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

Prova scritta del 19/06/2019

1. Sia p un numero primo dispari e si consideri la congruenza

   (*) $$x^4 \equiv -1 \mod p.$$

   (a) Dimostrare che (*) ha una soluzione se e solo se $\mathbb{Z}/p\mathbb{Z}^*$ contiene un elemento di ordine 8.

   (b) Determinare il più piccolo valore di p tale che (*) ha una soluzione. Trovare inoltre tutte le soluzioni di (*) per tale valore di p.

2. Sia G un gruppo e siano H un sottogruppo di G e K un sottogruppo di H.

   (a) Dimostrare che la funzione

   $$f\colon G/K \to G/H, \qquad aK \mapsto aH$$

   è ben definita e suriettiva.

   (b) Dato $g \in G$, dimostrare che la funzione

   $$\phi\colon H/K \to G/K, \qquad hK \mapsto ghK$$

   è ben definita e iniettiva e che $\mathrm{im}(\phi) = f^{-1}(gH)$.

   (c) Dimostrare che se G è finito, allora $[G : K] = [G : H][H : K]$.

3. Sia $A = \{x \in \mathbb{Q} : 6^k x \in \mathbb{Z}, \text{ per qualche } k \in \mathbb{N}\}$.

   (a) Dimostrare che A è un sottoanello di $\mathbb{Q}$ contenente $\mathbb{Z}$.

   (b) Dimostrare che un intero positivo è invertibile in A se e solo se è della forma $2^i 3^j$ per qualche $i, j \in \mathbb{N}$.

   (c) Dimostrare che non esiste nessun omomorfismo di anelli $\mathbb{Q} \to A$.

4. Sia $f \in \mathbb{Z}[X]$ un polinomio monico. Siano inoltre p e q due numeri primi tali che f non ha radici in $\mathbb{Z}/p\mathbb{Z}$, mentre f ha una sola radice in $\mathbb{Z}/q\mathbb{Z}$, e tale radice ha molteplicità 1.

   (a) Dimostrare che f non ha radici in $\mathbb{Q}$.

   (b) Dimostrare che, se $\deg(f) = 4$, allora f è irriducibile in $\mathbb{Z}[X]$.

   (c) Fornire un esempio in cui $\deg(f) = 5$, $p = 2$, $q = 3$ e f non è irriducibile in $\mathbb{Z}[X]$.

Soluzioni

1. (a) Se $x \in \mathbb{Z}$ verifica (*), allora (ponendo $\overline{a} := a + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ per ogni $a \in \mathbb{Z}$) $\overline{x}^4 = \overline{-1}$. In particolare, dato che $\overline{-1} \neq \overline{0}$, deve essere $\overline{x} \neq \overline{0}$, cioè $\overline{x} \in \mathbb{Z}/p\mathbb{Z}^*$. Inoltre

$$\overline{x}^8 = (\overline{x}^4)^2 = \overline{-1}^2 = \overline{(-1)^2} = \overline{1},$$

il che implica che l'ordine di $\overline{x}$ in $\mathbb{Z}/p\mathbb{Z}^*$ è un divisore (positivo) di 8. D'altra parte tale ordine non è un divisore di 4 perché $\overline{x}^4 = \overline{-1} \neq \overline{1}$ (essendo $p > 2$), e dunque deve essere 8.

Viceversa, se $\mathbb{Z}/p\mathbb{Z}^*$ contiene un elemento $\overline{x}$ (per qualche $x \in \mathbb{Z}$) di ordine 8, allora $\overline{x}^8 = \overline{1}$ e $\overline{x}^4 \neq \overline{1}$. Si ha pertanto

$$\overline{0} = \overline{x}^8 - \overline{1} = (\overline{x}^4 - \overline{1})(\overline{x}^4 + \overline{1})$$

e $\overline{x}^4 - \overline{1} \neq \overline{0}$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un dominio, deve essere allora $\overline{x}^4 + \overline{1} = \overline{0}$, il che dimostra che x è soluzione di (*).

