Università degli Studi di Roma "Tor Vergata"

CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2024–2025

Esame scritto del 10 Giugno 2025 — 1° appello, sessione estiva

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

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

[1] — Indicando con $\mathbb{F}_{121}$ il campo con 121 elementi, si dimostri che l'anello quoziente $\mathbb{Z}[x\,,y\,,z\,]\Big/\big(\,x^2+y\,z\,,11\,,x^2-10\,\big)$ è isomorfo all'anello $\mathbb{F}_{121}\big[\,t\,,t^{-1}\big]$ dei polinomi di Laurent in t a coefficienti in $\mathbb{F}_{121}$.

[2] — Sia G un gruppo di ordine 80.

(a) Dimostrare che in G esiste almeno un sottogruppo normale non banale, cioè diverso da $\{1_G\}$ e da G stesso.

(b) Dimostrare che per ciascuno dei valori $d \in \{1,2,4,5,8,16\}$ esiste in G un sottogruppo di ordine d.

(c) Dimostrare che se esiste in G un sottogruppo normale di ordine 5, allora esiste anche un sottogruppo di ordine 10.

[3] — Si consideri il sottoinsieme $\mathbb{Z}\big[\sqrt{-6}\,\big]$ del campo $\mathbb{C}$ dei numeri complessi definito da $\mathbb{Z}\big[\sqrt{-6}\,\big] := \big\{\,a+b\sqrt{-6}\;\big|\;a,b\in\mathbb{Z}\,\big\}$.

(a) Dimostrare che $\mathbb{Z}\big[\sqrt{-6}\,\big]$ è sottoanello di $\mathbb{C}$.

(b) Dimostrare che l'anello $\mathbb{Z}\big[\sqrt{-6}\,\big]$ è un dominio di integrità.

(c) Dimostrare che l'anello $\mathbb{Z}\big[\sqrt{-6}\,\big]$ è un dominio a fattorizzazione.

(d) Determinare alcune possibili fattorizzazioni in prodotto di fattori irriducibili per l'elemento 70 nell'anello $\mathbb{Z}\big[\sqrt{-6}\,\big]$.

(e) Determinare se l'anello $\mathbb{Z}\big[\sqrt{-6}\,\big]$ sia un dominio a ideali principali.

[4] — Sia $\mathbb{K} \in \{\mathbb{Q}, \mathbb{Z}_3\}$, $f(x) := (x^{11} - 1) \in \mathbb{K}[x]$ e sia $\mathbb{K}_f$ il campo di spezzamento di $f(x)$ su $\mathbb{K}$. Per ciascuno dei due casi $\mathbb{K} = \mathbb{Q}$ e $\mathbb{K} = \mathbb{Z}_3$, si determini:

(a) il grado dell'estensione $\mathbb{K} \subseteq \mathbb{K}_f$;

(b) la struttura del gruppo di Galois $G(\mathbb{K}_f/\mathbb{K})$ dell'estensione $\mathbb{K}_f/\mathbb{K}$.

(c) una descrizione esplicita del gruppo $G(\mathbb{K}_f/\mathbb{K})$ — come gruppo di automorfismi di $\mathbb{K}_f$.

[5] — Dato $n \in \mathbb{N}_+$ e $E_n := \{1, 2, \ldots, n\}$, si consideri l'azione del gruppo simmetrico $\mathcal{S}_n$ su $\mathbb{E} := E_n \times E_n \times E_n$ definita da

$$\sigma.(x, y, z) := (\sigma(x), \sigma(y), \sigma(z)) \qquad \forall\ \sigma \in \mathcal{S}_n,\ (x, y, z) \in E_n \times E_n \times E_n$$

Si descrivano le orbite della suddetta azione di $\mathcal{S}_n$ su $\mathbb{E} := E_n \times E_n \times E_n$.

ALGEBRA 2

2024-2025

F. GAVARINI

ESAME SCRITTO DEL 10/06/2025

1 Detto $\mathbb{F}_{121}$ il campo con 121 elementi, dimostrare che l'anello quoziente

$$\mathbb{Z}_{11}[x,y,z] \big/ (x^2+yz,\ 11,\ x^2-10) =: A$$

è isomorfo a $\mathbb{F}_{121}[t,t^{-1}]$.

Soluzione: Usiamo più volte il Teorema del Doppio Quoziente (=: T. d. D. Q.) !!!

$$\mathbb{Z}_{11}[x,y,z] \big/ (x^2+yz,\ 11,\ x^2-10) \cong$$

$$\cong \Big(\mathbb{Z}_{11}[x,y,z] \big/ (11) \Big) \Big/ \Big((x^2+yz,\ 11,\ x^2-10) \big/ (11) \Big) \qquad (1)$$

con $\varphi : \mathbb{Z}_{11}[x,y,z] \big/ (11) \xrightarrow{\cong} \mathbb{Z}_{11}[x,y,z]$ (2)

$$P(x,y,z) + (11) \longmapsto \overline{P}(x,y,z)$$

dove $\overline{P(x,y,z)} := \sum_{k,h,d} [a_{k,h,d}]_{11} \cdot x^k y^h z^d$

$\forall\ P(x,y,z) \in \mathbb{Z}_{11}[x,y,z]$.

NOTA: φ è un ISOMORFISMO, e tramite esso si ha

$$\varphi\left(\frac{(x^2+yz,\ 11,\ x^2-10)}{(11)}\right) =$$

$$= (x^2+yz,\ \overline{0},\ x^2-\overline{10}) = \tag{3}$$

$$= (x^2+yz,\ x^2+\overline{1})$$

dove si usa la notazione più leggera

$$\overline{a} := [a]_{11} \in \mathbb{Z}_{11}, \quad \forall\ a \in \mathbb{Z}$$

ALLORA è (per le (1), (2) e (3))

$$A \cong \mathbb{Z}_{11}[x,y,z] \Big/ (x^2+yz,\ x^2+\overline{1}) \tag{4}$$

e da nuovo per il T.d.D.Q. si ha

$$\mathbb{Z}_{11}[x,y,z] \Big/ (x^2+yz,\ x^2+\overline{1}) \cong \tag{5}$$

$$\cong \left(\mathbb{Z}_{11}[x,y,z] \Big/ (x^2+\overline{1})\right) \Big/ \left(\frac{(x^2+yz,\ x^2+\overline{1})}{(x^2+\overline{1})}\right)$$

con

$$\mathbb{Z}_{11}[x,y,z] \Big/ (x^2+\overline{1}) \cong \left(\mathbb{Z}_{11}[x] \Big/ (x^2+\overline{1})\right)[y,z] \tag{6}$$

MA $\mathbb{Z}_{11}$ è campo, e

$(x^2+\bar{1})$ è irriducibile in $\mathbb{Z}_{11}[x]$

— perché ha grado 2 e non ha radici in $\mathbb{Z}_{11}$ (verifica diretta!) —

ALLORA $\mathbb{Z}_{11}[x]/(x^2+\bar{1}) =: \mathbb{Z}_{11}(\alpha)$

è un CAMPO, estensione semplice di $\mathbb{Z}_{11}$ tramite l'elemento algebrico α (" $:= \sqrt{-\bar{1}}$ ") il cui polinomio minimo su $\mathbb{Z}_{11}$ è $x^2+\bar{1}$

QUINDI $\mathbb{Z}_{11}[x]/(x^2+\bar{1}) = \mathbb{Z}_{11}(\alpha)$ è un campo con 11^2 elementi,

DUNQUE $\mathbb{Z}_{11}[x]/(x^2+\bar{1}) \cong \mathbb{F}_{121}$ (7)

Insieme all'analisi precedente, ciò dà

$$\left(\mathbb{Z}_{11}[x]/(x^2+\bar{1})\right)[y,z] \cong \mathbb{F}_{121}[y,z] \quad (8)$$

e poi (6) e (8) insieme ~~danno~~

$$\varphi: \mathbb{Z}_{11}[x,y,z]/(x^2+\bar{1}) \cong \mathbb{F}_{121}[y,z] \quad (9)$$

