Università degli Studi di Roma "Tor Vergata"

CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2019–2020

Esame scritto del 7 Settembre 2020 — Sessione Autunnale, I appello

N.B.: compilare il compito in modo sintetico ma **esauriente**, *spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

– SVOLGIMENTO –

. . . . . * . . . . . .

[1] — Sia $G := GL_n(\mathbb{R})$ il gruppo delle matrici $n \times n$ invertibili a coefficienti in $\mathbb{R}$, con $n \in \mathbb{N}$. Sia poi $S := SL_n(\mathbb{R})$ il sottoinsieme di G delle matrici con determinante pari a 1, e sia $\Sigma := \mathbb{R}^\star \cdot I_n = \left\{ r\, I_n \,\middle|\, r \in \mathbb{R}^\star := \mathbb{R} \setminus \{0\} \right\}$ — dove I_n è la matrice identità di taglia n — l'insieme delle matrici *scalari* invertibili.

Dimostrare che:

(a) S e Σ sono sottogruppi di G;

(b) G è prodotto diretto (interno) $S \times \Sigma \iff n$ è dispari.

[2] — Sia A un anello commutativo e unitario, e sia $A[x]$ l'anello dei polinomi in una variabile x a coefficienti in A.

Dimostrare che, se $A[x]$ è un dominio a ideali principali, allora A è un campo.

[3] — *(a)* Calcolare il numero di anagrammi della parola "PAPPARDELLE".

(b) Considerando l'azione naturale — data dal prodotto di matrici per vettori colonna — del gruppo lineare generale $GL_2(\mathbb{C})$ sull'insieme $\mathbb{C}^2$, descrivere esplicitamente lo stabilizzatore del punto $v := \begin{pmatrix} 2 \\ -1 \end{pmatrix}$ in $\mathbb{C}^2$.

[4] — *(a)* Costruire esplicitamente un campo $\mathbb{F}_{16}$ che contenga esattamente 16 elementi, e determinare esplicitamente un generatore del gruppo moltiplicativo $\mathbb{F}_{16} \setminus \{0\}$.

(b) Costruire esplicitamente un campo $\mathbb{F}_{27}$ che contenga esattamente 27 elementi, e determinare esplicitamente un elemento che generi il gruppo moltiplicativo $\mathbb{F}_{27} \setminus \{0\}$.

(c) Indicando con $\mathbb{F}_q$ un arbitrario campo finito di cardinalità q, dimostrare che i due gruppi di Galois $Gal(\mathbb{F}_{16}/\mathbb{F}_2)$ e $Gal(\mathbb{F}_{27}/\mathbb{F}_3)$ non sono isomorfi l'uno all'altro.

[5] — Dimostrare che il polinomio

$$p(x) := \frac{2}{15}x^5 + \frac{4}{5}x^4 - x^3 + \frac{6}{5}x^2 - 3x + \frac{1}{5}$$

in $\mathbb{Q}[x]$ è irriducibile.

ESAME SCRITTO DI "ALGEBRA 2" – 7/9/2020

(2019/2020 – GAVARINI)

SVOLGIMENTO

— ∘ —

1 (a) Dimostrare che $S := SL_n(\mathbb{R})$ e $\Sigma := \mathbb{R}^* \cdot I_n$ sono sottogruppi di $G := GL_n(\mathbb{R})$

(b) Dimostrare che G è prodotto diretto (interno) di S per Σ $\Leftrightarrow$ $\Leftrightarrow$ n è dispari.

Soluzione:

(a) $S := SL_n(\mathbb{R}) = \{ g \in GL_n(\mathbb{R}) \mid \det(g) = 1 \}$ è il nucleo di $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$, che un morfismo di gruppi; perciò

$$S = \ker(\det) \trianglelefteq G$$

Σ è l'insieme delle "matrici scalari" invertibili, chiaramente isomorfo al gruppo moltiplicativo $\mathbb{R}^*$; come tale, è $\Sigma \leq G$.

