Prova scritta di Algebra

7 luglio 2016

1. Si consideri la mappa $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/18\mathbb{Z}$ la mappa definita da $x \mapsto [7x+3]_{18}$.

a) Si determinino le immagini tramite ϕ degli interi 0 e 1 e si dica se ϕ è un omomorfismo di anelli unitari motivando la risposta in modo appropriato.

b) Si determini la controimmagine di $[5]_{18}$.

c) Si dica se ϕ è iniettiva e/o suriettiva motivando la risposta.

2. In S_9 siano

$$\alpha = (1,4,5,3,6)(1,5,2,4)(3,7,9,8,1,5)(1,8,4,7,3,5) \text{ e } \beta = (8,1,7)(4,9)(1,2,3,4,5,8).$$

a) Si scrivano α e β come prodotto di cicli disgiunti e si dica se sono permutazioni pari o dispari motivando la risposta.

b) Si determini $H = \langle \alpha \rangle \cap \langle \beta \rangle$ e si dica se H è un sottogruppo di $\langle \alpha^2 \rangle$.

c) Si dica se $\langle \beta^2 \rangle = \langle \beta^4 \rangle$.

3. Siano G e H due gruppi e sia $f : G \to H$ un omomorfismo di gruppi. Sia g un elemento di G.

a) Provare che se g ha periodo finito n allora $f(g)$ ha periodo finito m, con m divisore di n.

b) Provare che se $f(g)$ ha periodo finito m, allora $g^m \in \mathrm{Ker} f$.

c) Trovare un esempio in cui $f(g)$ ha periodo finito mentre g ha periodo infinito.

4. Si consideri l'anello dei polinomi $\mathbb{Z}_7[x]$.

a) Si dica se $\mathbb{Z}_7[x]$ è un dominio a fattorizzazione unica motivando la risposta.

b) Sia I l'ideale generato da $p(x) := x^4 + x^3 - x^2 - 5x + 1 \in \mathbb{Z}_7[x]$. Si dica se I è un ideale massimale di $\mathbb{Z}_7[x]$.

c) Si determinino gli ideali massimali dell'anello quoziente $A := \mathbb{Z}_7[x]/I$.

d) Si trovi, se possibile, un divisore proprio di zero di A o eventualmente si dica perchè A non contiene divisori propri di zero.

5. Siano $f(x) = x^4 - 3x^3 + x - 3$ e $g(x) = x^3 - 10x + 3$ in $\mathbb{Q}[x]$.

a) Determinare il massimo divisore monico $d(x)$ di f e g.

b) Determinare due polinomi $a(x), b(x) \in \mathbb{Q}[x]$ tali che

$$d(x) = a(x)f(x) + b(x)g(x).$$

Soluzioni

Esercizio 1.

a) Si ha $\phi(0) = [7 \cdot 0 + 3]_{18} = [3]_{18}$ e $\phi(1) = [7 \cdot 1 + 3]_{18} = [10]_{18}$. Se ϕ fosse un omomorfismo di anelli dovrebbe essere $\phi(0) = [0]_{18}$. Poichè $\phi(0) = [3]_{18} \neq [0]_{18}$, possiamo concludere che ϕ non è un omomorfismo di anelli (nemmeno di gruppi).

b) La controimmagine di $[5]_{18}$ è l'insieme

$$\begin{aligned} \phi^{-1}([5]_{18}) &= \{x \in \mathbb{Z} \mid \phi(x) = [5]_{18}\} \\ &= \{x \in \mathbb{Z} \mid [7x+3]_{18} = [5]_{18}\} \\ &= \{x \in \mathbb{Z} \mid 7x + 3 \equiv 5 \bmod 18\}. \end{aligned}$$

La controimmagine di $[5]_{18}$ è quindi l'insieme delle soluzioni della congruenza

$$7x + 3 \equiv 5 \bmod 18$$

che, usando le proprietà delle congruenze, diventa

$$7x \equiv 2 \bmod 18.$$

Abbiamo che il massimo comun divisore tra 7 e 18 è 1 che divide 2. Quindi la congruenza ha soluzione. Una soluzione particolare è 8 perchè $7 \cdot 8 = 56 = 2 + 18 \cdot 3$. La soluzione generle è quindi $x = 8 + 18k$, $k \in \mathbb{Z}$ e quindi

$$\phi^{-1}([5]_{18}) = 8 + 18\mathbb{Z}.$$

c) ϕ non è iniettiva perchè come si è visto nel punto *b*) la controimmagine di $[5]_{18}$ contiene più di un elemento. Invece è suriettiva perchè la congruenza $7x + 3 \equiv a \bmod 18$ ha soluzioni per ogni $a \in \mathbb{Z}$; infatti, essendo $M.C.D.(7, 18) = 1$, si ha che per ogni $a \in \mathbb{Z}$, il $M.C.D.(7, 18)$ divide $a - 3$ e questa è la condizione sufficiente perchè la congruenza abbia soluzione.