INOLTRE, attraverso l'isomorfismo ψ in (9) si ha

$$\psi\left(\frac{(x^2+yz, x^2+\bar{1})}{(x^2+\bar{1})}\right) = (yz-\bar{1})$$

per cui (4), (5) e (9) insieme danno

$$A \cong \frac{\mathbb{F}_{127}[y,z]}{(yz-\bar{1})} \tag{10}$$

INFINE, abbiamo un isomorfismo

$$\lambda : \frac{\mathbb{F}_{127}[y,z]}{(yz-\bar{1})} \xrightarrow{\tilde{=}} \mathbb{F}_{127}[t,t^{-1}] \tag{11}$$

$$[P(y,z)]_{(yz-\bar{1})} \longmapsto P(t,t^{-1})$$

inoltre dal Teorema Fondamentale di Omomorfismo (per anelli) a partire dall'epimorfismo

$$\lambda' : \mathbb{F}_{127}[y,z] \twoheadrightarrow \mathbb{F}_{127}[t,t^{-1}]$$

$$P(y,z) \longmapsto P(t,t^{-1})$$

il cui nucleo è proprio l'ideale di $\mathbb{F}_{127}[y,z]$ generato da $(yz-\bar{1})$

INFINE, (10) e (11) insieme danno un isomorfismo composto

$$\mathbb{Z}_4[x,y,z] \Big/ (x^2+yz, 11, x^2-10) =: A \xrightarrow{\chi} \mathbb{F}_{121}[t,t^{-1}]$$

come richiesto. Esplicitamente, tale χ è descritto da

$$\left[\sum_{k,h,d} a_{k,h,d}\cdot x^k y^h z^d\right]_I \xmapsto{\chi} \sum_{k,h,d} [a_{k,h,d}]_{11}\cdot \alpha^k \cdot t^{h-d}$$

$\forall \sum_{k,h,d} a_{k,h,d}\cdot x^k y^h z^d \in \mathbb{Z}_4[x,y,z]$,

con $I := (x^2+yz, 11, x^2-10) \trianglelefteq \mathbb{Z}_4[x,y,z]$. □

CONTINUA

2 Sia G un gruppo di ordine 80.

Th: (a) $\exists$ in G almeno un sottogruppo normale N t.c. $N \neq \{1_G\}$ e $N \neq G$.

(b) $\forall\, d \in \{1, 2, 4, 5, 8, 16\}$, $\exists$ in G (almeno) un sottogruppo H_d di ordine d.

(c) Se $\exists$ in G un sottogruppo normale di ordine 8, allora $\exists$ anche un sottogruppo di ordine 10.

Soluzione:

(a) $|G| = 80 = 2^4 \cdot 5$, $\Rightarrow$

$\Rightarrow \exists$ in G dei 2-Sylow e dei 5-Sylow con 2^4 e 5^1 elementi, rispettivamente, dunque diversi da $\{1_G\}$ e da G.

SE $\nu_p := \#(p\text{-Sylow in } G)$, $\forall\, p \in \{2, 5\}$

si ha $\nu_2 \in (1 + 2\mathbb{N}) \cap \{1, 5\} = \{1, 5\}$

e $\nu_5 \in (1 + 5\mathbb{N}) \cap \{1, 2, 4, 8, 16\} = \{1, 16\}$

ORA abbiamo due casi:

(I) $\nu_5 = 1 \Rightarrow \exists!$ 5-Sylow Σ_5, ovvero

ma tale 5-Sylow è caratteristico in G, e in particolare è normale, e NON banale come richiesto $\rightsquigarrow$ (OK)

(II) $\nu_5 = 16 \Rightarrow \exists$ 16 diversi 5-Sylow.

$\forall$ 5-Sylow diversi Σ_5' e Σ_5'' si ha

$$\Sigma_5' \cap \Sigma_5'' = \{1_G\}$$

quindi ogni 5-Sylow "contribuisce" con 4 elementi - di ordine 5 - di G che contiene soltanto lui, più l'identità (che sta in tutti i sottogruppi)

QUINDI $\bigcup_{\substack{\Sigma_5 \text{ è} \\ \text{5-Sylow}}} (\Sigma_5 \setminus \{1_G\}) = \{g \in G \mid \omega(g) = 5\}$ (ordine di g)

è un sottoinsieme di G con

$$\left| \bigcup_{\substack{\Sigma_5 \text{ è} \\ \text{5-Sylow}}} (\Sigma_5 \setminus \{1_G\}) \right| = \sum_{\substack{\Sigma_5 \text{ è} \\ \text{5-Sylow}}} (\Sigma_5 \setminus \{1_G\}) = \nu_5 \cdot (5-1) = 16 \cdot 4 = 64$$

INOLTRE, in G c'è almeno un 2-Sylow Σ_2, i cui elementi hanno

ordine 1, o 2, o 4, o 8, o 16, quindi in particolare non stanno nel sottoinsieme $\bigcup_{\substack{\Sigma_5 \text{ è} \\ 5\text{-Sylow}}} \Sigma_5$. Perciò troviamo

$$80 = |G| \geq \left| \Sigma_2 \cup \left(\bigcup_{\substack{\Sigma_5 \text{ è} \\ 5\text{-Sylow}}} \Sigma_5 \right) \right| =$$

$$= |\Sigma_2| + \left| \bigcup_{\substack{\Sigma_5 \text{ è} \\ 5\text{-Sylow}}} \Sigma_5 \right| = 16 + 64 = 80$$

QUINDI il "$\geq$" qui sopra è un "$=$"

PERCIÒ è anche

$$G = \Sigma_2 \cup \left(\bigcup_{\substack{\Sigma_5 \text{ è} \\ 5\text{-Sylow}}} \Sigma_5 \right)$$

QUINDI in particolare

Σ_2 è l'UNICO 2-Sylow in G (cioè $\nu_2 = 1$) e così Σ_2 è caratteristico, e in particolare è normale, e NON banale, come richiesto ovvio (Ok)

IN BREVE, si ha

$\Sigma_5 \trianglelefteq G$ oppure $\Sigma_2 \trianglelefteq G$

(b) Abbiamo due casi distinti

Ⓘ $d \in \{1,2,4,8,16\}$ e Ⓘⓘ $d \in \{1,5\}$

Ⓘ SE $d \in \{1,2,4,8,16\}$, detto Σ_2 un 2-Sylow in G - che certamente esiste - siccome Σ_2 è un p-gruppo (per $p=2$) finito, contiene un sottogruppo di ogni ordine possibile, cioè di ordine un qualsiasi divisore di $|\Sigma_2|$; dato che $|\Sigma_2| = 16 = 2^4$ e i suoi divisori sono 1, 2, 4, 8 e 16, per ogni tale valore di d

$$\exists\ \underbrace{H_d \leq \Sigma_2}_{\text{è anche } H_d \leq G} : |H_d| = d \Rightarrow \text{OK}$$

Ⓘⓘ SE $d \in \{1,5\}$, si ripete il ragionamento qui sopra con $p=5$ invece che $p=2$! Allora $\exists$ in G un 5-Sylow Σ_5 - con $|\Sigma_5| = 5$, e quindi

$$\exists\ H_1 = \{1_G\},\ \exists\ H_5 = \Sigma_5 : |H_1| = 1,\ |H_5| = 5 \Rightarrow \text{OK}$$

(c) Per ipotesi, $\exists\ N_5 \trianglelefteq G : |N_5| \trianglelefteq G$.

Per il Teorema di Cauchy, esiste in G un elemento δ di ordine 2, il quale genera un sottogruppo $H_2 := \langle \delta \rangle = \{1_G, \delta\} \cong \mathbb{Z}_2$ di ordine 2 (d'altra parte, un tale H_2 esiste per (b), caso ②).

