Università degli Studi di Roma "Tor Vergata"
CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2024-2025

Esame scritto del 23 Settembre 2025 — 4° appello, sessione autunnale

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

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

[1] — Sia G un gruppo di ordine 175.

(a) Dimostrare che G è abeliano.

(b) Tenendo conto che il gruppo G è abeliano, determinare quale possa essere la sua struttura ciclica secondo il 1^0 *Teorema di Classificazione* e il 2^0 *Teorema di Classificazione* dei gruppi abeliani finiti.

[2] — Sia $\mathbb{F}_5$ il campo con 5 elementi, e sia $\mathbb{F}_5(\alpha)$ un campo estensione di $\mathbb{F}_5$ generato da un elemento α tale che $\alpha^4 + 4\,\alpha - 1 = 0$ in $\mathbb{F}_5(\alpha)$.

(a) Dimostrare che il grado dell'estensione di campi $\mathbb{F}_5(\alpha)/\mathbb{F}_5$ è 4.

(b) Descrivere esplicitamente un elemento non banale del gruppo di Galois $Gal(\mathbb{F}_5(\alpha)/\mathbb{F}_5)$, precisandone l'effetto sugli elementi di $\mathbb{F}_5$ e sul generatore α dell'estensione $\mathbb{F}_5(\alpha)/\mathbb{F}_5$.

(c) Determinare il numero totale di campi $\mathbb{F}$ intermedi dell'estensione $\mathbb{F}_5(\alpha)/\mathbb{F}_5$, cioè tali che $\mathbb{F}_5 \subseteq \mathbb{F} \subseteq \mathbb{F}_5(\alpha)$.

[3] — Si consideri l'anello $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Z}_5\}$ e il polinomio

$$f(x) := x^5 - 14\,x^4 - 15\,x^3 + 30\,x^2 + 24\,x - 6 \in \mathbb{A}[x]$$

(a) Fattorizzare $f(x)$ in polinomi irriducibili in $\mathbb{A}[x]$, per ogni scelta di $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Z}_5\}$.

(b) Determinare se esistano in $\mathbb{A}$ radici multiple di $f(x)$.

(continua...) ⟹

[4] — Descrivere, a meno di isomorfismi, tutti i gruppi G di ordine 28.

[5] — Sia G un gruppo. Per ogni G–spazio S, si dice G–sottospazio di S ogni sottoinsieme T in S tale che $g.t \in T$ per ogni $t \in T$ e ogni $g \in G$.

Per un anello unitario $(A\,;+,\cdot)$, si dice che un'azione $G \times A \longrightarrow A$ di G su A è *per automorfismi* se ogni applicazione

$$\sigma_g : A \longrightarrow A\,, \quad a \mapsto \sigma_g(a) := g.a \qquad (\forall\ a \in A)$$

— per ogni $g \in G$ — è un *automorfismo* dell'anello A. Inoltre, sia

$$U(A) := \{\, a \in A \,|\, \exists\, a^{-1} \in A \,\}$$

il gruppo (moltiplicativo) degli elementi *invertibili* di A, e sia

$$N(A) := \{\, a \in A \,|\, \exists\, n \in A : a^n = 0 \,\}$$

l'insieme degli elementi *nilpotenti* di A.

Dimostrare che:

(a) se $G \times A \longrightarrow A$ è un'azione *per automorfismi* del gruppo G (qualsiasi) sull'anello A, allora $U(A)$ e $N(A)$ sono G–sottospazi di A;

(b) la funzione $U(A) \times A \longrightarrow A$, $(\gamma, a) \mapsto \gamma.a := \gamma\, a\, \gamma^{-1}$, definisce un'azione su *per automorfismi* del gruppo $U(A)$ sull'anello A, detta azione per *coniugazione*;

(c) ogni ideale (bilatero) di A è un $U(A)$–sottospazio di A rispetto all'azione per coniugazione di $U(A)$ su A introdotta in *(b)*.

"ALGEBRA 2"

SCRITTO del 23 SETTEMBRE 2025

---

1. Sia G un gruppo di ordine 175.

(a) Dimostrare che G è abeliano.

(b) Tenendo conto che G è abeliano determinare la sua struttura ciclica secondo il 1° e il 2° Teorema di Classificazione dei gruppi abeliani finiti.

Soluzione:

(a) Sia $n_p := \#(\text{sottogruppi } p\text{-Sylow di } G)$, per ogni primo p che divide $|G|$.