Esercizio 2.

a) Si ha $\alpha = (1, 3, 6)(2, 5)(8, 4, 9)$ e $\beta = (7, 8)(1, 2, 3, 9, 4, 5)$. Il segno di α è $(-1)^2(-1)(-1)^2 = (-1)^5 = -1$ quindi α è dispari. Il segno di β è $(-1)(-1)^5 = 1$, quindi β è pari.

b) Abbiamo che

$$\langle\alpha\rangle = \{id, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$$

e

$$\langle\beta\rangle = \{id, \beta, \beta^2, \beta^3, \beta^4, \beta^5\}.$$

Calcoliamo le potenze di α e β:

$$\alpha^2 = (1, 3, 6)^2(2, 5)^2(8, 4, 9)^2 = (1, 6, 3)(8, 9, 4)$$

$$\alpha^3 = (1, 3, 6)^3(2, 5)^3(8, 4, 9)^3 = (2, 5)$$

$$\alpha^4 = (1, 3, 6)^4(2, 5)^4(8, 4, 9)^4 = (1, 6, 3)(8, 4, 9)$$

$$\alpha^5 = (1, 3, 6)^5(2, 5)^5(8, 4, 9)^5 = (1, 6, 3)(2, 5)(8, 9, 4)$$

$$\alpha^6 = id$$

$$\beta^2 = (7, 8)^2(1, 2, 3, 9, 4, 5)^2 = (1, 3, 4)(2, 9, 5)$$

$$\beta^3 = (7,8)^3(1,2,3,9,4,5)^3 = (7,8)(1,9)(2,4)(3,5)$$
$$\beta^4 = (7,8)^4(1,2,3,9,4,5)^4 = (1,4,3)(2,5,9)$$
$$\beta^5 = (7,8)^5(1,2,3,9,4,5)^5 = (7,8)(1,5,4,9,3,2)$$
$$\beta^6 = id.$$

Quindi $H = \{id\}$. H è sottogruppo di $\langle \alpha^2 \rangle$, perchè H è contenuto in $\langle \alpha^2 \rangle$ ed è un sottogruppo di S_9 perchè è intersezione di sottogruppi.

c) Si ha che

$$|\langle \beta^2 \rangle| = o(\beta^2) = \frac{o(\beta)}{M.C.D.(o(\beta), 2)} = 3 = \frac{o(\beta)}{M.C.D.(o(\beta), 4)} = o(\beta^4) = |\langle \beta^4 \rangle|.$$

Poichè $\langle \beta \rangle$ ha un solo sottogruppo di cardinalità 3 (per la struttura dei gruppi ciclici), possiamo dedurre che $\langle \beta^2 \rangle = \langle \beta^4 \rangle$.

Esercizio 3.

a) Poichè g ha periodo n abbiamo che $g^n = 1_G$. Applicando f a questa uguaglianza e usando il fatto che $f(1_G) = 1_H$ otteniamo

$$1_H = f(1_G) = f(g^n) = [f(g)]^n.$$

Pertanto $f(g)$ ha periodo finito m con m divisore di n.

b) Supponiamo ora che $f(g)$ abbia periodo m. Allora $[f(g)]^m = 1_H$. Ma f è un omomorfismo e quindi

$$1_H = [f(g)]^m = f(g^m),$$

cioè g^m sta nel nucleo di f.

c) Si prenda $G = (\mathbb{Z}, +, 0)$ e $H = (\mathbb{Z}/8\mathbb{Z}, +, [0]_8)$ e $f : G \to H$ definita da $x \mapsto [x]_8$. Il gruppo H ha ordine 8 e quindi ogni suo elemento ha periodo finito (un divisore di 8). Invece in $\mathbb{Z}$ tutti gli elementi diversi da 0 hanno periodo infinito. Possiamo quindi prendere ad esempio $g = 1$.

Esercizio 4.

a) Poichè $\mathbb{Z}_7$ è un campo, $\mathbb{Z}_7[x]$ è un dominio euclideo e quindi anche un dominio a fattorizzazione unica.

b) $I = (x^4+x^3-x^2-5x+1)$ è un ideale massimale di $\mathbb{Z}_7[x]$ se e solo se $p(x) := x^4+x^3-x^2-5x+1$ è irriducibile in $\mathbb{Z}_7[x]$. Si ha che

$$\begin{array}{rcl}
p(0) & = & 0^4 + 0^3 - 0^2 - 5 \cdot 0 + 1 = 1 \\
p(1) & = & 1^4 + 1^3 - 1^2 - 5 \cdot 1 + 1 = -3 \\
p(2) & = & 2^4 + 2^3 - 2^2 - 5 \cdot 2 + 1 = 4 \\
p(3) & = & 3^4 + 3^3 - 3^2 - 5 \cdot 3 + 1 = 1 \\
p(4) & = & p(-3) = (-3)^4 + (-3)^3 - (-3)^2 - 5(-3) + 1 = 1 \\
p(5) & = & p(-2) = (-2)^4 + (-2)^3 - (-2)^2 - 5(-2) + 1 = 1 \\
p(6) & = & p(-1) = (-1)^4 + (-1)^3 - (-1)^2 - 5(-1) + 1 = 5.
\end{array}$$