Allora si ha

$$\left.\begin{array}{l} N_5 \trianglelefteq G \\ H_2 \leq G \end{array}\right| \Rightarrow H_{10} := \langle H_2 \cup N_5 \rangle \leq G$$

con $H_{10} = H_2 \cdot N_5 = N_5 \cdot H_2$ e

$H_2 \cap N_5 \quad \{1_G\}$

$N_5 \trianglelefteq H_{10}$ $\Rightarrow$ H_{10} è prodotto semidiretto

$$H_{10} = H_2 \underset{\Phi}{\rtimes} N_5$$

(per un certo morfismo $\Phi : H_2 \longrightarrow Aut_G(N_5)$)

Quindi $H_{10} \leq G$ e

$$|H_{10}| = |H_2 \rtimes N_5| = |H_2 \times N_5| = |H_2| \cdot |N_5| = 2 \cdot 5 = 10$$

così H_{10} è sottogruppo di G di ordine 10, q.e.d.

3 Sia $\mathbb{Z}[\sqrt{-6}] := \left\{ \zeta \in \mathbb{C} \mid \begin{array}{l} \exists\, a,b \in \mathbb{Z} : \\ \zeta = a + b\sqrt{-6} \end{array} \right\}$

Th: (a) Dimostrare che $\mathbb{Z}[\sqrt{-6}]$ è sottoanello di $\mathbb{C}$.

(b) Dimostrare che $\mathbb{Z}[\sqrt{-6}]$ è dominio.

(c) Dimostrare che $\mathbb{Z}[\sqrt{-6}]$ è dominio a fattorizzazione.

(d) Determinare alcune fattorizzazioni in prodotto di fattori irriducibili per l'elemento 70 nell'anello $\mathbb{Z}[\sqrt{-6}]$

(e) Determinare se $\mathbb{Z}[\sqrt{-6}]$ sia un dominio a ideali principali.

Soluzione:

(a) $\mathcal{O}_{\mathbb{C}} = \mathcal{O}_{\mathbb{Z}} + \mathcal{O}_{\mathbb{Z}} \cdot \sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$

poi, $\forall\, (a'+b'\sqrt{-6}),\ (a''+b''\sqrt{-6}) \in \mathbb{Z}[\sqrt{-6}]$ si ha

$(a'+b'\sqrt{-6}) - (a''+b''\sqrt{-6}) = \underset{\in\mathbb{Z}}{(a'-a'')} + \underset{\in\mathbb{Z}}{(b'-b'')}\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$

&

$(a'+b'\sqrt{-6}) \cdot (a''+b''\sqrt{-6}) =$

$= \underset{\in\mathbb{Z}}{(a'a'' - 6\,b'b'')} + \underset{\in\mathbb{Z}}{(a'b'' + b'a'')}\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$

QUINDI $\mathbb{Z}[\sqrt{-6}] \neq \emptyset$ (contiene $0_{\mathbb{C}}$)

$\mathbb{Z}[\sqrt{-6}]$ è chiuso per differenza

$\mathbb{Z}[\sqrt{-6}]$ è chiuso per prodotto

PERCIÒ $\mathbb{Z}[\sqrt{-6}]$ è sottoanello di $\mathbb{C}$, q.e.d.

(b) Siccome $\mathbb{Z}[\sqrt{-6}]$ è sottoanello di $\mathbb{C}$ — per (a) — e $\mathbb{C}$ è un dominio (perché è un campo), allora anche $\mathbb{Z}[\sqrt{-6}]$ è un dominio (perché, in generale, $[A \leq B \ \& \ B \text{ dominio}] \Rightarrow A \text{ dominio}$).

(c) La norma dei numeri complessi

$$N : \mathbb{C} \longrightarrow \mathbb{R}_{\geq 0} \quad (\alpha + i\beta \longmapsto N(\alpha + i\beta) = \alpha^2 + \beta^2)$$

si restringe a una funzione

$$\nu : \mathbb{Z}[\sqrt{-6}] \longrightarrow \mathbb{N}$$
$$(a + b\sqrt{-6}) \longmapsto a^2 + 6b^2$$

che è una valutazione moltiplicativa (segue dal fatto che N stessa preserva il prodotto) ovvero $\mathbb{Z}[\sqrt{-6}]$ è un dominio di valutazione, e come tale

è automaticamente (anche) un dominio a fattorizzazione, q.e.d.

(d) Il calcolo ci dà le due fattorizzazioni

$$70 = 2 \cdot 5 \cdot (1+\sqrt{-6}) \cdot (1-\sqrt{-6}) \qquad (12)$$

&

$$70 = (2+\sqrt{-6})(2-\sqrt{-6}) \cdot (1+\sqrt{-6})(1-\sqrt{-6}) \qquad (13)$$

e ora vediamo che:

(I) – tutti i fattori in (12) e in (13) sono irriducibili;

(II) – le fattorizzazioni in (12) e in (13) non sono equivalenti.

(I) SIA $2 = \alpha \cdot \beta$, con $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$

$$\Downarrow$$

$$\Rightarrow \quad 4 = \nu(2) = \nu(\alpha \cdot \beta) = \nu(\alpha) \cdot \nu(\beta) \Rightarrow$$

$$\Rightarrow \quad 4 = \nu(\alpha) \cdot \nu(\beta) \quad \text{con } \nu(\alpha), \nu(\beta) \in \mathbb{N}_+$$

ma 4 si fattorizza in $\mathbb{N}_+$ come

$$4 = 1 \cdot 4 \quad \text{o} \quad 4 = 2 \cdot 2 \quad \text{o} \quad 4 = 4 \cdot 1$$

PERÒ $\nu(\gamma) \neq 2, \ \forall \gamma \in \mathbb{Z}[\sqrt{-6}]$

quindi sarà $\nu(\alpha) = 1$ o $\nu(\beta) = 1$

$\Rightarrow$ sarà $\alpha \in \{+1, -1\}$ o $\beta \in \{+1, -1\}$

$\Rightarrow \alpha \in U(\mathbb{Z}[\sqrt{-6}])$ o $\beta \in U(\mathbb{Z}[\sqrt{-6}]) \Rightarrow$

$\Rightarrow$ la fattorizzazione $2 = \alpha \cdot \beta$ è banale,

ans 2 è irriducibile in $\mathbb{Z}[\sqrt{-6}]$

SIA $5 = \alpha \cdot \beta$, con $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$

Come prima, $5 = \alpha \cdot \beta$

$\Downarrow$

$25 = \nu(5) = \nu(\alpha) \cdot \nu(\beta)$

$\Downarrow$

$(\nu(\alpha), \nu(\beta)) \in \{(1,25), (5,5), (25,1)\}$

$\nu(\gamma) \neq 5 \quad \forall \gamma \in \mathbb{Z}[\sqrt{-6}]$

quindi sarà $\nu(\alpha) = 1$ o $\nu(\beta) = 1 \Rightarrow$

$\Rightarrow \alpha \in U(\mathbb{Z}[\sqrt{-6}])$ o $\beta \in U(\mathbb{Z}[\sqrt{-6}]) \Rightarrow$

$\Rightarrow$ la fattorizzazione $5 = \alpha \cdot \beta$ è banale $\Rightarrow$

$\Rightarrow$ 5 è irriducibile in $\mathbb{Z}[\sqrt{-6}]$

SIA $(1 \pm \sqrt{-6}) = \alpha \cdot \beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}] \Rightarrow$

{ tratto i due casi insieme

$\Rightarrow 7 = \nu(1 \pm \sqrt{-6}) = \nu(\alpha) \cdot \nu(\beta) \Rightarrow$

$\Rightarrow 7 = \nu(\alpha) \cdot \nu(\beta)$, $\nu(\alpha), \nu(\beta) \in \mathbb{N}_+$ $\rightarrow$ $\nu(\alpha) = 1$ o $\nu(\beta) = 1$ $\Rightarrow$

$\Rightarrow \begin{cases} \alpha \in U(\mathbb{Z}[\sqrt{-6}]) \\ \vee \\ \beta \in U(\mathbb{Z}[\sqrt{-6}]) \end{cases}$ $\Rightarrow$ $(1 \pm \sqrt{-6}) = \alpha \cdot \beta$ è fattorizzazione $\Leftrightarrow$ banale

$(1 \pm \sqrt{-6})$ è irriducibile in $\mathbb{Z}[\sqrt{-6}]$, q.e.d.