(b) $(\Rightarrow)$ Se n è pari, si ha

$(-1)\cdot I_n \in \Sigma \cap S$, perché

$\det((-1)\cdot I_n) = (-1)^n = 1$ (ché n è pari!)

quindi $\Sigma \cap S \neq \{I_n = e_G\}$, perciò

$\hookrightarrow$ non è prodotto diretto (interno)

di S per Σ. Allora concludiamo

che $G = S \times \Sigma \Rightarrow n$ è dispari, q.e.d.

$(\Leftarrow)$ Sia n dispari. Allora

$\Sigma \cap S = \{I_n = e_G\}$, perché

$\forall\, g \in \Sigma \cap S, \Rightarrow g = r\cdot I_n$, $r \in \mathbb{R}^*$,

con $\det(g) = 1$ (ché $g \in S$);

ma $\det(g) = \det(r\cdot I_n) = r^n$, $\Rightarrow$

$\Rightarrow r^n = 1$, $\Rightarrow r = 1$, perché

$r \in \mathbb{R}^*$ e n è pari.

Questo mostra come l'argomento visto in precedenza - per n pari - mostra che invece per n dispari si ha $\Sigma \cap S = \{I_n\}$.

Comunque, per dimostrare che $G = S \times \Sigma$ possiamo procedere direttamente ricordando (e applicando) questo criterio: se esiste un endomorfismo $\mathcal{L} : G \longrightarrow G$ tale che $\mathcal{L}^2 = \mathcal{L}$, allora

$$G = I \rtimes K \quad \text{con} \tag{1}$$

$$I := \mathrm{Im}(\mathcal{L}) \leq G, \qquad K := \ker(\mathcal{L})$$

Nel caso in esame, consideriamo

$$\mathcal{L} := \delta_n : G = GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R}) =: G$$

$$g \longmapsto \delta_n(g)$$

Siccome n è dispari, tale δ_n è ben definita, perché

$$\forall\, r \in \mathbb{R}^*, \ \exists!\ r^{1/n} \in \mathbb{R}^*$$

($\exists!\ \rho \in \mathbb{R}^*$ tale che $\rho^n = r$);

inoltre, siccome $\det$ è un morfismo di gruppi, e potenze / radici sono "moltiplicative", tale δ_n è anche un morfismo di gruppi, dunque un omomorfismo di $G := GL_n(\mathbb{R})$.

Infine, il calcolo diretto ora'

$$\mathcal{L}^2(g) = \mathcal{L}(\mathcal{L}(g)) = \mathcal{L}\left(\det(g)^{1/n} \cdot I_n\right) =$$

$$= \det\left(\det(g)^{1/n} I_n\right)^{1/n} = \left[\text{da } \det(r \cdot I_n) = r^n\right]$$

$$= \left(\det(g)\right)^{1/n} \cdot I_n =$$

$$= \det(g)^{1/n} \cdot I_n = \mathcal{L}(g), \quad \forall g \in G$$

cioè $\delta_n^2 = \delta_n$. Quindi vale la (1), cioè

$$GL_n(\mathbb{R}) =: G = I \rtimes K$$

con $I = \mathrm{Im}(\delta_n) \leq G$, $K := \ker(\delta_n) \trianglelefteq G$

ORA, $K := \ker(\delta_n) = \ker(\det) =: SL_n(\mathbb{R})$

cioè $K = S$, perché ovviamente

$\delta_n(g) := \det(g)^{1/n} \cdot I_n \iff$

$\iff \det(g)^{1/n} = 1 \iff \det(g) = 1 \iff$

$\iff g \in \ker(\det) =: SL_n(\mathbb{R}) = S$

INOLTRE, $I := \mathrm{Im}(\delta_n) = \mathbb{R}^* \cdot I_n =: \Sigma$

perché ovviamente $\mathrm{Im}(\delta_n) \subseteq \mathbb{R}^* \cdot I_n$

e viceversa $\forall\, r \cdot I_n \in \mathbb{R}^* \cdot I_n$ si ha

$r \cdot I_n = \delta_n(\rho \cdot I_n)$ con $\rho := r^{1/n} \in \mathbb{R}^*$

(sempre perché n è dispari!...)