(b) Per il punto precedente, se esiste una soluzione di (*), $\mathbb{Z}/pZ^*$ contiene un elemento di ordine 8. Dunque, per il teorema di Lagrange, $8 \mid \#\mathbb{Z}/p\mathbb{Z}^* = p - 1$. Il più piccolo numero primo che verifica tale condizione è 17, e in effetti $p = 17$ è il valore cercato, dato che per esempio 2 è soluzione di (*). Inoltre, per quanto visto sopra, $x \in \mathbb{Z}$ è soluzione di (*) con $p = 17$ se e solo se $\overline{x} \in \mathbb{Z}/17\mathbb{Z}^*$ ha ordine 8. Poiché $\overline{2}$ ha ordine 8 anche $\overline{2}^i$ ha ordine $\frac{8}{\mathrm{mcd}(8,i)} = 8$ per ogni i intero dispari. In particolare hanno ordine 8 i 4 elementi distinti $\overline{2}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^5 = \overline{-2}$ e $\overline{2}^7 = \overline{-8}$. D'altra parte gli elementi di ordine 8 sono precisamente le radici nel campo $\mathbb{Z}/p\mathbb{Z}$ del polinomio di quarto grado $X^4 + 1$, e quindi sono al massimo 4. In conclusione le soluzioni di (*) per $p = 17$ sono $x \equiv \pm 2, \pm 8 \mod 17$.

2. (a) Se $g_1, g_2 \in G$ e $g_1K = g_2K$, allora $g_1^{-1}g_2 \in K$. Siccome $K \subset H$, $g_1^{-1}g_2 \in H$, dunque $g_1H = g_2H$. Pertanto f è ben definita. Se $x \in G/H$, allora $x = gH$ per qualche $g \in G$. Dunque $x = f(gK)$. Quindi f è suriettiva.

(b) Siano $h_1, h_2 \in H$. Osserviamo che $(gh_1)^{-1}(gh_2) = h_1^{-1}h_2$. Dunque $h_1K = h_2K \Rightarrow h_1^{-1}h_2 \in K \Rightarrow (gh_1)^{-1}(gh_2) \in K \Rightarrow gh_1K = gh_2K$. Pertanto ϕ è ben definita. Nello stesso modo $\phi(h_1K) = \phi(h_2K) \Rightarrow (gh_1)^{-1}(gh_2) \in K \Rightarrow h_1^{-1}h_2 \in K \Rightarrow h_1K = h_2K$. Quindi ϕ è iniettiva. Osserviamo poi che $f(\phi(hK)) = f(ghK) =$

$ghH = gH$. Questo dimostra l'inclusione $\mathrm{im}(\phi) \subset f^{-1}(gH)$. Viceversa, se $\bar{g}K \in f^{-1}(gH)$, allora $\bar{g}H = f(\bar{g}K) = gH \Rightarrow h := g^{-1}\bar{g} \in H \Rightarrow \bar{g} = gh \Rightarrow \bar{g}K = ghK = \phi(hK)$. Pertanto vale anche l'inclusione $f^{-1}(gH) \subset \mathrm{im}(\phi)$ e quindi abbiamo dimostrato l'uguaglianza $f^{-1}(gH) = \mathrm{im}(\phi)$.

(c) Poiché il dominio di una funzione è l'unione disgiunta delle fibre della funzione, si ha

$$\#(G/K) = \sum_{x \in G/H} \#f^{-1}(x).$$

Per il punto precedente $\#f^{-1}(x) = \#(H/K)$ per ogni $x \in G/H$, quindi

$$\begin{aligned}[G : K] = \#(G/K) &= \sum_{x \in G/H} \#(H/K) \\ &= \#(G/H)\#(H/K) = [G : H][H : K].\end{aligned}$$

In alternativa basta osservare che, essendo anche H e K finiti, per il teorema di Lagrange si ha

$$[G : K] = \frac{\#G}{\#K} = \frac{\#G}{\#H}\frac{\#H}{\#K} = [G : H][H : K].$$

3. (a) Chiaramente $\mathbb{Z} \subseteq A$ (in particolare $1 \in A$) perché $6^0 n = n \in \mathbb{Z}$ per ogni $n \in \mathbb{Z}$. Se poi $a, b \in A$, esistono $i, j \in \mathbb{N}$ tali che $m := 6^i a, n := 6^j b \in \mathbb{Z}$. Allora $6^{i+j}(a - b) = 6^j m - 6^i n \in \mathbb{Z}$ e $6^{i+j} ab = mn \in \mathbb{Z}$, il che dimostra che $a - b, ab \in A$, e pertanto A è un sottoanello di $\mathbb{Q}$.