ORA, più rapidamente:

$2 \pm \sqrt{-6} = \alpha \cdot \beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$

$\Downarrow \Pi$

$10 = \nu(2 \pm \sqrt{-6}) = \nu(\alpha) \cdot \nu(\beta)$, $\nu(\alpha), \nu(\beta) \in \mathbb{N}$

$\Downarrow \Pi$

$(\nu(\alpha), \nu(\beta)) \in \{(1,10), (2,5), (5,2), (10,1)\}$

MA già sappiamo che

$\nu(\gamma) \neq 2$ e $\nu(\gamma) \neq 5$ $\forall \gamma \in \mathbb{Z}[\sqrt{-6}]$

QUINDI sarà $\nu(\alpha) = 1$ o $\nu(\beta) = 1$ $\Rightarrow$

$\Rightarrow \alpha \in U(\mathbb{Z}[\sqrt{-6}])$ o $\beta \in U(\mathbb{Z}[\sqrt{-6}])$

$\Rightarrow$ la fattorizzazione $2 \pm \sqrt{-6} = \alpha \cdot \beta$ è banale

$\Rightarrow$ $(2 \pm \sqrt{-6})$ è irriducibile in $\mathbb{Z}[\sqrt{-6}]$, q.e.d.

(II) Osserviamo che $U(\mathbb{Z}[\sqrt{-6}]) = \{+1, -1\}$

perché "$\supseteq$" è ovvio, e "$\subseteq$" segue da

$\zeta \in U(\mathbb{Z}[\sqrt{-6}]) \iff \exists\, \zeta^{-1} : 1 = \zeta \cdot \zeta^{-1} \Rightarrow$

$\Rightarrow 1 = \nu(1) = \nu(\zeta) \cdot \nu(\zeta^{-1}) \Rightarrow$

$\Rightarrow \nu(\zeta) = 1 \Rightarrow a^2 + 6b^2 = 1 \Rightarrow a^2 = 1,\ b = 0$

$\zeta = a + b\sqrt{-6} \Rightarrow \nu(\zeta) = a^2 + b^2 \cdot 6$ (⇖)

(⇓ Π) $\zeta = \pm 1$

ALLORA $\forall\ \alpha \in \mathbb{Z}[\sqrt{-6}]$, gli elementi associati ad α sono soltanto $+\alpha$ e $-\alpha$ e siccome, ad esempio, il fattore 2 che figura nella fattorizzazione (12) è diverso dai quattro fattori in (13) e dai loro opposti, concludiamo che (12) e (13) sono due fattorizzazioni non equivalenti..

Cambiando segno ai fattori, sia (12) che (13) danno origine ad altre fattorizzazioni in irriducibili, ancora equivalenti a (12) o a (13), rispettivamente.

(e) Al punto (d) abbiamo trovato che l'elemento 70 in $\mathbb{Z}[\sqrt{-6}]$ ammette almeno due fattorizzazioni in prodotto di irriducibili non equivalenti ma

$\Rightarrow$ $\mathbb{Z}[\sqrt{-6}]$ non è dominio a fattorizzazione unica (=: D.F.U.)

$\Rightarrow$ $\mathbb{Z}[\sqrt{-6}]$ non è un dominio a ideali principali (=: D.I.P.),

perché in generale sappiamo che

Ogni D.I.P. è un D.F.U.

e quindi, viceversa,

R non è D.F.U. $\Rightarrow$ R non è D.I.P. □

CONTINUA

4 Sia $\mathbb{K} \in \{\mathbb{Q}, \mathbb{Z}_3\}$, $f(x) := x^{11} - 1 \in \mathbb{K}[x]$ e sia $\mathbb{K}_f$ il campo di spezzamento di $f(x)$ su $\mathbb{K}$. Per ciascuno dei casi $\mathbb{K} = \mathbb{Q}$ e $\mathbb{K} = \mathbb{Z}_3$, si determini:

(a) il grado $[\mathbb{K} : \mathbb{K}_f]$;

(b) la struttura del gruppo di Galois $G(\mathbb{K}_f/\mathbb{K})$ dell'estensione $\mathbb{K}_f/\mathbb{K}$.

(c) una descrizione esplicita di $G(\mathbb{K}_f/\mathbb{K})$ come gruppo di automorfismi di $\mathbb{K}_f$.

Soluzione: Per definizione è $\mathbb{K}_f = \mathbb{K}(\zeta_{11})$, cioè $\mathbb{K}_f$ è l'estensione ciclotomica di $\mathbb{K}$ generata da una radice 11^a primitiva di 1, cioè da un $\zeta_{11} \in \mathbb{K}^a$ di ordine (moltiplicativo) $\omega(\zeta_{11}) = 11$. Possiamo allora sfruttare alcuni risultati generali.

Il polinomio ciclotomico 11° è

$$p_{11}(x) = \frac{x^{11} - 1}{x - 1} = x^{10} + \cdots + x^2 + x + 1$$

(perché 11 è primo), e $p_{11}(\zeta_{11}) = 0$.

$\mathbb{K} = \mathbb{Q}$

$\mathbb{K} = \mathbb{Q}$ il polinomio ciclotomico n° è irriducibile $(\forall n \in \mathbb{N}_+)$, in particolare

$$p_{11}(x) = x^{10} + x^9 + \cdots + x^2 + x + 1$$

è irriducibile in $\mathbb{Q}[x]$. Poiché inoltre ζ_{11} è radice di $p_{11}(x)$, si conclude che

$$p_{11}(x) = p^{\mathbb{Q}}_{\zeta_{11}}(x) := \text{polinomio minimo di } \zeta_{11} \text{ su } \mathbb{Q}$$

QUINDI

$$\mathbb{Q}_f = \mathbb{Q}(\zeta_{11}) \cong \frac{\mathbb{Q}[x]}{\left(p^{\mathbb{Q}}_{\zeta_{11}}(x)\right)} =$$

$$= \frac{\mathbb{Q}[x]}{\left(x^{10} + \cdots + x^2 + x + 1\right)}$$

COSÌ $[\mathbb{Q}_f : \mathbb{Q}] = [\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] =$

$$= \partial\left(p^{\mathbb{Q}}_{\zeta_{11}}(x)\right) = \partial\left(x^{10} + \cdots + x + 1\right) = 10$$

CIOÈ

$$[\mathbb{Q}_f : \mathbb{Q}] = 10$$

il che risolve il punto (a) per $\mathbb{K} = \mathbb{Q}$.

(b) $\forall\, \varphi \in G(\mathbb{Q}_f/\mathbb{Q})$, si ha che

$\omega(\varphi(\zeta_{11})) = \omega(\zeta_{11}) = 11$, cioè

$\varphi(\zeta_{11})$ è anch'essa una radice 11^a primitiva di 1; ora, le radici 11^e di 1 formano un sottogruppo R_{11} di $(\mathbb{Q}_f^*; \cdot)$, che è ciclico di ordine 11, e i cui generatori sono esattamente le radici 11^e primitive. QUINDI l'isomorfismo di gruppi

$$(\mathbb{Z}_{11}; +) \xrightarrow{\cong} (R_{11}; \cdot)$$
$$\bar{a} \longmapsto \zeta_{11}^{a}$$

si restringe a una biiezione

$$\psi : U(\mathbb{Z}_{11}) \longrightarrow \{\text{radici } 11^e \text{ primitive di } 1\}$$
$$\bar{a} \longmapsto \zeta_{11}^{a}$$

Abbiamo allora una funzione

$$\mu : G(\mathbb{Q}_f/\mathbb{Q}) \longrightarrow U(\mathbb{Z}_{11})$$
$$\varphi \longmapsto \psi^{-1}(\varphi(\zeta_{11}))$$

che è iniettiva (perché $\varphi'(\zeta_{11}) = \varphi''(\zeta_{11})$ implica $\varphi' = \varphi''$, dato che $\mathbb{Q}_f = \mathbb{Q}(\zeta_{11})$, cioè ζ_{11} genera $\mathbb{Q}_f$ su $\mathbb{Q}$), ed è un morfismo di gruppi. Inoltre, $\mathbb{Q}_f/\mathbb{Q}$ è estensione di Galois, quindi

$$|G(\mathbb{Q}_f/\mathbb{Q})| = [\mathbb{Q}_f : \mathbb{Q}] = 10 = |U(\mathbb{Z}_{11})|$$

e quindi μ oltre che iniettiva è anche biiettiva, dunque è un isomorfismo

$$\mu : G(\mathbb{Q}_f/\mathbb{Q}) \xrightarrow{\cong} U(\mathbb{Z}_{11}) \cong (\mathbb{Z}_{10}; +)$$

e questo basta a descrivere la struttura del gruppo $G(\mathbb{Q}_f/\mathbb{Q})$, come ciclico, isomorfo a $(\mathbb{Z}_{10}; +)$.

