ALGEBRA 1 — 25/09/2024

$(G, \cdot)$
G è ciclico se $\exists\, g \in G$ t.c. $G = \langle g \rangle := \{ g^k \mid k \in \mathbb{Z} \}$

$\boxed{\text{TEO}}$

$$G \text{ ciclico} \Rightarrow G \cong \begin{cases} \mathbb{Z} & |G| = \infty \\ \mathbb{Z}/n\mathbb{Z} & |G| = n \end{cases}$$

dim. (da rivedere)
$\mathbb{Z} \to G = \langle g \rangle$
$1 \mapsto g$ → assegnamento che può essere esteso a isomorfismo in modo unico
$k \mapsto g^k \quad \forall k \ldots$

$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non è ciclico (per il teo. cinese del resto)

$= \{ (0,0), (1,0), (0,1), (1,1) \} = \langle (1,0), (0,1) \rangle =$

$= \{ a(1,0) + b(0,1) \mid a, b \in \mathbb{Z} \}$

$S \subseteq G \qquad G = \langle S \rangle$ se $G = \{ s_1 \ldots s_n \mid n \in \mathbb{N},\ s_i \in S \cup S^{-1} \}$
↳ si dimostra che è un gruppo

Esempio: $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$

Automorfismi di G

G gruppo $\quad \mathrm{Aut}(G) = \{ f : G \to G \mid \text{omo bigettivi} \}$

$(\mathrm{Aut}(G), \circ)$ è un gruppo

Esempi:
- $\mathrm{Aut}(\mathbb{Z}) = \{ \pm \mathrm{id} \}$
- $\mathrm{Aut}\ \mathbb{Z}/n\mathbb{Z} \cong \left(\mathbb{Z}/n\mathbb{Z} \right)^*$ $\qquad \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\ \bar{1} \mapsto \bar{a}$ è bigettivo $\Leftrightarrow$ surg. $\Leftrightarrow$ ord $\bar{a} = n \Leftrightarrow a \in \left(\mathbb{Z}/n\mathbb{Z} \right)^*$
- $\mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \right) \cong S_3$
- $\mathrm{Aut}(S_3) \cong S_3$
- $\mathrm{Aut}\big(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \ldots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ volte}} \big) = GL_n(\mathbb{F}_p)$

in questo caso la struttura di spazio vett. è analoga a quella di gruppo → $\bar{a} \in \mathbb{F}_p \quad \bar{a} \cdot v = \underbrace{v + \ldots + v}_{a \text{ volte}}$ $\quad a > 0 \qquad V = \left(\mathbb{Z}/p\mathbb{Z} \right)^n$

$e_1, \ldots, e_n$ base canonica

$e_1 \to v_1 \neq 0 \qquad p^n - 1$ scelte $\qquad$ la retta di v_1 ha p punti

$e_2 \to v_2 \in V \setminus \langle v_1 \rangle \qquad p^n - p$ scelte

$e_3 \to v_3 \in V \setminus \langle v_1, v_2 \rangle$ $\quad p^n - p^2$ scelte

$$|\mathrm{Aut}(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_{n\text{-volte}})| = (p^n-1)(p^n-p) \cdots (p^n - p^{n-1})$$

↓ uguale al numero di matrici non singolari $n \times n$ a coeff. in $\mathbb{F}_p$

$\Rightarrow |\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6 = (2^2-1)(2^2-2) = 3 \cdot 2$

$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \hookrightarrow S\underbrace{\{(1,0), (0,1), (1,1)\}}_{A} \cong S_3$

$\varphi \to \varphi|_A$

permutazioni di questi elementi

Automorfismi interni

G gruppo $\quad \varphi_g : G \to G$ (CONIUGIO)

$x \mapsto gxg^{-1}$ (coniugato di x)

Proposizione:

1) $\varphi_g \in \mathrm{Aut}(G)$

2) $\{\varphi_g \mid g \in G\} := \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$

automorfismi interni (insieme di tutti i coniugi)

DIM.

1) $\varphi_g : G \to G$

$x \mapsto gxg^{-1}$

- $\varphi_g(xy) = \varphi_g(x)\varphi_g(y) \quad \forall x,y \in G \quad \to$ facile verifica

$gxyg^{-1} = gxeyg = gxg^{-1}gyg = \varphi_g(x)\varphi_g(y)$

- φ_g iniettiva

$\ker \varphi_g = \{x \in G \mid \varphi_g(x) = gxg^{-1} = e\}$

↓

$x = g^{-1}g = e \to$ nucleo banale

- φ_g suriettiva

$\forall y \in G \ \exists x \in G \mid \varphi_g(x) = y$

$gxg^{-1} = y \qquad x = g^{-1}yg$

2) $\mathrm{Inn}(G) < \mathrm{Aut}(G)$

- $\varphi_e = id$
- $(\varphi_g)^{-1} = \varphi_{g^{-1}} \to \varphi_g \circ \varphi_{g^{-1}} = id \quad \varphi_{g^{-1}} \circ \varphi_g = id$

↓

$\varphi_g(\varphi_{g^{-1}}(x)) = \varphi_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$

(e l'altra è analoga)

- $\varphi_g \circ \varphi_h = \varphi_{gh}$

È normale?

$\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$

$\forall f \in \mathrm{Aut}(G) \quad f\,\mathrm{Inn}(G)\,f^{-1} \subseteq \mathrm{Inn}(G)$

$f \circ \varphi_g \circ f^{-1} \in \mathrm{Inn}(G) \quad \forall \varphi_g \in \mathrm{Inn}(G)$

$f \circ \varphi_g \circ f^{-1}(x) =$

$= f(g f^{-1}(x) g^{-1}) = f(g) f(f^{-1}(x)) f(g^{-1}) =$

$= f(g)\, x\, f(g)^{-1} = \varphi_{f(g)}$

$$\begin{cases} H \triangleleft G \quad H < G \\ gH = Hg \quad \forall g \in G \\ gHg^{-1} \subseteq H \end{cases}$$

basta questo contenimento $\forall g \in G$ (per l'inclusione opposta basta considerare il coniugio g^{-1})

G abeliano $\iff \mathrm{Inn}(G) = \{id\}$

Proposizione: $\mathrm{Inn}(G) \cong G/Z(G)$

$Z(G)$: centro

DIM.

$$\phi: G \to \mathrm{Inn}\,G, \quad g \mapsto \varphi_g$$

$\to$ voglio che abbia come Ker il centro e usare il 1° teo. di isomorfismo

ϕ è una mappa ben definita e surgettiva.

<u>ϕ omo</u>: $\phi(gh) = \phi(g) \circ \phi(h)$

$\varphi_{gh} = \varphi_g \circ \varphi_h$ (dim. immediata)

$\mathrm{Ker}\,\phi = \{g \in G \mid \phi(g) = \varphi_g = id\} = \{g \in G \mid gxg^{-1} = x \ \forall x \in G\} = Z(G)$

$gx = xg$

Dal 1° teo. di omomorfismo $\Rightarrow G/Z(G) \cong \mathrm{Inn}(G)$ $\square$

$G/\mathrm{Ker}(\varphi) \cong \mathrm{Imm}(\varphi)$

$H < G$ è normale $\iff$ è invariante per $\mathrm{Inn}(G)$

cioè se $\forall \varphi_g \in \mathrm{Inn}(G) \quad \varphi_g(H) = H$

Def. $H < G$ si dice *caratteristico* se $\forall f \in \mathrm{Aut}(G) \Rightarrow f(H) = H$

Chiaramente caratteristico $\Rightarrow$ normale

H carat. in $G \Rightarrow H \triangleleft G$

non vale il viceversa

<u>esercizio</u>: il centro è sempre caratteristico

$\langle (0,1) \rangle \triangleleft \mathbb{Z}_2 \times \mathbb{Z}_2$ ma non è caratteristico perché:

$f(1,0) = (0\,1)$
$f(0,1) = (1\,0)$ $\Rightarrow f(H) \neq H$

<u>OSSERVAZIONE</u>: non è vero come nel caso lineare che posso mandare un insieme minimale di generatori del gruppo dove voglio. Per esempio $\mathbb{Z} = \langle 2,3 \rangle$ ma questo assegnamento è contraddittorio $2 \xmapsto{\varphi} 4$, $3 \mapsto 5$ $\quad 6 = 3 \cdot 2 \mapsto 3 \cdot \varphi(2) = 12$, $2 \cdot \varphi(3) = 10$ i multipli comuni hanno + di una imm. (Si comportano come un insieme di generatori NON minimale)

$S_3 = \{id, (1\,2), (2,3), (1,3), (1\,2\,3), (1\,3\,2)\} = \langle (1\,2), (2,3), (1,3) \rangle$

$\mathrm{Inn}\,S_3 \triangleleft \mathrm{Aut}(S_3)$

$\mathrm{Inn}\,S_3 \cong S_3/Z(S_3) \quad Z(S_3) = e$

$S_3/Z(S_3) \cong S_3 \to \mathrm{Aut}(S_3)$ ha un sottogruppo isomorfo a S_3

Al più ho 6 automorfismi (permutazioni possibili degli elementi di ordine 2)

$\Rightarrow \mathrm{Aut}(S_3) \cong S_3$ perché ha cardinalità minore o uguale a S_3 e hanno un sottogruppo isomorfo a S_3

30/09/2024 (Parimo)

Def. G si dice GRUPPO CICLICO se $\exists g \in G \mid G = \langle g \rangle$

- Se $\mathrm{ord}(g) \in \mathbb{N} \Rightarrow G = \{e, g, \dots, g^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$

$$g^k \longmapsto \bar{k}$$

- Se $\mathrm{ord}(g) = \infty$

$$G = \{e, g, \dots, g^n, \dots\} \cong \mathbb{Z}$$
$$g^k \longmapsto k$$

$G = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\bar{m} \in \mathbb{Z}/n\mathbb{Z} \qquad \bar{m} = \{m + nk \mid k \in \mathbb{Z}\}$

Qual è $\mathrm{ord}(\bar{m})$? $\quad \mathrm{ord}(\bar{m}) = \min\{k \mid \bar{m}k = \bar{0}\}$

$$\bar{m}k = \bar{0} \Leftrightarrow n \mid km$$

$n = n'(m,n)$
$m = m'(m,n) \qquad (n', m') = 1$

$n \mid km \Leftrightarrow n'\cancel{(m,n)} \mid m'\cancel{(m,n)}k \Leftrightarrow n' \mid k$

Quindi l'ordine di $\bar{m}$ è $n' = \frac{n}{(m,n)}$ $\qquad \mathrm{ord}(\bar{m}) = \frac{n}{(m,n)}$

Quali sono i sottogruppi di G ciclico?

LEMMA Ogni sottogruppo di un gruppo ciclico è ciclico

DIM.

$G = \langle g \rangle > H$

$H = \{e\} \Rightarrow H = \langle e \rangle$

$H \neq \{e\} \Rightarrow \exists k \mid g^k \in H \wedge g^k \neq e$

Sia k_0 il più piccolo intero positivo tale che $g^{k_0} \in H$

(oss: esiste perché $g^k \in H \Rightarrow (g^k)^{-1} \in H \quad (g^k)^{-1} = g^{-k}$)
per cui c'è un k positivo

CLAIM: $H = \langle g^{k_0} \rangle$

Prendiamo $g^a \in H$, voglio mostrare che $k_0 \mid a$

Faccio la divisione euclidea $\quad a = qk_0 + r \qquad 0 \leq r < k_0, \; q \in \mathbb{Z}$

$g^a \in H \quad g^{k_0 \cdot (-q)} \in H \rightsquigarrow g^{a-k_0 q} \in H$

$g^{k_0 \cdot (-q)} = (g^{k_0})^{-q}$, $\quad g^{a-k_0 q} = g^r \Rightarrow r = 0 \Rightarrow k_0 | a$ $\square$

Sottogruppi di $\mathbb{Z}/n\mathbb{Z}$

$G = \mathbb{Z}/n\mathbb{Z} > H = \langle \bar{m} \rangle$

$\text{ord}(\bar{m}) = \frac{n}{(m,n)} \Rightarrow H \cong \mathbb{Z}_{\frac{n}{(m,n)}}$

Tutti i sottogruppi di $\mathbb{Z}_n$ sono isomorfi a $\mathbb{Z}/d\mathbb{Z}$ dove $d | n$

m, p due numeri in $\mathbb{Z}$, quando vale $\langle \bar{m} \rangle = \langle \bar{p} \rangle$?

$\text{ord}(\bar{m}) = \text{ord}(\bar{p}) \Leftrightarrow \frac{n}{(m,n)} = \frac{n}{(p,n)} \Leftrightarrow (m,n) = (p,n)$

↳ voglio dire che è anche una cond. sufficiente

CLAIM:

$\langle \bar{m} \rangle = \langle \overline{(m,n)} \rangle$

⊆ m è multiplo di (m,n)
$\exists h \mid m = h(m,n) \Rightarrow \bar{m} = h\overline{(m,n)}$

② Bezout:
$\exists\, a, b \mid (m,n) = am + bn \Rightarrow \overline{(m,n)} = a\bar{m}$ $\square$

$\Rightarrow$ c'è un unico sottogruppo per ogni divisore

Sottogruppi di $\mathbb{Z}$

$H < \mathbb{Z} \Rightarrow H = \langle n \rangle \quad n \in \mathbb{Z}$

$\langle n \rangle = \langle -n \rangle$

$\langle m \rangle = \langle n \rangle \Leftrightarrow m = \pm n$

$\Leftarrow$ OK!

$\Rightarrow m | n \wedge n | m \Rightarrow m = \pm n$

Esercizio $a, b \in \mathbb{Z}$, chi è $\langle a, b \rangle$?

$\langle (a,b) \rangle = \langle a, b \rangle \qquad \langle 2, 3 \rangle = \langle 1 \rangle$

↳ si tratta di un insieme minimale di generatori che non è di cardinalità minima

Esercizio G ha un insieme minimale finito di generatori $\Rightarrow$ tutti i sottoinsiemi minimali di generatori sono finiti

In questo caso chiamiamo G gruppo finitamente generato.

GRUPPO DIEDRALE

Def. $n \geq 3$. Chiamo D_n il gruppo delle isometrie di $\mathbb{R}^2$ che manda l'n-agono regolare in sé stesso.

(Reminder: le isometrie di $\mathbb{R}^2$ sono tutte mappe affini) (posso dire lineari se fisso l'origine nel centro del poligono)

(Sono rotazioni e riflessioni)

oss. D_n è un gruppo

- id è un'isometria
- la composizione di isom. è una isom.
- l'inversa di una isom. è una isom.

Elementi di D_n

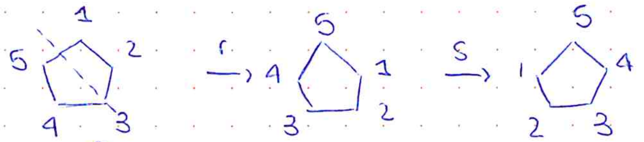
$\{e, r, \dots, r^{n-1}$
$s, sr, sr^2 \dots$
$sr^{n-1}\}$ ↑ r rotazione di $2\pi/n$

$r = \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$

Chi è rs?

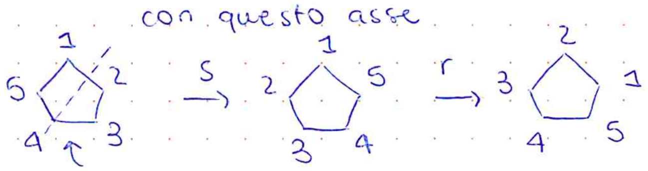
$s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ $\mathrm{Ord}(s) = 2$

sr:



↑ è la riflessione con questo asse

rs:



↑ riflessione

Con gli stessi disegni e con le matrici si osserva che $rs = sr^{-1}$

OSS: • $sr \neq rs \implies D_n$ non è abeliano
• $srs = r^{-1} \iff rs = sr^{-1}$

Ci sono altri elementi oltre a quelli della forma r^k, sr^k?

Prop. Gli elementi di D_n sono $\{e, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$

DIM Abbiamo visto che sono tutti distinti, resta da vedere che non ce ne sono altri

$\sigma \in D_n$ $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ mappa lineare

σ è determinata dai valori su una base di $\mathbb{R}^2$

$\{v_1, v_2\}$ sono una base

↑ v_i unisce il centro all' i-esimo vertice

$\sigma(v_1) = v_i$
$\sigma(v_2) = v_j$ $1 \leq i, j \leq n$

$r^{-(i-1)}\sigma(v_1) = v_1$ $r^{-(i-1)} \cdot \sigma \in D_n$

$\tau(v_1) = v_1$
$\tau(v_2) \in \{v_2, v_n\}$

↑ perchè τ è una isometria e v_2, v_n sono gli unici t.c. $\langle v_1, v_2 \rangle = \langle v_1, v_m \rangle$ ($\neq$ se $m \neq 2, n$)

- Se $\tau(v_2) = v_2 \Rightarrow \tau = id_{\mathbb{R}^2}$

$r^{-(i-1)}\sigma = e \Rightarrow \sigma = r^{i-1}$

- Se $\tau(v_2) = v_n \Rightarrow \tau = s$

$r^{-(i-1)}\sigma = s \Rightarrow \sigma = r^{i-1}s = s(sr^{i-1}s) = sr^{1-i}$

$\Rightarrow \sigma \in \{e, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$

Corollario: $|D_n| = 2n$ ← n riflessioni e n rotazioni (di cui 1 è e)

(Nel caso pari le riflessioni possono non avere punti fissi)

$D_n = \langle r, s\rangle$ D_n non è abeliano $\Rightarrow$ non è ciclico $\Rightarrow$
$\Rightarrow \langle r, s\rangle$ è minimale

OSS $D_n \circlearrowright \{1, \dots, n\}$ (insieme dei vertici) in maniera fedele

"agisce"

$\Rightarrow D_n < S_n$, $D_n = \langle \underbrace{(1, n, n-1, \dots, 2)}_{r}, (2\ n)(3\ n-1)\cdots(\frac{n+1}{2}\ \frac{n-1}{2})\rangle$ se n dispari

$(2\ n)(3\ n-1)\cdots(\frac{n}{2}+1\ \frac{n}{2}-1)\rangle$ se n pari

Centro & centralizzatore
(rivedi def.)

