Corso di Algebra 1 - a.a. 2014-2015

Prova scritta dell'8.9.2015

1. (a) Calcolare l'ordine di $\overline{29}$ in $\mathbb{Z}/56\mathbb{Z}^*$.

   (b) Determinare gli interi positivi x che verificano il seguente sistema di congruenze:
   $$\begin{cases} x \equiv 29^{131} \mod 56 \\ 16^x \equiv 11 \mod 7 \end{cases}$$

2. (a) Sia $f\colon \mathbb{Q} \to \mathbb{Q}$ un omomorfismo di gruppi. Dimostrare che esiste unico $q \in \mathbb{Q}$ tale che $f(a) = qa$ per ogni $a \in \mathbb{Q}$.

   (b) Dimostrare che il gruppo degli automorfismi $\mathrm{Aut}(\mathbb{Q})$ è isomorfo al gruppo moltiplicativo $\mathbb{Q}^*$.

3. Dato un anello A e $n \in \mathbb{Z}$, sia
   $$P_n(X) = 5X^4 + 9nX^3 + 6nX^2 + 15 \in A[X].$$
   Determinare per quali valori di n il polinomio P_n è irriducibile in ciascuno dei seguenti casi:

   (a) $A = \mathbb{Q}$;

   (b) $A = \mathbb{Z}$;

   (c) $A = \mathbb{Z}/2\mathbb{Z}$.

4. Si consideri l'ideale $I = (2X^2 + 3, X^2 - 1)$ di $\mathbb{Z}[X]$.

   (a) Dimostrare che $(5) \subseteq I$.

   (b) Si considerino gli ideali $J_1 = (X - \overline{1})$ e $J_2 = (X + \overline{1})$ di $\mathbb{Z}/5\mathbb{Z}[X]$. Indicando con $\pi\colon \mathbb{Z}[X] \to \mathbb{Z}/5\mathbb{Z}[X]$ l'omomorfismo di anelli indotto dalla proiezione naturale $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$, dimostrare che
   $$I = \pi^{-1}(J_1) \cap \pi^{-1}(J_2).$$

   (c) Dimostrare che $\mathbb{Z}[X]/I$ è isomorfo (come anello) a $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Soluzioni

1. (a) Essendo $\mathbb{Z}/56\mathbb{Z}^* \cong \mathbb{Z}/7\mathbb{Z}^* \times \mathbb{Z}/8\mathbb{Z}^*$ (dato che $56 = 7 \cdot 8$ con $\mathrm{mcd}(7,8) = 1$), si ottiene facilmente

$$\begin{aligned}\mathrm{ord}_{\mathbb{Z}/56\mathbb{Z}^*}(\overline{29}) &= \mathrm{mcm}(\mathrm{ord}_{\mathbb{Z}/7\mathbb{Z}^*}(\overline{29}), \mathrm{ord}_{\mathbb{Z}/8\mathbb{Z}^*}(\overline{29})) \\ &= \mathrm{mcm}(\mathrm{ord}_{\mathbb{Z}/7\mathbb{Z}^*}(\overline{1}), \mathrm{ord}_{\mathbb{Z}/8\mathbb{Z}^*}(\overline{5})) = \mathrm{mcm}(1,2) = 2.\end{aligned}$$

   (b) Per il punto precedente $29^2 \equiv 1 \mod 56$, da cui segue che

$$29^{131} = 29(29^2)^{65} \equiv 29 \cdot 1^{65} = 29 \mod 56,$$

   e dunque la prima congruenza si riduce a $x \equiv 29 \mod 56$. Per x positivo la seconda congruenza equivale a $\overline{16}^x = \overline{11}$ in $\mathbb{Z}/7\mathbb{Z}^*$. In tale gruppo $\mathrm{ord}(\overline{16}) = \mathrm{ord}(\overline{2}) = 3$ e $\overline{11} = \overline{4} = \overline{2}^2$, per cui $\overline{16}^x = \overline{11}$ se e solo se $x \equiv 2 \mod 3$. In conclusione, per x positivo, il sistema di partenza è equivalente al sistema

$$\begin{cases} x \equiv 29 \mod 56 \\ x \equiv 2 \mod 3. \end{cases}$$

   Essendo $\mathrm{mcd}(56,3) = 1$, per il teorema cinese del resto tale sistema ha un'unica soluzione modulo $56 \cdot 3 = 168$, che chiaramente è $x \equiv 29 \mod 168$.