ORA $|G| = 175 = 5^2 \cdot 7 \Rightarrow p = \begin{matrix} 5 \\ 7 \end{matrix}$

$n_5 \in (1+5\mathbb{N}) \cap \text{Div}(7) = \{1+5\mathbb{N}\} \cap \{1,7\} = \{1\} \Rightarrow$

$\Rightarrow n_5 = 1 \Rightarrow \exists!$ 5 Sylow $K_5 \trianglelefteq_k G \Rightarrow$

$\Rightarrow K_5 \trianglelefteq G$ (è normale in G)

e $|K_5| = 5^2 = 25$

e analogamente

$$\nu_7 \in (1+7\mathbb{N}) \cap \mathrm{Div}(5^2) = (1+7\mathbb{N}) \cap \{1, 5, 25\} =$$

$$= \{1\} \Rightarrow \nu_7 = 1 \Rightarrow \exists!\ 7\text{-Sylow } K_7 \trianglelefteq_k G \Rightarrow$$

$$\Rightarrow K_7 \trianglelefteq G \quad (\text{è normale in } G)$$

$$\text{e} \quad |K_7| = 7$$

POI

$$K_5 \cap K_7 \leq G \Rightarrow \text{per Teor. LAGRANGE}$$

si ha $|K_5 \cap K_7| \mid_N \begin{cases} |K_5| = 25 \\ |K_7| = 7 \end{cases} \longmapsto$

$$\Rightarrow |K_5 \cap K_7| = 1, \Rightarrow K_5 \cap K_7 = \{1_G\}$$

INOLTRE, $\exists$ una funzione

$$\mu' := \mu_G|_{K_5 \times K_7} : K_5 \times K_7 \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

che è iniettiva: infatti

$$\mu'(x_1, y_1) = \mu'(x_2, y_2) \Rightarrow x_1 y_1 = x_2 y_2 \Rightarrow$$

$$\Rightarrow x_2^{-1} \cdot x_1 = y_2 y_1^{-1} \quad \text{con } x_1, x_2 \in K_5,\ y_1, y_2 \in K_7$$

$$\uparrow \qquad \uparrow$$

$$K_5 \qquad K_7 \longrightarrow x_2^{-1} x_1 = y_2 y_1^{-1} \in K_5 \cap K_7 = \{1_G$$

QUINDI

$$x_2^{-1} x_1 = y_2 y_1^{-1} = 1_G \Rightarrow$$

$\Rightarrow \quad x_1 = x_2 \ \& \ y_1 = y_2 \Rightarrow$

$\Rightarrow \quad (x_1, y_1) = (x_2, y_2) \Rightarrow$

$\Rightarrow$ μ' è iniettiva, q.e.d.

ALLORA, poiché μ' è iniettiva si ha

$$|\mathrm{Im}(\mu')| = |K_5 \times K_7| = |K_5| \cdot |K_7| = 25 \cdot 7 =$$

$$= 175 = |G|$$

cioè $|\mathrm{Im}(\mu')| = |G|$ e così

μ' è suriettiva. D'altra parte è

$$\mathrm{Im}(\mu') = K_5 \cdot K_7 \quad (\leq G, \text{ a priori})$$

quindi è $K_5 \cdot K_7 = G$

Insieme a $K_5 \trianglelefteq G$, $K_7 \trianglelefteq G$ e

$K_5 \cap K_7 = \{1_G\}$, questo ci dice

che G è prodotto diretto (interno) dei

suoi sottogruppi normali K_5 e K_7,

cioè $K_5 \times K_7 \cong G$ (come gruppi)

con μ' come isomorfismo (uno dei tanti)

ADESSO $K_7 \cong \mathbb{Z}_7$ ← abeliano

$|K_5| = 5^2$ con 5 primo ⇒

⇒ K_5 è abeliano (per un risultato generale)

QUINDI

K_7 abeliano
K_5 abeliano
$\Big\}$ ⇒ $K_5 \times K_7$ abeliano

⇓

& $K_5 \times K_7 \cong G$ ⇒ G è abeliano (on)

(b) Il sottogruppo K_5 ha ordine $|K_5| = 25 = 5^2$ ed è abeliano,

QUINDI è del tipo

$K_5 \cong \mathbb{Z}_{5^2=25}$ oppure $K_5 \cong \mathbb{Z}_5^{\times 2} = \mathbb{Z}_5 \times \mathbb{Z}_5$