$D_n = \langle r, s\rangle$

$Z(r)$?

Sicuramente $\langle r\rangle \subseteq Z(r)$ $ord(r) = n \Rightarrow |\langle r\rangle| = n$

$\langle r\rangle < Z(r) < D_n$ Lagrange: $n \mid |Z(r)| \mid 2n$

$|\langle r\rangle| = n$ $|D_n| = 2n$

$$|Z(r)| = \begin{cases} n & \Rightarrow Z(r) = \langle r\rangle \\ 2n \Rightarrow Z(r) = D_n \ \lightning \ rs \neq sr \end{cases}$$

$Z(s)$?

Quando vale $sx = xs$ con $x \in D_n$?

- se $x \in R \Rightarrow x = r^k$ $sr^k = r^k s \iff sr^k s = r^k \iff (srs)^k = r^k$

$\iff r^{-k} = r^k \iff r^{2k} = e \iff ord(r) \mid 2k \iff k = 0$ o $k = \frac{n}{2}$ ← ∃ solo se n pari

- se $x \notin R$ $x = sr^k$, $0 \leq k < n$

$sx = xs \iff ssr^k = sr^k s \iff r^{-k} = r^k \iff r^{2k} = e \iff$
$\iff k = 0 \vee k = n/2$

Se n dispari $Z(s) = \{e, s\} \cong \mathbb{Z}_2$

n pari $Z(s) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = \{e, s, r^{n/2}, sr^{n/2}\}$

OSS Se $G = \langle g_1, \dots, g_n \rangle$, allora $Z(G) = \bigcap_{i=1}^{n} Z(g_i)$

$\Rightarrow Z(D_n) = Z(r) \cap Z(s) = \{e, r^{n/2}\}$ se n pari

$r^{n/2} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -id$

01/10/2024
(Del Corso)

Azione di un gruppo su un insieme

G gruppo, X insieme

Def. Un'azione di G su X è un omomorfismo

$\varphi: G \to S(X)$
$g \mapsto \varphi_g$ $\quad \varphi_g \; X \to X$ bigettiva $\quad G \circlearrowleft X$
$x \mapsto \varphi_g(x) = \begin{cases} g \cdot x \\ {}^{x}g \end{cases}$

Esempio 1

Azione di G su G di coniugio

$X = G \quad \varphi: G \to S(G)$ "azione di coniugio"
$g \mapsto \varphi_g \quad (x \mapsto gxg^{-1})$

Esempio 2

$X = \{$ sottogruppi di $G\}$

$\varphi: G \to S(G)$
$x \mapsto \varphi_g \; (H \to gHg^{-1})$

Esempio 3

$\mathbb{K}^* \quad X = V$ sp. vett. su $\mathbb{K}$

$\varphi: \mathbb{K}^* \to S(V)$
$\lambda \mapsto \varphi_\lambda \; (v \mapsto \lambda v)$

Data $\varphi: G \to S(X)$, φ definisce una relazione di equivalenza su X $\quad \underline{x \sim y \text{ se } \exists g \in G \text{ t.c. } \varphi_g(x) = y}$

riflessiva: $x \sim x$, basta prendere $g = e_G \quad \varphi_{e_G} = id$

simm: $x \sim y \Rightarrow y \sim x$
$\hookrightarrow \exists g \in G \mid \varphi_g(x) = y \quad \varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(y)$

φ omomorfismo $\Rightarrow \varphi_{g^{-1}} \circ \varphi_g = \varphi_{g^{-1}g} = \varphi_{e_G} = id$

$\Rightarrow x = \varphi_{g^{-1}}(y) \Rightarrow y \sim x$

trans.: $x \sim y \wedge y \sim z \Rightarrow x \sim z$

$\exists\, g, h \mid \varphi_g(x) = y \wedge \varphi_h(y) = z$

$z = \varphi_h(y) = \varphi_h(\varphi_g(x)) = \varphi_{hg}(x) \Rightarrow x \sim z$

Def.
- $orb(x) := [x]_\sim = \{y \in X \mid x \sim y\}$
- $St(x) := \{g \in G \mid \varphi_g(x) = x\}$

"unione disgiunta"

→ $X = \bigsqcup_{x \in R} orb(x)$ R = rappresentanti delle classi di equivalenza

→ $St(x) < G$ (esercizio)

Proposizione Gli elementi di $orb(x)$ sono in corrispondenza biunivoca con le classi laterali di $St(x)$

Corollario (lemma orbita-stabilizzatore)

G finito $\quad |orb(x)| = \frac{|G|}{|St(x)|}$

DIM.

$orb(x) \xrightarrow{\psi} \{\text{classi laterali sx } St(x) \text{ in } G\}$

$y = \varphi_g(x) \longmapsto g\,St(x)$

- Buona definizione di ψ:

$\varphi_g(x) = \varphi_h(x) \Rightarrow g\,St(x) = h\,St(x)$?

$\varphi_{h^{-1}g}(x) = \varphi_{h^{-1}} \circ \varphi_g(x) = x \Rightarrow h^{-1}g \in St(x) \Rightarrow g \in hSt(x) \Rightarrow g\,St(x) = h\,St(x)$

- Iniettività: $y, z \in orb(x)$

$\psi(y) = \psi(z) \Rightarrow y = z$

$y = \varphi_g(x) \qquad g\,St(x) = h\,St(x)$

$z = \varphi_h(x) \qquad g = hk \quad k \in St(x)$

$y = \varphi_g(x) = \varphi_{hk}(x) = \varphi_h \circ \varphi_k(x) = \varphi_h(x) = z$

- Suriettività:

~~$\forall g \in St$~~ $\forall\, g\,St(x)\ \exists y$ tale che $\psi(y) = g\,St(x)$. Basta prendere $y = \varphi_g(x)$

negli esempi precedenti....

Esempio 1

$orb(x) = Cl_x$ = classe di coniugio di x

$\{\varphi_g(x) \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$

$St(x) = \{g \in G \mid \varphi_g(x) = gxg^{-1} = x\} = Z_G(x)$ CENTRALIZZATORE di x

(posso vedere il centralizzatore come uno stabilizzatore rispetto a una certa azione - quella di coniugio)

$Cl_x = \{x\} \iff Z(x) = G \iff x \in Z(G)$

Esempio 2

$orb(H) = \{gHg^{-1} \mid g \in G\}$ = coniugati di H

$St(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ normalizzatore di H in G

$H \subseteq N_G(H)$

$\# orb(H) = [G : N_G(H)]$ indice in G del normalizzatore $\equiv$ # di classi laterali $\equiv$ cardinalità del quoziente

$H \trianglelefteq G \iff orb(H) = \{H\} \iff N_G(H) = G$ $\quad H \trianglelefteq N_G(H) \ \forall H$

più grande sottoinsieme con questa proprietà

$\# Cl_x = [G : Z_G(x)]$

Se $|G| < +\infty$

$|Cl_x| \mid |G|$

anche se non è un sottogruppo

In generale $G \circlearrowleft X$ $\quad |orb(x)| \mid |G|$

OSS: $H \trianglelefteq G \iff H = \bigcup_{x \in H} Cl_x$

$\iff gHg^{-1} = H \ \forall g \in G \iff \underbrace{ghg^{-1} \in H \ \forall g \in G}_{Cl(h)} \ \forall h \in H$

questo dimostra ☺

Formula delle classi

$G \circlearrowleft X \qquad X = \dot{\bigcup}_{x \in R} orb(x)$

se $|X| < +\infty \Rightarrow |X| = \sum_{x \in R} |orb(x)|$

Se $X = G$ e considero il coniugio $|G| < +\infty$

$$|G| = \sum_{x \in R} |Cl_x| = \sum_{x \in R} |G| / |Z_G(x)| = \sum_{x \in Z(G)} 1 + \sum_{x \in R'} |G| / |Z_G(x)| =$$

$R' = R \setminus Z(G)$

$$= |Z(G)| + \sum_{x \in R \setminus Z(G)} |G| / |Z_G(x)|$$ → formula delle classi

perché le orbite degli elementi di H sono in H e ne forniscono una partizione

$H \triangleleft G$

$$|H| = |Z(G) \cap H| + \sum_{x \in (R \setminus Z(G)) \cap H} |G| / |Z_G(x)|$$

Applicazione: i **p-gruppo**

potrebbe comunque essere tutto il gruppo, credo

1) il centro di un p-gruppo è "non banale" (non ha solo l'identità)

$$\underset{p^n}{|G|} = |Z(G)| + \underbrace{\sum_{x \in R'} |G| / \underset{\hookrightarrow p^{k_x}}{|Z_G(x)|}}_{p \cdot m} \qquad k_x \geq 1$$

$\Rightarrow |Z(G)| = p^n - p \cdot m \qquad p \mid |Z(G)|$

2) Un gruppo di ordine p^2 è abeliano

$|G| = p^2 \qquad |Z(G)| = \begin{cases} \cancel{1} & \text{no, dalla 1)} \\ \cancel{p} & \leftarrow G/Z(G) \text{ ha ordine } p \Rightarrow \text{sarebbe ciclico } \lightning \\ p^2 \end{cases}$

perché $G/Z(G)$ ciclico implica che...

$G/Z(G) = \langle x Z(G) \rangle$

$a, b \in G$

$a \in x^\alpha Z(G)$, $b \in x^\beta Z(G)$ $\Rightarrow$ $a = x^\alpha z_1$, $b = x^\beta z_2$ $\qquad z_i \in Z(G)$

$ab = x^\alpha z_1 x^\beta z_2 = z_2 x^\beta z_1 x^\alpha = ba$

TEOREMA (Cauchy)

$|G| = n \quad p$ primo t.c. $p \mid n \Rightarrow \exists x \in G \ \operatorname{ord} x = p$

DIM.

→ G ciclico $\Rightarrow G \cong \mathbb{Z}/n\mathbb{Z} \quad [n/p]$ ha ordine p

→ G abeliano

$|G| = p \cdot m$ per induzione su m

- $m = 1 \Rightarrow G$ ciclico ✓

Passo induttivo (supponiamo vera la tesi $\forall d < m$)

$x \in G$, $x \neq e$ $\qquad \operatorname{ord} x = |G| \Rightarrow G$ ciclico ✓

$\operatorname{ord} x < |G|$ → $\operatorname{ord}(x) = p \cdot d \ (d < m)$ $\Rightarrow \langle x \rangle$ contiene un elemento (x^d) di ordine p

→ $p \nmid \operatorname{ord}(x)$

posso fare il quoziente perché sono gruppi abeliani

$\Rightarrow p \mid |G/\langle x \rangle| = p \cdot k \quad k < m$

Allora applico al quoziente l'ip. induttiva

$\exists\ \bar{y} \in G/\langle x\rangle$ con $\operatorname{ord}\bar{y} = p$

$\pi_{\langle x\rangle}: G \to G/\langle x\rangle$
$y \mapsto \bar{y}$

$\operatorname{ord}\bar{y} \mid \operatorname{ord} y \Rightarrow p \mid \operatorname{ord} y \Rightarrow \exists$ un elemento in $\langle y\rangle$ di ordine p

→ G gruppo generico

$|G| = p \cdot n$ per induzione su n
- $n = 1$ ✓

Supponiamo vera la tesi per gruppi di ordine pk $1 \leq k < n$

1) $\exists H \lneq G$ $p \mid |H| \Rightarrow H = p \cdot k$ con $k < n \Rightarrow$ concludo per ip. induttiva

2) $\forall H \lneq G$ $p \nmid |H|$
↓ uso la formula delle classi

$$p \cdot n = |G| = |Z(G)| + \sum_{x \in R'} |G|/|Z_G(x)|$$

non diviso da p $\Rightarrow p \mid |G|/|Z_G(x)|$ $\forall x \Rightarrow$

perché sono tutti sottogruppi propri

$\Rightarrow p$ divide la sommatoria

$\Rightarrow p \mid |Z(G)| \Rightarrow Z(G)$ non è proprio $\Rightarrow G$ abeliano □

02/10/2024

TEOREMA (Cayley)

Ogni gruppo G è isomorfo a un gruppo di permutazioni

$$\left[\begin{array}{l} \lambda : G \to S(G) \\ \quad g \mapsto \lambda g : x \mapsto gx \end{array}\right]$$ RAPPRESENTAZIONE REGOLARE SINISTRA

λ: omo. iniettivo

In particolare, se $|G| = n \Rightarrow G \hookrightarrow S_n$

↳ un esempio di immersione possibile (non è unica)

DIM. λ omo. iniettivo

- $\lambda(gh) = \lambda(g) \circ \lambda(h)$ $\forall h, g \in G$?

$\lambda(g) \circ \lambda(h)(x) = \lambda_g(\lambda_h(x)) = \lambda g(hx) = ghx = \lambda_{gh}(x)$

- $\operatorname{Ker}\lambda = \{g \in G \mid \lambda g x = gx = x\ \forall x\} = \{e\}$ □

Esempio $\mathbb{Z}/10\mathbb{Z} \hookrightarrow S_{10} = S(\{\bar{1}, \dots, \overline{10}\})$

$\bar{1} \to \lambda_{\bar{1}}$ $\begin{cases} \bar{1} \to \bar{1}+\bar{1} = \bar{2} \\ \bar{2} \to \bar{1}+\bar{2} = \bar{3} \\ \bar{k} \to \bar{1}+\bar{k} = \overline{k+1} \end{cases}$

immagine di $\bar{1}$ tramite l'immersione
↓
$(1, 2, \dots, 10) = \sigma$

$$\bar{\bar{2}} \longmapsto \lambda_{\bar{2}} = \lambda_{\bar{1}} \circ \lambda_{\bar{1}} = \sigma^2$$

$$\boxed{\operatorname{ord} g^k = \frac{\operatorname{ord} g}{\operatorname{MCD}(\operatorname{ord} g, k)}}$$

in un gruppo ciclico $G = \langle g \rangle$

$$G \hookrightarrow S(G)$$
$$g \longmapsto \lambda_g \qquad g_1 \to g g_1 \to g^2 g_1$$

ord.d

è una permutazione $\Rightarrow (g_1 \; g g_1 \; \cdots \; g^{d-1} g_1)$

$\Downarrow$

perché devono comparire tutti gli elementi di G

l'immagine di g sono $\frac{n}{d}$ cicli di lunghezza d dove $d = \operatorname{ord} g$

<u>Esempio</u> $G = \mathbb{Z}/_2 \times \mathbb{Z}_2 \hookrightarrow S_4$

$$(\bar{1}, \bar{0}) \longmapsto (a\,b)(c\,d)$$

$(0,1)$
$(1,1)$ } vanno in el. della stessa forma $\rightarrow$ sono $\binom{4}{2}\binom{2}{2}\frac{1}{2} = 3$

$\{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} = V_4$ $\hookrightarrow$ sottogruppo di Klein.

(Ho tanti modi di immergerlo quanti sono gli automorfismi di V_4)

Studio di S_n

$\sigma \in S_n \quad \sigma: 1 \to \cdots$
$\vdots$
$n \to \cdots$

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

$\downarrow$ lo indico con

$(1, \sigma(1), \sigma(\sigma(1)) \cdots)$

$\langle \sigma \rangle \to S\{1, \dots, n\}$ $\Rightarrow$ azione del gruppo ciclico generato da σ sull'insieme $\{1, 2, \dots, n\}$

$\sigma \mapsto \sigma$ (inclusione)

$\operatorname{orb}(x) = \{x, \sigma(x), \dots, \sigma^{d-1}(x)\} \qquad d = \operatorname{ord} \sigma$

PROP.

