Prova scritta di Algebra

9 giugno 2016

1. Si risolva il seguente sistema di congruenze lineari

$$\begin{cases} x \equiv 4 \mod 7 \\ 11x \equiv 2 \mod 15 \\ x \equiv 3 \mod 8 \end{cases}$$

2. In S_{10} sia $\alpha = (7,10)(2,1,6,8,5,7)(6,2,8)(5,9)(9,5,4)(1,9)$.

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 determinino i sottogruppi di $\langle\alpha\rangle$ e si dica se $\langle\alpha^3\rangle = \langle\alpha^7\rangle$.

c) Si scriva la tabella motiplicativa del gruppo quoziente $\langle\alpha\rangle/\langle\alpha^3\rangle$

3. Sia $G = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}\}$ e sia $\delta : G \longrightarrow \mathbb{R}^*$, $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mapsto e^a$.

a) Si verifichi che G è un sottogruppo di $GL(2,\mathbb{R})$.

b) Si verifichi che la mappa δ è un omomorfismo di gruppi di G nel gruppo moltiplicativo dei numeri reali non nulli.

c) Si determini il nucleo di δ e si dica se δ è suriettiva.

4. Si consideri l'anello dei polinomi $\mathbb{Z}_5[x]$.

a) Si dica se $\mathbb{Z}_5[x]$ è un dominio a ideali principali motivando la risposta.

b) Sia I l'ideale generato da $p(x) := x^4 + 3x^2 + 2 \in \mathbb{Z}_5[x]$. Si dica se I è un ideale massimale di $\mathbb{Z}_5[x]$.

c) Si determinino gli ideali massimali dell'anello quoziente $A := \mathbb{Z}_5[x]/I$. A è un campo?

5. Siano $f(x) = x^5 + x^4 - 2x^3 + x^2 + x - 2$ e $g(x) = x^3 + 3x^2 + x - 2$ 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. Poichè $MCD(7, 15, 8) = 1$, il sistema ha soluzione.
La prima equazione del sistema ha soluzione

$$x = 4 + 7k \quad k \in \mathbb{Z}.$$

Sostituendo nella seconda si ottiene

$$11(4 + 7k) \equiv 2 \bmod 15$$

da cui moltiplicando e riducendo tutti i numeri modulo 15,

$$\begin{aligned} -1 + 2k &\equiv 2 \bmod 15 \\ 2k &\equiv 3 \bmod 15 \\ k &\equiv 24 \bmod 15 \\ k &\equiv 9 \bmod 15 \end{aligned}$$

dove nel penultimo passaggio si è moltiplicato ambo i membri per 8. Si ottiene quindi come soluzione

$$k = 9 + 15h \quad h \in \mathbb{Z},$$

da cui otteniamo le soluzioni comuni delle prime due conguenze

$$x = 4 + 7(9 + 15h) = 67 + 105h \quad h \in \mathbb{Z}. \tag{1}$$

Sostituiamo queste soluzioni nella terza equazione

$$\begin{aligned} 67 + 105h &\equiv 3 \bmod 8 \\ 3 + h &\equiv 3 \bmod 8 \\ h &\equiv 0 \bmod 8 \end{aligned}$$

da cui otteniamo la soluzione

$$h = 8l \quad l \in \mathbb{Z}.$$

Sostituendo infine il valore di h nell'espressione (1) otteniamo le soluzioni del sistema

$$x = 67 + 105(8l) = 67 + 840l.$$

Esercizio 2.

a) $\alpha = (1, 9, 6)(2, 5, 4, 10, 7)$ è prodotto di cicli disgiunti.
$\alpha = (1, 9)(9, 6)(2, 5)(5, 4)(4, 10)(10, 7)$ è prodotto di trasposizioni
α è pari, perché esprimibile come prodotto di un numero pari di trasposizioni.

b) Scrivendo α come prodotto di cicli disgiunti, le lunghezze dei suoi cicli sono 3 e 5, perció il periodo di α è $m.c.m.(3,5) = 15$. Quindi $\langle\alpha\rangle$ è un gruppo ciclico di ordine 15 e per il teorema sui sottogruppi dei gruppi ciclici, i sottogruppi di $\langle\alpha\rangle$ sono tutti ciclici e in corrinspondenza 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 $\langle\gamma\rangle$ dove γ deve essere una potenza di α di periodo 3. Quindi si può prendere $\gamma = \alpha^5$ ottenendo cosi il sottogruppo $\langle\alpha^5\rangle$. In modo analogo si vede che il sottogruppo di ordine 5 è $\langle\alpha^3\rangle$.