2. (a) Posto $q = f(1)$, per ogni $n \in \mathbb{Z}$ si ha $f(n) = nf(1) = qn$. In generale, dato $a \in \mathbb{Q}$, esistono $n, m \in \mathbb{Z}$ con $m \neq 0$ tali che $a = n/m$. Risulta allora

$$qn = f(n) = f(ma) = mf(a),$$

   da cui si ottiene $f(a) = qn/m = qa$. L'unicità di q è ovvia, dovendo essere $q = q1 = f(1)$.

   (b) Consideriamo $\alpha\colon \mathrm{Aut}(\mathbb{Q}) \to \mathbb{Q}^*$ definita da $\alpha(f) = f(1)$. Intanto α è ben definita perché $\alpha(f) \in \mathbb{Q}^*$ (cioè $f(1) \neq 0 = f(0)$, essendo f iniettiva) per ogni $f \in \mathrm{Aut}(\mathbb{Q})$. Quanto visto nel punto precedente garantisce che α è iniettiva: se $f, g \in \mathrm{Aut}(\mathbb{Q})$ sono tali che $\alpha(f) = \alpha(g)$, entrambi coincidono con l'endomorfismo di $\mathbb{Q}$ definito dalla moltiplicazione per $f(1) = g(1)$, dunque $f = g$. È inoltre facile vedere che α è suriettiva: è immediato verificare che per ogni $q \in \mathbb{Q}$ la funzione $f_q\colon \mathbb{Q} \to \mathbb{Q}$ definita da $f_q(a) = qa$ è un omomorfismo,

ed è chiaro che se $q \neq 0$ allora f_q è un automorfismo (con inverso $f_{q^{-1}}$) tale che $\alpha(f_q) = q$. Per concludere che $\mathrm{Aut}(\mathbb{Q}) \cong \mathbb{Q}^*$, basta allora dimostrare che α è un omomorfismo di gruppi. Sempre per quanto visto al punto precedente, si ha infatti

$$\alpha(f \circ g) = (f \circ g)(1) = f(g(1)) = f(1)g(1) = \alpha(f)\alpha(g)$$

per ogni $f, g \in \mathrm{Aut}(\mathbb{Q})$.

3. Ricordiamo preliminarmente che un polinomio di grado positivo a coefficienti in $\mathbb{Z}$ (o più in generale in un dominio a fattorizzazione unica) è irriducibile se e solo se è primitivo ed è irriducibile come polinomio a coefficienti in $\mathbb{Q}$ (o più in generale nel campo dei quozienti del dominio).

   (a) P_n è irriducibile per ogni $n \in \mathbb{Z}$. Infatti, se n non è multiplo di 5, allora P_n è (primitivo e) irriducibile in $\mathbb{Z}[X]$ per il criterio di Eisenstein relativo al primo 3, dunque in particolare è irriducibile in $\mathbb{Q}[X]$. Se invece $n = 5m$ è un multiplo di 5, allora P_n è associato (in $\mathbb{Q}[X]$) a $5^{-1}P_n = X^4 + 9mX^3 + 6mX^2 + 3$, che è ancora (primitivo e) irriducibile in $\mathbb{Z}[X]$ per il criterio di Eisenstein relativo al primo 3, e quindi anche irriducibile in $\mathbb{Q}[X]$.

   (b) P_n è irriducibile se e solo se n non è multiplo di 5: abbiamo già osservato nel punto precedente che P_n è irriducibile in $\mathbb{Z}[X]$ se n non è multiplo di 5, mentre P_n non è primitivo (e dunque non è irriducibile) se n è multiplo di 5, perché in quel caso il massimo comune divisore dei suoi coefficienti è chiaramente 5.