Ne segue che $G \cong K_5 \times K_7$ implica

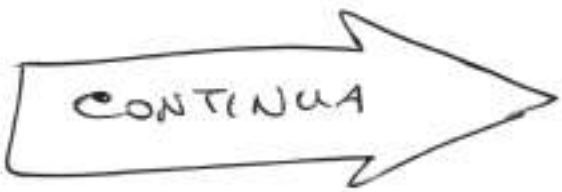
$G \cong \mathbb{Z}_{25} \times \mathbb{Z}_7$ o $G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$

struttura ciclica secondo il 2° Teorema di classificazione

e anche

$$G \cong \mathbb{Z}_{25\cdot 7 = 175} \quad \not\cong \quad G \cong \mathbb{Z}_{5\cdot 7} \times \mathbb{Z}_5$$
$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$
$$G \cong \mathbb{Z}_{175} \quad \not\cong \quad G \cong \mathbb{Z}_{35} \times \mathbb{Z}_5$$

struttura ciclica secondo il 1° Teorema di Classificazione (OK)



2 Sia $\mathbb{F}_5$ il campo con 5 elementi, e sia $\mathbb{F}_5(\alpha)$ il campo estensione di $\mathbb{F}_5$ generato da un elemento α tale che

$$\alpha^4 + 4\alpha - 1 = 0 \quad \text{in } \mathbb{F}_5(\alpha).$$

(a) Dimostrare che $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 4$.

(b) Descrivere un elemento non banale di $Gal(\mathbb{F}_5(\alpha)/\mathbb{F}_5)$, precisandone l'effetto sugli elementi di $\mathbb{F}_5$ e sul generatore α di $\mathbb{F}_5(\alpha)$.

(c) Determinare il numero totale di campi $\mathbb{F}$ intermedi, cioè tali che

$$\mathbb{F}_5 \subseteq \mathbb{F} \subseteq \mathbb{F}_5(\alpha).$$

Soluzione:

(a) L'ipotesi $\alpha^4 + 4\cdot\alpha - 1 = 0$ in $\mathbb{F}_5(\alpha)$ ci dice che α è radice del polinomio

$$p(x) = x^4 + 4x - 1 = x^4 - x - 1 \in \mathbb{F}_5[x]$$

QUINDI α è algebrico su $\mathbb{F}_5$, con grado $\partial_\alpha \leq \partial(p(x)) = 4$, e perciò

avremo $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = \partial_\alpha \leq \partial(p(x)) = 4$

ALLORA sarà

$[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 4 \iff p(x)$ è irriducibile

ORA, si ha

$p(x)$ è irriducibile $\iff$ $p(x)$ non ha fattori di grado 1 o 2

MA: $p(x)$ ha fattori di grado 1 $\iff$ $\exists\, \beta \in \mathbb{F}_5 \cong \mathbb{Z}_5$: $p(\beta) = 0$

e i calcoli danno ($\mathbb{F}_5 \cong \mathbb{Z}_5$)

$\beta = 0 \Rightarrow p(0) = -1 \neq 0$

$\beta = 1 \Rightarrow p(1) = -1 \neq 0$

$\beta = 2 \Rightarrow p(2) = 16 - 2 - 1 = 1 - 2 - 1 = -2 \neq 0$

$\beta = 3 \Rightarrow p(3) = 81 - 3 - 1 = 1 - 3 - 1 = -3 \neq 0$

$\beta = 4 = p(4) = 4^4 - 4 - 1 = (-1)^4 - (-1) - 1 = 1 \neq 0$

quindi $\nexists\, \beta \in \mathbb{F}_5 : p(\beta) = 0$

$p(x)$ ha fattori di grado 2 $\iff$ $\exists\, a, b, c, d, e, f \in \mathbb{F}_5$:

$a \neq 0$, $d \neq 0$,

$$(ax^2+bx+c)\cdot(dx^2+ex+f) = p(x)$$

Inoltre, poiché dev'essere $a \cdot d = 1$,

possiamo sempre "normalizzare" a e d

in modo che siano $a = 1 = d$,

quindi la condizione precedente diventa

$p(x)$ ha fattori di grado 2 $\iff$ $\exists\, b, c, e, f \in \mathbb{F}_5$:

$$(x^2+bx+c)(x^2+ex+f) = p(x)$$

A questo punto i calcoli siamo

$$(x^2+bx+c)\cdot(x^2+ex+f) = p(x) = x^4 - x - 1 \iff$$

$$\iff x^4 + (e+b)\cdot x^3 + (f+be+c)\cdot x^2 + (ce+bf)\cdot x + c\cdot f = x^4 - x - 1 \iff$$