L'ultimo passaggio segue dal fatto che $(\mathbb{Z}_{11}; +, \cdot)$ è un campo finito, e allora il suo gruppo delle unità $(U(\mathbb{Z}_{11}); \cdot)$ è ciclico, e quindi — dato che ha $|U(\mathbb{Z}_{11})| = |\mathbb{Z}_{11} \setminus \{0\}| = 10$ elementi — è isomorfo a $(\mathbb{Z}_{10}; +)$.

Questo risponde al quesito (b) per $\mathbb{K} = \mathbb{Q}$.

(c) Basta esplicitare l'isomorfismo

$$\mu : G(\mathbb{Q}_f/\mathbb{Q}) \xrightarrow{\cong} U(\mathbb{Z}_{11})$$

dato in (b). Ogni $\varphi \in G(\mathbb{Q}_f/\mathbb{Q})$ corrisponde biiettivamente a 1! classe $\bar{a} \in U(\mathbb{Z}_{11})$, che è quella tale che

$$\varphi(\zeta_{11}) = \zeta_{11}^{a}$$

Usando questa formula, gli elementi φ in $G(\mathbb{Q}_f/\mathbb{Q})$ sono tutti e soli gli automorfismi di $\mathbb{Q}_f$ descritti da

$$\varphi = \varphi_{\bar{a}} = \mu^{-1}(\bar{a}) : \begin{cases} q \longmapsto \varphi_{\bar{a}}(q) := q \quad (\forall q \in \mathbb{Q}) \\ \zeta_{11} \longmapsto \varphi_{\bar{a}}(\zeta_{11}) = \zeta_{11}^{a} \end{cases}$$

$$\forall\, \bar{a} \in U(\mathbb{Z}_{11})$$

e poiché tramite $\mathbb{Q}_f \cong \mathbb{Q}[x]/(f(x))$ ogni elemento di $\mathbb{Q}_f$ corrisponde a 1! classe di congruenza $[P(x)]_{f(x)}$ con $P(x) \in \mathbb{Q}[x]$, che esprime l'elemento $P(\zeta_{11}) \in \mathbb{Q}_f$, in generale ogni $\varphi_{\bar{a}}$ è descritto da $\varphi_{\bar{a}}(P(\zeta_{11})) = P(\zeta_{11}^{a})$.
Questo risponde al quesito (c) per $\mathbb{K} = \mathbb{Q}$.

$\mathbb{K} = \mathbb{Z}_3$

(a) Per $\mathbb{K} = \mathbb{Z}_3$ possiamo "riciclare" – con modifiche – vari passaggi dell'analisi fatta per $\mathbb{K} = \mathbb{Q}$, ma anche sfruttare un approccio diverso.

Come prima, è sempre (in generale)

$$\mathbb{K}_f = \mathbb{K}(\zeta_{11}) \cong \frac{\mathbb{K}[x]}{(p_{\zeta_{11}}^{\mathbb{K}}(x))}$$

dove il polinomio minimo di ζ_{11} su $\mathbb{K}$, che è $p_{\zeta_{11}}^{\mathbb{K}}(x)$, certamente divide il polinomio ciclotomico $p_{11}(x)$; in particolare sarà

$$d = \partial(p_{\zeta_{11}}^{\mathbb{K}}(x)) \leq \partial(p_{11}(x)) = 10$$

e QUINDI

$$[\mathbb{K}_f : \mathbb{K}] = [\mathbb{K}(\zeta_{11}) : \mathbb{K}] = \partial(p_{\zeta_{11}}^{\mathbb{K}}(x)) = d \leq 10$$

D'altra parte, $\mathbb{K} = \mathbb{Z}_3$ è un campo finito, e la sua estensione finita di grado d $\mathbb{K}_f = \mathbb{Z}_3(\zeta_{11})$ è allora a sua volta un campo finito, con

$$|\mathbb{K}_f| = |\mathbb{Z}_3(\zeta_{11})| = |\mathbb{Z}_3|^{[\mathbb{Z}_3(\zeta_{11}):\mathbb{Z}_3]} =$$

$$= |\mathbb{Z}_3|^d = 3^d$$

ALLORA $\mathbb{K}_f = \mathbb{Z}_3(\zeta_{11})$ è un campo di cardinalità 3^d (con $d \leq 10$) che contiene ζ_{11}, cioè un elemento di ordine moltiplicativo 11; $\Rightarrow$ $\Rightarrow$ il gruppo moltiplicativo $\mathbb{K}_f^* := \mathbb{K}_f \setminus \{0\}$ contiene un elemento di ordine 11, quindi

$$11 \mid_{\mathbb{N}} |\mathbb{K}_f^*| = |\mathbb{K}_f \setminus \{0\}| = 3^d - 1$$

cioè 11 divide $(3^d - 1)$, per il Teorema di Lagrange. Inoltre, $\mathbb{K}_f$ è il minimo campo con queste proprietà, il che equivale a dire che il numero d dev'essere minimo possibile.

ORA $d=1 \Rightarrow 3^1 - 1 = 2 \notin 11\text{-}\mathbb{N}_+$

$d=2 \Rightarrow 3^2 - 1 = 8 \notin 11\text{-}\mathbb{N}_+$

$\vdots$

$d=5 \Rightarrow 3^5 - 1 = 243 - 1 = 242 = 11 \cdot 22 \in 11\mathbb{N}_+$

cioè $d = 5$ è il minimo valore tale che $(3^d - 1)$ sia multiplo di 11.

QUINDI è $d \geq 5$, ma d'altra parte il campo $\mathbb{F}_{3^5}$ con 3^5 elementi ha gruppo moltiplicativo $\mathbb{F}_{3^5}^*$ che è ciclico di ordine $3^5 - 1 = 242$; essendo ciclico, esso contiene un elemento di ordine t (cioè una radice t^a primitiva di 1) per ogni divisore t dell'ordine $|\mathbb{F}_{3^5}^*| = 242$, in particolare per $t = 11$, $\Rightarrow$ $\Rightarrow$ $\mathbb{F}_{3^5}$ contiene una radice 11^a primitiva di 1, sia ζ_{11}, ed è il minimo campo estensione di $\mathbb{Z}_3$ con questa proprietà; PERCIÒ

$$K_f = (\mathbb{Z}_3)_f = \mathbb{F}_{3^5}$$

In particolare, ne segue che

$$[\mathbb{K}_f : \mathbb{K}] = [\mathbb{F}_{35} : \mathbb{Z}_{13}] = [\mathbb{F}_{35} : \mathbb{F}_3] = 5$$

cioè $\underline{[\mathbb{K}_f : \mathbb{K}] = 5}$

che risponde al quesito (a) per $\mathbb{K} = \mathbb{Z}_{13}$.

(b) Come per $\mathbb{K} = \mathbb{Q}$ — è un fatto generale — anche per $\mathbb{K} = \mathbb{Z}_{13}$ esiste il monomorfismo

$$\mu : G(\mathbb{K}_f/\mathbb{K}) \longrightarrow U(\mathbb{Z}_{11})$$
$$\varphi \longmapsto \bar{a} \quad (\text{t.c. } \varphi(\zeta_{11}) = \zeta_{11}^a)$$

però adesso questo <u>NON</u> è suriettivo, perché (per il punto (a))

$$|G(\mathbb{K}_f/\mathbb{K})| = [\mathbb{K}_f : \mathbb{K}] = [\mathbb{F}_{35} : \mathbb{F}_3] = 5$$

mentre $|U(\mathbb{Z}_{11})| = 10$.

