Prova scritta di Algebra

9 Febbraio 2017

1. Si risolva il seguente sistema di congruenze lineari

$$\begin{cases} x \equiv 8 \mod 3 \\ 3x \equiv 2 \mod 5 \\ x \equiv 3 \mod 8 \end{cases}$$

2. In S_9 sia $\alpha = (1,3)(3,5,6)(5,3)(4,2,7)(2,1,4,7,5,9)(8,9,5)$

a) Si scriva α come prodotto di cicli disgiunti e come prodotto di trasposizioni. Si dica se α è pari o dispari motivando la risposta.

b) Si elenchino i sottogruppi di $\langle\alpha\rangle$ e si dica se $\langle\alpha^4\rangle = \langle\alpha^7\rangle$.

c) Si scriva la tabella motiplicativa del gruppo quoziente $\langle\alpha\rangle/\langle\alpha^4\rangle$

3. Siano $R = M_2(\mathbb{Z})$ e $I = \{\begin{pmatrix} 5a & 5b \\ 5c & 5d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}\}$.

a) Si mostri che la mappa $\varphi\colon R \to M_2(\mathbb{Z}/5\mathbb{Z})$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ è un omomorfismo di anelli suriettivo (dove $\bar{x} := [x]_5$).

b) Si provi che I è un ideale di R.

c) Si dica se I è un ideale massimale di R (sugg. usare i punti a) e b)).

4. Sia I l'ideale di $\mathbb{Q}[x]$ generato dal polinomio $f(x) = x^2 + 3$.

a) Si dica se I è un ideale massimale di $Q[x]$ motivando la risposta.

b) Si dica se l'elemento $(x+2)+I$ è un elemento invertibile nell'anello $A := \mathbb{Q}[x]/I$ e in caso affermativo si calcoli l'inverso.

5. Si consideri il polinomio:

$$f(x) = x^5 + 2x^4 + 3x^3 + 6x^2 - 40x - 80.$$

Si fattorizzi $f(x)$ in prodotto di fattori irriducibili in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$.

Risoluzione

1. La soluzione del sistema è $x = 17 + 105k$.

2. Si ha $\alpha = (1,3,4)(2,5,6,8,9)$ e come prodotto di trasposizioni

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

Quindi α è pari.

b) Scrivendo α come prodotto di cicli disgiunti, le lunghezze dei suoi cicli sono $3,5$ perció il periodo di α è $m.c.m.(3,5) = 15$. Quindi $< \alpha >$ è un gruppo ciclico di ordine 15 e per il teorema sui sottogruppi dei gruppi ciclici, i sottogruppi di $< \alpha >$ sono tutti ciclici e in corrispondenza biunivoca con i divisori di 15, ovvero: $1,3,5,15$. La corrispondenza è quella che fa corrispondere ad ogni sottogruppo il suo ordine. Abbiamo quindi il sottogruppo corrispondente a 1 che è $\{id\}$ e quello corrispondente a 15 che è $\langle\alpha\rangle$. Al divisore 3 corrisponde il sottogruppo $< \alpha^5 >$. In modo analogo si vede che il sottogruppo di ordine 5 è $< \alpha^3 >$.

Si ha che $\langle\alpha^4\rangle \neq \langle\alpha^6\rangle$, infatti α^4 ha periodo $15/MCD(15,4) = 15$ e quindi $\langle\alpha^4\rangle = \langle\alpha\rangle$. Invece α^6 ha periodo $15/MCD(15,6) = 5$ e quindi $< \alpha^6 >$ è l'unico sottogruppo di $< \alpha >$ di ordine 5.

c)

$\cdot$	$\langle\alpha\rangle$	$\langle\alpha\rangle\alpha$	$\langle\alpha\rangle\alpha^2$
$\langle\alpha\rangle$	$\langle\alpha\rangle$	$\langle\alpha\rangle\alpha$	$\langle\alpha\rangle\alpha^2$
$\langle\alpha\rangle\alpha$	$\langle\alpha\rangle\alpha$	$\langle\alpha\rangle\alpha^2$	$\langle\alpha\rangle$
$\langle\alpha\rangle\alpha^2$	$\langle\alpha\rangle\alpha^2$	$\langle\alpha\rangle$	$\langle\alpha\rangle\alpha$

3. Vediamo che HN è sottogruppo di G. Intanto $HN \neq \emptyset$ perchè $1_G \in H \cap N$ e $1_G = 1_G \cdot 1_G \in HN$. Siano $g_1, g_2 \in HN$. Allora $g_1 = h_1 n_1$ e $g_2 = h_2 n_2$ per qualche $h_1, h_2 \in H$ e $n_1, n_2 \in N$. Abbiamo

$$g_1 g_2^{-1} = (h_1 n_1)(h_2 n_2)^{-1} = (h_1 n_1)(n_2^{-1} h_2^{-1}) = h_1 (h_2^{-1} h_2)(n_1 n_2^{-1}) h_2^{-1} =$$

$$= (h_1 h_2^{-1}) h_2 (n_1 n_2^{-1}) h_2^{-1}$$

Ora $(h_1 h_2^{-1}) \in H$ perchè H è un sottogruppo, $n_1 n_2^{-1} \in N$ perchè N è un sottogruppo e $h_2(n_1 n_2^{-1})h_2^{-1} \in N$ perchè N è normale in G. Pertanto $g_1 g_2^{-1} \in HN$ e HN è un sottogruppo di G.

