Corso di Algebra 1 - a.a. 2015-2016

Prova scritta del 6.9.2016

1. Trovare le soluzioni dell'equazione $x^2 + x = \overline{2}$ in $\mathbb{Z}/4\mathbb{Z}$.

   Trovare inoltre il più piccolo intero $y > 500$ tale che

$$\begin{cases} 3y \equiv 5 \mod 7 \\ 2y \equiv 3 \mod 5 \\ y^2 + y \equiv 2 \mod 4 \end{cases}$$

2. Sia G un gruppo. Stabilire quali delle seguenti affermazioni sono vere.

   (a) Se G non è banale ed esiste un omomorfismo iniettivo $G \to \mathbb{Z}$, allora G è isomorfo a $\mathbb{Z}$.

   (b) Esiste un omomorfismo iniettivo $G \to \mathbb{Z}/12\mathbb{Z}$ se e solo se esiste un omomorfismo suriettivo $\mathbb{Z}/12\mathbb{Z} \to G$.

   (c) Se esiste un omomorfismo iniettivo $G \to S_3$, allora esiste un omomorfismo suriettivo $S_3 \to G$.

3. Per ciascuno dei seguenti sottoinsiemi di $A = \mathbb{R}[X]$ verificare se è un ideale e/o un sottoanello:

$$V_1 = \{p \in A : p(1) = 0\}$$
$$V_2 = \{p \in A : p(1) = 1\}$$
$$V_3 = \{p \in A : p(X) = p(-X)\}$$
$$V_4 = \{p \in A : p(X) = p(X+1)\}$$

   Stabilire inoltre per quali $i \in \{1, 2, 3, 4\}$ vale $V_i = \mathbb{R}$.

4. Siano K e F due campi, e sia $f \colon K[X] \to F$ un omomorfismo di anelli.

   (a) Dimostrare che $\ker(f)$ è un ideale primo di $K[X]$.

   (b) Dimostrare che, se f non è iniettivo, allora $\mathrm{im}(f)$ è un campo.

   (c) Se $K = \mathbb{Q}$, $F = \mathbb{R}$ e $f(X) = \sqrt{2}$, determinare $\ker(f)$ e $\mathrm{im}(f)$.

Soluzioni

1. È immediato verificare che $x^2 + x = \overline{0}$ se $x = \overline{0}$ o $x = \overline{3}$, mentre $x^2 + x = \overline{2}$ se $x = \overline{1}$ o $x = \overline{2}$. Dunque le soluzioni dell'equazione sono $x = \overline{1}$ e $x = \overline{2}$ in $\mathbb{Z}/4\mathbb{Z}$.

   Dato che $\mathrm{mcd}(3, 7) = 1$ (rispettivamente $\mathrm{mcd}(2, 5) = 1$), la prima (rispettivamente la seconda) congruenza del sistema ha un'unica soluzione modulo 7 (rispettivamente modulo 5), che si trova facilmente essere $y \equiv 4 \mod 7$ (rispettivamente $y \equiv 4 \mod 5$). Essendo $\mathrm{mcd}(7, 5) = 1$, per il teorema cinese del resto le prime due congruenze hanno un'unica soluzione modulo $7 \cdot 5 = 35$, che è ovviamente $y \equiv 4 \mod 35$. Per la prima parte le soluzioni dell'ultima congruenza sono $y \equiv 1, 2 \mod 4$, e quindi le soluzioni del sistema di partenza sono l'unione delle soluzioni dei due sistemi

$$\begin{cases} y \equiv 4 \mod 35 \\ y \equiv 1 \mod 4 \end{cases} \qquad \begin{cases} y \equiv 4 \mod 35 \\ y \equiv 2 \mod 4 \end{cases}$$

   Poiché $\mathrm{mcd}(35, 4) = 1$, di nuovo per il teorema cinese del resto ciascuno di tali sistemi ha un'unica soluzione modulo $35 \cdot 4 = 140$. È facile vedere che la soluzione del primo sistema è $y \equiv 109 \mod 140$ (quindi $y = \ldots, 109, 249, 389, 529, \ldots$) e quella del secondo $y \equiv 74 \mod 140$ (quindi $y = \ldots, 74, 214, 354, 494, 634, \ldots$). Ne segue che la più piccola soluzione > 500 è $y = 529$.