QUINDI abbiamo una fattorizzazione di G in prodotto semidiretto (interno)

$$G = \Sigma \rtimes S \quad (\text{o } G = S \rtimes \Sigma) \quad (2)$$

MA ora osserviamo che gli elementi di Σ sono centrali in G, in particolare si ha

$$\sigma \cdot s \cdot \sigma^{-1} = s \qquad \forall\, \sigma \in \Sigma,\ s \in S$$

perché ogni $\sigma \in \Sigma$ è una matrice scalare (e moltiplicare per $\sigma = z \cdot I_n$ un'altra matrice s significa soltanto moltiplicare ogni coefficiente di s per z, sia che si consideri $\sigma \cdot s$, sia che si consideri $s \cdot \sigma$).

Allora da $\sigma \cdot s \cdot \sigma^{-1} = s$ $(\forall \sigma \in \Sigma, s \in S)$ segue che l'azione (per coniugio) di Σ su S è banale, e pertanto il prodotto in (2) è in effetti un prodotto diretto, q.e.d.

(CONTINUA...)

2 Sia A un anello commutativo unitario. Dimostrare che, se $A[x]$ è un dominio a ideali principali, allora A è un campo.

Soluzione:

Sia $A[x]$ un dominio a ideali principali, per ipotesi.

Poiché A è sottoanello di $A[x]$, siccome $A[x]$ è dominio anche A è un dominio.

Per dimostrare che A è un campo, mostriamo ora che ogni $a \in A \setminus \{0\}$ è invertibile in A (e allora non sarà nemmeno necessario sapere che - come già visto - A è un dominio...).

Sia $I := (a, x) \trianglelefteq A[x]$ l'ideale di $A[x]$ generato da $\{a, x\}$; per ipotesi I è ideale principale, dunque esiste $p(x) \in A[x]$ che lo genera, cioè $(a, x) =: I = (p(x))$.

In particolare abbiamo

$$a = p(x) \cdot h(x), \qquad x = p(x) \cdot k(x)$$

per opportuni $h(x), k(x) \in A[x]$; ora,

poiché $\partial(a) = 0$ (a è una costante non nulla!) da $a = p(x) \cdot h(x)$ segue che

$\partial(p(x)) = 0$, cioè $p(x) = c \in A \setminus \{0\}$,

con $x = c \cdot k(x)$, da cui segue che

$\exists\, c^{-1} \in A$ e $k(x) = c^{-1} \cdot x$.

((Allora possiamo sostituire il generatore $p(x) = c$ dell'ideale I con l'elemento 1, ma non è necessario))

ORA da $(a, x) = I = (p(x)) = (c) \ni 1$

ricaviamo in particolare

$$1 = a \cdot r(x) + x \cdot s(x) \qquad (3)$$

per opportuni $r(x), s(x) \in A[x]$.

Nella (3) il termine noto della parte destra è quello di $a \cdot r(x)$, così abbiamo $1 = a \cdot r_0$ dove r_0 è il termine noto di

$$r(x) = r_0 + r_1 \cdot x + \cdots + r_d \cdot x^d \quad (r_i \in A, \forall i);$$

ma $1 = a \cdot r_0$ significa che a è invertibile, con $r_0 = a^{-1} (\in A)$, q.e.d

(CONTINUA...)

Un altro possibile metodo è questo.