- Ogni permutazione si scrive in modo unico come prodotto di cicli disgiunti

$\langle \sigma \rangle \hookrightarrow S(\{1, \dots, n\}) \qquad X = \{1, \dots, n\}$

$\sigma \longmapsto \sigma \qquad X = \bigodot_{x \in R} \operatorname{orb}(x)$

i cicli di σ sono le orbite viste come insieme ordinato □

- $\sigma = \sigma_1 \circ \cdots \circ \sigma_n$ $\hookrightarrow$ cicli disgiunti $\qquad \operatorname{Ord} \sigma = \operatorname{mcm}[\operatorname{ord} \sigma_i \; | \; i = 1, \dots, n]$

σ_1 ciclo di lunghezza d $\quad (x, \sigma(x), \dots, \sigma^{d-1}(x)) \Rightarrow$ ha chiaramente ord. d

(per dimostrarlo basta dire che ogni ciclo deve essere l'identità perché agiscono su insiemi disgiunti)

- Un K ciclo ha K strutture distinte

$\{x_1, \dots, x_K\}$ $\quad \frac{K!}{K} \rightarrow$ # di K-cicli distinti che posso formare a partire dall'insieme $\{x_1, \dots, x_K\}$

PROP.
S_n è generato dalle trasposizioni

- S_n generato dalle permutazioni cicliche
- Ogni ciclo è prodotto di trasposizioni

$$(1 \dots K) = (1K) \cdots (1\,3)(1\,2)$$

Esercizio ⊛

In S_8 calcolare $|Z(\sigma)|$ con $\sigma = (1\,2\,3)(4\,5\,6)$

$$|Z_{S_8}(\sigma)| = {|S_8|}/{|orb(\sigma)|}$$

$orb(\sigma) = Cl_\sigma \rightarrow$ permutazioni con la stessa decomposizione in cicli

Classe di coniugio in S_n

PROP. Due perm. sono coniugate in $S_n \iff$ hanno lo stesso tipo di decomposizione in cicli disgiunti

$(\Rightarrow)$ il coniugio è omo.

$\sigma = \sigma_1 \cdots \sigma_K$

$\gamma\sigma\gamma^{-1} = \gamma\sigma_1\gamma^{-1}\gamma\sigma_2\gamma^{-1} \cdots \gamma\sigma_K\gamma^{-1} \Rightarrow$ WLOG posso considerare il coniugio su ogni singolo ciclo a patto di verificare alla fine che sono ancora disgiunti

$\sigma = (a_1 \cdots a_d) \qquad \gamma\sigma\gamma^{-1} \qquad \gamma(a_i) = b_i$

$$\gamma\sigma\gamma^{-1} = \begin{cases} b_{i+1} & x = b_i \\ x & \rightarrow x \neq b_i \end{cases}$$

cioè x è immagine tramite γ di un punto fisso di σ

$b_i \xrightarrow{\gamma^{-1}} a_i \rightarrow a_{i+1} \rightarrow b_{i+1}$

$x \xrightarrow{\gamma^{-1}} \gamma^{-1}(x) \xrightarrow{\sigma} \gamma^{-1}(x) \xrightarrow{\gamma} x$

$\gamma\sigma\gamma^{-1} = (b_1, \dots, b_d)$

(non c'è una sola γ, ma tante quante le classi laterali del centralizzatore)

$(\Leftarrow)$ $\sigma \quad (a_1 \cdots a_\ell)(b_1 \cdots b_m)(c_1 \cdots c_t) \cdots$ disgiunti

$\rho \quad (a_1' \cdots a_\ell')(b_1' \cdots b_m')(c_1' \cdots c_t') \cdots$

th: sono coniugate $\exists \gamma$ t.c. $\gamma\sigma\gamma^{-1} = \rho$

$\gamma: \begin{array}{l} a_i \rightarrow a_i' \\ b_i \rightarrow b_i' \\ c_i \rightarrow c_i' \end{array}$

$$a_i' \xrightarrow{\rho} a_{i+1}'$$

$$a_i' \xrightarrow{r^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{r} a_{i+1}' \quad \Rightarrow \text{funziona}$$

Tornando all'esercizio ⊛

$$|Z(\sigma)| = |S_8| / |Cl_\sigma|$$

$$(a\ b\ c)(d\ e\ f) \qquad |Cl_\sigma| = \frac{\binom{8}{3} 2! \binom{5}{3} 2!}{2!} = 8!/36$$

$$\Rightarrow |Z(\sigma)| = 36$$

$$Z(\sigma) = \langle (1,2,3), (4,5,6), (14)(25)(36), (7\ 8) \rangle$$

- Il prodotto di gruppi è un gruppo $\Leftrightarrow$ commutano

$$\downarrow$$

$$H, K < G$$

In generale HK NON sottogruppo (trova esempi)

$$HK = \{hk \mid h \in H \wedge k \in K\}$$

$$HK < G \Leftrightarrow HK = KH \Leftarrow H \subseteq N_G(K) \quad \text{(esercizio)}$$

$$\forall hk = k'h'$$

- $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$

$$H \times K \to HK \quad \text{(mappa di insiemi)}$$

$$(h,k) \mapsto hk$$

$$\shortparallel$$

$$(h', k') \mapsto h'k'$$

$$\Downarrow$$

$$hk = h'k' \Rightarrow h'^{-1}h = k'^{-1}k \Rightarrow \in H \cap Z$$

$$h = h'z$$
$$k = z^{-1}k'$$

$$\operatorname{sgn} \sigma = \pm 1$$

$$\sigma = \tau_1 \circ \dots \circ \tau_d \quad \text{con } \tau_i \text{ trasposizioni}$$

$$\Rightarrow \operatorname{sgn} \sigma = (-1)^d$$

$$\operatorname{sgn}: S_n \to \{\pm 1\}$$

- omo surgettivo

$\operatorname{Ker} \operatorname{sgn} := A_n \to$ GRUPPO ALTERNO

$$S_n / A_n \cong \{\pm 1\}$$

Classificazione dei sottogruppi di D_n

$\langle r \rangle = C_n \rightarrow$ ciclico con n elementi $\quad R := \langle r \rangle$ gruppo delle rotazioni
$\langle s \rangle = C_2$

Per ogni divisore d di n $\exists !$ sottogruppo di ordine d, che è $\langle r^{n/d} \rangle$

Il gruppo R è normale? Si

→ indice = numero di classi laterali

$\rightarrow$ 1) R ha indice 2 $\Rightarrow$ è normale

Teo $H < G$, $[G : H] = 2 \Rightarrow H \triangleleft G$

Dim $g \in G \setminus H$, $\quad G = H \sqcup gH = H \sqcup Hg \Rightarrow gH = Hg$

↳ unione disgiunta

$gHg^{-1} = H$, cioè H normale

$\rightarrow$ 2) $srs = r^{-1} = r^{n-1} \in R$
entrambi i generatori di D_n fissano $R \Rightarrow R$ normale

$\rightarrow$ 3) $R = \mathrm{Ker}(\det)$, dove $\det : D_n \rightarrow \{\pm 1\} \cong C_2$

$$\det \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = -1 \qquad \det \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = 1$$

$H < D_n$

- Se $H < R \Rightarrow H = \langle r^d \rangle$
- Se $H \not< R \Rightarrow \det|_H$ è suriettivo

l'identità va in 1 e c'è almeno un elemento che non è in R

$\mathrm{Ker}(\det|_H) = H \cap R \qquad H/_{H \cap R} \cong C_2$ I teo di omomorfismo

$H \cap R < R \Rightarrow H \cap R = \langle r^d \rangle$ per qualche $d | n$

$|H| = 2 |H \cap R|$

Sia $h \in H \setminus (H \cap R)$, allora $H = (H \cap R) \sqcup h(H \cap R)$
$h = sr^\alpha$, $0 \leq \alpha < n$

$\Rightarrow$ gli elementi di H sono $\{e, r^d, \dots, r^{n-d}, sr^\alpha, sr^{\alpha+d}, \dots, sr^{\alpha+n-d}\}$

Voglio dimostrare che dato $d | n$ e $0 \leq \alpha < n$, l'insieme di sopra è un sottogruppo.

$$\{e, r^d, r^{2d}, \dots, r^{n-d}, sr^\alpha, sr^{\alpha+d}, \dots, sr^{\alpha+n-d}\} = \underbrace{\langle sr^\alpha \rangle}_{\cong C_2} \underbrace{\langle r^d \rangle}_{\cong C_{n/d}}$$

prodotto

Lemma G gruppo, $H, K < G$

$$HK < G \Leftrightarrow HK = KH$$

Dim

$\Rightarrow$ HK gruppo. $\quad \forall k \in K$ vale $k \in HK$
$\forall h \in H$ vale $h \in HK$

$\Rightarrow kh \in HK \Rightarrow KH \subseteq HK$

$$hk \in HK \Rightarrow (hk)^{-1} = \underbrace{k^{-1}h^{-1}}_{\in KH} \in HK$$

Ma ogni elemento di HK è l'inverso di un elemento di KH, da cui $HK \subseteq KH$

($\Leftarrow$) i • $hk, h'k' \in HK \Rightarrow hkh'k' \in HK$
 • $e \in HK$ ✓ (segue dalle altre due)
ii • $hk \in HK \Rightarrow k^{-1}h^{-1} \in HK$

i) $h\underbrace{kh'}k' = hh''k''k \in HK$

ii) $k^{-1}h^{-1} \in KH = HK$ $\square$

tornando al diedrale...

$$H = \langle r^d \rangle \langle sr^a \rangle, \quad H < D_n \iff \langle r^d \rangle \langle \overset{\{e,\, sr^a\}}{\overset{\shortparallel}{sr^a}} \rangle = \langle sr^a \rangle \langle r^d \rangle$$

$$\langle r^d \rangle \langle sr^a \rangle = \{e, r^d, \dots, r^{n-d}, \overset{sr^a}{r^d sr^a}, \dots, r^{n-d}sr^a\} =$$
$$= \{e, r^d, \dots, r^{n-d}, \overset{sr^a}{sr^{a-d}}, \dots, sr^{a+d-n}\} =$$
$$= \{e, r^d, \dots, r^{n-d}, \overset{sr^a}{sr^{a-d}}, \dots, \overset{sr^{a-(n-1)d}}{sr^{a+d}}\} =$$
$$\hookrightarrow sr^{a-2d}, sr^{a-3d}, \dots, sr^{a+d}$$
$$= \langle sr^a \rangle \langle r^d \rangle \quad \text{In questo caso } H = \langle r^d, sr^a \rangle$$

Recap:

$$H < D_n \begin{cases} \nearrow H = \langle r^d \rangle \\ \searrow H = \langle r^d, sr^a \rangle \text{ con } d \mid n \text{ e } 0 \leq a < n \end{cases}$$

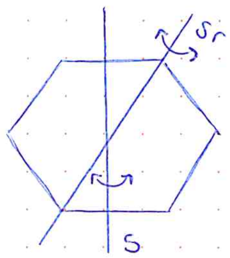
anzi $0 \leq a < d$ (perché $\langle r^d, sr^a \rangle = \langle r^d, sr^{a+d} \rangle$)

$\downarrow$

gruppo generato da una riflessione e una rotazione di $2\pi d/n \Rightarrow H \cong D_{n/d}$

⚠ $d = n$, $H = C_2 \cong$ "D_1"

$d = n/2$, $H \cong C_2 \times C_2 \cong$ "D_2"



$H < D_6$

$H = \langle r^2, s \rangle \cong D_3$

$H = \langle r^2, sr \rangle \cong D_3$

OSS. Se $0 \leq a < b < d$, allora $\langle r^d, sr^a \rangle \neq \langle r^d, sr^b \rangle$ ma sono isomorfi tra di loro.

- Quali sono tra questi i sottogruppi caratteristici?

Oss $H < D_n$, se $H \cong C_d \Rightarrow H$ è caratteristico, perché $\varphi(H)$ è un gruppo ciclico della stessa forma ma tale gruppo è unico

In particolare sono anche normali. $H < R$, $|H| \geq 3 \Rightarrow$ normale e caratteristico

Se $H = \langle r^d, sr^\alpha \rangle$

$H \triangleleft D_n \iff rHr^{-1} = H \wedge sHs = H$

$rHr^{-1} = \langle r^d, rsr^\alpha r^{-1} \rangle = \langle r^d, sr^{\alpha-2} \rangle = H \iff 2 \equiv 0 \ (d) \iff d|2 \iff d=1 \vee d=2$

$sHs = \langle sr^ds, \cancel{s}\cancel{s}r^\alpha s \rangle = \langle r^{-d}, sr^{-\alpha} \rangle = H \iff a \equiv -a \ (d)$ (non aggiunge nessuna condizione se $d=1 \vee d=2$)

$\Rightarrow H = \langle r^d, sr^\alpha \rangle \triangleleft D_n \iff$ $d=1$ $a=0$ $H = D_n$; $d=2$ $a=0$ $H \cong D_{n/2}$; $d=2$ $a=1$ $H \cong D_{n/2}$ $\big\}$ ci sono solo se n è pari

Gruppi ciclici di ordine 2 dentro D_n:

$H = \langle r^{n/2} \rangle = Z(D_n) \rightarrow$ caratteristico

$H = \langle sr^\alpha \rangle \rightarrow$ non normali per il calcolo precedente

Rimane da verificare se $\langle r^2, s \rangle$ e $\langle r^2, sr \rangle$ sono caratteristici.

Non lo sono, $\underset{\substack{\downarrow \\ \text{rotazione di} \\ \pi/n \text{ gradi}}}{r^{1/2}} g r^{-1/2}$ è un automorfismo che manda uno nell'altro

$\langle r^{1/2}, s \rangle \cong D_{2n} \triangleright D_n$

$r^{1/2} g r^{-1/2}$ fissa $D_n \Rightarrow \underset{\text{coniugio per } r^{1/2}}{C_{r^{1/2}}} \in Aut(D_n)$

$r^{1/2} s r^{-1/2} = sr^{-1} \in \langle r^2, sr \rangle$

$r^{1/2} \langle r^2, s \rangle r^{-1/2} = \langle r^2, sr \rangle$

In conclusione i sgr. normali di D_n sono
- $\langle r \rangle$ e i suoi sottogruppi
- $\langle r^2, s \rangle$
- $\langle r^2, sr \rangle$

$\big\}$ se n è pari $\cong D_{n/2}$

- Quali sono i quotienti di D_n? D_n/N $N \triangleleft D_n$

$N \triangleleft D_n$ ha indice 2 oppure è ciclico

$\downarrow$ $D_n/N \cong C_2$ $\qquad$ $\downarrow$ $D_n/\langle r^d \rangle \cong D_d$

$\bar{r} \leftarrow r$

$\bar{s} \leftarrow s$

bisogna verificare a mano che è un isomorfismo

$\varphi: D_d \rightarrow D_n/\langle r^d \rangle$

$\varphi(r^k) = \overline{r^k}$ $\qquad$ $\varphi(sr^k) = \overline{sr^k}$

• È un omomorfismo

$$\varphi(s^{\varepsilon}r^{k})\,\varphi(s^{\varepsilon'}r^{k'}) = \varphi(s^{\varepsilon}r^{k}s^{\varepsilon'}r^{k'}) \quad \forall\, \varepsilon,\varepsilon' \in \{0,1\}$$
$$\forall\, k,k' \in \{0,\dots,d-1\}$$

$$\varphi(s^{\varepsilon}r^{k})\,\varphi(s^{\varepsilon'}r^{k'}) = \begin{cases} \overline{s^{\varepsilon}r^{k+k'}} & \text{se } \varepsilon'=0 \\ \overline{s^{\varepsilon+1}r^{-k+k'}} & \text{se } \varepsilon'=1 \end{cases}$$

$$\varphi(s^{\varepsilon}r^{k}s^{\varepsilon'}r^{k'}) = \begin{cases} \overline{s^{\varepsilon}r^{k+k'}} \ (\mathrm{mod}\ d) & \text{se } \varepsilon'=0 \\ s^{\varepsilon+1} & \end{cases}$$

φ omomorfismo. È bigettivo $\Rightarrow$ è isomorfismo

Classi di coniugio in D_n

$Cl(x) = \{gxg^{-1} \mid g \in G\}$

$|Cl(x)| = |G| / |Stab(x)|$

nel diedrale: $Cl(e) = \{e\}$

$Cl(r) = \{r, r^{-1}\}$

$Cl(r^k) = \{r^k, r^{-k}\}$

$Cl(r^{n/2}) = \{r^{n/2}\}$

devono essere tutti gli elementi che non appaiono nelle orbite precedenti

$Cl(s) = \begin{cases} \{s, sr, \dots, sr^{n-1}\} \to \text{se } n \text{ dispari} \\ \{s, sr^2, sr^4, \dots, sr^{n-2}\} \to \text{se } n \text{ pari} \end{cases}$

$Stab(s) \overset{S}{=} \{g \in G \mid gsg^{-1}\} = Z(s)$

$n \equiv 1\ (2)$: $\langle s \rangle$, C_2 $\to$ $|Cl(s)| = n$

$n \equiv 0\ (2)$: $\langle r^{n/2}, s \rangle$, $C_2 \times C_2$ $\to$ $|Cl(s)| = n/2$

riflessioni che passano per 2 vertici o per 2 punti medi, che non sono coniugate tra loro

Se n è pari c'è anche $Cl(sr) = \{sr, sr^3, \dots, sr^{n-1}\}$

08/10/2024
Patimo

Ancora diedrale

per favore basta

Contare gli elementi di $Aut(D_n)$

$D_n = \langle r, s \rangle \Rightarrow f \in Aut(D_n)$ è determinato da $f(r)$ e $f(s)$

- $f(r) = r^k$ dove $(k,n) = 1 \Rightarrow \varphi(n)$ possibilità
- $f(s) = ?$ Elementi di ordine 2: sr^k, $\cancel{r^{n/2}}$
  ↳ non va bene (ad esempio perché è nel centro)

Abbiamo al più $\varphi(n) \cdot n$ possibilità

Dobbiamo dimostrare che $\forall (i,j)$ con $(i,n) = 1$, $0 \leq j < n$

$$\exists! \ f_{i,j} : D_n \xrightarrow{\sim} D_n \quad \text{t.c.} \quad f_{i,j}(r) = r^i$$
$$f_{i,j}(s) = sr^j$$

Dobbiamo contare gli f_{ij}

$$f_{ij}(s^\varepsilon r^a) = s^\varepsilon r^{j\varepsilon} r^{ai} \qquad f_{ij} \in Aut(D_n)?$$
$$\varepsilon \in \{0,1\}$$
$$0 \leq a < n$$

$$f_{ij}(s^\varepsilon r^a) f_{ij}(s^{\varepsilon'} r^{a'}) \overset{?}{=} f_{ij}(s^\varepsilon r^a s^{\varepsilon'} r^{a'}) \quad \text{Sì!}$$

conti, conti, conti ...