$$\iff \begin{cases} 1 = 1 \\ e+b = 0 \\ f+be+c = 0 \\ ce+bf = -1 \\ c\cdot f = -1 \end{cases} \iff \begin{cases} e+b = 0 \\ -c^{-1}+be+c = 0 \\ c\cdot e - bc^{-1} = -1 \\ f = -c^{-1} \end{cases} \iff$$

$$\Leftrightarrow \begin{cases} e = -b \\ -c^{-1} - b^2 + c = 0 \\ -bc - be^{-1} = -1 \\ f = -c^{-1} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} e = -b \\ b^2 = c - c^{-1} \\ b \cdot (c + c^{-1}) = 1 \\ f = -c^{-1} \end{cases} \Leftrightarrow \begin{cases} e = -b \\ (c + c^{-1})^{-2} = c - c^{-1} \\ b = (c + c^{-1})^{-1} \\ f = -c^{-1} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} e = -b \\ e^3 + e^{+1} - e^{-1} - e^{-3} = 1 \\ b = (e + e^{-1})^{-1} \\ f = -e^{-1} \end{cases} \Rightarrow$$

$\nexists$ soluzioni in $\mathbb{F}_5$ di

$$x^3 + x - x^{-1} - x^3 = 1$$

quindi $p(x)$ non ha fattori di grado 2

CONCLUDENDO, $p(x)$ è irriducibile,

QUINDI $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = \partial(p(x)) = 4$

(e $p(x)$ è il polinomio minimo di α su $\mathbb{F}_5$)

(b) Dal punto (a) sappiamo che $\mathbb{F}_5(\alpha)$ è estensione di $\mathbb{F}_5$ di grado 4, dunque è un

campo finito con $|\mathbb{F}_5|^{[\mathbb{F}_5(\alpha):\mathbb{F}_5]} = 5^4$ elementi. In tal caso, la teoria generale ci dice che il gruppo di Galois $Gal(\mathbb{F}_5(\alpha)/\mathbb{F}_5)$ è ciclico di ordine il grado, cioè , dunque

$$Gal(\mathbb{F}_5(\alpha)/\mathbb{F}_5) \cong \mathbb{Z}_4$$

ed è generato dall'automorfismo di Frobenius $\phi : \mathbb{F}_5(\alpha) \longrightarrow \mathbb{F}_5(\alpha)$

$$x \longmapsto x^5 = x^p$$

dove $p := 5$ è la caratteristica dei campi in esame. In particolare è $\phi \neq id_{\mathbb{F}_5(\alpha)}$ (con ϕ è non banale)

con $\phi(x) := x^5 = x \quad \forall\, x \in \mathbb{F}_5$

e $\phi(\alpha) := \alpha^5 = \alpha^1 \cdot \alpha^4 = \alpha^1 \cdot (\alpha+1) = \alpha^2 + \alpha$

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

(c) Per il teorema di Corrispondenza di Galois, i campi intermedi sono in corrispondenza biunivoca con i sottogruppi del gruppo di Galois

$$G := Gal(\mathbb{F}_5(\alpha)/\mathbb{F}_5) \cong \mathbb{Z}_4$$

Tale gruppo G è ciclico di ordine 4, quindi i suoi sottogruppi sono in biiezione con i divisori dell'ordine $|G| = |\mathbb{Z}_4| = 4 = 2^2$, che sono $\{1, 2, 2^2 = 4\}$, cioè sono esattamente 3.

PERCIÒ il numero totale di campi $\mathbb{F}$ intermedi è 3. (di cui due sono i casi banali, cioè $\mathbb{F}_5$ e $\mathbb{F}_5(\alpha)$ stessi).

CONTINUA

3 Sia $f(x) := x^5 - 14x^4 - 15x^3 + 30 \cdot x^2 + 24x - 6$

in $A[x]$, con $A \in \{\mathbb{Z}_4, \mathbb{Z}_5\}$.

Th: (b) $\exists$ radici multiple di $f(x)$

nell'anello A $(\in \{\mathbb{Z}_4, \mathbb{Z}_5\})$?

(a) fattorizzare $f(x)$ in irriducibili

in $\mathbb{Z}_4[x]$ e in $\mathbb{Z}_5[x]$.

Sol.: Con Ruffini si trova che

$f(-1) = 0$, cioè $\alpha = -1$ è radice di $f(x)$

(in $\mathbb{Z}_4$ e in $\mathbb{Z}_5$), quindi

$$f(x) = (x+1) \cdot (x^4 - 15 \cdot x^3 + 30 \cdot x - 6) =$$

$$= (x+1) \cdot q(x)$$

in $\mathbb{Z}_4[x]$ e in $\mathbb{Z}_5[x]$.