   (c) P_n è irriducibile se e solo se n è dispari. Infatti per n pari $P_n = X^4 + \overline{1} = (X + \overline{1})^4$ non è irriducibile. Invece per n dispari $P_n = X^4 + X^3 + \overline{1}$ è irriducibile perché non ha radici ($P_n(\overline{0}) = P_n(\overline{1}) = \overline{1}$) e non è divisibile per l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}/2\mathbb{Z}[X]$, cioè $X^2 + X + \overline{1}$.

4. (a) Si ha $5 = 2X^2 + 3 - 2(X^2 - 1) \in I$, e quindi $(5) \subseteq I$. È utile osservare anche che $I = (5, X^2 - 1)$: ciò segue subito da quanto appena visto e dal fatto che, analogamente,

$$2X^2 + 3 = 5 + 2(X^2 - 1) \in (5, X^2 - 1).$$

   (b) Posto $I_1 = (5, X - 1)$ e $I_2 = (5, X + 1)$ in $\mathbb{Z}[X]$, poiché π è un omomorfismo suriettivo con $\ker(\pi) = (5)$, risulta $\pi^{-1}(J_i) = I_i$ (e $\pi(I_i) = J_i$), per $i = 1, 2$. Essendo $X^2 - 1 = (X - 1)(X + 1)$, è allora chiaro che

$$I = (5, X^2 - 1) \subseteq I_1 \cap I_2 = \pi^{-1}(J_1) \cap \pi^{-1}(J_2).$$

Per dimostrare l'inclusione opposta, dato $P \in I_1 \cap I_2$, si ha

$$\pi(P) \in \pi(I_1) \cap \pi(I_2) = J_1 \cap J_2.$$

D'altra parte $J_1 \cap J_2 = J_1 J_2$ perché $J_1 + J_2 = \mathbb{Z}/5\mathbb{Z}[X]$ (infatti $X + \overline{1} - (X - \overline{1}) = \overline{2} \in \mathbb{Z}/5\mathbb{Z}[X]^*$). Essendo

$$J_1 J_2 = ((X - \overline{1})(X + \overline{1})) = (X^2 - \overline{1}),$$

si conclude che $P \in \pi^{-1}((X^2 - \overline{1})) = (5, X^2 - 1) = I$.

(c) Per il terzo teorema di isomorfismo per anelli

$$\mathbb{Z}[X]/I \cong (\mathbb{Z}[X]/(5))/(I/(5)).$$

Ora, $\mathbb{Z}[X]/(5) \cong \mathbb{Z}/5\mathbb{Z}[X]$, e (ricordando che $I = (5, X^2 - 1)$) è chiaro che in questo isomorfismo l'ideale $I/(5)$ di $\mathbb{Z}[X]/(5)$ corrisponde a $(X^2 - \overline{1})$ in $\mathbb{Z}/5\mathbb{Z}[X]$. Se ne deduce che

$$\mathbb{Z}[X]/I \cong \mathbb{Z}/5\mathbb{Z}[X]/(X^2 - \overline{1}).$$

Come visto nel punto precedente, J_1 e J_2 sono due ideali coprimi di $\mathbb{Z}/5\mathbb{Z}[X]$ tali che $J_1 J_2 = (X^2 - \overline{1})$, dunque per il teorema cinese per anelli si ha

$$\mathbb{Z}/5\mathbb{Z}[X]/(X^2 - \overline{1}) \cong \mathbb{Z}/5\mathbb{Z}[X]/J_1 \times \mathbb{Z}/5\mathbb{Z}[X]/J_2.$$

Per concludere basta allora notare che $\mathbb{Z}/5\mathbb{Z}[X]/J_i \cong \mathbb{Z}/5\mathbb{Z}$ per $i = 1, 2$, essendo vero più in generale che $A[X]/(X - a) \cong A$ per ogni anello A e per ogni $a \in A$.