$\Rightarrow f_{ij}$ omomorfismo di gruppi

INIETTIVITÀ: $Ker(f_{ij}) = \{ s^\varepsilon r^a \mid \varepsilon = 0, n \mid \cancel{j\varepsilon} + ai \}$

↓ i coprimo con n $\Rightarrow n \mid a$

$\Rightarrow Ker(f_{ij}) = \{e\}$

allora è un isomorfismo

Esercizio 2 - prima settimana

$L \trianglelefteq H \trianglelefteq G \Rightarrow L \trianglelefteq G$? ⊛

$L \trianglelefteq G \Leftrightarrow gLg^{-1} = L \quad \forall g \in G$

$H \trianglelefteq G \Leftrightarrow gHg^{-1} = H \quad \forall g \in G$

$H \trianglelefteq G \Rightarrow c_g(x) = gxg^{-1} \quad c_g \in Aut(H) \quad \forall g \in G$

<u>OSS</u> $L < H$ caratteristico, allora è fissato da $c_g \in Aut(H) \Rightarrow L \trianglelefteq G$

In generale ⊛ è falsa.

Per trovare un controesempio serve L normale e non caratteristico

$G = D_3 \triangleright H = R$ → l'unico sottogruppo proprio è $\{e\}$ ed è normale in D_3

$G = D_4 \triangleright H = \langle r^2, s \rangle \cong$ "D_2" $C_2 \times C_2$

$L \triangleleft H$, $L = \langle s \rangle \cong C_2$, $L \ntriangleleft G$ OK!

Esercizio 3

G gruppo finito, $H < G$ proprio $\quad \lambda g \lambda^{-1} = h \Rightarrow g = \lambda^{-1} h \lambda \in \bigcup_{x \in g} xHx^{-1}$

$\Rightarrow G \neq \bigcup_{g \in G} gHg^{-1}$ $(\Leftrightarrow \exists g \in G \mid Cl(g) \cap H = \emptyset)$

$G \circlearrowleft \{gHg^{-1} \mid g \in G\}$ coniugio $\quad |Orb(H)| = |G| / |Stab(H)|$ $\quad Stab(H) = N_G(H)$ ↑ normalizzatore $=$ $\{g \in G \mid gHg^{-1} = H\}$

$|\{gHg^{-1}\}| = [G : N_G(H)] \leqslant [G : H]$

$(H < N_G(H))$

$|gHg^{-1}| = |H| \ \forall g \in G \Rightarrow$ Vogliamo coprire G con $[G:H]$ insiemi di $|H|$ elementi $\quad [G:H] \cdot |H| = |G|$, per cui l'unica possibilità è che non ci siano intersezioni $\Leftrightarrow \forall g, g' \in G$

$gHg^{-1} \cap g'Hg'^{-1} = \emptyset$ oppure gHg^{-1} e $g'Hg'^{-1}$ coincidono

↓ impossibile perché c'è l'identità

↓ impossibile perché l'unione di tutti sarebbe H che è proprio in G

Esempio con un gruppo ∞:

$G = GL_n(\mathbb{C}) = \{A \in Mat_{n \times n}(\mathbb{C}) \mid \det A \neq 0\}$

↳ sono tutte triangolabili

$\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} < GL_n(\mathbb{C})$ e $GL_n(\mathbb{C}) = \bigcup_{x \in GL_n(\mathbb{C})} x \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} x^{-1}$ $\quad$ per cui non vale se il gruppo è ∞

↑ sottogruppo delle triangolari superiori

$\Rightarrow G = GL_n(\mathbb{F}_p)$ non tutte le matrici in G sono triangolarizzabili

Esercizio 4

G finito, $|G| > 2$, $Aut(G) \neq \{e\}$

- CASO 1: G non abeliano $\Rightarrow \exists x \notin Z(G) \mid c_x(g) = xgx^{-1} \neq g$ per qualche g

↱ perché $Inn(G) \cong G/Z(G)$ è non banale se $Z(G) \neq G$

- CASO 2 G abeliano $\begin{aligned} G &\xrightarrow{inv} G \\ g &\mapsto g^{-1} \end{aligned}$ è un automorfismo (non lo è se G non è abeliano)

$inv = id$ se $g = g^{-1}$ $\forall g \in G$, cioè tutti gli elementi hanno ordine 2

$$\Updownarrow$$

claim: $$\boxed{\begin{gathered} ord(g) = 2 \quad \forall g \in G \setminus \{e_G\} \\ \Updownarrow \\ G \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^K \end{gathered}}$$

(non deriva immediatamente dal teo. di struttura?)

Se dimostro il claim ho finito, posso considerare ad esempio l'automorfismo che scambia le prime due coordinate.

DIM. (claim) Per indutione tutti i sottogruppi di G sono di questa forma

$H = \{e\}$ ✓

$|H| = 2 \Rightarrow H \cong \mathbb{Z}/2\mathbb{Z}$ ✓

Altrimenti prendo $H < G$, supponiamo valga per tutti i sottogruppi di H

Sia $K < H$ massimale $(K < L < H \Rightarrow K = L \vee L = H)$
(come so che esiste?)

Per ip. $K \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^a$ $h \in H \setminus K$, $H = \langle K, h \rangle$ perché K massimale

$H = \langle K, h \rangle \cong K \times \mathbb{Z}/2\mathbb{Z}$

$$|\langle K, h\rangle| = |K \underbrace{\langle h \rangle}_{\cong \mathbb{Z}/2\mathbb{Z}}| = \frac{|K| 2}{\underbrace{K \cap \langle h \rangle}_{=\{e\}}} = 2|K|$$

STO USANDO G COMMUTATIVO (?)

$\langle K, h \rangle = K \sqcup Kh$

$$\begin{aligned} \varphi : \langle K, h \rangle &\to K \times \mathbb{Z}/2\mathbb{Z} \\ K &\mapsto K \times \bar{0} \\ Kh &\mapsto K \times \bar{1} \end{aligned}$$

(è facile verificare che è un isomorfismo)

$\Rightarrow H \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{a+1}$ □

Esercitio 5

G p-gruppo $(|G| = p^n)$, allora G contiene una <u>catena completa di sottogruppi normali</u>, cioè $\exists H_i \trianglelefteq G$, $|H_i| = p^i$ con

$\{e\} = H_0 < H_1 < \cdots < H_n = G$

$Z(G) \neq \{e\}$ (già visto)

Vogliamo trovare $z \in Z(G)$ di ordine p (Cauchy, oppure

$$z_0 \in Z(G) \quad \text{ord}\, z_0 = p^K \quad \text{ord}(z_0^{p^{K-1}}) = p$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \;\; z$$

perche' gli elementi di $\langle z \rangle$ commutano con tutti gli altri

$$H_1 = \langle z \rangle \triangleleft G$$

Dimostro l'enunciato per induzione su n

$n=0$ ✓
$n=1$ ✓
$n=2$

Per induzione assumo l'enunciato per $G/_{H_1} =: \hat{G}$

$$|\hat{G}| = p^{n-1}$$

Trovo $\hat{H}_1 < \hat{H}_2 < \cdots < \hat{H}_{n-1}$ normali in $\hat{G}$ con $|\hat{H}_i| = p^i$

$\hat{H}_i = L_i/_{H_1}$ dove L_i sono sottogruppi di G che contengono H_1

$|L_i| = p^{i+1}$

$\Rightarrow$ Posso prendere $H_i = L_{i-1}$, devo verificare che $H_i \triangleleft G$

$$\hat{H}_i \triangleleft \hat{G} \overset{?}{\Rightarrow} H_i \triangleleft G \qquad \hat{H}_i \overset{*}{=} L_i/_{H_i} = H_{i+1}/_{H_i}$$

ciò e' automatico dal teo. di corrispondenza perche' la normalità si mantiene

Sia $g \in G$ $\quad \cancel{gH_ig^{-1}}$

$\cancel{\hat{H}_i \triangleleft \hat{G} \,/\, \forall \hat{g} \in \hat{G} \quad \hat{g}\hat{H}_i\hat{g}^{-1} = \hat{H}_i}$

$\cancel{\hat{g} = gH_1 \qquad gH_1\hat{H}_i gH_1 = gH_1\hat{H}_iH_1g^{-1}} = gH_{i+1}g^{-1}$

$$\hat{H}_i = \{ hH_1 \mid h \in H_{i+1} \} \overset{\text{come insieme}}{=} H_{i+1}$$

$$\forall g \in G \quad gH_1\hat{H}_i g^{-1}H_1 = \hat{H}_i \iff g\underbrace{H_1\hat{H}_iH_1}_{\hat{H}_i}g^{-1} = \hat{H}_i$$

$$\iff gH_{i+1}g^{-1} = H_{i+1} \iff H_{i+1} \triangleleft G$$

La bigezione usata nella dimostrazione del teorema di corrispondenza (vedi lezione successiva) conserva la normalità

$*$ TEOREMA DI CORRISPONDENZA

nella prossima lezione la Del Corso lo ha fatto meglio

$N \triangleleft G$

$$\left\{ \begin{matrix}\text{sottogruppi} \\ \text{di } G/_N\end{matrix} \right\} \xrightarrow{\sim} \left\{ \begin{matrix}\text{sottogruppi di} \\ G \text{ che contengono } N\end{matrix} \right\}$$

$$H/_N \longleftarrow H$$

DIM

$$\cancel{H < G/_N} \Rightarrow H = \{ hN \mid h \in \hat{H} \}$$

Voglio verificare che $\cup H$ e' anche un sottogruppo di G che contiene N

$hn, h'n' \in UH$, allora $hnh'n' \in h''N$ per qualche h''

$hnh'n' = h''n'' \in UH$ per qualche $n'' \in N$

NB! Se il gruppo è finito non serve verificare che ci siano gli inversi, perche' l'inverso di ogni elemento sarà dato da una sua potenza.

In ogni caso: $hn \in UH$ $\quad (hN)^{-1} \in H \quad \exists\, hn'$ t.c. $(hn)^{-1} = hn' \in UH$

$\Rightarrow UH$ sottogruppo $\quad \to$ questo verifica solo la buona def.

09/10/2024
Del Corso

Teorema di omomorfismo (1° teo di omo)

$f: G \to G'$ omo
$N \triangleleft G \quad N \subseteq \ker f$
$\Rightarrow \exists!$ omo $\varphi: G/N \to G'$

Tale che
$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_N"'] \arrow[dr, phantom, "\circlearrowleft"] & G' \\ G/N \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$
commuti

Inoltre si ha $\operatorname{Im}\varphi = \operatorname{Im} f$, $\quad \ker\varphi = \ker f / N$

in particolare se $N = \ker f \Rightarrow \varphi$ è iniettivo e quindi $G/\ker f \cong \operatorname{Im} f$

DIM.
$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_N"'] & G' \\ G/N \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

$\varphi \circ \pi_N = f$
$\varphi(\pi_N(x)) = f(x)$

$\varphi(xN) = f(x) \quad \forall x \in G$
↳ è l'unica φ possibile, se è un omo ben definito bene, altrimenti non ho speranze.

- Buona def.

$xN = yN \overset{?}{\Rightarrow} f(x) = f(y)$
$\Updownarrow$
$x \in yN \qquad x = yn \quad n \in N \subseteq \ker f$

$f(x) = f(yn) = f(y)\cancel{f(n)} = f(y)$

- Omomorfismo

$\varphi(xN\,yN) \overset{?}{=} \varphi(xN)\varphi(yN) = f(x)f(y) \quad \forall\, xN, yN \in G/N$
$\quad \| \; N \triangleleft G$
$\varphi(xyN) = f(xy) = f(x)f(y)$

$\mathrm{Im}\,\varphi = \{ \underbrace{\varphi(xN)}_{f(x)} \mid \underset{x \in G}{xN \in G/N} \} = \mathrm{Im} f$

$\ker\varphi = \{ xN \mid \varphi(xN) = f(x) = e' \} = \{ xN \mid x \in \ker f \} = \ker f/N$

$N = \ker f \Rightarrow \ker f/N = N/N = \{eN\} \Rightarrow \varphi$ iniettivo

$\Rightarrow G/\ker f \cong \mathrm{Im} f$ (perché φ è chiaramente suriettivo sull'immagine)

Corollario 1 (2° teo di omo)

G gruppo, $H, K \triangleleft G$ $\quad H \subseteq K$

$\Rightarrow \dfrac{G/H}{K/H} \cong G/K$

Imm. e controimmagine di sottogruppi sono sottogruppi, la normalità si comporta bene con la controimmagine e anche con l'immagine se l'omo è suriettivo

<u>Esempio</u> $\quad \mathbb{Z}/n\mathbb{Z} \quad d \mid n \quad d\mathbb{Z}/n\mathbb{Z}$

$G = \mathbb{Z} \quad H = n\mathbb{Z} \quad K = d\mathbb{Z}$

$$\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/d\mathbb{Z}$$

1) Quello che ho scritto ha senso

$H \triangleleft G, \; H \triangleleft K, \; \dfrac{K}{H} \triangleleft \dfrac{G}{H}$

<u>DIM.</u>

$$\begin{tikzcd} G \arrow[r, "\pi_K"] \arrow[d] & G/K \\ G/H \arrow[ur, "\varphi"'] & \end{tikzcd}$$

suriettiva

φ data dal 1° teo di omo $H \subseteq K = \ker \pi_K$

$$\begin{tikzcd} G/H \arrow[r, "\varphi"] \arrow[d] & G/K \\ \dfrac{G/H}{\ker\varphi} \arrow[ur, "S"'] & \end{tikzcd}$$

$\dfrac{G/H}{\ker\varphi} = \dfrac{G/H}{K/H}$

Corollario 2 (3° teo di omo)

$H, K \triangleleft G \qquad \dfrac{H}{H \cap K} \cong \dfrac{HK}{K}$ $\rightarrow$ NB! Se sono entrambi normali è automatico che il sottoinsieme HK sia anche un sottogruppo

(Non potrei fare H/K perché servirebbe $K \triangleleft H$)

<u>DIM</u> $\pi : H \twoheadrightarrow HK/K$

$\qquad h \longmapsto hK$

$G \xrightarrow{\pi_K} G/K$

$g \longmapsto gK$

π è suriettiva $\quad \forall xK \in HK/K \quad \exists h \in H \mid \pi(h) = hK = xK$

$\downarrow$

$x = hk \quad hkK = hK$

$\ker\pi = \{ h \in H \mid hK = \pi(h) = K \}$

$hK = K$

$\Updownarrow$

$h \in K \Rightarrow \ker\pi = H \cap K$

$H/H\cap K \cong HK/K$ (1° teo)

TEOREMA DI CORRISPONDENZA

G gruppo, $N \trianglelefteq G$ $\quad \pi_N : G \to G/N$ proj

allora π_N induce una corrispondenza biunivoca tra i sottogruppi di G/N e i sttgrp. di G che contengono N

Tale corrispondenza conserva indici di sottogruppi e normalità.

DIM.

$$X = \{H \leqslant G \mid N \subseteq H\} \longleftrightarrow \mathcal{I} = \{\mathcal{H} \leqslant G/N\}$$

$$H \xmapsto{\alpha} \pi_N(H)$$

$$\pi_N^{-1}(\mathcal{H}) \xleftarrow[\beta]{} \mathcal{H}$$

$$\left.\begin{array}{l} \alpha \circ \beta(\mathcal{H}) = \mathcal{H} \\ \beta \circ \alpha(H) = H \end{array}\right) \text{ TESI}$$

la controimmagine di un sgr. è un sgr.

- α ben def., perché π_N è omo. e gli omo conservano i sgr.
- β ben def.: $\pi_N^{-1}(\mathcal{H}) < G$ $\quad e_{G/N} = N \subset \mathcal{H}$, perché $\mathcal{H}$ sgr. di G/N

  $N = \ker \pi_N = \pi_N^{-1}(e_{G/N}) \subset \pi^{-1}(\mathcal{H})$

$$\alpha \circ \beta(\mathcal{H}) = \pi_N(\pi_N^{-1}(\mathcal{H})) = \mathcal{H}$$

↳ perché π_N suriettiva

$$\beta \circ \alpha(H) = \pi_N^{-1}(\pi_N(H)) \supseteq H$$

↓
potenzialmente quando faccio π_N^{-1} l'insieme da cui ero partita potrebbe ingrandirsi questo non accade...

