Prova scritta di Algebra

4 Luglio 2013

1. Si risolva il seguente sistema di congruenze lineari

$$\begin{cases} x \equiv 2 \mod 3 \\ 2x \equiv 1 \mod 5 \\ x \equiv 3 \mod 2 \end{cases}$$

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

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 $\langle\alpha\rangle = \langle\alpha^5\rangle$.

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

3. Sia $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{Q}, ac \neq 0\}$ e sia $\delta : G \longrightarrow \mathbb{Q}^*$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto ac$.

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

b) Si determini il nucleo di δ.

c) Si dica se δ è suriettiva.

4. In $\mathbb{Q}[x]$ sia $f = x^3 - 1$.

a) Si descrivano gli elementi dell'ideale (f);

b) Si determinimo gli ideali massimali di $\mathbb{Q}[x]$ contenenti (f).

c) Si dica se $\mathbb{Q}[x]/(f)$ è un campo, motivando la risposta.

5. Si considerino i seguenti polinomi:

$$f(x) = x^3 + 2x^2 + 2x - 1, \qquad g(x) = x^4 + x^2 - 2x - 1.$$

a) Verificare che $f(x)$ è irriducibile in $\mathbb{Z}_3[x]$.

b) Si scomponga $g(x)$ nel prodotto di polinomi irriducibili in $\mathbb{Z}_3[x]$.

c) In $\mathbb{Q}[x]$, si determini il massimo comun divisore monico tra $f(x)$ e $g(x)$ e lo si esprima nella forma

$$a(x)f(x) + b(x)g(x)$$

con $a(x), b(x) \in \mathbb{Q}[x]$.

Soluzioni

Esercizio 1. Poiché l'inverso moltiplicativo di $[2]_5$ in $\mathbb{Z}_5$ è $[3]_5$, la seconda congruenza diventa: $x \equiv 3 \bmod 5$. Inoltre l'ultima congruenza diventa $x \equiv 1 \bmod 2$ essendo $[3]_2 = [1]_2$. Il sistema si puó quindi riscrivere:

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 1 \mod 2 \end{cases}$$

che per il teorema cinese del resto ammette soluzione.
Posto $N = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 2 = 30$ si ha $N_1 = N/n_1 = 30/3 = 10$, $N_2 = N/n_2 = 30/5 = 6$, $N_3 = N/n_3 = 30/2 = 15$.
Troviamo le soluzioni particolari delle congruenze

$$N_i y = 1 \bmod n_i.$$

$10y = 1 \bmod 3$ ha come soluzione particolare $y_1 = 1$
$6y = 1 \bmod 5$ ha come soluzione particolare $y_2 = 1$
$15y = 1 \bmod 2$ ha come soluzione particolare $y_3 = 1$.
Quindi una soluzione particolare del sistema di congruenze è:

$$x_0 = \sum_{i=1}^{3} N_i b_i y_i = 10 \cdot 2 \cdot 1 + 6 \cdot 3 \cdot 1 + 15 \cdot 1 \cdot 1 = 53.$$

Dunque le soluzioni del sistema sono $x = 53 + 30k, k \in \mathbb{Z}$, ovvero

$$x = 23 + 30k, \quad k \in \mathbb{Z}.$$

Esercizio 2.

a) $\alpha = (134)(56)(89)$ è prodotto di cicli disgiunti.
$\alpha = (13)(14)(56)(89)$ 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 $3, 2$ e 2, perció il periodo di α è $m.c.m.(3, 2, 2) = 6$. Quindi $< \alpha >$ è un gruppo ciclico di ordine 6 e per il teorema sui sottogruppi dei gruppi ciclici, i sottogruppi di $< \alpha >$ sono tutti ciclici e in corrinspondenza biunivoca con i divisori di 6, ovvero: $1, 2, 3, 6$. 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 6 che è $\langle \alpha \rangle$. Al divisore 3 corrisponde

il sottogruppo $< \gamma >$ dove γ deve essere una potenza di α di periodo 3. Quindi si può prendere $\gamma = \alpha^2$ oppure $\gamma = \alpha^4$ ottenendo cosi il sottogruppo $< \alpha^2 >$. In modo analogo si vede che il sottogruppo di ordine 2 è $< \alpha^3 >$.

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

c)

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

Esercizio 3.

a) Siano $g, h \in G$. Allora

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

con $a, c, a', c' \in \mathbb{Q}^*$ e $b, b' \in \mathbb{Q}$. Abbiamo che

$$\delta(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}) = \delta(\begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}) = (aa')(cc')$$

$$= (ac)(a'c') = \delta(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix})\delta(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}).$$

Questo dimostra che δ è un omomorfismo di gruppi.

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

$$\{g \in G \mid \delta(g) = 1\} = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \mid ac = 1\}$$

$$\{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in \mathbb{Q}, a \neq 0\}.$$

c) δ è suriettiva, infatti per ogni $y \in \mathbb{Q}^*$ possiamo prendere la matrice

$$g = \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}$$

in G e abbiamo che $\delta(g) = y \cdot 1 = y$.