$\longrightarrow$ fattorizziamo anche $q(x)$.

In $\mathbb{Z}[x]$: il Criterio di Eisenstein

per $p = 3$ sta che

$q(x)$ è irriducibile in $\mathbb{Z}[x]$

QUINDI: (a) la fattorizzazione in irriducibili di $f(x)$ in $\mathbb{Z}[x]$ è

$$f(x) = (x+1) \cdot (x^4 - 15x^3 + 30 \cdot x - 6)$$

ora (a) per $A = \mathbb{Z}$ è fatto.

In $\mathbb{Z}_5[x]$: riscriviamo $q(x)$ in $\mathbb{Z}_5[x]$

$$q(x) := x^4 - 15 \cdot x^3 + 30x - 6 =$$

$$= x^4 - 1 = (x^2-1)(x^2+1) =$$

$$= (x+1)\cdot(x-1)\cdot(x^2+1) = (x+1)(x-1)(x+2)(x-2)$$

QUINDI: (a) la fattorizzazione in irriducibili di $f(x)$ in $\mathbb{Z}_5[x]$ è

$$(x+1)^2 \cdot (x-1) \cdot (x+2) \cdot (x-2)$$

(b) $f(x)$ ha 1! radice multipla $\alpha = -1$, con molteplicità 2.

ORA, se $\beta \in \mathbb{Z}_5$ fosse una radice multipla di $f(x)$, sarà certamente

$\beta \neq -1$ (perché (-1) non è radice di $q(x)$, in quanto $q(x)$ è irriducibile con grado maggiore di 1), QUINDI

β dev'essere radice multipla di $q(x)$

MA $q(x) \in \mathbb{Z}_5[x] \leq \mathbb{Q}[x]$
$\mathrm{char}(\mathbb{Q}) = 0$
$q(x)$ è irriducibile
$\Rightarrow$ (*) $q(x)$ è separabile

CIOÈ

$q(x)$ non ha radici multiple

COSÌ concludiamo che

$\nexists$ radici multiple di $f(x)$ in $\mathbb{Z}_5$

N.B.: se non si ricorda (o non si vuole applicare) il risultato (*), la stessa conclusione si raggiunge calcolando la derivata $q'(x)$ e poi $d(x) := \mathrm{MCD}(q(x), q'(x))$ trovando che $d(x) \sim 1$ e quindi

$q(x)$ non ha radici multiple.

1 Sia G gruppo, $|G| = 28 = 2^2 \cdot 7$.
Determinare la struttura di G.

Sol.: $|G| = 28 = 2^2 \cdot 7 \Rightarrow$

$\Rightarrow \exists$ p-Sylow Σ_p per $p = \begin{cases} 2 \\ 7 \end{cases}$

$\nu_p := |\{p\text{-Sylow}\}|$

$$\nu_p \in \begin{cases} (1+7\mathbb{N}) \cap \{1,2,4\} = \{1\}, & p=7 \\ (1+2\mathbb{N}) \cap \{1,7\} = \{1,7\}, & p=2 \end{cases}$$

cioè

$$\nu_7 = 1 \Rightarrow \exists\,! \; N_7 = K_7 = \Sigma_7 \trianglelefteq_n G$$

& $\nu_2 \in \{1,7\}$

1° CASO: $\boxed{\nu_2 = 1} \Rightarrow \exists\,! \; N_2 = K_2 = \Sigma_2 \trianglelefteq_n G \Rightarrow$

$\Rightarrow \exists\, K_7, K_2 \trianglelefteq G : \quad K_2 \cap K_7 = \{1_G\}$

$K_7 \leq K_2 \cdot K_4 \Rightarrow 7 = |K_7| \delta_N |K_2 \cdot K_4| \delta_N |G| = 4 \cdot 7$

$K_2 \cdot K_7 \leq G$ s.c.

$K_2 \leq K_2 \cdot K_7 \Rightarrow 4 = |K_2| \delta_N |K_2 \cdot K_7| \delta_N |G| = 4 \cdot 7$

QUINDI $K_2 \cdot K_7 \leq G \Rightarrow |K_2 \cdot K_7| \, \delta_N \, |G|$ (= 4·7)

con $7 \; \delta_N \; |K_2 \cdot K_7|$ & $4 \; \delta_N \; |K_2 \cdot K_7|$ $\Rightarrow$ $|K_2 \cdot K_7| = 4 \cdot 7 = |G|$

$$K_2 \cdot K_2 = K_2 \cdot K_7 = G$$

così è $G \cong K_2 \times K_7$ = prodotto diretto di K_2 e K_7

INOLTRE, è $|K_7| = 7 \Rightarrow K_7 \cong \mathbb{Z}_7$

& $|K_2| = 2^2 \Rightarrow K_2$ abeliano, $|K_2| = 2^2$ (2 primo)