$A < G$
$\pi_N(A) = AN/N$ $\quad \pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}(H/N) = \{g \in G \mid gN \in H/N\} =$

$= \{g \in G \mid \exists h \in H \text{ con } gN = hN\}$

↓
$g = \underbrace{hn}$ $\quad n \in N$

$\in H$ perché $N \subseteq H$

$$\Rightarrow \pi_N^{-1}(H/N) = H$$

ip. necessarie:
- $N, H \trianglelefteq G$
- $N \subseteq H$

$H \in X$ $\quad H \trianglelefteq G \iff \alpha(H) \trianglelefteq G/N$

H/N

$(\Rightarrow)$ Dal 2° teo di omomorfismo $\quad \dfrac{G/N}{H/N} \overset{\varphi}{\cong} G/H$

$$\begin{tikzcd} G \arrow[r] \arrow[d] & G/H \\ G/N \arrow[ur, "\varphi"'] & \end{tikzcd}$$

$H/N = \ker \varphi$ $\quad$ quindi $H/N \trianglelefteq G/N$

$(\Leftarrow)$ $\mathcal{H} \triangleleft G/N$

$\pi^{-1}(\mathcal{H}) = \beta(\mathcal{H}) \triangleleft G$
$\quad \overset{\shortparallel}{H}$

$\pi^{-1}(\mathcal{H}) = H \quad \mathcal{H} = H/N = \{gN \mid g \in H\}$
$\forall g \in G \quad gNhNg^{-1}N = ghg^{-1}N \quad \forall h \in H$
$\Rightarrow ghg^{-1} \in H \Rightarrow H \triangleleft G$

$H \in X$
$[G : H] = [G/N : \underset{\overset{\shortparallel}{H/N}}{\alpha(H)}]$

$g, r \in G$

$gH = rH \iff (gN)^{H/N} = (rN)^{H/N}$ (esercizio)

ESEMPIO:
$G = \mathbb{Z} \qquad N = n\mathbb{Z}$

I sgr di $\mathbb{Z}/n\mathbb{Z} \longleftrightarrow$ sgr di $\mathbb{Z}$ che contengono $n\mathbb{Z}$
$n\mathbb{Z} \subseteq d\mathbb{Z} \iff d \mid n$

$d\mathbb{Z}/n\mathbb{Z} \leftarrow d\mathbb{Z}$

G_1, G_2 gruppi
$G_1 \times G_2$ è un gruppo $\quad (x, y) * (t, u) = (x *_1 t, y *_2 u)$

- Identità (e_1, e_2)
- inverso di $(x, y) \to (x^{-1}, y^{-1})$

OSS $\quad \{e_1\} \times G_2 \triangleleft G = G_1 \times G_2 \qquad (e_1 g_2)(g_1 e_2) = (g_1 e_2)(e_1 g_2)$
$G_1 \times \{e_2\} \triangleleft G$

Teo $\quad G$ gruppo, $H, K \triangleleft G$ (i)
$H \cap K = \{e\}$ (ii)
$HK = G$ (iii)
$\Rightarrow G \cong H \times K$

Es. $S_n = A_n \cdot \langle (12) \rangle = A_n \cup A_n(12)$

DIM.

Lemma $\quad H, K \triangleleft G \quad H \cap K = \{e\}$

$\Rightarrow hk = kh \quad \forall h \in H \; k \in K$

$$\underbrace{\overbrace{hkh^{-1}}^{H}k^{-1}}_{\in K} = e \Rightarrow hk = kh$$
($\underbrace{kh^{-1}}$: $\in K \in H$) sta nell'intersezione

$$G \xleftarrow{\varphi} H \times K$$
$$hk \longleftarrow (h, k)$$

- φ è una mappa surgettiva per (iii)
- φ omomorfismo
$\varphi((h_1 k_1)(h_2 k_2)) = \varphi((h_1 h_2, k_1 k_2)) = h_1 h_2 k_1 k_2 =$

lemma
$\downarrow$
$= h_1 k_1 h_2 k_2 = \varphi((h_1 k_1))\, \varphi((h_2 k_2))$.

$\ker \varphi = \{ (h,k) \in H \times K \mid \varphi(h,k) = hk = e \} = \{(e,e)\}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \downarrow$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad h = k^{-1} \in H \cap K = \{e\}$

14/10/2024
Patino

ES 5 (gruppi derivati)

G gruppo $\quad G' = \langle ghg^{-1}h^{-1} \mid g,h \in G \rangle$

G' sgr caratteristico di G. Se $N \triangleleft G$ e G/N abeliano $\Rightarrow G' \subseteq N$ ($G' < N$)

In questo senso G/G' è il più grande quoziente abeliano

Solutione:

G' caratteristico

questo dimostra che $\varphi(G') \subseteq G'$ che basta a concludere solo se G' è finito

$\varphi \in \mathrm{Aut}(G) \qquad \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} \in G'$

$[g,h] = ghg^{-1}h^{-1}$ "commutatore" $\qquad\qquad \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$

$H = \langle S \rangle \Rightarrow \varphi(H) = \langle \varphi(S) \rangle$

φ automorfismo, quindi $\varphi(g), \varphi(h)$ descrivono tutti gli elementi di G al variare di g e h

$G' = \langle [g,h] \mid g,h \in G \rangle = \langle [\varphi(g), \varphi(h)] \mid g,h \in G \rangle = G'$ ✓

<u>OSS:</u> G/G' è abeliano

$aG', bG' \in G/G' \qquad aG'bG' = bG'aG' \iff abG' = baG' \iff$

$\iff a^{-1}b^{-1}abG' = G' \iff [a^{-1}, b^{-1}] \in G'$ ✓ $\quad G/G'$ commutativo

Sia $N \triangleleft G \mid G/N$ abeliano, voglio $G' < N$

$\qquad\qquad \hookrightarrow \forall a,b \in G \quad aNbN = bNaN \iff [a^{-1}, b^{-1}] \in N$

$\Rightarrow G' < N \qquad$ (<u>OSS</u> $H = \langle S \rangle$ e $L < G \mid S \subset L \Rightarrow H < L$)

ES 3 (Teo di Poincaré)

G gruppo, $H < G \quad [G:H] = n$

Allora esiste $N \triangleleft G$, $N \subset H \mid \; |G/N| \mid n!$

$G \circlearrowleft G/H \quad \rightsquigarrow \varphi : G \to S_{G/H} \cong S_n$

omomorfismo di gruppi

$x.aH = xaH$
(è ben definito)

$\ker\varphi \triangleleft G \qquad \ker\varphi < H$
$\qquad\qquad\qquad xH = H \Rightarrow x \in H$

$\qquad\qquad\qquad (H = \mathrm{Stab}_G(H))$, $H \in G/H$

$G/\ker\varphi \overset{\bar\varphi}{\hookrightarrow} S_n \qquad \bar\varphi(G/\ker\varphi) < S_n \qquad |G/\ker\varphi| = |\bar\varphi(G/\ker\varphi)| \mid n!$ (Lagrange)

ES 1

G gruppo finito, $H < G$ | $[G:H] = p \to$ più piccolo primo che divide $|G| \Rightarrow H \triangleleft G$

(si può verificare che è davvero una permutazione)

$\varphi : x \longmapsto \varphi_x \in S(G/H)$
$aH \longmapsto xaH$

$G \circlearrowleft G/_H \rightsquigarrow \varphi : G \to S_p$ omo.

$\varphi|_H : H \to S_{p-1}$ (fissa la classe laterale H e permuta le altre)

$MCD(|S_{p-1}|, |G|) = 1$

$\varphi(H) < S_{p-1} \Rightarrow |\varphi(H)| \mid (p-1)!$, $|\varphi(H)| \mid |H| \Rightarrow |\varphi(H)| = 1$

$\varphi(H) \cong H/\ker\varphi$

↳ se è coprimo con $|G|$ lo è anche con $|H|$

$\varphi|_H(h) = id$

$\Rightarrow H = \ker \varphi|_H$

$G > \ker\varphi > H$, ma $[G:H]$ è primo $\Rightarrow G = \cancel{\ker\varphi}$ (imp.) $\vee$ $H = \ker\varphi$

$aH = H \Rightarrow a \in H$

$\Downarrow$

$H \triangleleft G$

OSS $(|G|, |H|) = 1$

$\varphi : G \to H$ omomorfismo è triviale $\varphi(g) = e \ \forall g \in G$

ES 2

G gruppo, $|G| < +\infty$, $p \mid |G|$

$X = \{ (g_1 \cdots g_p) \in G^p \mid g_1 \cdots g_p = e \}$

Teo di Cauchy: $\exists g \mid G \mid g^p = e \iff \exists x \in X \mid x = (g\, g \cdots g),\ g \neq e$

$\mathbb{Z}/_{p\mathbb{Z}} \circlearrowleft X$

$\bar{1}(g_1 \cdots g_p) = (g_2\, g_3 \cdots g_p\, g_1)$

$\bar{k}\,(g_1 \cdots g_p) = (g_{k+1} \cdots g_p\, g_1 \cdots g_k)$

$|Orb(x)| = \dfrac{|\mathbb{Z}_p|}{\mathbb{Z}_{\mathbb{Z}_p}(x)}$

↓ per cui valgono tutti p

$$|X| = \sum_{x \in R} |Orb(x)| = \sum_{\substack{R \ni x \\ |Orb(x)|=1}} |Orb(x)| + \sum_{\substack{x \in R \\ |Orb(x)|>1}} |Orb(x)| \quad ⊛$$

$$p \mid \sum_{\substack{x \in R \\ |Orb(x)|>1}} |Orb(x)| = \sum_{\substack{x \in R \\ |Orb(x)|=p}} |Orb(x)|$$

$|X| = |G|^{p-1}$ (basta scegliere una $(p-1)$-upla e prendere come ultimo elemento l'inverso)

$\Rightarrow p \mid |X|$

allora da ⊛ $p \mid \sum_{\substack{x \in R \\ |Orb(x)|=1}} |Orb(x)|$ = # di orbite con un solo elemento $\geq p \Rightarrow$ ne esiste uno non triviale

non può essere 0 perché c'è l'identità

$\square$

ES 4

Classificare i gruppi di ordine 10 ($C_{10} \cong \mathbb{Z}/10\mathbb{Z}$, D_5)

$10 = 2 \cdot 5$

Per Cauchy $\exists H < G$ di ordine 5
$H = \langle r \rangle$, con $ord(r) = 5$

$[G : H] = 2 \Rightarrow H$ normale

Per Cauchy $\exists s \neq e \mid s^2 = e$

$$|\langle r \rangle \langle s \rangle| = \frac{|\langle r \rangle| \cdot |\langle s \rangle|}{|\langle r \rangle \cap \langle s \rangle|} = 10 = |G|$$

$\langle r \rangle \langle s \rangle = G \Rightarrow G = \{ e \;\; r \;\; r^2 \;\; r^3 \;\; r^4 \;\; s \;\; rs \;\; r^2s \;\; r^3s \;\; r^4s \}$

Quanto fa sr?

$sr = r^k \iff r^{k-1} = s$ ↯
$sr = s \iff r = e$ ↯
$sr = r^2 s \iff srs = r^2$
$r = \underbrace{ss}_{e} r \underbrace{ss}_{e} = sr^2s = (srs)^2 = r^4$ ↯ analogamente non può essere $sr = r^3 s$

$\langle r \rangle \trianglelefteq G \Rightarrow c_s \in Aut(\langle r \rangle) \cong Aut(\mathbb{Z}/p\mathbb{Z})$
$\downarrow$
$p-1$ elementi

$c: G \to Aut(\langle r \rangle)$ omo
$g \mapsto c_g : x \to gxg^{-1}$

che divide 2

$c_s \in Aut(\langle r \rangle)$ ha ordine 2

$srs = r \iff rs = sr \rightarrow G$ è abeliano e c'è un solo gruppo abeliano di ord. 10
$srs = r^{-1} \iff sr = r^{-1}s = r^4 s$
$\downarrow$
come nel diedrale
$\varphi : D_5 \xrightarrow{\sim} G$
$r^k s^\varepsilon \mapsto r^k s^\varepsilon$

$\square$

ES 5

$|G| = 15 \Rightarrow G$ ciclico

$\exists r$ di ordine 5 $\quad H = \langle r \rangle \triangleleft G$ (indice minimo)
$\exists t$ di ordine 3

ha sempre senso considerarlo quando ho un sgr normale

$$\varphi: G \to Aut(H) \cong Aut(\mathbb{Z}/p\mathbb{Z}) \qquad p = 5$$
$$g \mapsto c_g$$

ha 4 elementi

$\varphi(t) = id_H \Rightarrow trt^{-1} = r \Rightarrow tr = rt$

perché t ha ord. 3

$$|\langle r \rangle \langle t \rangle| = \frac{|\langle r \rangle| \cdot |\langle t \rangle|}{|\langle r \rangle \cap \langle t \rangle|} = 15 = |G|$$

Teo di struttura (esiste un unico gruppo abeliano di cardinalità 15)

$\Rightarrow G = \langle r, t \rangle, \quad r, t \in Z(G) \Rightarrow G = Z(G) \Rightarrow G \cong C_{15}$

OSS I gruppi di ordine pq, p e q primi $p > q$ e $q \nmid p-1$ sono ciclici (stesso ragionamento dell'esercizio)

15/10/2024
Del Corso

PRODOTTO SEMIDIRETTO

H, K gruppi $\quad \varphi: K \to Aut(H)$ omo
$\qquad k \mapsto \varphi_k$

Si dice prodotto semidiretto di H e K via φ

$H \rtimes_\varphi K \quad (K \ltimes_\varphi H)$

il prodotto cartesiano $H \times K$ con l'operazione definita da

$$(h, k) \cdot (h', k') := (h\varphi_k(h'), kk')$$

NB! Posso scegliere un qualsiasi omo. tra K e Aut(H)

Prop: $H \rtimes_\varphi K$ è un gruppo

- chiuso per l'operazione
- (e_H, e_K) è l'el. neutro $\quad (e_H, e_K)(h,k) = (h,k)(e_H, e_K) = (h,k)$

$(h\varphi_k(e_H), ke_K) = (h,k)$

$(e_H\varphi_{e_K}(h), e_K k) = (e_H id(h), k) = (h,k)$

↳ e_K viene mandato da φ nell'identità di H (perché φ omomorfismo)

- ci sono gli inversi
↓
l'inverso di (h,k)

è $(\varphi_k^{-1}(h), k^{-1}) = (\varphi_{k^{-1}}(h^{-1}), k^{-1}) \qquad \varphi$ omo $\varphi_{e_K} = id$

$(h,k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), e_K) \overset{!}{=} (h\varphi_{kk^{-1}}(h^{-1}), e_K) = (e_H, e_K)$

OSS 1

$H \rtimes_\varphi K$ è il prodotto diretto $\iff \varphi_k = id \quad \forall k \in K$ $\Rightarrow$ φ è l'omomorfismo stupido che manda ogni elemento di K nell'identità di H

OSS 2 $\bar{H} = H \times \{e_K\}$ $\quad$ $\bar{H}, \bar{K} < G$
$\bar{K} = \{e_H\} \times K$

Dim.
- $(h, e_K)(h', e_K) = (h\varphi_{e_K}(h'), e_K) = (hh', e_K) \in \bar{H}$
- $(e_H, e_K) \in \bar{H}$
- $(h, e_K)^{-1} = (\varphi_{e_K}(h^{-1}) e_K) = (h^{-1}, e_K) \in \bar{H}$

$\bar{H} \triangleleft H \rtimes_\varphi K = G$ infatti è il $\ker \pi$ dove $\pi: G \to K$, $(h,k) \mapsto k$

$G \to H$, $(h,k) \mapsto h$ NON è un omomorfismo

$(h k) \mapsto h$
$(h' k') \mapsto h'$
$(h k)(h', k') \mapsto h\varphi_k(h')$
e in generale $\cancel{k}\varphi_k(h') \neq \cancel{k}h'$

OSS 3 $\bar{H} \cdot \bar{K} = G$
$\bar{H} \cap \bar{K} = (e_H, e_K)$

Teorema G gruppo, $H, K \leq G$

1) $H \triangleleft G$
2) $HK = G$ $\quad \Rightarrow \quad G \cong H \rtimes_\varphi K$
3) $H \cap K = \{e\}$

$$\boxed{\begin{array}{l} \varphi: K \to Aut(H) \\ k \mapsto \varphi_k: h \to khk^{-1} \end{array}}$$

DIM. $G \xleftarrow{F} H \rtimes_\varphi K$
$hk \longleftarrow (h,k)$

- F omo:

$F((h,k)\cdot(h',k')) = F(hk)F(h',k')$

$\quad = F(h\varphi_k(h'), kk')$ $\qquad$ $= hkh'k'$ $\qquad$ $kh'\cancel{k'}\cancel{k}$

$\quad = \cancel{h}\varphi_k(h')k\cancel{k'} \stackrel{?}{=} \cancel{h}kh'\cancel{k'} \iff \varphi_k(h')k = kh'$ ✓

- F surgettivo $\Rightarrow$ garantito dall' ipotesi 2 ✓
- F iniettivo

$F(h,k) = hk = e_G \iff h = k^{-1} \in H \cap K = \{e_G\} \Rightarrow h = k = e_G$ ✓

□

$G = H \rtimes_\varphi K$ $\qquad$ $\varphi: K \to Aut(H)$

$\bar{H} \triangleleft G, \ \bar{K} < G$ $\qquad$ $\bar{\varphi}: \bar{K} \to Aut(\bar{H})$
$(e_H, k) \mapsto \bar{\varphi}_k: (h, e_K) \mapsto (\varphi_k(h), e_K)$

$(e_H, k)(h, e_K)(e_H, k^{-1}) = (\varphi_k(h), k)(e_H, k^{-1}) = (\varphi_k(h), e_K)$
↑
quello dato dalla φ di partenza