Ma tramite μ abbiamo che

$\mathrm{Im}(\mu) = \mu(G(\mathbb{K}_f/\mathbb{K}))$ è un sottogruppo di $U(\mathbb{Z}_{11})$, <u>isomorfo</u> a $G(\mathbb{K}_f/\mathbb{K})$, di ordine 5 e ciclico, dunque isomorfo a $(\mathbb{Z}_5; +)$; ovvero $G(\mathbb{K}_f/\mathbb{K}) \cong \mathbb{Z}_5$, che risponde a (b) per $\mathbb{K} = \mathbb{Z}$

(c) Siccome $U(\mathbb{Z}_{11}) \cong \mathbb{Z}_{10}$ è ciclico di ordine 10, $\forall$ divisore t di 10 $\exists!$ sottogruppo $H_t \leq U(\mathbb{Z}_{11}) : |H_t| = t$

ovvero in particolare (per $t=5$)

$\exists!$ sottogruppo $H_5 \leq U(\mathbb{Z}_{11}) : |H_5| = 5$

Per il punto (b) allora è

$$H_5 = \mathrm{Im}(\mu) = \mu(G(\mathbb{K}_f/\mathbb{K})) \cong G(\mathbb{K}_f/\mathbb{K})$$

Tale H_5 è generato da un elemento $\bar{c}$ in $U(\mathbb{Z}_{11})$ di ordine 5: ad esempio, un tale elemento è $\bar{c} = \bar{3}$, e $H_5 = \{\bar{1}, \bar{3}, \bar{9}, \overline{27}, \overline{81}\}$

ALLORA da $\mu : G(\mathbb{K}_f/\mathbb{K}) \xrightarrow{\cong} H_5 = \langle \bar{3} \rangle$

$\varphi \longmapsto \bar{a} \; (: \varphi(\zeta_{11}) = \zeta_{11}^{a})$

si ha che tutti i φ in $G(\mathbb{K}_f/\mathbb{K})$ sono del tipo

$$\varphi = \varphi_{\bar{a}} : \begin{cases} q \longmapsto \varphi_{\bar{a}}(q) := q & (\forall\, q \in \mathbb{Z}_3) \\ \zeta_{11} \longmapsto \varphi_{\bar{a}}(\zeta_{11}) = \zeta_{11}^{a} \end{cases}$$

$\forall\, \bar{a} \in H_5$

$\quad\|\quad$ e in generale $\varphi(P(\zeta_{11})) = P(\zeta_{11}^{a})$

$\{\bar{1}, \bar{3}, \bar{9}, \overline{27}, \overline{81}\}$ $\quad \forall\, P(\zeta_{11}) \in \mathbb{Z}_3(\zeta_{11}) \cong \mathbb{Z}_3[x] / (P_{\zeta_{11}}^{\mathbb{Z}_3}(x))$

5. Dato $n \in \mathbb{N}_+$ e $E_n := \{1, 2, \dots, n\}$, si consideri l'azione del gruppo simmetrico $\Sigma_n := \Sigma(E_n)$ sull'insieme $E_n \times E_n \times E_n =: \mathbb{E}$ definita da $(\forall \sigma \in \Sigma, \forall (x,y,z) \in E_n \times E_n \times E_n)$

$$\sigma.(x,y,z) := (\sigma(x), \sigma(y), \sigma(z))$$

Si descrivano le Σ_n-orbite in $E_n \times E_n \times E_n$.

Soluzione:

$\forall P_0 := (x_0, y_0, z_0) \in E_n \times E_n \times E_n =: \mathbb{E}$

calcoliamo la sua Σ_n-orbita,

cioè $\mathcal{O}_{P_0} = \Sigma_n . P_0$.

Ci sono diversi casi da distinguere, che dipendono esclusivamente dalla eventualità che due o tre delle "coordinate" di P_0 coincidano. Siano

$$\mathbb{E}_\emptyset := \{(x,y,z) \in \mathbb{E} \mid x \neq y, y \neq z, z \neq x\}$$

$$\mathbb{E}_{(1,2,3)} := \{(x,y,z) \in \mathbb{E} \mid x = y = z\}$$

$$\mathbb{E}_{(1,2)} := \{(x,y,z) \in \mathbb{E} \mid x = y \neq z\}$$

$$\mathbb{E}_{(2,3)} := \{(x,y,z) \in \mathbb{E} \mid x \neq y = z\}$$

$$\mathbb{E}_{(1,3)} := \{(x,y,z) \in \mathbb{E} \mid x = z \neq y\}$$

Vediamo dunque i vari casi

$\underline{P_0 \in \mathbb{E}_\emptyset}$: $\forall\, P_0 \in \mathbb{E}_\emptyset$ si ha

$P_0 = (x_0, y_0, z_0)$ con $x_0 \overset{*}{\#} y_0 \overset{*}{\#} z_0$ $\Rightarrow$

$\Rightarrow \sigma(x_0) \overset{*}{\#} \sigma(y_0) \overset{*}{\#} \sigma(z_0)$ $\forall \sigma \in \mathfrak{S}_n$ perché σ è iniettiva $\Rightarrow$

$\Rightarrow \sigma . P_0 = (\sigma(x_0), \sigma(y_0), \sigma(z_0)) \in \mathbb{E}_\emptyset$

$\underline{\text{CIOÈ}}$ $P_0 \in \mathbb{E}_\emptyset \Rightarrow \sigma . P_0 \in \mathbb{E}_\emptyset$, $\forall \sigma \in \mathfrak{S}_n$

$\underline{\text{DUNQUE}}$ $\mathcal{O}_{P_0} = \mathfrak{S}_n . P_0 \subseteq \mathbb{E}_\emptyset$ $\forall P_0 \in \mathbb{E}_\emptyset$

VICEVERSA, sia $P' = (x', y', z') \in \mathbb{E}_\emptyset$; $\longrightarrow$

ma $x' \overset{*}{\#} y' \overset{*}{\#} z'$ è certamente

$\exists\, \sigma' \in \mathfrak{S}_n : \sigma(x_0) = x',\ \sigma(y_0) = y',\ \sigma(z_0) = z'$

così che $\sigma' . P_0 = (\sigma'(x_0), \sigma'(y_0), \sigma'(z_0)) = P'$

$\underline{\text{CIOÈ}}$ $P' = \sigma' . P_0 \in \mathfrak{S}_n . P_0 = \mathcal{O}_{P_0}$ $(\forall P' \in \mathbb{E}_\emptyset)$

$\underline{\text{DUNQUE}}$ $\mathbb{E}_\emptyset \subseteq \mathfrak{S}_n . P_0 = \mathcal{O}_{P_0}$

QUINDI abbiamo

$$\mathcal{O}_{P_0} = \mathbb{E}_\varnothing \qquad \forall\, P_0 \in \mathbb{E}_\varnothing$$

in particolare $\mathbb{E}_\varnothing$ è una Σ_n-orbita.

N.B.: tutto questo ha senso <u>se</u> $n \geq 3$, ché allora è $\mathbb{E}_\varnothing \neq \phi$.