$K_2 \cong \mathbb{Z}_4$

o $K_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$

PERCIÒ

$n_2 = 1 \Rightarrow G \cong \begin{cases} \mathbb{Z}_4 \times \mathbb{Z}_7 \cong \mathbb{Z}_{28} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_{14} \times \mathbb{Z}_2 \end{cases}$

per il Teorema Cinese del Resto

2° CASO: $\nu_2 = 7 \Rightarrow \exists$ 7 distinti 2-Sylow, con 4 elementi ciascuno.

Sia Σ_2 uno di essi. Allora

$\Sigma_2 \leq G$, $\quad K_7 \trianglelefteq G \Rightarrow \Sigma_2 \cdot K_7 = K_7 \cdot \Sigma_2 \leq G$

$|\Sigma_2 \cap K_7| = 1 \Rightarrow \Sigma_2 \cap K_7 = \{1_G\}$

$|\Sigma_2 \cdot K_7| = 4 \cdot 7 = |G| \Rightarrow \Sigma_2 \cdot K_7 = G = K_7 \cdot \Sigma_2$

perché

$4 = |\Sigma_2| \; \delta_N \; |\Sigma_2 \cdot K_7|$

&

$7 = |K_7| \; \delta_N |\Sigma_2 \cdot K_7|$

QUINDI è

$G \cong K_7 \rtimes_\Phi \Sigma_2$

per un certo

$\Phi : \Sigma_2 \longrightarrow Aut_G(K_7)$

POSSIBILI Φ?

CASO I: $\Sigma_2 \cong \mathbb{Z}_4$

$\Phi : \mathbb{Z}_4 \cong \Sigma_2 \longrightarrow Aut_G(\mathbb{Z}_7) \cong (U(\mathbb{Z}_7); \cdot) = (\mathbb{Z}_6; +)$

$[1]_4 \longmapsto \Phi([1]_4) =: [z]_6$

$\Rightarrow \exists!\ \Phi$ $\forall$ scelta di $\Phi([1]_4) = [z]_6 \in \mathbb{Z}_6$ $\quad = [z]_7 \in U(\mathbb{Z}_7)$

IN PARTICOLARE

$$\Phi = \left([2]_4 \cong 6 \longmapsto id_{\mathbb{Z}_7} \cong [0]_6 \right)$$

$$\Phi([1]_4) = [0]_6$$

gli altri danno prodotti semidiretti

$$K_7 \underset{\Phi}{\rtimes} \Sigma_2 \cong \mathbb{Z}_7 \underset{\Phi}{\rtimes} \mathbb{Z}_4$$

che <u>non</u> sono diretti e sono tutti a due a due isomorfi tra loro.

<u>MA</u> dev'essere (per l'ordine)

$$\omega(\Phi([1]_4)) = \omega([2]_4) = 4$$

con $\omega(\Phi([1]_4)) \; \delta_N \; |Aut_g(\mathbb{Z}_7)| = |\mathbb{Z}_6| = 6$

<u>QUINDI</u> $\omega([1]_4) = 2$

$\mathbb{Z}_6 \cong U(\mathbb{Z}_7)$

$\Phi([1]_4) \in \{[3]_6\} \Rightarrow \Phi([1]_4) = [3]_6 \cong [6]_2$

$Aut_g(\mathbb{Z}_7)$

<u>così</u> è necessariamente

$$\Phi([1]_4) = \mu([6]_7) = \mu([-1]_7) \cong [3]_6 \in (\mathbb{Z}_6, +)$$

$$(\bar{a} \longmapsto \bar{6} \cdot \bar{a} = -\bar{a})$$

CASO

$\Phi_- := \Phi : \mathbb{Z}_4 \longmapsto Aut_g(\mathbb{Z}_2)$

$[0]_4 \longmapsto id_{\mathbb{Z}_2}$

$[1]_4 \longmapsto ([a]_2 \mapsto -[a]_2)$

$[z]_4 = z \cdot [1]_4 \longmapsto ([a]_2 \mapsto (-1)^z \cdot [a]_2)$

CONCLUSIONE: se $\Sigma_2 \cong \mathbb{Z}_4$, $\exists$ due casi

① $G \cong K_2 \underset{\Phi_+}{\rtimes} \Sigma_2 = \mathbb{Z}_{4_2} \underset{\Phi_+}{\rtimes} \mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_{28}$