(b) Un intero positivo n è invertibile in A se e solo se $\frac{1}{n} \in A$, e per definizione questo succede se e solo se esiste $k \in \mathbb{Z}$ tale che $\frac{6^k}{n} \in \mathbb{Z}$. Dunque $n \in A^*$ se e solo se $n \mid 6^k = 2^k 3^k$ per qualche $k \in \mathbb{N}$, e (tenendo conto del teorema fondamentale dell'aritmetica) questo è vero se e solo se $n = 2^i 3^j$ per qualche $i, j \in \mathbb{N}$.

(c) Supponiamo per assurdo che $f\colon \mathbb{Q} \to A$ sia un omomorfismo di anelli. Allora $f|_{\mathbb{Z}}$ è l'unico omomorfismo di anelli $\mathbb{Z} \to A$, cioè l'inclusione. Poiché un omomorfismo di anelli manda elementi invertibili in elementi invertibili, per ogni intero positivo n si ha $n = f(n) \in A^*$, dato che $n \in \mathbb{Q}^*$. Questo è però falso, perché, per il punto precedente, $n \notin A^*$ se n non è della forma $2^i 3^j$ per qualche $i, j \in \mathbb{N}$ (per esempio $n = 5$). Dunque non esiste nessun omomorfismo di anelli $\mathbb{Q} \to A$.

4. (a) Se f avesse una radice $x \in \mathbb{Q}$, allora (essendo f monico) x sarebbe intera, quindi $[x]_p$ sarebbe una radice di f in $\mathbb{Z}/p\mathbb{Z}$, contro l'ipotesi.

   (b) Supponiamo per assurdo che $f = gh$ sia una fattorizzazione non banale in $\mathbb{Z}[X]$. Possiamo supporre che anche g e h siano monici e che $0 < \deg(g) \leq \deg(h)$. Se $\deg(g) = 1$, allora g e quindi f avrebbero una radice in $\mathbb{Z}$, contraddicendo il punto precedente. Perciò l'unica possibilità è $\deg(g) = \deg(h) = 2$. Per ipotesi o g o h ha una radice in $\mathbb{Z}/q\mathbb{Z}$. Supponiamo che sia g ad avere la radice. Per il teorema di Ruffini in $\mathbb{Z}/q\mathbb{Z}[X]$ il polinomio g si fattorizza in un fattore lineare per un altro fattore lineare. Dunque g ha due radici distinte o una solo radice doppia. Entrambe le possibilità sono escluse per ipotesi. Quindi non può esistere una fattorizzazione non banale.

   (c) Ragionando come nel punto (b) si vede che le fattorizzazioni non banali possibili sono $f = gh$ con $\deg(g) = 2$, $\deg(h) = 3$. Quindi cerchiamo due polinomi $g, h \in \mathbb{Z}[X]$, g quadratico e h cubico, tali che g non ha radice né su $\mathbb{Z}/2\mathbb{Z}$, né su $\mathbb{Z}/3\mathbb{Z}$, mentre h non ha radice su $\mathbb{Z}/2\mathbb{Z}$ ed ha una sola radice su $\mathbb{Z}/3\mathbb{Z}$ e questa è semplice. Quindi innazitutto $g \mod 2$ deve essere l'unico polinomio quadratico senza radici in $\mathbb{Z}/2\mathbb{Z}$, cioè $g = X^2 + X + 1 \mod 2$. Vogliamo inoltre che g non abbia radici su $\mathbb{Z}/3\mathbb{Z}$. Possiamo scegliere per esempio $g = X^2 + 3X + 1$. Questo soddisfa le richieste. Per costruire h, imponiamo che abbia una sola radice in $\mathbb{Z}/3\mathbb{Z}$: per esempio possiamo imporre che $h = (X-1)g = (X-1)(X^2+3X+1) = X^3+2X^2-2X-1 \mod 3$. Il polinomio X^3+2X^2-2X-1 ha però una radice in $\mathbb{Z}/2\mathbb{Z}$. Lo modifichiamo in modo da renderlo privo di radici in $\mathbb{Z}/2\mathbb{Z}$, senza però cambiare la sua classe $\mod 3$. Per esempio possiamo sottrarre $3X$: scegliamo cioè $h = X^3+2X^2-5X-1$. Allora $h = (X-1)g \mod 3$, mentre $h = X^3 + X + 1 \mod 2$ non ha radici. Quindi $f = gh$ è un polinomio riducibile con le proprietà richieste.