Quindi $p(x)$ non ha radici in $\mathbb{Z}_7$. Questo non significa che $p(x)$ è irriducibile perchè il polinomio ha grado 4. cerco una fattorizzazione come prodotto di due polinomi di secondo grado. Dall' uguaglianza

$$x^4 + x^3 - x^2 - 5x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

ricaviamo il sistema

$$\begin{cases} a + c = 1 \\ b + ac + d = -1 \\ ad + bc = -5 \\ bd = 1 \end{cases} \qquad \begin{cases} c = 1 - a \\ b + a(1 - a) + d = -1 \\ ad + b(1 - a) = -5 \\ bd = 1 \end{cases}$$

Dall'ultima equazione si ricava che b e d devono essere uno l'inverso dell'altro. Qunidi le possibili coppie (b, d) sono $(1, 1), (2, 4), (3, 5), (4, 2), (5, 3), (-1, -1)$. Se $b = d$, dalla penultima equazione si ricava $b = -5$ e dall'ultima $b^2 = 1$ che è impossibile. Quindi deve essere $b \neq d$. Dobbiamo quindi considerare i due casi $(b, d) = (2, 4)$ e $(b, d) = (3, 5)$.

Supponiamo $(b, d) = (2, 4)$. La terza equazione diventa:

$$4a + 2 - 2a = -5$$

da cui ricaviamo $2a = 0$, quindi $a = 0$ e (dalla prima equazione) $c = 1$. Ottenaimo così la fattorizzazione

$$x^4 + x^3 - x^2 - 5x + 1 = (x^2 + 2)(x^2 + x + 4).$$

Quindi $p(x)$ non è irriducibile e I non è massimale.

c) Gli ideli massimali di A sono del tipo $(f(x))/I$ con $f(x)$ polinomio irriducibile che divide $p(x)$. Quindi gli ideali massimali di A sono

$$\frac{(x^2 + 2)}{I} \quad \text{e} \quad \frac{(x^2 + x + 4)}{I}.$$

d) Un divisore di zero di A è $(x^2 + 2) + I$ perchè è un elemento diverso da zero e $[(x^2 + 2) + I][(x^2 + x + 4) + I] = p(x) + I = 0 + I$.

Esercizio 5. Usiamo l'algoritmo di Euclide per determinare il massimo comun divisore di f e g e i due polinomi $a(x)$ e $b(x)$.

$$\begin{array}{rrrr|l} x^4 - 3x^3 & & + x - 3 & & x^3 - 10x + 3 \\ \cline{5-5} -x^4 & + 10x^2 - 3x & & & x - 3 \\ \hline -3x^3 + 10x^2 - 2x - 3 & & & & \\ 3x^3 & - 30x + 9 & & & \\ \hline & 10x^2 - 32x + 6 & & & \end{array}$$

Osserviamo $10x^2 - 32x + 6 = 2(5x^2 - 16x + 3)$.

$$\begin{array}{r|l} x^3 \qquad\qquad - 10x + 3 & 5x^2 - 16x + 3 \\ \cline{2-2} -x^3 + \frac{16}{5}x^2 - \frac{3}{5}x \qquad & \frac{1}{5}x + \frac{16}{25} \\ \hline \frac{16}{5}x^2 - \frac{53}{5}x + 3 & \\ -\frac{16}{5}x^2 + \frac{256}{25}x - \frac{48}{25} & \\ \hline -\frac{9}{25}x + \frac{27}{25} & \end{array}$$

Osserviamo che $-\frac{9}{25}x + \frac{27}{25} = -\frac{9}{25}(x-3)$.

$$
\begin{array}{r|l}
5x^2 - 16x + 3 & x - 3 \\ \cline{2-2}
-5x^2 + 15x \quad & 5x - 1 \\ \cline{1-1}
-x + 3 & \\
x - 3 & \\ \cline{1-1}
0 &
\end{array}
$$

Algoritmo di Euclide

$$
\begin{array}{ccc}
1 & 0 & f \\
0 & 1 & g \\
1 & -(x-3) & 10x^2 - 32x + 6 \\
-\frac{1}{5}x - \frac{16}{25} & 1 - (x-3)(1/5x + 16/25) & -\frac{9}{25}x + \frac{27}{25} \\
* & * & 0
\end{array}
$$

ottenendo cosi che

$$
a(x) = \frac{5}{9}\left(\frac{1}{2}x + \frac{8}{5}\right) \quad \text{e} \quad b(x) = -\frac{5}{9}\left(\frac{1}{2}x^2 + \frac{1}{10} + \frac{1}{5}\right).
$$