.

   (b) Dimostrare che $(I : J)J \subseteq I \subseteq (I : J)$.

   (c) Dimostrare che, se A è un dominio a ideali principali e $I \subseteq J$, allora $(I : J)J = I$.

4. Consideriamo il polinomio $p = X^4 + 2X^3 + 2X^2 - X + 1$.

   (a) Fattorizzare p in $\mathbb{Z}/3\mathbb{Z}[X]$.

   (b) Dimostrare che p è irriducibile in $\mathbb{Q}[X]$ e in $\mathbb{Z}[X]$.

Soluzioni

1. (a) f è un omomorfismo perché, essendo G abeliano,

$$f(ab) = (ab)^k = a^k b^k = f(a)f(b)$$

per ogni $a, b \in G$. Poiché G è finito, f è biunivoco (dunque un automorfismo di G) se e solo se è iniettivo se e solo se $\ker(f) = \{1_G\}$. Sia dunque $a \in \ker(f)$, cioè $a \in G$ tale che $a^k = 1_G$. Per il teorema di Lagrange $\mathrm{ord}(a) \mid n$ e, d'altra parte, $a^k = 1_G$ implica $\mathrm{ord}(a) \mid k$. Se ne deduce che $\mathrm{ord}(a) \mid \mathrm{mcd}(n, k) = 1$, quindi $\mathrm{ord}(a) = 1$ e $a = 1_G$.

   (b) Per ogni $n \in \mathbb{Z}$ poniamo $\overline{n} := n + 17\mathbb{Z} \in \mathbb{Z}/17\mathbb{Z}$. Si tratta di dimostrare che per ogni $\overline{a} \in \mathbb{Z}/17\mathbb{Z}$ esiste unico $\overline{x} \in \mathbb{Z}/17\mathbb{Z}$ tale che $\overline{x}^k = \overline{x^k} = \overline{a}$. Poiché 17 è un numero primo, $\mathbb{Z}/17\mathbb{Z}$ è un campo. Se $\overline{a} = \overline{0}$ (cioè $17 \mid a$), $\overline{x}^k = \overline{0}$ se e solo se $\overline{x} = \overline{0}$, dato che $\mathbb{Z}/17\mathbb{Z}$ è un dominio. Se invece $\overline{a} \neq \overline{0}$ (cioè $17 \nmid a$), per lo stesso motivo si ha $\overline{x} \neq 0$ per ogni $\overline{x}$ tale che $\overline{x}^k = \overline{a}$. Tenendo presente che $\mathbb{Z}/17\mathbb{Z}^* = \mathbb{Z}/17\mathbb{Z} \setminus \{\overline{0}\}$ ci siamo allora ridotti a dimostrare che per ogni $\overline{a} \in \mathbb{Z}/17Z^*$ esiste unico $\overline{x} \in \mathbb{Z}/17\mathbb{Z}^*$ tale che $\overline{x}^k = \overline{a}$. Quest'ultimo fatto segue dal punto precedente, che si può applicare perché il gruppo moltiplicativo $\mathbb{Z}/17\mathbb{Z}^*$ ha ordine 16 e $\mathrm{mcd}(k, 16) = 1$ (essendo k dispari).

2. (a) Sia $X := \{1, \ldots, n\}$ e sia $P := X \cap 2\mathbb{Z}$, $D := X - 2\mathbb{Z}$. Allora $X = D \sqcup P$ e $H = \{\sigma \in S_n : \sigma(P) \subset P, \sigma(D) \subset D\}$. Se $\sigma \in S_n$, σ è biunivoca, dunque $\sigma(P) \subset P \Longrightarrow \sigma(P) = P$ e $\sigma(D) = \sigma(D)$. Dunque $H = \{\sigma \in S_n : \sigma(P) = P\}$. Chiaramente $\mathrm{id}_X \in H$. Se $\sigma \in H$, allora $\sigma(P) = P$, dunque $\sigma^{-1}(P) = P$, quindi $\sigma^{-1} \in H$. Siano poi $\sigma, \tau \in H$. Allora $(\sigma\tau)(P) = \sigma(\tau(P)) = \sigma(P) = P$. Dunque $\sigma\tau \in H$. Pertanto H è un sottogruppo di S_n.