$G \cong \bar{H} \rtimes_{\bar{\varphi}} \bar{K}$ $\qquad$ $\bar{H}\bar{K} = G$
$\bar{H} \cap \bar{K} = (e_H, e_K)$

$H \rtimes_\varphi K \cong \bar{H} \rtimes_{\bar{\varphi}} \bar{K}$
$\qquad\qquad\qquad\qquad \downarrow$
$\qquad\qquad\qquad$ coniugio

Per il teo. $G \cong \bar{H} \rtimes_{\bar{\varphi}} \bar{K}$ $\quad \bar{\varphi}: \bar{K} \to Aut(\bar{H})$

$$(e_H, k) \mapsto \varphi_k \; (: (h, e_K) \mapsto (e_H, k)(h, e_K)(e_H, k^{-1}))$$

$$= (\varphi_k(h), k)(e_H, k^{-1}) = (\varphi_k(h), e_K)$$

Esempio 1

$S_n \cong A_n \rtimes_\varphi \langle (12) \rangle$

A_n ha indice minimo

(i) $A_n \trianglelefteq S_n \quad K = \langle (12) \rangle < S_n$

(ii) $A_n \langle (12) \rangle = S_n$

(iii) $A_n \cap \langle (12) \rangle = \{e\}$

$$\varphi : \langle (12) \rangle \to Aut(A_n)$$
$$e \mapsto id_{A_n}$$
$$(12) \mapsto \varphi_{(12)} \quad (\sigma \mapsto (12)\sigma(12))$$

Esempio 2

$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$

$H = \langle r \rangle \trianglelefteq D_n$

$K = \langle s \rangle < D_n$

$HK = D_n$

$H \cap K = \{id\}$

$D_n \cong \langle r \rangle \rtimes_\psi \langle s \rangle$

$$\psi : \langle s \rangle \to Aut(\langle r \rangle)$$
$$e \mapsto id_{\langle r \rangle}$$
$$s \mapsto \varphi_s \; (r \mapsto srs = r^{-1})$$

$$\varphi : \mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$
$$(1 \to \bar{a}) \mapsto \bar{a}$$

$\left((\mathbb{Z}/n\mathbb{Z})^* \text{ ciclico SSE } n = 2, 4, p^k, 2p^k \quad p \text{ primo dispari} \right)$

dimostrato nella prossima lezione

$$(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\varphi : \bar{1} \mapsto \varphi_{\bar{1}} \; [1]_n \to [-1]_n$$

Esempio 3

Gruppi di ordine pq, p e q primi distinti $(q>p)$

$|G| = pq$

Per Cauchy $\exists\, x, y \in G \mid \begin{array}{l} \mathrm{ord}(x) = q \\ \mathrm{ord}(y) = p \end{array}$

$H = \langle x \rangle$, $K = \langle y \rangle$

$H \cap K = \{e\}$ $HK = G$ perche' $|HK| = \dfrac{|H|\cdot|K|}{|H\cap K|} = qp$

H è normale perche' ha indice il più piccolo primo che divide $|G|$

(è anche caratteristico perche' è l'unico sgr di quell'ordine).

$\Rightarrow G \cong H \rtimes_\varphi K$ $\quad \varphi : K \to \mathrm{Aut}(H)$

$\mathbb{Z}/_{q\mathbb{Z}} \rtimes_\varphi \mathbb{Z}/_{p\mathbb{Z}}$ Vado a guardare le possibili φ

$\underset{\text{ord } p}{\varphi : \langle y \rangle} \to \underset{\text{ord } q-1}{\mathrm{Aut}(\langle x \rangle)} \cong \mathbb{Z}/_{q-1}$

$\varphi_0 : y \mapsto id$
$\quad x \mapsto yxy^{-1} = x \leadsto \mathbb{Z}/_{pq\mathbb{Z}}$

$p \nmid q-1 \Rightarrow G \cong \mathbb{Z}/_{pq\mathbb{Z}}$

$p \mid q-1 \Rightarrow \psi : \langle y \rangle \to \mathrm{Aut}(\langle x \rangle)$
$\quad y \mapsto \varphi_y \quad x \mapsto x^{\ell}$

$(\ell, q) = 1$

$\mathrm{ord}(\varphi_y) = \mathrm{ord}\,\ell = p$ $\qquad \mathrm{ord}\,\varphi_y = k \Leftrightarrow \varphi_y^k = id$ k minimo

$\varphi_y^k(x) = x^{\ell^k} = x \Leftrightarrow \ell^k \equiv 1\ (q)$

Se $\varphi_y \neq id$, allora il suo ordine deve essere necessariamente p. Affinche' ciò sia vero lo deve essere anche l'ordine di ℓ, per questo motivo

16/10/2024

Teorema di struttura dei gruppi abeliani finiti

G gruppo abeliano finito $\Rightarrow G \cong \mathbb{Z}/_{n_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{n_s\mathbb{Z}}$ e questa scrittura è unica se $n_{i+1} \mid n_i \quad \forall i = 1, \dots, s-1$

($G = H \times K \Rightarrow Z(G) = Z(H) \times Z(K) \Rightarrow$ il prodotto di gruppi ciclici è sempre abeliano)

Es. $|G| = 2^3 \cdot 3^2$ abeliani

$\mathbb{Z}/_{72\mathbb{Z}}$, $\mathbb{Z}/_{12\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}}$, $\mathbb{Z}/_{24\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$, $\mathbb{Z}_{36} \times \mathbb{Z}_2$

$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \times \mathbb{Z}_6$

$\mathbb{Z}_{18} \times \mathbb{Z}_4 \cong \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \cong$
$\cong \mathbb{Z}_{36} \times \mathbb{Z}_2$

Schema di dimostrazione:

$G(p) = \{ x \in G \mid \operatorname{ord} x = p^k \text{ per qualche } k \}$ p primo t.c. $p \mid |G|$

↳ p-gruppo (per Cauchy non è banale), caratteristico in G (perché gli automorfismi conservano l'ordine)

↳ negli abeliani è un sgr. perché $\operatorname{ord}(xy) \mid \operatorname{mcm}[\operatorname{ord}(x), \operatorname{ord}(y)]$ nei non abeliani in generale non lo è

TEO 1

G abeliano, $|G| = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ p_i primi $p_i \neq p_j \quad \forall i \neq j$

$\Rightarrow G \cong G(p_1) \times \dots \times G(p_r)$ ← "componenti di p-torsione"

Tale decomposizione è unica a meno dell'ordine dei fattori

TEO 2

G p-gruppo abeliano

$\exists$ e sono unici $r_1 \geq r_2 \geq \dots \geq r_t \mid G \cong \mathbb{Z}/_{p^{r_1}\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p^{r_t}\mathbb{Z}}$

TEO 1 + TEO 2 $\Rightarrow$ Teo. di struttura

$|G| = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$

$$G \cong G(p_1) \times \dots \times G(p_r) \cong \begin{array}{l} \mathbb{Z}_{p_1^{h_{11}}} \times \dots \times \mathbb{Z}_{p_1^{h_{1t_1}}} \\ \vdots \\ \mathbb{Z}_{p_r^{h_{r1}}} \times \dots \times \mathbb{Z}_{p_r^{h_{rt_r}}} \end{array}$$

↓

$\mathbb{Z}/_{n_1\mathbb{Z}}$

$n_1 = \prod_{i=1}^{r} p_i^{h_{i1}}$

$n_j = \prod_{i=1}^{r} p_i^{h_{ij}}$

$\cong \mathbb{Z}/_{n_1} \times \mathbb{Z}/_{n_2} \times \dots \times \mathbb{Z}/_{n_t}$ $\quad t = \max\{t_i\}$

Es. $|G| = 2^3 \cdot 3^2$

$G \cong G(2) \times G(3)$

$G(2) \cong \begin{matrix} \mathbb{Z}_8 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \end{matrix} \qquad G(3) = \begin{matrix} \mathbb{Z}_9 \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \end{matrix}$ $\quad 3 \cdot 2$ possibilità

$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \to \mathbb{Z}_{36} \times \mathbb{Z}_2$

$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_{12} \times \mathbb{Z}_6$

$\boxed{\text{TEO}}$ $(\mathbb{Z}_n)^*$ è ciclico $\iff n = 2, 4, p^k, 2p^k$ $\quad$ p primo dispari, $k \geq 0$

$(\mathbb{Z}/_{p\mathbb{Z}})^*$ è ciclico

(es. preliminare 10 di aritmetica) $\to$ G abeliano, $x, y \in G$, $\text{ord}\, x = m$, $\text{ord}\, y = n$ $\Rightarrow \exists\, z \in G \mid \text{ord}\, z = [m, n]$

Sia $h = \max \{\text{ord}\, x \mid x \in (\mathbb{Z}/_{p\mathbb{Z}})^*\} \Rightarrow \forall x \in (\mathbb{Z}/_{p\mathbb{Z}})^* \Rightarrow \text{ord}\, x \mid h$

$\forall x \in \mathbb{Z}_p^* \quad x^h = \bar{1}$

$p(t) = t^h - 1 \in \mathbb{F}_p[x]$

ha in $\mathbb{F}_p$ $p-1$ radici $\Rightarrow p - 1 \leq \underset{\text{numero max di radici}}{h} \mid p-1 \Rightarrow h = p-1$

$\Rightarrow$ $(\mathbb{Z}/_{n\mathbb{Z}})^*$ ciclico $\qquad$ Dal teo. cinese: $\mathbb{Z}/_{a\mathbb{Z}} \times \mathbb{Z}/_{b\mathbb{Z}} \cong \mathbb{Z}/_{ab\mathbb{Z}} \iff (a,b) = 1$

$\downarrow$ posso farlo se n non è potenza di un primo

$n = ab \quad (a,b) = 1 \quad \begin{matrix} a > 1 \\ b > 1 \end{matrix}$ $\qquad ([1]_a, [1]_b) \leftarrow [1]_{ab}$

$\mathbb{Z}_n^* \cong \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ $\qquad \mathbb{Z}_a^* \times \mathbb{Z}_b^* \cong \mathbb{Z}_{ab}^*$

$a > 2$ e $b > 2 \Rightarrow \varphi(a)$ e $\varphi(b)$ pari

$\alpha \in \mathbb{Z}_a^* \quad \text{ord}\, \alpha = 2$

$\beta \in \mathbb{Z}_b^* \quad \text{ord}\, \beta = 2$ $\qquad$ un gruppo ciclico ha $\varphi(2)$ elementi di ord 2

$(\alpha, 1) \; (1, \beta) \; (\alpha, \beta)$ hanno ord 2 $\lightning$

$\Rightarrow n = p^k$
$\quad n = 2p^k$

Ora voglio far vedere che p deve essere $\neq 2$...

$\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$\mathbb{Z}/_{2^n\mathbb{Z}}^{*}$ ha un quoziente isomorfo a $\mathbb{Z}_8^*$ — Perché i quozienti di gruppi ciclici sono ciclici

$n \geq 3 \Rightarrow (\quad)^* \cdots (\mathbb{Z}_8)^*$

($\Leftarrow$)

p dispari $(\mathbb{Z}_{p^k})^*$ è ciclico

$\hookrightarrow$ ha ordine $\varphi(p^k) = (p-1)p^{k-1}$

Basta mostrare che $\exists\, x,y \in (\mathbb{Z}/_{p^k\mathbb{Z}})^*$ $\text{ord}\,x = p-1$, $\text{ord}\,y = p^{k-1}$ (a quel punto come generatore andrà bene il prodotto)

$\pi : \mathbb{Z}_{p^k} \to \mathbb{Z}_p$
$[x]_{p^k} \mapsto [x]_p$

riesco a far passare l'omo agli star?

$\text{ord}\,\pi(x) = p-1 \Rightarrow \text{ord}\,\pi(x) \mid \text{ord}\,x \Rightarrow$ in $\langle x \rangle$ c'è un elemento di ord. $p-1$

$\pi : \mathbb{Z}_{p^k}^* \to \mathbb{Z}_p^*$
$[x]_{p^k} \mapsto [x]_p$

è ancora un omo surgettivo

$\exists\, \bar{x} \in \mathbb{Z}_p^*$ $\text{ord}\,\bar{x} = p-1$

$x \in \mathbb{Z}_{p^k}^* \mid \pi(x) = \bar{x}$

$p-1 = \text{ord}\,\bar{x} \mid \text{ord}\,x$ quindi per x OK!

Per trovare un y di ordine p^{k-1} lo esibisco esplicitamente:

$y = 1+p$

$y^{p^{k-1}} = 1$

$y^{p^{k-2}} \neq 1$

mi basta controllare questo perché se fosse $y^{p^{k-i}} = e$, con $i > 2$ avrei $y^{p^{k-2}} = \left(y^{p^{k-i}}\right)^{p^{i-2}} = e^{p^{i-2}} = e$

~~$(1+p)^{p^h} \equiv 1 + p^{h+1} \quad (p^{h+2})$~~

~~$(1+p)^p = 1 + \binom{p}{1}p + \binom{p}{2}p^2 + \dots + p^p$~~

~~$(1+p)^{p^h} = \left((1+p)^{p^{h-1}}\right)^p = (1 + p^h + \alpha p^{h+1})^p \quad (p^{h+2})$~~

~~$= 1 + \binom{p}{1}(p^h + \cancel{\alpha p^{h+1}}) \dots \quad (p^{h+2})$~~

~~$= 1 + p^{h+1} \quad (p^{h+2})$~~

vedi appunti sull'ipad

~~$(1+p)^{p^{k-2}} = 1 + p^{k-1} \quad (p^k)$~~

~~$(1+p)^{p^{k-1}} = 1 + p^k \quad (p^{k+1})$~~

~~$\equiv 1 \quad (p^k)$~~

comunque il senso è dimostrare per induzione

$(1+p)^{p^n} \equiv 1 + p^{n+1} \quad (p^{n+2})$

da cui deriva facilmente quello che vogliamo.

$|G| = p \cdot q \quad q > p \quad$ Per Cauchy $\exists\, x, y \in G \quad \text{ord}\, x = q$, $\text{ord}\, y = p$

$p \nmid q-1 \qquad H = \langle x \rangle \quad K = \langle y \rangle$

$G = HK \quad H \triangleleft G \quad H \cap K = \{e\} \qquad \mathbb{Z}_q^* \cong \mathbb{Z}_{q-1}$

$G = H \rtimes_\varphi K \qquad \varphi : K \to \text{Aut}(H)$

$y \mapsto 1 \quad \to$ prodotto diretto $\Rightarrow G \cong \mathbb{Z}_{pq}$ (ciclico)

$y \mapsto$ elem. di ord $p \qquad p \mid q-1$

$|G| = 21 \quad p = 3 \quad q = 7 \quad 3 \mid 7-1$

$\Phi : \mathbb{Z}_3 \to \text{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6$

$\bar{1} \mapsto \varphi$ — id; $x \mapsto x^\ell$

$\varphi^3(x) = x^{\ell^3} \qquad \ell^3 \equiv 1 \ (7)$

$\varphi^3(1) = \ell^3 \qquad \ell^3 \equiv 1 \ (7) \quad \ell$ ha ord 3

$\ell = 2, 4$

(1 0)(0 1) $\quad G_2 = \mathbb{Z}_7 \rtimes_\varphi \mathbb{Z}_3 \qquad \mathbb{Z}_3 \to \text{Aut}\, \mathbb{Z}_7$

$\bar{1} \mapsto \varphi \quad 1 \mapsto 2$

(0 1)(0 2) $\quad G_4 = \mathbb{Z}_7 \rtimes_\psi \mathbb{Z}_3 \qquad \mathbb{Z}_3 \to \text{Aut}\, \mathbb{Z}_7$

$\bar{1} \mapsto \psi \quad 1 \mapsto 4$

$(a\ b)(c\ d) \overset{\varphi}{=} (a + \varphi_b(c),\ bd)$

$\overset{\psi}{=}$

$(a + \psi_b(c),\ bd)$

vale anche per il prodotto di più di 2 primi distinti

21/10/2024
Patino

$|G| = pq,\ p \neq q \quad G$ abeliano $\Rightarrow G$ ciclico

LEMMA $\to x, y \in G$ commutanti, $m = \text{ord}\, x \quad n = \text{ord}\, y$

$(m, n) = 1 \Rightarrow \text{ord}(xy) = mn$

$(xy)^{mn} = x^{mn} y^{mn} = e$

$d = \text{ord}(xy) \quad d \mid mn$

$e = (xy)^d = x^d y^d \Rightarrow x^d = y^{-d} \in \langle x \rangle \cap \langle y \rangle = \{e\}$

$|\langle x \rangle \cap \langle y \rangle|$ divide sia m che $n \Rightarrow$ è uguale ad 1

$m|d,\ n|d \Rightarrow d = mn$

- Se $xy \neq yx$? <u>ES</u> $D_n = \langle rs \rangle$ s, rs hanno ord 2 $rss = r \Rightarrow$ ord n
- Se m,n non coprimi?

