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

Prova scritta del 09/09/2019

1. Siano $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ e sia $I := \{i \in \{1,2,3,4\} \,:\, x_i \text{ è pari}\}$.
   (a) Dimostrare che, se $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod 2$, allora $\#I$ è pari. È vero il viceversa?
   (b) Dimostrare che, se $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod 4$, allora $\#I = 0$ o $\#I = 4$. È vero il viceversa?
   (c) Dimostrare che, se $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod 8$, allora $\#I = 4$. È vero il viceversa?

2. Sia G un gruppo non banale e sia K l'intersezione di tutti i sottogruppi diversi da $\{1\}$ di G.
   (a) Dimostrare che K è un sottogruppo normale di G.
   (b) Dimostrare che, se $K \neq \{1\}$, allora K è ciclico di ordine un numero primo.
   (c) Supponendo che G sia ciclico, dimostrare che $K \neq \{1\}$ se e solo se l'ordine di G è una potenza di un numero primo.

3. Siano A un anello commutativo, I un ideale primo di A e K il campo dei quozienti del dominio A/I.
   (a) Dimostrare che esiste un omomorfismo di anelli $A \to K$.
   (b) Dimostrare che, se $A = \mathbb{Z}$, allora non esiste un omomorfismo di anelli $K \to A$.
   (c) Fornire un esempio in cui esiste un omomorfismo di anelli $K \to A$.

4. Dato un intero $n > 1$, si consideri il polinomio $p_n := X^n + 4X + n$.
   (a) Dimostrare che esistono infiniti valori di n tali che p_n è irriducibile in $\mathbb{Z}[X]$.
   (b) Determinare il più piccolo valore n_0 di n tale che p_n ha una radice in $\mathbb{Q}$.
   (c) Fattorizzare p_{n_0} in $\mathbb{Q}[X]$.

Soluzioni

1. (a) È facile verificare che $i \in I \Longrightarrow x_i^2 \equiv 0 \mod 4$ e $i \notin I \Longrightarrow x_i^2 \equiv 1 \mod 4$. Dunque

$$\sum_{i=1}^{4} x_i^2 \equiv 4 - \#I \mod 4. \tag{1}$$

In particolare $\sum_{i=1}^{4} x_i^2 \equiv \#I \mod 2$. Dunque se $\sum_{i=1}^{4} x_i^2 \equiv 0 \mod 2$, allora $\#I$ è pari e vale anche il viceversa.

(b) Da (1) segue immediatamente che $\sum_{i=1}^{4} x_i^2 \equiv 0 \mod 4$ se e soltanto se $\#I \equiv 0 \mod 4$ cioè se e soltanto se $\#I = 0$ o $\#I = 4$.

(c) Supponiamo che $\sum_{i=1}^{4} x_i^2 \equiv 0 \mod 8$. Allora $\sum_{i=1}^{4} x_i^2 \equiv 0 \mod 4$. Per il punto (b) $\#I = 0$ oppure $\#I = 4$. Basta escludere il caso $\#I = 0$. Se $i \notin I$, allora $x_i = 1 + 2y_i$ per qualche $y_i \in \mathbb{Z}$ e $x_i^2 = 1 + 4y_i^2 + 4y_i = 1 + 4y_i(y_i + 1)$. O y_i è pari o $y_i + 1$ lo è. Dunque $x_i^2 \equiv 1 \mod 8$. Abbiamo dimostrato che se $i \notin I$, allora $x_i^2 \equiv 1 \mod 8$. Se fosse $\#I = 0$, avremmo quindi $\sum_{i=1}^{4} x_i^2 \equiv 4 \mod 8$. Il viceversa non vale, come si vede per esempio scegliendo $x_1 = x_2 = x_3 = 0$ e $x_4 = 2$.

2. (a) K è un sottogruppo perché intersezione di sottogruppi. Va poi dimostrato che $gag^{-1} \in K$ per ogni $g \in G$ e per ogni $a \in K$. Per definizione, $gag^{-1} \in K$ se e solo se $gag^{-1} \in H$ per ogni $H \neq \{1\}$ sottogruppo di G. Poiché $gag^{-1} \in H$ se e solo se $a = g^{-1}(gag^{-1})g \in g^{-1}Hg$, basta osservare che $g^{-1}Hg \neq \{1\}$ è un sottogruppo di G, quindi $a \in g^{-1}Hg$ perché $a \in K$.

(b) Se $H \neq \{1\}$ è un sottogruppo di K, allora H è anche un sottogruppo di G, e quindi, per definizione, $K \subseteq H$, da cui $K = H$ (ciò dimostra che K ha solo i sottogruppi banali). Preso allora $a \in K \setminus \{1\}$, deve essere $\langle a \rangle = K$, cioè K è ciclico. K non può essere infinito, perché in quel caso sarebbe isomorfo a $\mathbb{Z}$, che ha sottogruppi non banali (per esempio $2\mathbb{Z}$). Allora $K \cong \mathbb{Z}/n\mathbb{Z}$ per qualche $n > 1$, e deve essere n primo, perché altrimenti esiste un divisore d di n tale che $1 < d < n$, e quindi tale che $\langle \overline{d} \rangle$ è un sottogruppo non banale di $\mathbb{Z}/n\mathbb{Z}$.