2. (a) Vera. Se infatti $f\colon G \to \mathbb{Z}$ è un omomorfismo iniettivo, risulta $G \cong \mathrm{im}(f)$. Essendo $\mathrm{im}(f)$ un sottogruppo di $\mathbb{Z}$, esiste $n \in \mathbb{N}$ tale che $\mathrm{im}(f) = n\mathbb{Z}$. Inoltre $n > 0$ perché G non è banale e f è iniettivo. La tesi segue allora dal fatto che, se $n > 0$, $n\mathbb{Z}$ è un gruppo ciclico (generato da n) infinito, quindi isomorfo a $\mathbb{Z}$.

   (b) Vera. In effetti, se esiste un omomorfismo iniettivo $G \to \mathbb{Z}/12\mathbb{Z}$, analogamente a prima G è isomorfo a un sottogruppo di $\mathbb{Z}/12\mathbb{Z}$, per cui G è ciclico (perché un sottogruppo di un gruppo ciclico è ciclico) di ordine un divisore d di 12 (per il teorema di Lagrange). Esiste allora un generatore g di G con $\mathrm{ord}(g) = d$, ed è chiaro che la funzione $\mathbb{Z}/12\mathbb{Z} \to G$ definita da $\overline{a} \mapsto g^a$ è un omomorfismo suriettivo. Viceversa, se esiste un omomorfismo suriettivo $f\colon \mathbb{Z}/12\mathbb{Z} \to G$, per il primo teorema di isomorfismo $G \cong (\mathbb{Z}/12\mathbb{Z})/\ker(f)$, e quindi G è ciclico (perché un quoziente di un gruppo ciclico è ciclico) di ordine un divisore d di 12 (per

il teorema di Lagrange). Come prima esiste un generatore g di G con $\mathrm{ord}(g) = d$, e si vede subito che la funzione $G \to \mathbb{Z}/12\mathbb{Z}$ definita da $g^i \mapsto \frac{\overline{12i}}{d}$ è un omomorfismo iniettivo.

(c) Falsa. Prendendo infatti $G = \mathbb{Z}/3\mathbb{Z}$, esiste un omomorfismo iniettivo $G \to S_3$ (per esempio quello definito da $\overline{a} \mapsto (1,2,3)^a$) ma non esiste un omomorfismo suriettivo $f\colon S_3 \to G$ (altrimenti, per il primo teorema di isomorfismo, $G \cong S_3/\ker(f)$ e quindi $\ker(f)$ sarebbe un sottogruppo normale di ordine 2 di S_3, che però non esiste).

3. V_1 è un ideale: chiaramente $0 \in V_1$; se $p, q \in V_1$, allora $(p+q)(1) = p(1) + q(1) = 0 + 0 = 0$, cioè $p + q \in V_1$; se $p \in V_1$ e $q \in A$, allora $(pq)(1) = p(1)q(1) = 0q(1) = 0$, cioè $pq \in V_1$. Invece V_1 non è un sottoanello perché $1 \notin V_1$.

   V_2 non è né un ideale né un sottoanello, dato che $0 \notin V_2$.

   V_3 e V_4 non sono ideali perché $1 \in V_3, V_4$ ma $X = X1 \notin V_3, V_4$. Invece V_3 e V_4 sono sottoanelli: abbiamo già osservato che $1 \in V_3, V_4$; se $p, q \in V_3$ (rispettivamente $p, q \in V_4$), allora

   $$(p-q)(X) = p(X) - q(X) = p(-X) - q(-X) = (p-q)(-X),$$

   cioè $p - q \in V_3$ (rispettivamente

   $$(p-q)(X) = p(X) - q(X) = p(X+1) - q(X+1) = (p-q)(X+1),$$

   cioè $p - q \in V_4$); se $p, q \in V_3$ (rispettivamente $p, q \in V_4$), allora

   $$(pq)(X) = p(X)q(X) = p(-X)q(-X) = (pq)(-X),$$

   cioè $pq \in V_3$ (rispettivamente

   $$(pq)(X) = p(X)q(X) = p(X+1)q(X+1) = (pq)(X+1),$$

   cioè $pq \in V_4$).