Si ha che $\langle\alpha^3\rangle \neq \langle\alpha^7\rangle$, infatti α^3 ha periodo $15/MCD(15,3) = 5$ e quindi $\langle\alpha^3\rangle$ è l'unico sottogruppo di $\langle\alpha\rangle$ di ordine 5, mentre α^7 ha periodo $15/MCD(15,7) = 15$ e quindi $\langle\alpha^7\rangle = \langle\alpha\rangle$.

c)

$\cdot$	$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha^2$
$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha^2$
$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha^2$	$\langle\alpha^3\rangle$
$\langle\alpha^3\rangle\alpha^2$	$\langle\alpha^3\rangle\alpha^2$	$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle\alpha$

Esercizio 3.

a) Si ha che $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$. Inoltre, siano $g, h \in G$. Allora

$$g := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ and } h := \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

con $a, b \in \mathbb{R}$. Abbiamo che

$$g^{-1} := \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$$

e

$$hg^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b-a \\ 0 & 1 \end{pmatrix} \in G.$$

Quindi G è un sottogruppo di $GL(2,\mathbb{R})$.

b) Si ha che

$$\delta(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) = \delta(\begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}) = e^{a+b}$$
$$= e^a e^b = \delta(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix})\delta(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}).$$

Questo dimostra che δ è un omomorfismo di gruppi.

c) Il nucleo di δ è per definizione l'insieme

$$\{g \in G \mid \delta(g) = 1\} = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G \mid e^a = 1\}$$

$$= \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a = 0\} = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}.$$

δ non è suriettiva, infatti per ogni a numero reale, e^a è sempre un numero reale positivo. Quindi i numeri reali negativi non stanno nell'immagine di δ.

Esercizio 4.

a) Poichè $\mathbb{Z}_5$ è un campo, $\mathbb{Z}_5[x]$ è un dominio euclideo e quindi anche un dominio a ideali principali.

b) L'ideale $I = (p(x))$ è massimale in $\mathbb{Z}_5[x]$ se e solo se $p(x)$ è irriducibile in $\mathbb{Z}_5[x]$. Poichè $p(x) = (x+2)(x+3)(x^2+2)$ è la fattorizzazione in irriducibili in $\mathbb{Z}_5[x]$, $p(x)$ non è irriducibile e quindi I non è massimale.

c) Sappiamo dal punto b) che I non è un ideale massimale di $\mathbb{Z}_5[x]$. Poichè il quoziente $\mathbb{Z}_5[x]/I$ è un campo se e solo se I è un ideale massimale, possiamo dedurre che A non è un campo.

Sia J un ideale massimale di A. Allora per i teorema di corrispondenza, $J = L/I$, con L ideale di $\mathbb{Z}_5[x]$ contenente I. Allora $L = (g)$ con $g \in \mathbb{Z}_5[x]$ ed inoltre g deve essere un polinomio che divide $p(x)$. Infine J è massimale in A se e solo se L è massimale in $\mathbb{Z}_5[x]$ e quindi $g(x)$ deve essere irriducibile. Poichè $p(x) = (x+2)(x+3)(x^2+2)$ è la fattorizzazione in irriducibili di $p(x)$, g può essere $x+2$, $x+3$ oppure x^2+2. Quindi gli ideali massimali di A sono $\frac{(x+2)}{I}$, $\frac{(x+3)}{I}$ e $\frac{(x^2+2)}{I}$.

Esercizio 5.

a) Per trovare il massimo comun divisore tra f e g usiamo l'algoritmo di Euclide. Esso ci fornirà anche i polinomi $a(x)$ e $b(x)$ richiesti nel punto b).

$$\begin{array}{r|l}
x^5 + x^4 - 2x^3 + x^2 + x - 2 & x^3 + 3x^2 + x - 2 \\
\cline{2-2}
-x^5 - 3x^4 - x^3 + 2x^2 & x^2 - 2x + 3 \\
\cline{1-1}
-2x^4 - 3x^3 + 3x^2 + x - 2 & \\
2x^4 + 6x^3 + 2x^2 - 4x & \\
\cline{1-1}
3x^3 + 5x^2 - 3x - 2 & \\
-3x^3 - 9x^2 - 3x + 6 & \\
\cline{1-1}
-4x^2 - 6x + 4 &
\end{array}$$

$$\begin{array}{r|l} x^3 \quad +3x^2+x-2 & -4x^2-6x+4 \\ \hline -x^3-3/2x^2+x & -1/4x-3/8 \\ \hline 3/2x^2 \quad +2x \ -2 & \\ -3/2x^2-9/4x+3/2 & \\ \hline -1/4x-1/2 & \end{array}$$

Per semplificare i calcoli dividiamo $-4x^2-6x+4$ per $x+2$ anzichè per $-1/4x-1/2$.

$$\begin{array}{r|l} -4x^2-6x+4 & x+2 \\ \hline 4x^2+8x & -4x+2 \\ \hline 2x \ +4 & \\ -2x-4 & \\ \hline 0 & \end{array}$$

L'algoritmo di Euclide ci da

$$\begin{array}{ccc} 1 & 0 & f \\ 0 & 1 & g \\ 1 & -(x^2-2x+3) & -4x^2-6x+4 \\ 1/4x+3/8 & 1-(x^2-2x+3)(1/4x+3/8) & -1/4x-1/2 \\ * & * & 0 \end{array}$$

da cui otteniamo che un massimo comun divisore di f e g è $-1/4x-1/2$ e quindi il massimo comun divisore monico è $x+2$. inoltre

$$-1/4x-1/2 = f(x)(1/4x+3/8)+g(x)[1-(x^2-2x+3)(1/4x+3/8)]$$

e moltiplicando ambo i membri per -4

$$x+2 = f(x)(-x-3/2)+g(x)[-4+(x^2-2x+3)(x+3/2)].$$

Quindi $a(x) = -x-3/2$ e $b(x) = x^3-1/2x^2+1/2$.