<u>SE</u> invece è $n \leq 2$ (cioè $n \in \{1, 2\}$)

ALLORA $\mathbb{E}_\varnothing = \phi$ (per definizione)

e questo passo si può scartare dalla analisi. ◇

<u>INOLTRE</u>, calcoliamo $|\mathcal{O}_{P_0}| = |\mathbb{E}_\varnothing|$, $\forall P_0 \in \mathbb{E}_\varnothing$

La teoria generale dà

$$|\mathcal{O}_{P_0}| = |\Sigma_n| / |\mathcal{St}_{P_0}^{\Sigma_n}| \qquad (14)$$

dove $\mathcal{St}_{P_0}^{\Sigma_n}$:= stabilizzatore di P_0 in Σ_n =

$$= \{\sigma \in \Sigma_n \mid \sigma . P_0 = P_0\} =$$

$$= \{\sigma \in \Sigma_n \mid \sigma(x_0) = x_0, \sigma(y_0) = y_0, \sigma(z_0) = z_0\}$$

Allora è $\mathcal{St}_{P_0}^{\Sigma_n} = \Sigma(E_n \setminus \{x_0, y_0, z_0\}) \cong \Sigma_{n-3}$

QUINDI la (14) ci dà

$$|\mathcal{O}_{P_0}| = \frac{|\Sigma_n|}{|St_{P_0}^{\Sigma_n}|} = \frac{|\Sigma_n|}{|\Sigma_{n-3}|} = \frac{n!}{(n-3)!} = \underbrace{n\cdot(n-1)\cdot(n-2)}$$

cioè

$$|\mathcal{O}_{P_0}| = n(n-1)(n-2) \qquad \forall\, P_0 \in \mathbb{E}_\emptyset$$

IN ALTERNATIVA, calcoliamo direttamente

$$|\mathbb{E}_\emptyset| = \left| \{(x,y,z) \in \mathbb{E} := E_n^{\times 3} \mid x \neq y,\ y \neq z,\ z \neq x\} \right| =$$

$$= n \cdot (n-1) \cdot (n-2)$$

perché $\#\left(\text{scelte (libere) di } x \in E_n\right) = n$

$$\#\left(\text{scelte di } y \in E_n \setminus \{x\}\right) = n-1$$

$$\#\left(\text{scelte di } z \in E_n \setminus \{x,y\}\right) = n-2$$

con' $|\mathbb{E}_\emptyset| = n\cdot(n-1)\cdot(n-2)$

che è coerente con $\mathbb{E}_\emptyset = \mathcal{O}_{P_0}$, $\forall P_0 \in \mathbb{E}_\emptyset$

<u>$P_0 \in \mathbb{E}_{(1,2)}$:</u> $\forall\ P_0 \in \mathbb{E}_{(1,2)}$ si ha

$P_0 = (x_0, y_0, z_0)$ con $x_0 = y_0 \neq z_0$ $\Rightarrow$

$\Rightarrow \sigma(x_0) = \sigma(y_0) \neq \sigma(z_0)$ $\forall \sigma \in \Sigma_n$ (σ è iniettiva!)

quindi $\sigma . P_\delta = (\sigma(x_\delta), \sigma(y_\delta), \sigma(z_\delta)) \in \mathbb{E}_{(1,2)}$

$\forall \sigma \in \Sigma_n$

così

$$\mathcal{O}_{P_\delta} = \Sigma_n . P_\delta \subseteq \mathbb{E}_{(1,2)}$$

VICEVERSA, $\forall \; P' = (x', y', z') \in \mathbb{E}_{(1,2)}$

si ha $x' = y' \neq z'$ e allora

$$\exists\, \sigma' \in \Sigma_n : \quad \begin{matrix} \sigma'(x_\delta) = x' \\ \| \\ \sigma'(y_\delta) = y' \end{matrix} \quad \& \quad \sigma'(z_\delta) = z'$$

così che $\sigma' . P_\delta = (\sigma'(x_\delta), \sigma'(y_\delta), \sigma'(z_\delta)) = P'$

CIOÈ $P' = \sigma' . P_\delta \in \Sigma_n . P_\delta = \mathcal{O}_{P_\delta}, \; \forall P' \in \mathbb{E}_{(1,2)}$

DUNQUE $\mathbb{E}_{(1,2)} \subseteq \Sigma_n . P_\delta = \mathcal{O}_{P_\delta} \; \forall P_\delta \in \mathbb{E}_{(1,2)}$

QUINDI abbiamo che

$$\boxed{\mathcal{O}_{P_\delta} = \mathbb{E}_{(1,2)}} \qquad \forall P_\delta \in \mathbb{E}_{(1,2)}$$

in particolare $\mathbb{E}_{(1,2)}$ è una Σ_n-orbita.

INOLTRE, calcoliamo $|\mathcal{O}_{P_\delta}| = |\mathbb{E}_{(1,2)}|$, $\forall P_\delta \in \mathbb{E}_{(1,2)}$

Da un lato, vale sempre la (14), con lo stabilizzatore di P_δ ($\in \mathbb{E}_{(1,2)}$) dato da

$$\mathcal{St}_{P_0}^{\mathfrak{S}_n} = \{\sigma \in \mathfrak{S}_n \mid \sigma(x_0) = x_0,\ \sigma(z_0) = z_0\}$$

$\Rightarrow \{\sigma(y_0) = y_0$ perché è $y_0 = x_0$

e quindi è

$$\mathcal{St}_{P_0}^{\mathfrak{S}_n} = \mathfrak{S}(E_n \setminus \{x_0, z_0\}) \cong \mathfrak{S}_{n-2}$$

QUINDI la (14) ci dà

$$|\mathcal{O}_{P_0}| = \frac{|\mathfrak{S}_n|}{|\mathcal{St}_{P_0}^{\mathfrak{S}_n}|} = \frac{|\mathfrak{S}_n|}{|\mathfrak{S}_{n-2}|} = \frac{n!}{(n-2)!} = n\cdot(n-1)$$

cioè

$$|\mathcal{O}_{P_0}| = n\cdot(n-1) \quad \forall\ P_0 \in \mathbb{E}_{(1,2)}$$

Dall'altro lato, il calcolo diretto ci dà

$$|\mathbb{E}_{(1,2)}| = |\{(x,y,z) \in \mathbb{E} = E_n^{\times 3} \mid x = y \neq z\}| =$$

$$= n\cdot(n-1)$$

perché $\#(\text{scelte (libere) di } x \in E_n) = n$

$$\#(\text{scelte di } y = x) = 1$$

$$\#(\text{scelte di } z \in E_n \setminus \{x\}) = n-1$$

così $|\mathbb{E}_{(1,2)}| = n\cdot 1\cdot(n-1) = n\cdot(n-1)$

che è coerente con $\mathbb{E}_{(1,2)} = \mathcal{O}_{P_0}$, $\forall\ P_0 \in \mathbb{E}_{(1,2)}$

$P_\sigma \in \mathbb{E}_{(2,3)}$ & $P_\sigma \in \mathbb{E}_{(1,3)}$: sono casi del tutto analoghi a $P_\sigma \in \mathbb{E}_{(1,2)}$, e il risultato è parallelo! Si trova quindi

$$\mathcal{O}_{P_\sigma} = \mathbb{E}_{(2,3)} \qquad \forall\, P_\sigma \in \mathbb{E}_{(2,3)}$$

con $|\mathcal{O}_{P_\sigma}| = |\mathbb{E}_{(2,3)}| = n(n-1)$

N.B.: qui si suppone che $n \geq 2$; se $n < 2$ ($\Leftrightarrow n = 1$) è $\mathbb{E}_{(i,j)} = \emptyset$

&

$$\mathcal{O}_{P_\sigma} = \mathbb{E}_{(1,3)} \qquad \forall\, P_\sigma \in \mathbb{E}_{(1,3)}$$

con $|\mathcal{O}_{P_\sigma}| = |\mathbb{E}_{(1,3)}| = n(n-1)$

$P_\sigma \in \mathbb{E}_{(1,2,3)}$: $\forall\, P_\sigma \in \mathbb{E}_{(1,2,3)}$ si ha

$P_\sigma = (x_\sigma, y_\sigma, z_\sigma)$ con $x_\sigma = y_\sigma = z_\sigma \Rightarrow$

$\Rightarrow \forall \sigma \in \mathcal{S}_n$ è $\sigma(x_\sigma) = \sigma(y_\sigma) = \sigma(z_\sigma) \Rightarrow$

$\Rightarrow \sigma \cdot P_\sigma = (\sigma(x_\sigma), \sigma(y_\sigma), \sigma(z_\sigma)) \in \mathbb{E}_{(1,2,3)}$, $\forall \sigma \in \mathcal{S}_n$

QUINDI $\mathcal{O}_{P_\sigma} = \mathcal{S}_n \cdot P_\sigma \subseteq \mathbb{E}_{(1,2,3)}$, $\forall P_\sigma \in \mathbb{E}_{(1,2,3)}$