   $V_i = \mathbb{R}$ se e solo se $i = 4$. Infatti $V_1 \neq \mathbb{R}$ e $V_2 \neq \mathbb{R}$, visto che $\mathbb{R}$ è un sottoanello di A, mentre V_1 e V_2 non lo sono. Inoltre $V_3 \neq \mathbb{R}$ perché $X^2 \in V_3 \setminus \mathbb{R}$. Infine, è chiaro che $\mathbb{R} \subseteq V_4$ e resta da dimostrare che $V_4 \subseteq \mathbb{R}$. Dato $p \in V_4$, sia $a := p(0) \in \mathbb{R}$. Poiché $p(X+1) = p(X)$, si dimostra facilmente per induzione che $p(n) = a$ per ogni $n \in \mathbb{N}$. Allora $q := p - a \in A$ verifica $q(n) = p(n) - a = 0$ per ogni $n \in \mathbb{N}$. Tenendo conto che un polinomio non nullo a coefficienti in un dominio ha un numero finito di radici (pari al massimo al suo grado), si conclude che $q = 0$, cioè $p = a \in \mathbb{R}$.

4. (a) $\ker(f)$ è un ideale primo se e solo se $K[X]/\ker(f)$ è un dominio. Per il primo teorema di isomorfismo per anelli, $K[X]/\ker(f) \cong \mathrm{im}(f)$, e $\mathrm{im}(f)$ è un dominio perché sottoanello di F, che è un dominio. Dunque $\ker(f)$ è un ideale primo di $K[X]$.

   (b) Se f non è iniettivo, $\ker(f)$ è un ideale primo non nullo di $K[X]$. Allora $\ker(f)$ è massimale, perché $K[X]$ è un dominio a ideali principali. Ne segue che $\mathrm{im}(f) \cong K[X]/\ker(f)$ è un campo.

   (c) Osserviamo preliminarmente che $f(a) = a$ per ogni $a \in \mathbb{Q}$. Infatti $f(n) = n$ per ogni $n \in \mathbb{Z}$ perché $f|_{\mathbb{Z}} \colon \mathbb{Z} \to \mathbb{R}$ è un omomorfismo di anelli, e l'unico omomorfismo di anelli $\mathbb{Z} \to \mathbb{R}$ è l'inclusione. Se ne deduce che, se $a = nm^{-1}$ con $n, m \in \mathbb{Z}$ e $m \neq 0$, allora

$$f(a) = f(nm^{-1}) = f(n)f(m)^{-1} = nm^{-1} = a.$$

   Quindi f è l'omomorfismo di valutazione in $\sqrt{2}$, cioè $f(p) = p(\sqrt{2})$ per ogni $p \in \mathbb{Q}[X]$. Si trova allora $\ker(f) = (X^2 - 2)$: infatti $X^2 - 2 \in \ker(f)$ (e quindi $(X^2 - 2) \subseteq \ker(f)$) perché $f(X^2 - 2) = \sqrt{2}^2 - 2 = 0$. D'altra parte, essendo $X^2 - 2$ irriducibile (perché di secondo grado e senza radici) nel dominio a ideali principali $\mathbb{Q}[X]$, l'ideale $(X^2 - 2)$ è massimale. Dato che $\ker(f) \neq \mathbb{Q}[X]$ (poiché $1 \notin \ker(f)$), deve essere $\ker(f) = (X^2 - 2)$ per definizione di ideale massimale. È infine chiaro che $\mathrm{im}(f)$ coincide con il sottoanello (anche sottocampo, per il punto precedente) di $\mathbb{R}$

$$\mathbb{Q}[\sqrt{2}] := \{p(\sqrt{2}) \,:\, p \in \mathbb{Q}[X]\}.$$

   Tenendo conto che $\sqrt{2} \notin \mathbb{Q}$ e $\sqrt{2}^2 = 2 \in \mathbb{Q}$, è anche facile vedere che $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$.