  $d \mid mcm(m,n)$

  x, x^{-1} $ord(x \cdot x^{-1}) = 1$

Esercizio $\rightarrow m = ord\,x$ $n = ord\,y$ $\frac{mn}{(m,n)^2} \mid ord(x \cdot y)$ (x e y commutano)

Esercizio 7

dimostrare che esiste una bigezione

$$\{\varphi : D_n \to G \text{ omo}\} \leftrightarrow \left\{(x,y) \in G^2 \;\middle|\; \begin{matrix} x^n = e = y^2 \\ yxy = x^{-1} \end{matrix}\right\}$$

GRUPPI DEFINITI DA GENERATORI & RELAZIONI

Gruppi liberi

Def F_n gruppo libero su n generatori è il gruppo in cui gli elementi sono le parole nell'alfabeto $\{x_1^{\pm 1}, \dots, x_n^{\pm 1}\}$ e l'op. di gruppo è la concatenazione

$$F_n = \{ x_{i_1}^{\varepsilon_1} \cdot x_{i_2}^{\varepsilon_2} \cdots x_{i_\ell}^{\varepsilon_\ell} \}$$

$\ell \in \mathbb{N}$
$i_j \in \{1, \dots, n\}$
$\varepsilon_j \in \{\pm 1\}$

<u>OSS</u> $\emptyset \in F_n$ è l'elemento neutro

- $F_1 = \{ x^{\pm k} \mid k \in \mathbb{Z} \} \cong \mathbb{Z}$

$F_2 \ni xyxy^{-1} = g$

$g^{-1} = yx^{-1}y^{-1}x^{-1}$

$gg^{-1} = xyx\cancel{y^{-1}}\cancel{y}\cancel{x^{-1}}\cancel{y^{-1}}\cancel{x^{-1}} = \emptyset$

Def. Una parola in F_n si dice RIDOTTA se non contiene una sottoparola del tipo $x_i x_i^{-1}$ o $x_i^{-1} x_i$

$F_n \cong \{\text{parole ridotte}\}$

gli x_i $i = 1, \dots, n$ sono i generatori di F_n

PROPRIETÀ UNIVERSALE $Hom(F_n, G) \cong \{(g_1, \dots, g_n) \in G^n\}$

$\varphi \longmapsto (\varphi(x_1) \cdots \varphi(x_n))$

verifica che definisce un unico omo. $\rightarrow (\varphi : x_i \to g_i) \longleftarrow (g_1, \dots, g_n)$

$\varphi: F_2 \to D_n$ $\quad \varphi$ surg.
$x_1 \mapsto r$
$x_2 \mapsto s$

$\varphi: F_2/_{\ker\varphi} \xrightarrow{\sim} D_n \qquad \ker\varphi = ?$

$x_2^2, x_1^n, \; x_2 x_1 x_2 x_1 \in \ker\varphi$
$\downarrow$
CLAIM: $\ker\varphi$ è il più piccolo gruppo normale che contiene $x_2^2, x_1^n, x_2x_1x_2x_1$

Equivalentemente $\ker\varphi = \langle$ coniug. di $x_2^2, x_1^n, x_2x_1x_2x_1 \rangle$

$\varphi(x_2 x_1^n x_2^{-1}) = ses = e$

OSS. se $\forall g \in G$ $gSg^{-1} = S \Rightarrow$
$\Rightarrow \langle S \rangle \lhd G$

DIM. $N = \langle$ coniugati di $x_2^2, x_1^n, x_2x_1x_2x_1 \rangle \lhd F_2$

Dimostriamo $N = \ker\varphi$. Supponiamo $N \subset \ker\varphi$

Supponiamo valga il contenimento stretto

Mi basta mostrare che $|F_2/_N| \leq 2n$
$\hookrightarrow$ chi sono i suoi elementi?

sono $x_1^{a_1} x_2^{a_2} x_1^{a_3} \dots x_2^{a_e} N \quad a_i \in \mathbb{Z}$

$0 \leq a_{2n+1} < n$
$0 \leq a_{2n+2} < 1$

inoltre, $x_1^a x_2^b N = x_1^{a-1}(x_1x_2)x_2^{b-1} N = x_1^{a-1} x_2 x_1^{-1} x_2^{b-1} N =$
$= x_2 x_1^{-a} x_2^{b-1} N = x_2^b x_1^{(-1)^b a} N$

Quindi $\exists\ 0 \leq a < n,\ 0 \leq b \leq 1 \mid \delta = x_2^b x_1^a N$

Quindi $|F_2/_N| = 2n \Rightarrow N = \ker\varphi$

TORNANDO ALL'ESERCIZIO

$$\begin{tikzcd} D_n \arrow[r, "\psi"] & G \\ F_2 \arrow[u, "\varphi"] \arrow[ur, "\psi\circ\varphi"'] & \end{tikzcd} \qquad F_2 \to G$$

$\psi\circ\varphi$
$\cap$
$\mathrm{Hom}(F_2, G) \xrightarrow{\sim} \{(g_1 g_2) \in G\}$

$\mathrm{Hom}(D_n, G) = \{f: F_2 \to G \mid \ker f \supset N\}$
$\shortparallel$
$\mathrm{Hom}(F_2/_N, G) \cong \{(g_1 g_2) \in G \mid g_1^n = e,\ g_1g_2g_1g_2 = e,\ g_2^2 = e\}$

$\mathrm{Hom}(F_2, G) \xrightarrow{\sim} G^2$
$\cup$
$\mathrm{Hom}(D_n, G) \to$
$f \longmapsto (f(x_1), f(x_2))$

i generatori di N sono nel ker

$N \subset \ker f$ se $\underset{g_1^n}{f(x_1^n)} = e$, $\underset{g_2^2}{f(x_2^2)} = e$, $\underset{g_1 g_2 g_1 g_2}{f(x_1 x_2 x_1 x_2)} = e$

$\mathrm{Hom}(D_n, G) \cong \{(g_1, g_2) \mid g_1^n = e,\ g_2^2 = e\ \ g_1 g_2 g_1 g_2 = e\} \subset G^2$

$\cong$

$\mathrm{Hom}(F_2/N, G) \cong \{\varphi : F_2 \to G \mid N \subset \ker\varphi\} \subset \mathrm{Hom}(F_2, G)$

Def. $G = \langle \underset{\text{generatori}}{x_1, \dots, x_n} \mid r_1, \dots, r_k \rangle$

è il quotiente di F_n per il più piccolo gr. normale che contiene $r_1, \dots, r_k$

ES $D_n = \langle x_1, x_2 \mid x_1^n,\ x_2^2,\ x_1 x_2 x_1 x_2 \rangle$

$\mathbb{Z}/p\mathbb{Z} = \langle x \mid x^p \rangle$

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} = \langle x, y \mid x^p, y^q, [x,y] = xyx^{-1}y^{-1} \rangle$

NB! la def. non è unica

$D_n \cong \langle s, t \mid s^2, t^2, (st)^n \rangle$

$S_n = \langle x_1, \dots, x_n \mid \cdots \rangle$

Ex 8 Trovare quante classi di isomorfismo di gruppi di ordine pq ci sono in cui p, q primi e $q \mid p-1$

in G

$\exists x \mid |\langle x \rangle| = p$

$\exists y \mid |\langle y \rangle| = q$ $\quad \langle x \rangle \triangleleft G \quad \langle x \rangle \cong \mathbb{Z}_p$

$yxy^{-1} = x^i$

$c_y \in \mathrm{Aut}(\langle x \rangle) \cong \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}/_{p-1}\mathbb{Z}$

coniugio $\quad \mathrm{ord}(c_y) \mid q$

c_y corrisponde ad un multiplo di $\left(\frac{p-1}{q}\right) \Rightarrow q$ possibilità

$J(c_y) = \bar{0}$

$c_y(x) = G \Rightarrow G$ abeliano (hp:) $\Rightarrow G$ ciclico

Se $J(c_y) \neq 0$

$G = \langle x \rangle \rtimes_\varphi \langle y \rangle \qquad \varphi = c_y$

Voglio dimostrare che $\forall i \in \mathbb{Z}/p\mathbb{Z}^*$ con $\mathrm{ord}(i) = q$, $\mathrm{ord}(j) = q$

$G_i = \mathbb{Z}_p \rtimes_{\varphi_i} \mathbb{Z}_q \cong G \qquad \mathbb{Z}_p \rtimes_{\varphi_j} \mathbb{Z}_q$

$\varphi_i(\bar{1} = i \in \mathbb{Z}_p)$ $\varphi_j(\bar{1}) = j \in \mathbb{Z}_p^*$

Voglio descrivere G_i per generatori e relazioni

CLAIM $G_i = \langle x\, y \mid x^p, y^q, yxy^{-1}x^{-i} \rangle$

Dim $N \triangleleft F_2$ più piccolo gruppo normale che contiene

$x^p, y^q, yxy^{-1}x^{-i}$

$G_i \cong F_2/M$ $M \triangleleft F_2$ $N \subset M$

$M = N$, mi basta $|F_2/N| \leq pq$

$\sigma \in F_2/N$ è $x^{a_1} y^{a_2}, \dots y^{a_e} \in \mathbb{N}$

Uso la rel. per scrivere $\sigma = x^a y^b N$

$\hookrightarrow yxy^{-1}x^{-i} \in \mathbb{N}$

Infatti: $yxy^{-1}x^{-i} N = N \iff x^{-1}y^{-1} N = y^{-1}x^{-i} N$

$\iff yxN = x^i y N$

$|F_2/N| \leq pq \Rightarrow N = M$ □

dimostro $G_i \cong G_j$

$\mathrm{Hom}(G_i, G_j) \simeq \left\{ (x_1 x_2) \in G_j^2 \;\middle|\; \begin{array}{l} x_1^p = e \\ x_2^q = e \\ x_2 x_1 x_2^{-1} = x_1^i \end{array} \right\}$

$x_1 = x \in G_j$
$x_2 = y^k \in G_j$

$y^k x y^{-k} = x^{i} \iff x^i = x^{j^k}$

Definisce un morfismo se $j^k \equiv i \ (q)$

$j, i \in \mathbb{Z}_p^*$ di ordine q: j e i uno multiplo dell'altro

perche' $\mathbb{Z}_p^*$ ciclico $\Rightarrow$ posso sempre trovare k

Ho trovato un omo suriettivo tra G_i e $G_j \Rightarrow$ iso □

TEOREMA DI SYLOW

G gruppo finito

È vero il viceversa? $\forall d \mid |G| \; \exists H \leq G \; |H| = d$?

- Lagrange $\forall H \leq G \Rightarrow |H| \mid |G|$
- Se G ciclico $\forall d \mid |G| \; \exists! H \leq G \mid |H| = d$
- Se G è qualsiasi e $d = p$ primo $\mid p \mid |G| \; \exists x \in G \; o(x) = p$
- G abeliano

G ciclico, $|H| = 45$ $\quad H = \{e\} \cup H_3 \cup \underbrace{H_5}_{\text{elementi di ordine 15}} \cup H_{15} \cup H_{45}$

$G = G_{p_1} \times \dots \times G_{p_r}$ $\quad |G| = p_1^{e_1} \dots p_r^{e_r}$ $\quad G_p = \{x \in G \mid \text{ord}\, x = p^k \text{ per qualche } K\}$

G_p componenti di p-torsione

$G_p = \prod_{j=1}^{n} \mathbb{Z}/p^{d_j}$ $\qquad d \mid |G| \Rightarrow d = p_1^{c_1} \dots p_r^{c_r}$

$0 \leq c_i \leq e_i$

$\sum_j d_j = c \quad c \leq e = \sum_i e_i$

$G_p = \mathbb{Z}_{p^5} \times \mathbb{Z}_{p^4} \times \mathbb{Z}_{p^4} \times \mathbb{Z}_p$ $\qquad e = 14$

$d = p^{11}$

$H_p = \mathbb{Z}_{p^5} \times \mathbb{Z}_{p^4} \times p^2\mathbb{Z}/p^4\mathbb{Z} \times \{0\}$

$H = H_{p_1} \times \dots \times H_{p_r}$ $\qquad |H| = p_1^{c_1} \dots p_r^{c_r}$

$\downarrow \qquad\qquad \downarrow$

$p_1^{c_1} \qquad\quad p_r^{c_r}$

- In A_4 non ci sono sottogruppi di ordine 6

Per assurdo $\exists H \leq A_4 \quad |H| = 6$

$H \trianglelefteq A_4$ (indice 2)

$\exists \sigma \in H \quad \text{ord}\, \sigma = 2$ (Cauchy)

deve essere di ordine 2 e deve essere pari

$(a\,b)(c\,d) \quad Cl_{A_4}(\sigma) \subseteq H$

$|A_4| = |Cl_{A_4}(\sigma)| \cdot |Z_{A_4}(\sigma)|$

$Z_{A_4}(\sigma) = Z_{S_4}(\sigma) \cap A_4$ $\qquad |Z_{S_4}(\sigma)| = 8 \qquad 8 \nmid 12 = |A_4|$

$Cl_{A_4}(\sigma) \subseteq Cl_{S_4}(\sigma)$ $\qquad \Downarrow$

Posso concludere che

$|Z_{A_4}(\sigma)| = 4$ e $|Cl_{A_4}(\sigma)| = 3$

$V_4 = \{e, (12)(34), (13)(24), (14)(32)\} \subset H$ $\lightning$ $\quad 4 \nmid 6 = |H|$

max potenza di p che divide |G|

Def. $p^n \parallel |G|$ un sgr di G di ord. p^n è detto p-sottogruppo di Sylow

Teorema di Sylow

G gruppo finito $|G| = p^n \cdot m$ $(p,m)=1$, p primo

ESISTENZA $\forall\, 0 \leq \alpha \leq n$ $\exists\, H \leq G$ $|H| = p^\alpha$

INCLUSIONE $\forall\, 0 \leq \alpha \leq n-1$ ogni sgr di ordine p^α è incluso in un sgr di ordine $p^{\alpha+1}$

In particolare ogni p-sgr è contenuto in un p-Sylow

CONIUGIO Due qualsiasi p-Sylow di G sono coniugati

NUMERO $n_p = \#$ p-Sylow di G $\Rightarrow n_p = [G : N_G(S)]$ dove S è un p-Sylow $(n_p \mid |G|)$

$n_p \equiv 1 \ (p)$

M sottoinsieme qualunque

DIM. ESISTENZA $\mathcal{M} = \{ M \subseteq G \mid |M| = p^\alpha \}$

$$|\mathcal{M}| = \binom{p^n m}{p^\alpha} = \prod_{i=0}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i}$$

ho tirato fuori il primo termine

massimo esponente di p che divide $p^n m - i$

$$\mathrm{ord}_p(p^n m - i) = \mathrm{ord}_p(p^\alpha - i) \qquad i = 1 \dots p^\alpha - 1$$

$\mathrm{ord}_p(x) = k$ $p^k \parallel x$ (cioè $p^k \mid x$ e $p^{k+1} \nmid x$)

$i = p^\varepsilon \delta$ $\varepsilon < \alpha$ $(\delta, p) = 1$

$$p^\alpha - p^\varepsilon \delta = p^\varepsilon (p^{\alpha-\varepsilon} - \delta), \qquad p^{\alpha-\varepsilon} - \delta \equiv -\delta \ (p) \not\equiv 0$$

$$p^n m - p^\varepsilon \delta = p^\varepsilon \underbrace{(p^{n-\varepsilon} m - \delta)}_{\equiv -\delta \not\equiv 0 \ (p)}$$

$$\Rightarrow \left(p, \prod_{i=1}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i} \right) = 1 \qquad p^{n-\alpha} \parallel \left(\prod_{i=1}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i} \right) p^{n-\alpha}$$

$p^{n-\alpha} \parallel |\mathcal{M}|$ $\quad G \circlearrowright \mathcal{M}$

$$\varphi : G \to S(\mathcal{M})$$
$$g \mapsto \varphi_g \quad M \to gM$$

è bigettiva perché $\varphi_{g^{-1}}$ è la sua inversa

$$\mathcal{M} = \bigcup_{i=1}^{t} \mathrm{orb}\, M_i \qquad |\mathcal{M}| = \sum_{i=1}^{t} |\mathrm{orb}(M_i)|$$

$$\Rightarrow p^{n-\alpha} \parallel |\mathcal{M}| \Rightarrow \exists\, i \mid p^{n-\alpha+1} \nmid |\mathrm{orb}(M_i)|$$

$$p^{n-\alpha+i} \nmid |orb(M_i)| = \frac{|G|}{|St(M_i)|} = \frac{p^n m}{|St(M_i)|}$$

$$\Rightarrow p^\alpha \mid |St(M_i)| = s \qquad s \geq p^\alpha$$

$$\begin{aligned} St(M_i) &\to M_i \qquad \text{fisso } m \in M_i \\ g &\mapsto gm \end{aligned}$$

È una mappa iniettiva per la legge di cancellazione

$$gm = hm \iff g = h$$

$$p^\alpha \leq s = |St(M_i)| \leq |M_i| = p^\alpha \quad \Rightarrow \quad |St(M_i)| = p^\alpha$$

<u>INCLUSIONE E CONIUGIO</u>

S p-Sylow di G $\qquad X = \{\text{classi laterali di } S \text{ in } G\}$

$H \subseteq G \quad |H| = p^\alpha \qquad |X| = \frac{|G|}{|S|} = \frac{p^n m}{p^n} = m$

$$\begin{aligned} \varphi : H &\to S(X) \\ h &\mapsto \varphi_h : gS \to hgS \end{aligned}$$

$$X = \bigcup_{i=1}^{r} orb(g_i S)$$

$$m = |X| = \sum_{i=1}^{r} |orb\, g_i(S)| = \sum_{i=1}^{r} \frac{|H|}{|St_H(g_i S)|} = \sum_{i=1}^{r} p^{\alpha_i}$$