(c) Se G è ciclico infinito, si può supporre $G = \mathbb{Z}$ (a meno di isomorffismo). Allora i sottogruppi di G sono tutti e soli della forma

$\langle d\rangle$ con $d \in \mathbb{N}$; inoltre un tale sottogruppo coincide con il sottogruppo banale $\{0\}$ se e solo se $d = 0$. Dunque in questo caso $K = \bigcap_{d>0} d\mathbb{Z} = \{0\}$. Se invece G è ciclico finito, si può supporre $G = \mathbb{Z}/n\mathbb{Z}$ (a meno di isomorfismo) per qualche $n > 1$. Allora i sottogruppi di G sono tutti e soli della forma $\langle \overline{d}\rangle$ con d divisore positivo di n; inoltre un tale sottogruppo coincide con il sottogruppo banale $\{\overline{0}\}$ se e solo se $d = n$. In particolare, se $n = p^m$ con p primo e $m > 0$, i divisori di n sono p^l con $0 \leq l \leq m$, e quindi $K = \bigcap_{0\leq l<m} \langle \overline{p^l}\rangle = \langle \overline{p^{m-1}}\rangle \neq \{\overline{0}\}$. D'altra parte, se n non è una potenza di un numero primo, esistono $a, b > 1$ tali che $n = ab$ e $\mathrm{mcd}(a, b) = 1$ (per cui $a, b < n = \mathrm{mcm}(a, b)$). In questo caso $K \subseteq \langle \overline{a}\rangle \cap \langle \overline{b}\rangle = \langle \overline{\mathrm{mcm}(a, b)}\rangle = \langle \overline{n}\rangle = \{\overline{0}\}$, cioè $K = \{\overline{0}\}$.

3. (a) Sia $\pi\colon A \to A/I$ la proiezione al quoziente e sia $i\colon A/I \to K$ l'inclusione. Poiché sia π che i sono omomorfismi di anelli, anche la composizione $i \circ \pi\colon A \to K$ lo è.

   (b) Per $A = \mathbb{Z}$ può essere $I = \{0\}$ o $I = p\mathbb{Z}$ con p numero primo. Se $I = \{0\}$, si ha $A/I \cong \mathbb{Z}$ e $K \cong \mathbb{Q}$. Non esiste un omomorfismo di anelli $f\colon \mathbb{Q} \to \mathbb{Z}$ perché altrimenti

   $$1 = f(1) = f\left(\frac{1}{2} + \frac{1}{2}\right) = f\left(\frac{1}{2}\right) + f\left(\frac{1}{2}\right) = 2f\left(\frac{1}{2}\right),$$

   che è impossibile in $\mathbb{Z}$. Se invece $I = p\mathbb{Z}$, si ha $A/I = \mathbb{Z}/p\mathbb{Z}$, che è un campo, e quindi anche $K \cong \mathbb{Z}/p\mathbb{Z}$. Non esiste un omomorfismo di anelli $f\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}$ perché, essendo in particolare un omomorfismo di gruppi, si avrebbe $\mathrm{ord}(f(\overline{1})) \mid \mathrm{ord}(\overline{1}) = p$, e quindi (tenendo conto che 0 è l'unico elemento di ordine finito di $\mathbb{Z}$) $f(\overline{1}) = 0 \neq 1$.

   (c) Sia $A = \mathbb{Q}[X]$ e $I = (X)$. Risulta infatti $A/I \cong \mathbb{Q}$ e quindi (essendo $\mathbb{Q}$ un campo) anche $K \cong \mathbb{Q}$. Chiaramente esiste un omomorfismo di anelli $\mathbb{Q} \to \mathbb{Q}[X]$, cioè l'inclusione.

4. (a) Basta scegliere $n = 2m$ con m dispari e applicare il criterio di Eisenstein rispetto al primo 2.

   (b) Se p_n ha una radice questa è intera e divide n. In questo modo si verifica che p_n non ha radici per $n = 2, 3, 4$. Invece -1 è radice di p_5, dunque $n_0 = 5$.

   (c) Per il teorema di Ruffini, $X + 1$ divide p_5. Dividendo otteniamo $p_5 = (X+1)q$ con $q = X^4 - X^3 + X^2 - X + 5$, e vogliamo dimostrare che q è irriducibile in $\mathbb{Q}[X]$. Essendo q monico a coefficienti interi,

è sufficiente dimostrare che la sua riduzione $\overline{q} = X^4 + X^3 + X^2 + X + \overline{1}$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$. Questo è vero perché $\overline{q}$ non ha radici in $\mathbb{Z}/2\mathbb{Z}$ e non è divisibile $X^2+X+\overline{1}$, che è l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}/2\mathbb{Z}[X]$.