Vediamo ora che $H \cap N$ è un sottogruppo normale di H. $H \cap N$ è intersezione di due sottogruppi di G e quindi è un sottogruppo di G. Essendo contenuto in H, esso è anche un sottogruppo di H. Vediamo che è normale in H. Siano $n \in H \cap N$ e $h \in H$. Dobbiamo verificare che $h^{-1} n h \in H \cap N$. È chiaro che $h^{-1} n h$ è un elemento di H perchè h e n stanno in H e H è un sottogruppo di G (quindi è chiuso per inversi e prodotti). Inoltre, $n \in N$ e poichè N è normale in G anche $h^{-1}nh \in N$. Così $h^{-1}nh \in H \cap N$.

4. *a*) Abbiamo

$$\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) = \varphi(\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}) =$$

$$= \begin{pmatrix} \overline{a+a'} & \overline{b+b'} \\ \overline{c+c'} & \overline{d+d'} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} + \begin{pmatrix} \overline{a'} & \overline{b'} \\ \overline{c'} & \overline{d'} \end{pmatrix} = \varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) + \varphi(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}).$$

e

$$\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) = \varphi(\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}) =$$

$$= \begin{pmatrix} \overline{aa'+bc'} & \overline{ab'+bd'} \\ \overline{ca'+dc'} & \overline{cb'+dd'} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \begin{pmatrix} \overline{a'} & \overline{b'} \\ \overline{c'} & \overline{d'} \end{pmatrix} = \varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix})\varphi(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}).$$

Ciò prova che φ è un omomorfismo di anelli. È immediato vedere che è suriettivo.

b) Abbiamo che $Ker\varphi = I$, quindi I è un ideale di R.

c) Applicando il primo teorema di omomorfismo per gli anelli a φ abbiamo che $R/I \cong M_2(\mathbb{Z}/3\mathbb{Z})$. Ora $M_2(\mathbb{Z}/3\mathbb{Z})$ non è un campo perchè contiene matrici non nulle che non sono invertibili, ad esempio

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}.$$

Dall'isomorfismo segue che R/I non è un campo e quindi I non è un ideale massimale.

5.

a) Essendo $f(x)$ un polinomio di terzo grado, $f(x)$ è irriducibile in $\mathbb{Z}_5[x]$ se e solo se non ha radici in $\mathbb{Z}_5$. Per semplicità di notazione non sciveremo le parentesi quadre. Abbiamo:

$$f(0) = 3 \neq 0$$
$$f(1) = 1 \neq 0$$
$$f(2) = 1 \neq 0,$$
$$f(3) = 4 \neq 0,$$
$$f(4) = 2 \neq 0,$$

dunque $f(x)$ è irriducibile in $\mathbb{Z}_5[x]$.

b) Si osserva che 1 e -1 sono radici di $g(x)$ e

$$g(x) = f(x)(x^2 - 1).$$

Quindi la fattorizzazione in irriducibili di $g(x)$ in $\mathbb{Z}_5[x]$ è

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

c) Determiniamo il massimo comun divisore tra f e g con il metodo delle divisioni successive. Il massimo comun divisore sarà l'ultimo resto non nullo.

$$
\begin{array}{r|l}
x^4+2x^3+2x^2+3x+2 & x^2+2x+3 \\ \cline{2-2}
-x^4-2x^3-3x^2 & x^2-1 \\ \cline{1-1}
x^2+3x+2 & \\
-x^2+2x+3 & \\ \cline{1-1}
5x+5 &
\end{array}
$$

$$
\begin{array}{r|l}
x^2+2x+3 & x+1 \\ \cline{2-2}
-x^2-x & x+1 \\ \cline{1-1}
x+3 & \\
-x-1 & \\ \cline{1-1}
2 &
\end{array}
$$

Quindi un massimo comun divisore di f e g è 2. Ciò implica che il massimo comun divisore monico è 1. Determiniamo ora i polinomi $a(x)$ e $b(x)$.

Dalla prima divisione abbiamo che

$$x+1=\frac{1}{5}g(x)-\frac{1}{5}f(x)(x^2-1)$$

dalla seconda divisione abbiamo che

$$2=f(x)-(x+1)^2.$$

Sostituendo un $(x+1)$ nella seconda uguaglianza abbiamo

$$2=f(x)-(x+1)[\frac{1}{5}g(x)-\frac{1}{5}f(x)(x^2-1)]$$

e dividendo tutto per 2

$$1=\frac{1}{2}f(x)-\frac{1}{10}g(x)(x+1)+\frac{1}{10}f(x)(x+1)(x^2-1)$$

$$1=f(x)\frac{1}{10}(x^3+x^2-x+4)+g(x)\frac{1}{10}(-x-1).$$

Pertanto

$$a(x)=\frac{1}{10}(x^3+x^2-x+4) \quad \text{e} \quad b(x)=\frac{1}{10}(-x-1).$$