Per ogni $a \in A$ abbiamo un epimorfismo di anelli $ev_a : A[x] \longrightarrow\!\!\!\!\rightarrow A$

$$p(x) \longmapsto p(a)$$

con nucleo $\ker(ev_a) = ((x-a))$, per cui $A = \mathrm{Im}(ev_a) \cong A$

Allora $A \cong A[x]/((x-a))$ è un campo $\Leftrightarrow$ l'ideale $((x-a))$ in $A[x]$ è massimale; dato che $A[x]$ è, per ipotesi, un dominio a ideali principali, $I := ((x-a))$ è massimale se e soltanto se il suo generatore $(x-a)$ è irriducibile: ma $(x-a)$ è chiaramente irriducibile perché è di grado 1 e monico, $\Rightarrow$

$\Rightarrow$ si conclude che l'ideale $I := ((x-a))$ è massimale in $A[x]$, e quindi $A[x]/((x-a)) \cong A$ è un campo, q.e.d.

(CONTINUA---)

[3] (a) Calcolare il numero di anagrammi della parola $p :=$ "PAPPARDELLE"

(b) Descrivere lo stabilizzatore di $v := \begin{pmatrix} 2 \\ -1 \end{pmatrix} (\in \mathbb{C}^2)$ per l'azione naturale di $GL_2(\mathbb{C})$ su $\mathbb{C}^2$.

Soluzione:

(a) Gli anagrammi richiesti sono gli elementi dell'orbita $\mathcal{O}_p$ di p per l'azione di S_{11} sulle parole di 11 lettere. Allora

$$|\mathcal{O}_p| = |S_{11}| / |St_p|$$

dove St_p è lo stabilizzatore di p.

Siccome le 11 lettere di p si ripartiscono in

3 "P", 2 "A", 2 "E", 2 "L", 1 "R", 1 "D"

si ha $St_p \cong S_3 \times S_2 \times S_2 \times S_2 \times S_1 \times S_1$,

quindi $|St_p| = 3! \cdot 2! \cdot 2! \cdot 2! \cdot 1! \cdot 1!$

e così

$$\#\{\text{anagrammi di } \rho\} = |\mathcal{O}_\rho| = \frac{|S_{11}|}{|\mathcal{H}_\rho|} = \frac{11!}{3!\,2!\,2!\,2!\cdot 1!\,1!} =$$

$$= \binom{11}{3,2,2,2,1,1}$$

(b) Una matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ appartiene allo stabilizzatore $\mathcal{H}_v$ di v se e soltanto se $g \cdot v = v$, cioè se e soltanto se

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$$

cioè

$$\begin{cases} 2a - b = 2 \\ 2c - d = -1 \end{cases}$$

cioè

$$\begin{cases} b = 2a - 2 = 2(a-1) \\ d = 2c + 1 \end{cases}$$

da cui otteniamo la descrizione

$$\mathcal{L}t_r = \left\{ \begin{pmatrix} a & 2(a-1) \\ c & 2c+1 \end{pmatrix} \;\middle|\; \begin{array}{l} a, c \in \mathbb{C} \\ a+c \neq 0 \end{array} \right\} \qquad (4)$$

dove la condizione $a+c \neq 0$ corrisponde alla condizione

$$\begin{pmatrix} a & 2(a-1) \\ c & 2c+1 \end{pmatrix} \in GL_2(\mathbb{C})$$

in quanto

$$\det \begin{pmatrix} a & 2(a-1) \\ c & 2c+1 \end{pmatrix} = a(2c+1) - c \cdot 2(a-1) =$$

$$= \cancel{2ac} + a - \cancel{2ac} + 2c = a + 2c$$

e quindi

$$\det \begin{pmatrix} a & 2(a-1) \\ c & 2c+1 \end{pmatrix} \neq 0 \iff a + 2c \neq 0$$

Naturalmente sono possibili altre descrizioni di $\mathcal{L}t_r$, ma tutte equivalenti alla (4).

(CONTINUA...)

4 (a) Costruire un campo $\mathbb{F}_{16}$ tale che $|\mathbb{F}_{16}| = 16$, e trovare un generatore del gruppo moltiplicativo $\mathbb{F}_{16} \setminus \{0\}$.