Esercizio 4.

a) Gli elementi dell'ideale (f) sono tutti i polinomi di $\mathbb{Q}[x]$ che si scrivono come prodotto fa dove a è un polinomio in $\mathbb{Q}[x]$.

b) Sia I un ideale massimale contenente (f). Allora $I = (g)$ con $g \in \mathbb{Q}[x]$ perchè $\mathbb{Q}[x]$ è un dominio a ideali principali ed inoltre g deve essere un polinomio irriducibile (perchè I è massimale) che divide f (perchè $(f) \subseteq I$. Poichè $x^3 - 1 = (x-1)(x^2+x+1)$ è la fattorizzazione in irriducibili di $x^3 - 1$, g può essere o $x - 1$ oppure $x^2 + x + 1$. Quindi gli ideali massimali che contengono (f) sono $(x-1)$ e (x^2+x+1).

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

Esercizio 5.

a) Essendo $f(x)$ un polinomio di terzo grado, $f(x)$ è irriducibile in $\mathbb{Z}_3[x]$ se e solo se non ha radici in $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$. Per semplicità di notazione non sciveremo le parentesi quadre. Abbiamo:

$$f(0) = -1 \neq 0$$

$$f(1) = 1 \neq 0$$

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

dunque $f(x)$ è irriducibile in $\mathbb{Z}_3[x]$. Per semplicita' di notazione

b) Si osserva che 2 è radice di $g(x)$, quindi $(x-2)$ deve dividere $g(x)$:

$$\begin{array}{r|l}
x^4 + x^2 - 2x - 1 & x - 2 \\
\cline{2-2}
-x^4 + 2x^3 & x^3 + 2x^2 + 2x - 1 \\
\cline{1-1}
2x^3 + x^2 - 2x - 1 & \\
-2x^3 + x^2 & \\
\cline{1-1}
2x^2 - 2x - 1 & \\
-2x^2 + x & \\
\cline{1-1}
-x - 1 & \\
x - 2 & \\
\cline{1-1}
0 &
\end{array}$$

Poiché il quoziente è il polinomio $f(x)$, che per il punto a) è irriducibile,

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

è espresso come prodotto di polinomi irriducibili in $\mathbb{Z}_3[x]$.

c) Per trovare il $MCD(f(x), g(x))$ usiamo il metodo delle divisioni successive:

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

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

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

Quindi il $MCD(f(x), g(x)) = -3$ e il $MCD(f(x), g(x))$ monico è 1.
Esprimiamo il $MCD(f(x), g(x))$ nella forma $a(x)f(x) + b(x)g(x)$

$$\begin{aligned} -3 &= (3x^2+3x-3) - 2x\left(\tfrac{3}{2}x+\tfrac{3}{2}\right) = \\ &= (3x^2+3x-3) - \left[f(x) - (3x^2+3x-3)\left(\tfrac{1}{3}x+\tfrac{1}{3}\right)\right]\left(\tfrac{3}{2}x+\tfrac{3}{2}\right) = \\ &= (3x^2+3x-3)[\left(\tfrac{1}{3}x+\tfrac{1}{3}\right)\left(\tfrac{3}{2}x+\tfrac{3}{2}\right)+1] - f(x)\left(\tfrac{3}{2}x+\tfrac{3}{2}\right) = \\ &= [g(x) - f(x)(x-2)][\left(\tfrac{1}{3}x+\tfrac{1}{3}\right)\left(\tfrac{3}{2}x+\tfrac{3}{2}\right)+1] - f(x)\left(\tfrac{3}{2}x+\tfrac{3}{2}\right) = \\ &= g(x)[\left(\tfrac{1}{3}x+\tfrac{1}{3}\right)\left(\tfrac{3}{2}x+\tfrac{3}{2}\right)+1] - \\ &\quad -f(x)\{(x-2)[\left(\tfrac{1}{3}x+\tfrac{1}{3}\right)\left(\tfrac{3}{2}x+\tfrac{3}{2}\right)+1] + \left(\tfrac{3}{2}x+\tfrac{3}{2}\right)\} \end{aligned}$$

da cui, svolgendo i calcoli si ottiene

$$-3 = g(x)\left(\frac{1}{2}x^2+x+\frac{3}{2}\right) + f(x)\left(-\frac{1}{2}x^3-x+\frac{3}{2}\right)$$

Per esprimere il $MCD(f(x), g(x))$ monico nella forma $a(x)f(x) + b(x)g(x)$ basta moltiplicare a entrambi i membri il valore $-\frac{1}{3}$

$$1 = g(x)\left(-\frac{1}{6}x^2-\frac{1}{3}x-\frac{1}{2}\right) + f(x)\left(\frac{1}{6}x^3+\frac{1}{3}x-\frac{1}{2}\right)$$