con $\Phi_+ : \mathbb{Z}_4 \longrightarrow Aut_g(\mathbb{Z}_2)$

$[z]_4 \longmapsto id_{\mathbb{Z}_2}$

② $G \cong K_2 \underset{\Phi_-}{\rtimes} \Sigma_2 \cong \mathbb{Z}_2 \underset{\Phi_-}{\rtimes} \mathbb{Z}_4$

con $\Phi_- : \mathbb{Z}_4 \longrightarrow Aut_g(\mathbb{Z}_2)$

$[z]_4 \longmapsto ([a]_2 \longmapsto (-1)^z \cdot [a]_2)$

CASO II: $\Sigma_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$\mathbb{Z}_2^{\times 2}$ è generato da $a_1 := ([1]_2, [0]_2)$, $a_2 := ([0]_2, [1]_2)$ entrambi di ordine 2. Allora

$\Phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow Aut_g(\mathbb{Z}_7)$

è data dalla scelta (libera) di

$\Phi(a_1)$ e $\Phi(a_2)$, che devono

avere ordine 1 o 2.

ORA, in $Aut_g(\mathbb{Z}_7) \cong U(\mathbb{Z}_7)$

$\exists!$ elemento σ di ordine 2,

dato da $\sigma : ([c]_7 \longmapsto -[c]_7)$

ALLORA le possibilità sono

(I) $\Phi(a_1) = id_{\mathbb{Z}_7}, \Phi(a_2) = id_{\mathbb{Z}_7} \Rightarrow$

$\Rightarrow \Phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow Aut_g(\mathbb{Z}_7), (a_1, a_2) \longmapsto id_{\mathbb{Z}_7}$

(II) $\Phi(a_1) = \sigma, \Phi(a_2) = id_{\mathbb{Z}_7} \Rightarrow$

$\Rightarrow \Phi([1]_2, [1]_2) = \sigma, \quad \Phi([0]_2, [0]_2) = id_{\mathbb{Z}_7}$

(III) $\Phi(a_1) = id_{\mathbb{Z}_7}, \Phi(a_2) = \sigma, \Rightarrow$

$\Rightarrow \Phi([1]_2, [1]_2) = \sigma, \Phi([0]_2, [0]_2) = id_{\mathbb{Z}_7}$

(IV) $\Phi(a_1) = \sigma, \quad \Phi(a_2) = \sigma, \Rightarrow$

$\Rightarrow \Phi([1]_2, [1]_2) = id_{\mathbb{Z}_2}, \Phi([0]_2, [0]_2) = id$

Il caso (I) dà

$$G \cong K_4 \underset{\Phi}{\rtimes} \Sigma_2 \cong K_4 \times \Sigma_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$\| 2$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2$$

mentre i casi (II), (III) e (IV)

danno tre prodotti semidiretti, non diretti,

$$G \cong K_4 \underset{\Phi}{\rtimes} \Sigma_2 \cong \mathbb{Z}_4 \underset{\Phi}{\rtimes} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

che sono a due a due isomorfi tra loro. □

CONTINUA

5 Sia G un gruppo e A un anello unitario, con

$$U(A) := \{ a \in A \mid \exists a^{-1} \in A \},$$

$$N(A) := \{ a \in A \mid \exists n \in \mathbb{N} : a^n = 0 \}.$$

(a) Se $G \times A \longrightarrow A$ è un'azione di G su A per automorfismi, dimostrare che $U(A)$ e $N(A)$ sono G-sottospazi di A.

(b) Dimostrare che $U(A) \times A \longrightarrow A$, $(g, a) \longmapsto g.a := g a g^{-1}$ definisce un'azione per automorfismi di $U(A)$ su A.

(c) Dimostrare che ogni ideale (bilatero) di A è un $U(A)$-sottospazio di A rispetto alla $U(A)$-azione in (b).

Soluzione:

Caso di $U(A)$: $\forall a \in U(A)$, $\exists a^{-1} \in A$:

$a \cdot a^{-1} = 1 = a^{-1} \cdot a$, e allora è anche

$(g.a) \cdot (g.a^{-1}) = g.(a a^{-1}) = g.1 = 1$

perché l'azione è per automorfismi, e questo implica (anche) che $g.1 = 1$, $(\forall g \in G)$

in quanto $\forall a \in A$ si ha $(\forall g \in G)$

$$(g.1)\cdot a = (g.1)\cdot(g.(g^{-1}.a)) =$$

$$= g.(1\cdot(g^{-1}.a)) = g.(g^{-1}.a) = a$$

e analogamente è

$$a\cdot(g.1) = a \qquad \forall a \in A \quad (\forall g \in G)$$

quindi $g.1$ ha le proprietà di un "elemento unità" dell'anello A, che sappiamo essere <u>unico</u> (quando esiste), e quindi è $g.1 = 1$, $\forall g \in G$, q.e.d.