(b) Costruire un campo $\mathbb{F}_{27}$ tale che $|\mathbb{F}_{27}| = 27$, e trovare un generatore del gruppo moltiplicativo $\mathbb{F}_{27} \setminus \{0\}$.

(c) Dimostrare che i gruppi di Galois $Gal(\mathbb{F}_{16}/\mathbb{F}_2)$ e $Gal(\mathbb{F}_{27}/\mathbb{F}_3)$ non sono isomorfi l'uno all'altro.

Soluzione:

(a) $|\mathbb{F}_{16}| = 16 = 2^4 \Rightarrow \mathbb{F}_{16}$ deve avere sottocampo fondamentale $\mathbb{F}_2$,

$\Rightarrow \mathbb{F}_{16}$ è estensione di $\mathbb{F}_2$ di grado $\log_2(16) = \log_2(2^4) = 4 \Rightarrow$

$\Rightarrow \mathbb{F}_{16}$ si può costruire nella forma

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(p(x))$$

con $p(x) \in \mathbb{F}_2[x]$, $\partial(p(x)) = 4$, e

$p(x)$ irriducibile.

OR1, $p(x) \in \mathbb{F}_2[x]$, $\partial(p(x)) = 4 \Rightarrow$

$$\Rightarrow p(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

con $a_i \in \mathbb{F}_2 \cong \mathbb{Z}_2 \quad \forall i = 0, 1, 2, 3, 4$

e $a_4 \neq 0$.

Possiamo scegliere $a_4 (\neq 0)$ arbitrariamente, fissiamo $a_4 = 1$; poi restano $2^4 = 16$ scelte per gli altri 4 coefficienti, ma il $p(x)$ che otteniamo dev'essere irriducibile.

Ad esempio $x^4 + x$ e $x^4 + 1$ non sono irriducibili, perché hanno radice $x = 0$ e $x = 1$, rispettivamente.

Scegliendo $a_0 = 0$ si ha sempre che $x = 0$ è radice di $p(x)$, dunque fissiamo $a_0 \neq 0$, e scegliamo $a_0 = 1$

Così $p(x) = x + a_3 x^3 + a_2 x^2 + a_1 x + 1$

e restano $2^3 = 8$ possibili scelte...

Proviamo con $(a_3, a_2, a_1) = (0, 0, 1)$, cioè

$$p(x) := x^4 + x + 1$$

Si ha $p(0) = 1 \neq 0$, $p(1) = 1 \neq 0$, $\Rightarrow$

$\Rightarrow$ $p(x)$ non ha radici $\Leftrightarrow$ $p(x)$ non è fattorizzabile con fattori di grado 1.

Vediamo allora se $p(x)$ è fattorizzabile nella forma $p(x) = h(x) \cdot k(x)$

con $\partial(h(x)) = 2 = \partial(k(x))$.

Possiamo assumere che i coefficienti direttivi di $h(x)$ e $k(x)$ siano 1 (ché il loro prodotto deve essere 1) e allo stesso modo che siano 1 i loro termini noti; allora

$$h(x) = x^2 + ax + 1$$
$$k(x) = x^2 + bx + 1$$

ORA $p(x) = h(x) \cdot k(x) \Rightarrow$

$$\Rightarrow x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1) =$$
$$= x^4 + (a+b)x^3 + (1 + ab + 1)x^2 + (a+b)x + 1$$

QUINDI
$$\begin{cases} a + b = 0 \\ 1 + ab + 1 = 0 \\ a + b = 1 \end{cases} \Rightarrow (\Sigma) \Rightarrow$$

$\Rightarrow \nexists$ fattorizzazione $p(x) = h(x) \cdot k(x)$

con $\partial(h(x)) = 2 = \partial(k(x))$

ALLORA $p(x) := x^4 + x + 1 \in \mathbb{F}_2[x]$

è irriducibile in $\mathbb{F}_2[x]$,

di grado 4, e quindi

$\mathbb{F}_{16} := \dfrac{\mathbb{F}_2[x]}{(x^4 + x + 1)}$ è un campo

con $2^4 = 16$ elementi, q.e.d.