   (b) Una trasposizione $\sigma = (ij)$ appartiene ad H se e soltanto se i numeri i e j sono entrambi pari oppure sono entrambi dispari. La trasposizione $\sigma = (13)$ appartiene ad H. Se $\tau = (12)$, allora $\tau\sigma\tau^{-1} = (12)(13)(12) = (23) \notin H$. Dunque H non è normale.

   (c) Se $n = 5$, allora $P = \{2, 4\}$ e $D = \{1, 3, 5\}$. L'insieme $K := \{\sigma \in S_5 : \sigma(2) = 2, \sigma(4) = 4\}$ è un sottogruppo di S_5 isomorfo a S_3 e pertanto non abeliano. Siccome $K \subset H$, neanche H è abeliano. Più concretamente $(13), (35) \in H$ e $(13)(35) = (135) \neq (153) = (15)(13)$, dunque H non è abeliano.

3. (a) Chiaramente $0 \in (I : J)$ perché $0b = 0 \in I$ per ogni $b \in J$. Se poi $a, a' \in (I : J)$, anche $a + a' \in (I : J)$: per ogni $b \in J$ si ha infatti $(a + a')b = ab + a'b \in I$, dato che $ab, a'b \in I$ per ipotesi. Resta da vedere che, se $a \in A$ e $a' \in (I : J)$, anche $aa', a'a \in (I : J)$. Per quanto riguarda aa', per ogni $b \in J$ si ha $(aa')b = a(a'b) \in I$ perché $a'b \in I$ per ipotesi e I è un ideale sinistro. Venendo infine ad $a'a$, per ogni $b \in J$ si ha $(a'a)b = a'(ab) \in I$ perché $ab \in J$ (essendo J un ideale sinistro).

   (b) Ogni elemento del prodotto di ideali $(I : J)J$ è una somma (finita) di elementi della forma ab con $a \in (I : J)$ e $b \in J$. L'inclusione $(I : J)J \subseteq I$ segue allora dal fatto che (per definizione di $(I : J)$) $ab \in I$ per ogni $a \in (I : J)$ e per ogni $b \in J$. D'altra parte, $I \subseteq (I : J)$ perché per ogni $a \in I$ si ha $ab \in I$ per ogni $b \in J$ (essendo I un ideale destro), cioè $a \in (I : J)$.

   (c) Grazie al punto precedente basta dimostrare $I \subseteq (I : J)J$. Poiché I e J sono ideali principali, esistono $x, y \in A$ tali che $I = (x)$ e $J = (y)$; inoltre $x \in (x) = I \subseteq J = (y)$, per cui esiste $z \in A$ tale che $x = zy$. Risulta $z \in (I : J)$ perché per ogni $b \in J = (y)$ esiste $a \in A$ tale che $b = ya$, per cui

$$zb = zya = xa \in (x) = I.$$

   Ciò dimostra che $x = zy \in (I : J)J$, e questo implica $I = (x) \subseteq (I : J)J$ (essendo $(I : J)J$ un ideale).

4. (a) Su $\mathbb{Z}/3\mathbb{Z}$ si ha $p = X^4 + 2X^3 + 2X^2 + 2X + 1$, la cui unica radice è 2. Dividendo p per $X - 2 = X + 1$ si trova

$$p = (X + 1)(X^3 + X^2 + X + 1).$$

   2 è radice anche di $X^3 + X^2 + X + 1$. Dividendo di nuovo si trova $X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$. Il polinomio $X^2 + 1$ non ha radici, dunque è irriducibile. Quindi la fattorizzazione è $p = (X + 1)^2(X^2 + 1)$.

   (b) Su $\mathbb{Z}/2\mathbb{Z}$ si ha $p = X^4 + X + 1$, che non ha radici. Dunque non ha fattori lineari. Se p non fosse irriducibile, sarebbe prodotto di fattori quadratici. Siccome il coefficiente di X^4 e il termine noto sono 1, i fattori devono essere della forma $X^2 + aX + 1$ e $X^2 + bX + 1$, con $a, b \in \mathbb{Z}/2\mathbb{Z}$. Ma

$$\begin{aligned}(X^2 + aX + 1)(X^2 + bX + 1) = \\ = X^4 + (a + b)X^3 + abX^2 + (a + b)X + 1.\end{aligned}$$

Dunque si avrebbe $a = b = 0$ e $a + b = 1$, assurdo. Quindi p è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$. Siccome è monico, dunque primitivo, è irriducibile anche in $\mathbb{Z}[X]$.