Dunque abbiamo $(\forall \alpha \in U(A),\ \forall g \in G)$

$$(g.\alpha)\cdot(g.\alpha^{-1}) = 1$$

e analogamente è anche

$$(g.\alpha^{-1})\cdot(g.\alpha) = 1$$

dunque $g.\alpha^{-1}$ ha le proprietà tipiche dell'inverso di $g.\alpha$, quindi

$$\exists\ (g.\alpha)^{-1} = g.\alpha^{-1} \in A$$

così è $g.\alpha \in U(A)$, q.e.d.

Caso di $N(A)$: $\forall\ a \in N(A),\ \forall\ g \in G,$

$\exists\ n \in \mathbb{N} : a^n = 0$, e allora è

$(g.a)^n = (g.a\ \ = g.0 = 0$

perché l'azione è per automorfismi, e questo implica (anche) che $g.0 = 0$ $(\forall g \in G)$

(che si dimostra come $g.1 = 1$)

dunque $(g.a)^n = 0$ e così è $g.a \in N(A)$, q.e.d.

(b) Data $U(A) \times A \xrightarrow{\sigma} A$ $((\gamma, a) \mapsto \gamma.a := \gamma a \gamma^{-1})$, proviamo che è un'azione. Si ha

(I) $1_A.a = 1_A \cdot a \cdot 1_A^{-1} = a$, $\forall a \in A$

(II) $\gamma_1.(\gamma_2.a) = \gamma_1(\gamma_2 a \gamma_2^{-1})\gamma_1^{-1} =$

$= (\gamma_1\gamma_2)a(\gamma_2^{-1}\gamma_1^{-1}) = (\gamma_1\gamma_2)a(\gamma_1\gamma_2)^{-1} = (\gamma_1\gamma_2).a$

$\forall\ a \in A,\ \forall\ \gamma_1, \gamma_2 \in U(A)$

e allora (I)+(II) $\Leftrightarrow$ σ è un'azione (del gruppo $U(A)$ sull'insieme A).

Proviamo ora che la suddetta azione σ è per automorfismi: $\forall \gamma \in U(A)$, $\forall a_1, a_2 \in A$

$$\sigma_\gamma(a_1+a_2) := \gamma(a_1+a_2)\gamma^{-1} =$$

$$= \gamma a_1 \gamma^{-1} + \gamma a_2 \gamma^{-1} = \sigma_\gamma(a_1) + \sigma_\gamma(a_2)$$

&

$$\sigma_\gamma(a_1 a_2) := \gamma a_1 a_2 \gamma^{-1} = \gamma a_1 \gamma^{-1} \cdot \gamma a_2 \gamma^{-1} =$$

$$= \sigma_\gamma(a_1) \cdot \sigma_\gamma(a_2)$$

quindi $\sigma_\gamma : A \to A$ $(a \mapsto \sigma_\gamma(a) := \gamma a \gamma^{-1})$

è un <u>morfismo</u> dell'anello A, $\forall \gamma \in U(A)$

In aggiunta, ogni morfismo σ_γ $(\gamma \in U(A))$ è anche invertibile, con inverso $\sigma_{\gamma^{-1}}$

(segue dal fatto che σ è un'azione - di un gruppo su un insieme - in generale)

PERCIÒ σ_γ è automorfismo dell'anello A $\quad \forall \gamma \in U(A)$

(c) Sia $I \trianglelefteq A$ un ideale bilatero di A

In particolare è

$$\alpha' \cdot i \in I, \quad i \cdot \alpha'' \in I, \quad \forall i \in I, \forall \alpha', \alpha'' \in A$$

ALLORA $\forall i \in I$, $\forall \gamma \in U(A)$, si ha che

$$r \cdot i := r i r^{-1} = \begin{cases} (ri)r^{-1} = i' \cdot r^{-1} \in I \\ r \cdot (ir^{-1}) = r \cdot i'' \in I \end{cases}$$

(con $i' := ri \in I$, $i'' := ir^{-1} \in I$)

così $r \cdot i \in I$ $\quad (\forall\, i \in I,\ \forall\, r \in U(A))$

CIOÈ I è un $U(A)$-sottoparte di A, q.e.d. □