INOLTRE, $\mathbb{F}_{16}$ ha base su $\mathbb{F}_2$

$B := \{ \alpha^n \mid n = 0, 1, 2, 3 \}$ con $\alpha := \bar{x}$

Studiamo le potenze di $\alpha := \bar{x}$ $(\in \mathbb{F}_{16} \setminus \{0\})$

$\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 \neq$, $\alpha^3 \neq$, ...

Siccome $\mathbb{F}_{16} \setminus \{0\}$ ha ordine $16 - 1 = 15$,

generatore sarà ogni suo elemento

di ordine 15; altri ordini possibili

sono 1, 3, e 5. Per $\alpha = \bar{x}$ abbiamo

$\alpha^1 = \alpha \neq 1$ (perché elemento di B e $\neq 1$)

$\alpha^3 \neq 1$ (come prima), e così anche

$$\alpha^5 = \alpha^1 \cdot \alpha^4 = \alpha^1 \cdot (-\alpha - 1) = \alpha(\alpha+1) =$$
$$= \alpha^2 + \alpha \neq 1 \quad (\text{perché } 1, \alpha, \alpha^2 \text{ sono in } B)$$

perché $\alpha^4 + \alpha + 1 = 0 \Rightarrow$

$\Rightarrow \alpha^4 = -\alpha - 1 = \alpha + 1 \quad (\text{char}(\mathbb{F}_{16}) = 2)$.

allora α non ha ordine 1, né 3, né 5, dunque ha ordine 15, e quindi è un generatore di $(\mathbb{F}_{16} \setminus \{0\}; \cdot)$.

(b) Ragionando come in (a), andiamo a costruire $\mathbb{F}_{27}$ nella forma

$$\mathbb{F}_{27} := \mathbb{F}_3[x] / (p(x))$$

con $p(x) \in \mathbb{F}_3[x]$ polinomio irriducibile in $\mathbb{F}_3[x]$ di grado $\log_3(27) = 3$.

Dunque

$$p(x) = a \cdot x^3 + b x^2 + c x + d$$

possiamo assumere $p(x)$ monico, cioè $a = 1$; poi possiamo assumere $d \neq 0$ (altrimenti $p(x)$ ha radice $x = 0$) e quindi scegliamo $d = 1$. Allora

$$p(x) = x^3 + bx^2 + c\cdot x + 1$$

e ci restano $3^2 = 9$ scelte per la coppia di coefficienti $(b, c) \in \mathbb{F}_3^2$.

Ad esempio, non vanno bene

$x^3 + 1$ (ha radice $x = -1 = 2$)

$x^3 + x + 1$ (ha radice $x = 1$)

$x^3 + x^2 + 1$ (ha radice $x = 1$)

Proviamo ora

$$p(x) := x^3 - x + 1$$

$$p(0) = 1 \neq 0, \quad p(1) = 1 \neq 0,$$

$$p(2) = -1 = 2 \neq 0$$

QUINDI $p(x)$ non ha radici in $\mathbb{F}_3$, e siccome $\partial(p(x)) = 3$, si conclude che $p(x)$ è irriducibile in $\mathbb{F}_3[x]$.

ALLORA

$$\mathbb{F}_{27} := \frac{\mathbb{F}_3[x]}{(x^3 - x + 1)}$$ è un campo con $3^3 = 27$ elementi, q.e.d.

INOLTRE, $\mathbb{F}_{27}$ ha base su $\mathbb{F}_3$

$B := \{1, \alpha, \alpha^2\}$ con $\alpha := \bar{x}$

e il gruppo moltiplicativo $\mathbb{F}_{27}^* := \mathbb{F}_{27} \setminus \{0\}$ ha $27-1 = 26$ elementi. Poiché $26 = 13 \cdot 2$, gli elementi di $\mathbb{F}_{27}^*$ hanno ordine $1, 2, 13$ o 26; quelli di ordine 26 sono i generatori.