VICEVERSA, $\forall\, P' = (x', y', z') \in \mathbb{E}_{(1,2,3)}$ si ha $x' = y' = z'$ e $\exists\, \sigma \in \mathcal{S}_n$: $\sigma'(x_\sigma) = x'$ $\left(\Leftrightarrow \begin{matrix}\sigma'(y_\sigma) = y' \\ \sigma'(z_\sigma) = z'\end{matrix}\right)$

così che $\sigma' \cdot P_\sigma = (\sigma'(x_\sigma), \sigma'(y_\sigma), \sigma'(z_\sigma)) = P'$

CIOÈ $P' = \sigma' \cdot P_\sigma \in \mathfrak{S}_n \cdot P_\sigma = \mathcal{O}_{P_\sigma}$ $\forall P' \in \mathbb{E}_{(1,2,3)}$ $\forall P_\sigma \in \mathbb{E}_{(1,2,3)}$

DUNQUE

$$\mathbb{E}_{(1,2,3)} \subseteq \mathfrak{S}_n \cdot P_\sigma = \mathcal{O}_{P_\sigma} \quad \forall P_\sigma \in \mathbb{E}_{(1,2,3)}$$

QUINDI abbiamo che

$$\boxed{\mathcal{O}_{P_\sigma} = \mathbb{E}_{(1,2,3)}} \quad \forall P_\sigma \in \mathbb{E}_{(1,2,3)}$$

in particolare $\mathbb{E}_{(1,2,3)}$ è una $\mathfrak{S}_n$-orbita.

INOLTRE, calcoliamo $|\mathcal{O}_{P_\sigma}| = |\mathbb{E}_{(1,2,3)}|$, $\forall P_\sigma \in \mathbb{E}_{(1,2,3)}$

Da un lato, vale la (14) con

$$\mathfrak{St}^{\mathfrak{S}_n}_{P_\sigma} = \{\sigma \in \mathfrak{S}_n \mid \sigma(x_\sigma) = x_\sigma\} \overset{(\sigma(y_\sigma)=y_\sigma \ \& \ \sigma(z_\sigma)=z_\sigma)}{=} \overset{(\text{che } y_\sigma = x_\sigma \ \& \ z_\sigma = x_\sigma)}{=}$$

$$= \mathfrak{S}(E_n \setminus \{x_\sigma\}) \cong \mathfrak{S}_{n-1}$$

QUINDI la (14) ci dà

$$|\mathcal{O}_{P_\sigma}| = \frac{|\mathfrak{S}_n|}{|\mathfrak{St}^{\mathfrak{S}_n}_{P_\sigma}|} = \frac{|\mathfrak{S}_n|}{|\mathfrak{S}_{n-1}|} = \frac{n!}{(n-1)!} = n$$

cioè $|\mathcal{O}_{P_\sigma}| = n \quad \forall P_\sigma \in \mathbb{E}_{(1,2,3)}$

D'altro canto, il calcolo diretto dà

$$|\mathbb{E}_{(1,2,3)}| = |\{(x,y,z) \in \mathbb{E} = E_n^{\times 3} \mid x=y=z\}| =$$

$$= |\{(t,t,t) \mid t \in E_n\}| = n$$

così $|\mathbb{E}_{(1,2,3)}| = n$,

che è coerente con $\mathbb{E}_{(1,2,3)} = \mathcal{O}_{P_\sigma}$, $\forall P_\sigma \in \mathbb{E}_{(1,2,3)}$

CONCLUSIONE: le Σ_n-orbite in $\mathbb{E} := E_n \times E_n \times E_n$ sono cinque[1], precisamente

$$\mathbb{E}_\emptyset, \mathbb{E}_{(1,2)}, \mathbb{E}_{(2,3)}, \mathbb{E}_{(1,3)}, \mathbb{E}_{(1,2,3)} \qquad (15)$$

definite a pagina 28.

[1] Per $n \geq 3$; per $n \leq 2$ vedasi qui sotto...!

NOTA: siccome le orbite di un gruppo G in un G-spazio $\mathcal{E}$ formano una partizione di $\mathcal{E}$, adesso verifichiamo che (15) dia una partizione di $\mathbb{E}$.

Distinguiamo i vari casi (i primi due sono "degeneri")

$(n=1)$ in questo caso è

$$E_1 = \{1\}, \quad \mathbb{E} := E_1 \times E_1 \times E_1 = \{(1,1,1)\} = \mathbb{E}_{(1,2,3)}$$

con $\mathbb{E}_\emptyset = \emptyset$, $\mathbb{E}_{(1,2)} = \emptyset$, $\mathbb{E}_{(2,3)} = \emptyset$, $\mathbb{E}_{(1,3)} = \emptyset$

ovvio $\exists!$ orbita, che è $\mathbb{E}_{(1,2,3)} = \mathbb{E}$ (ovviamente è una partizione!)

$n=2$ in questo caso è

$\mathbb{E}_\varnothing = \varnothing$, quindi le

S_2-orbite in $\mathbb{E}$ sono quattro,

precisamente

$$\mathbb{E}_{(1,2)},\ \mathbb{E}_{(2,3)},\ \mathbb{E}_{(1,3)},\ \mathbb{E}_{(1,2,3)}$$

Esse sono non vuote e disgiunte, per definizione! Inoltre, il totale dei loro elementi è

$$\left| \mathbb{E}_{(1,2)} \amalg \mathbb{E}_{(2,3)} \amalg \mathbb{E}_{(1,3)} \amalg \mathbb{E}_{(1,2,3)} \right| =$$

$$= \left|\mathbb{E}_{(1,2)}\right| + \left|\mathbb{E}_{(2,3)}\right| + \left|\mathbb{E}_{(1,3)}\right| + \left|\mathbb{E}_{(1,2,3)}\right| =$$

$$= 2\cdot(2-1) + 2\cdot(2-1) + 2\cdot(2-1) + 2 = 8 =$$

$$= 2\cdot 2\cdot 2 = |E_2|\cdot|E_2|\cdot|E_2| = |E_2 \times E_2 \times E_2| = |\mathbb{E}|$$

cioè le orbite complessivamente hanno tanti elementi quanto l'intero spazio $\mathbb{E}$, quindi la loro unione è tutto $\mathbb{E}$, q.e.d.

(CONTINUA ...)

$\forall\, n \geq 3$ in questo caso è

$$\mathbb{E}_{\emptyset} \neq \emptyset,\ \mathbb{E}_{(1,2)} \neq \emptyset,\ \mathbb{E}_{(2,3)} \neq \emptyset,$$
$$\mathbb{E}_{(1,3)} \neq \emptyset \quad \text{e} \quad \mathbb{E}_{(1,2,3)} \neq \emptyset$$

così ci sono esattamente cinque $\mathfrak{S}_n$-orbite. Per definizione, esse sono vuote e a due a due disgiunte; inoltre, il totale dei loro elementi è

$$\left| \mathbb{E}_{\emptyset} \amalg \mathbb{E}_{(1,2)} \amalg \mathbb{E}_{(2,3)} \amalg \mathbb{E}_{(1,3)} \amalg \mathbb{E}_{(1,2,3)} \right| =$$

$$= |\mathbb{E}_{\emptyset}| + |\mathbb{E}_{(1,2)}| + |\mathbb{E}_{(2,3)}| + |\mathbb{E}_{(1,3)}| + |\mathbb{E}_{(1,2,3)}| =$$

$$= n\cdot(n-1)(n-2) + n\cdot(n-1) + n\cdot(n-1) +$$
$$+ n\cdot(n-1) + n =$$
$$= n\cdot\big((n-1)(n-2) + (n-1)\cdot 3 + 1\big) =$$
$$= n\cdot((n-1)(n+1) + 1) = n\cdot((n^2-1)+1) = n^3$$

$|\mathbb{E}| = |\mathbb{E}_n^{\times 3}|$

così le orbite complessivamente hanno tanti elementi quanto l'intero spazio $\mathbb{E}$, quindi la loro unione è tutto $\mathbb{E}$, q.e.d.