Proviamo α, calcolandone l'ordine:

$\alpha^1 = \alpha \neq 1$, ché $\alpha \in B$ (lin. indip. da 1)

$\alpha^2 = \alpha^2 \neq 1$, ché $\alpha^2 \in B$ (come prima)

$$\alpha^{13} = \alpha^{3\cdot 4+1} = (\alpha-1)^4 \cdot \alpha =$$

$$= (\alpha^4 - 4\cdot\alpha^3 + \binom{4}{2}\alpha^2 - 4\cdot\alpha + 1)\cdot\alpha =$$

$$= (\alpha\cdot(\alpha-1) - 4\cdot(\alpha-1) + 6\alpha^2 - 4\alpha + 1)\cdot\alpha =$$

$$= (\alpha^2 - \alpha - 4\alpha + 4 + \cancel{6\alpha^2} - 4\alpha + 1)\cdot\alpha =$$

($\cancel{6\alpha^2} = 0$)

$$= (\alpha^2 - \cancel{9\alpha} + 5)\cdot\alpha = \alpha^3 + 2\alpha =$$

($\cancel{9\alpha} = 0$, $5 = 2$)

$$= \alpha - 1 + 2\alpha = \cancel{3\alpha} - 1 = -1 \neq 1$$

($\cancel{3\alpha} = 0$)

quindi l'ordine di α <u>non</u> è 1, <u>non</u> è 2 e <u>non</u> è 13, perciò è necessariamente 26, e dunque $\alpha := \bar{x}$ è un generatore del gruppo moltiplicativo $\mathbb{F}_{27}^*$.

(c) Dalla teoria generale sappiamo che, per ogni $n \in \mathbb{N}_+$ e ogni primo p, il gruppo di Galois $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ è ciclico di ordine n (generato dall'automorfismo di Frobenius $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $a \mapsto a^p$).

Ma allora, per $(n,p) = (4,2)$ e $(n,p) = (3,3)$ troviamo

$$\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) \cong \mathbb{Z}_4 \quad \text{e}$$

$$\mathrm{Gal}(\mathbb{F}_{27}/\mathbb{F}_3) \cong \mathbb{Z}_3 \ ;$$

pertanto, dato che $\mathbb{Z}_4 \ncong \mathbb{Z}_3$ concludiamo che è anche

$$\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) \ncong \mathrm{Gal}(\mathbb{F}_{27}/\mathbb{F}_3).$$

(CONTINUA...)

5 Dimostrare che il polinomio

$$p(x) := \frac{2}{15} \cdot x^5 + \frac{4}{5} x^4 - x^3 + \frac{6}{5} x^2 - 3x + \frac{1}{5}$$

in $\mathbb{Q}[x]$ è irriducibile.

Soluzione:

Chiaramente $p(x)$ è irriducibile (in $\mathbb{Q}[x]$) se e soltanto se è irriducibile il polinomio ad esso associato

$$p_+(x) := 15 \cdot p(x) =$$

$$= 2 \cdot x^5 + 12 \cdot x^4 - 15 \cdot x^3 + 18 \cdot x^2 - 45x + 3$$

Ora, $p_+(x) \in \mathbb{Z}[x]$, e $p_+(x)$ è primitivo: pertanto

$p_+(x)$ è irriducibile in $\mathbb{Q}[x]$ $\iff$ $p_+(x)$ è irriducibile in $\mathbb{Z}[x]$

Infine, applicando il Criterio di Eisenstein al polinomio $p_+(x)$ in $\mathbb{Z}[x]$ rispetto al primo $p = 3$ otteniamo che $p_+(x)$ è irriducibile.

In conclusione, $p(x)$ è irriducibile.