$\exists i \mid \alpha_i = 0 \qquad H = St_H(g_i S)$

$orb(g_i S) = \{g_i S\} \qquad \forall h \in H \quad hg_i S = g_i S$

$hg_i \in g_i S \Rightarrow h \in g_i S g_i^{-1} \quad \forall h \in H$

$\forall H \quad |H| = p^\alpha \quad 0 \leq \alpha \leq n \quad \exists g \in G \mid H \subseteq gSg^{-1}$

$\alpha = n$, H p-Sylow per cardinalità ho $H = gSg^{-1}$ (coniugio)

LEMMA: G p-gruppo

$H \lneq G \Rightarrow N_G(H) \supsetneq H$ (per induzione su $p^n \mid |G|$)

S p-Sylow che contiene H strettamente

Applico il lemma con $G = S$ $\qquad N_S(H) \supsetneq H$

$N_S(H)/H$ p-gruppo non banale, $\bar{x} \in N_S(H)/H$ $\quad ord\, \bar{x} = p$

$\pi^{-1}(\langle \bar{x} \rangle)$ è un sgr. di S di ordine $p^{\alpha+i}$ che contiene H

NUMERO $n_p = \#\, p\text{-Sylow} = [G : N_G(S)] \qquad n_p \mid |G|$

$\quad\quad\quad\quad\quad\quad \overset{\shortparallel}{\#\,\text{orb}(S)}$

$\quad\quad\quad\quad\quad\quad\quad \hookrightarrow$ coniugio

$$n_p \equiv 1 \quad (p)$$

$\phi : S \to S(X) \qquad X = \{p\text{-Sylow di } G\}$

$x \mapsto \varphi_x$

$T \to xTx^{-1}$

$$X = \bigcup_{i=1}^{f} \text{orb}(T_i)$$

$$n_p = |X| = \sum_{i=1}^{f} |\text{orb}(T_i)| = \sum_i \frac{\overset{p^n}{\shortparallel}{|S|}}{|St(T_i)|} = \sum_i p^{d_i}$$

Dico che c'è un'unica orbita banale $\Rightarrow n_p \equiv 1 \ (p)$

$$\text{orb}(S) = \{S\}$$

$T \in X \quad \text{orb}(T) = \{T\} \iff xTx^{-1} = T \quad \forall x \in S \Rightarrow S \subseteq N_G(T)$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \Downarrow$

$ST \leqslant G \Rightarrow |ST| = \dfrac{p^n \cdot p^n}{|S \cap T|} \;\Big|\; p^n \cdot m \qquad ST = TS$

$|S \cap T| = p^n \Rightarrow T = S$ $\square$

ESEMPIO

$|G| = 12 = 2^2 \cdot 3 \qquad P_2 \cong \begin{cases} \mathbb{Z}_4 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \end{cases} \qquad P_3 \cong \mathbb{Z}_3$

$P_2 P_3 = G$

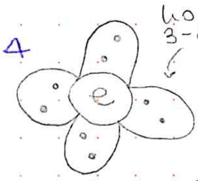
$P_3 \cong \mathbb{Z}_3$

$P_2 \cap P_3 = \{e\}$

$n_3 \equiv 1 \quad (3)$

$n_3 \mid 12 \qquad n_3 = \begin{cases} 1 & P_3 \trianglelefteq G \\ 4 \end{cases}$

ho 4 3-Sylow



$\Rightarrow$ ho 8 elementi di ordine 3

$12 - 8 = 4$ el.

P_2 è unico e quindi normale (non ho spazio per un altro p-Sylow)

$|G| = 12 \Rightarrow G \cong \mathbb{Z}_{12} \vee D_6 \vee \mathbb{Z}_6 \times \mathbb{Z}_2 \vee A_4 \vee \mathbb{Z}_3 \rtimes \mathbb{Z}_4$

$\quad D_6 \cong \mathbb{Z}_2 \times D_3 \qquad A_4 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3$

23/10/2024
Patimo

Esercizio 1

$$\sigma = (1\,2)(2\,3)\overset{(3\,4)}{\curlyvee}(4\,5)$$
$$\shortparallel$$
$$(1\,2\,3\,4\,5)$$

Esercizio 2

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 8 & 5 & 2 & 3 & 9 & 6 & 7 \end{pmatrix}$$

$$\sigma = (2\,4\,5)(3\,8\,6)(7\,9) = (2\,4)(4\,5)(3\,8)(8\,6)(7\,9)$$

Esercizio 3

\# K-cicli in S_n $(n \geq k)$

$\sigma = (a_1, \dots a_k)$ $\quad a_1, a_k \in \{1, \dots, n\}$ tutti distinti

$$\binom{n}{k}(k-1)! = \frac{n!}{k!(n-k)!}(k-1)! = \frac{n!}{(n-k)!} \cdot \frac{1}{k}$$

\# σ che sono prodotto di 2 k-cicli disgiunti $(n \geq 2k)$

$$\binom{n}{2k}\frac{(2k)!}{k^2} \cdot \frac{1}{2}$$

sono equivalenti

Scegliendo prima il primo ciclo e poi il secondo

$$\binom{n}{k}(k-1)!\binom{n-k}{k}(k-1)!\,\frac{1}{2}$$

Esercizio 4

$\sigma = (1\,2\,3\,4\,5) \in S_5$

Voglio determinare chi è $Z(\sigma) = \{\tau \in S_5 \mid \sigma\tau = \tau\sigma\}$

Cerco un'azione di S_5 in cui $Z(\sigma)$ appare come stabilizzatore

$\Rightarrow$ CONIUGIO

sono tutti i 5 cicli

$S_5 \circlearrowright \mathcal{C}\ell(\sigma) = \{\tau\sigma\tau^{-1} \mid \tau \in S_5\}$

$\mathrm{Stab}(\sigma) = \{\tau \mid \tau\sigma\tau^{-1} = \sigma\} = Z(\sigma)$

$$|\mathrm{Stab}(\sigma)| = \frac{|S_5|}{|\mathcal{C}\ell(\sigma)|} = \frac{5!}{\binom{5}{5}4!} = 5$$

$Z(\sigma) = \langle\sigma\rangle$

$\sigma = (1\,2\,3\,4\,5) \in S_{10}$ $\quad Z(\sigma) = ?$

$\sigma = (1\ 2\ 3\ 4\ 5) \in S_{10}$ $\quad Z(\sigma) = ?$

$$|Z(\sigma)| = \frac{|S_{10}|}{|Cl(\sigma)|} = \frac{10!}{\binom{10}{5}4!} = 5 \cdot 5!$$

τ fissa $1,2,3,4,5 \Rightarrow \tau$ commuta con σ

$$\underset{\substack{\cong \\ S_5}}{\{\tau \text{ che fissano } 1,\dots,5\}} < S_{10}$$

$H < Z(\sigma)$ $\quad \sigma \notin H$ $\quad \langle\sigma\rangle \cap H = \{e\}$

$H\langle\sigma\rangle < S_{10}$

$|H\langle\sigma\rangle| = 5 \cdot 5! \quad \Rightarrow H\langle\sigma\rangle = Z(\sigma) \cong H \times \langle\sigma\rangle \cong S_5 \times \mathbb{Z}/5\mathbb{Z}$

$\tau = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10) \in S_{10}$

$$|Z(\tau)| = \frac{|S_{10}|}{|Cl(\tau)|} = \frac{\cancel{10!}}{\frac{1}{2 \cdot 5^2} \cdot \cancel{10!}} = 50$$

$s = (1\ 6)(2\ 7)(3\ 8)(4\ 9)(5\ 10) \in Z(\tau)$

$\tau \in Z(\tau)$ $\quad \langle s, \tau\rangle = \langle s\rangle \times \langle\tau\rangle$ $\quad |\langle s,\tau\rangle| = 10$

$\tau_1 = (1\ 2\ 3\ 4\ 5) \in Z(\tau)$

$\tau_2 = (6\ 7\ 8\ 9\ 10) \in Z(\tau)$

$|\langle\tau_1, \tau_2\rangle| = 25$

$|\langle s, \tau_1, \tau_2\rangle| \geq 50 \quad \Rightarrow Z(\tau) = \langle s, \tau_1, \tau_2\rangle$

$\langle\tau_1, \tau_2\rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$

$\triangle$

$Z(\tau)$ (indice 2)

$\langle s\rangle \cap \langle\tau_1, \tau_2\rangle = \{e\}$

$Z(\tau) = \langle\tau_1, \tau_2\rangle \rtimes \langle s\rangle = (\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$

$\varphi(s) \in Aut(\mathbb{Z}_5 \times \mathbb{Z}_5)$

$s\tau_1 s^{-1} = \tau_2 \quad \Rightarrow \varphi(s)(x\ y) = (y\ x)$

$\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$

$N(\sigma) = \{\tau \in S_5 \mid \tau\langle\sigma\rangle\tau^{-1} = \langle\sigma\rangle\} =$

$= \{\tau \in S_5 \mid \tau\sigma\tau^{-1} = \sigma^i \quad i = 1\ 2\ 3\ 4\}$

$S_5 \circlearrowright$ {sgr generati da un 5-ciclo} $= \{\langle\tau\rangle \mid \tau$ 5-ciclo$\}$

$\mathrm{Stab}(\langle\sigma\rangle) = N(\sigma)$

$$|N(\sigma)| = \frac{|S_5|}{|\{\langle\tau\rangle \mid \tau \text{ 5-ciclo}\}|} \quad {=}x$$

$\langle\sigma\rangle = \langle\tau\rangle \iff \tau = \sigma^j \quad j = 1, 2, 3, 4$

$$x = \frac{\#\text{ di 5 cicli}}{4} = 3! \quad \Rightarrow x = 5 \cdot 4 = 20$$

$\sigma \in N(\sigma)$

$\tau\sigma\tau^{-1} = \sigma^i \qquad i = 1 \Rightarrow \tau\sigma = \sigma\tau$

$\tau \in Z(\sigma)$

$\tau\sigma\tau^{-1} = \sigma^2$

$\Updownarrow$

$(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5)) = (1\ 3\ 5\ 2\ 4)$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = (2\ 3\ 5\ 4)$$

$\tau \in N(\sigma) \qquad \mathrm{ord}\,\tau = 4$

$\langle\tau\rangle \cap \langle\sigma\rangle = \{e\} \qquad |\langle\tau\rangle\langle\sigma\rangle| = 20$

$N(\sigma) = \langle\tau, \sigma\rangle$

$\langle\sigma\rangle \triangleleft N(\sigma)$ per def.

$N(\sigma) \cong \langle\sigma\rangle \rtimes_\varphi \langle\tau\rangle \cong \mathbb{Z}_5 \rtimes_\varphi \mathbb{Z}_4 \qquad \sigma \to (1,0) \quad \tau \to (0,1)$

$2 = \varphi(1) \in \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^* \qquad \mathbb{Z}_5^* \cong \mathbb{Z}_4$

$\varphi: \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$

$\varphi(1)(1) = i$ dove $\tau\sigma\tau^{-1} = \sigma^i$

Esercizio 5

Classi di coniugio in S_5 e A_5

$$\left.\begin{array}{ll} cl(e) & cl((12)(34)) \\ cl((12)) & cl((12)(345)) \\ cl((123)) & \\ cl((1234)) & \\ cl((12345)) & \end{array}\right\} \text{In } S_5$$

In A_5

$A_5 = cl_S(e) \cup cl_S((123)) \cup cl_S(12345) \cup cl_S((12)(34))$

$cl_A(\sigma) = \{\tau\sigma\tau^{-1} \mid \tau \in A_5\} \subset cl_S(\sigma)$

Sono diversi se $\exists\, \rho \in S_5 \setminus A_5 \mid \rho\sigma\rho^{-1} \notin cl_A(\sigma)$

$$|cl_A(\sigma)| = \frac{|A_5|}{|Z_{A_5}(\sigma)|} = \frac{60}{|Z_{S_5}(\sigma) \cap A_5|}$$

$$|cl_S(\sigma)| = \frac{|S_5|}{|Z_{S_5}(\sigma)|} = \frac{120}{|Z_{S_5}(\sigma)|}$$

$cl_A(e) = cl_S(e) = \{e\}$

$$|cl_A((123))| = \frac{60}{|Z_S((123)) \cap A_5|}$$

stessa scomposizione in cicli disgiunti

$\wedge$

$$|cl_S((123))| = \frac{120}{|Z_S((123))|} = \binom{5}{3} 2 = 20$$

ha card. 6

$Z_S((123)) = \langle (123), (4,5) \rangle$

il centralizzatore contiene un elemento dispari

$$\Rightarrow |cl_A((123))| = \frac{60}{3} = 20$$

per cui $cl_A((123)) = cl_S((123))$

$$|cl_A((12345))| = \frac{60}{|Z((12345)) \cap A_5|} = \frac{60}{|Z((12345))|} = 12$$

$$|cl_S((12345))| = \frac{120}{|Z(12345)|} = 24 \qquad cl_A(12345) \subsetneq cl_S(12345)$$

Ogni classe di coniugio in S_n è unione di una o più classi di coniugio di A_n

$cl_S((12345)) \supset cl_A(\tau)$ con $\tau \in cl_A(12345)$

$\tau = (2\,1\,3\,4\,5) = (12)(12345)(12)$

Se prendo $q \in S_5$ vale $q \in A_5$ oppure $q(12) \in A_5$

$q\sigma q^{-1} \in cl(\sigma)$ $\quad q \in A_5 \Rightarrow q\sigma q^{-1} \in cl_A(\sigma)$

$\quad q \notin A_5 \Rightarrow q(12) \in A_5$

$$g\sigma g^{-1} = \underbrace{g(12)}(12)\underbrace{\sigma(12)}_{\tau}\underbrace{(12)g^{-1}} \in Cl_A(\tau)$$

$S_n = A_n \langle (12) \rangle$

$\tau = (12)\sigma(12)$

$$Cl_S(\sigma) = Cl_A(\sigma) \cup Cl_A(\tau)$$

↳ queste due sono uguali o disgiunte

Ma non può essere $\tau \in Cl_A(\tau)$, perché $Cl_S(\sigma) \neq Cl_A(\sigma)$ (lo so per cardinalità)

$\Rightarrow \tau \notin Cl_A(\sigma)$

$$Cl_S(1\,2\,3\,4\,5) = Cl_A(1\,2\,3\,4\,5) \cup Cl_A(2\,1\,3\,4\,5)$$

$\sigma = (12)(34)$

$|Cl_S(\sigma)| = 15 \Rightarrow |Z_S(\sigma)| = \frac{120}{15} = 8$

$(12) \in Z_S(\sigma)$

$Z_S(\sigma) \cap Z_A(\sigma) \lneq Z_S(\sigma)$

$|Cl_A(\sigma)| = \frac{60}{|Z_S(\sigma) \cap A_S|} \geq \frac{60}{4} = 15 \Rightarrow Cl_A(\sigma) = Cl_S(\sigma)$

Riepilogo:

$Cl_A(e)$	1
$Cl_A((123))$	20
$Cl_A((1\,2\,3\,4\,5))$	12
$Cl_A((2\,1\,3\,4\,5))$	12
$Cl_A((12)(34))$	15

28/10/2024
Patino

- $n \geq 3$, A_n è generato dai 3 cicli.

$\sigma \in A_n \quad \sigma = \sigma_1 \cdots \sigma_k \quad \sigma_i$ cicli disgiunti di lunghezza l_i

Cicli dispari → lungh. pari
Cicli pari → lungh. dispari

OSS $\sigma \in A_n \iff$ ha un numero pari di cicli pari

A_n è generato dai cicli dispari e dai prodotti di due cicli pari disgiunti.

Sia $H = \langle (i\,j\,k) \rangle \leq A_n$ al variare di i, j, k in $\{1, \dots, n\}$, i, j, k a due a due distinti (cioè prendo come generatori tutti i 3-cicli)

↳ poiché tutti i generatori sono in A_n

Devo dimostrare che tutti i cicli di lunghezza dispari $\in H$

e i prodotti di due cicli pari disgiunti $\in H$

- σ ciclo di lungh. dispari

$\sigma = (\sigma_1 \cdots \sigma_{2k+1})$

OSS $\sigma = (\sigma_1\ \sigma_2 \cdots \sigma_{2k-1})(\sigma_{2k-1}\ \sigma_{2k}\ \sigma_{2k+1}) =$

$= (\sigma_1\ \sigma_2\ \sigma_3)(\sigma_3\ \sigma_4\ \sigma_5) \cdots (\sigma_{2k-1}\ \sigma_{2k}\ \sigma_{2k+1})$

- $\sigma = (\sigma_1 \cdots \sigma_{2k})(\tau_1 \cdots \tau_{2h})$

$\sigma = (\sigma_1 \cdots \sigma_{2k-2})(\tau_1 \cdots \tau_{2h-2})(\sigma_{2k-2}\ \sigma_{2k-1}\ \sigma_{2k})(\tau_{2h-2}\ \tau_{2h-1}\ \tau_{2h}) =$

$= \underbrace{(\sigma_1\ \sigma_2)(\tau_1\ \tau_2)}_{\in H?} h \qquad h \in H$

$= (\sigma_1\ \sigma_2\ \tau_1)(\sigma_2\ \tau_1\ \tau_2) \quad \in H$ $\square$

$n \geq 5$, A_n generato da elementi prodotto di due trasposizioni disgiunte

$K = \langle (i\,j)(k\,\ell) \mid i\ j\ k\ \ell \text{ disgiunti} \rangle \subseteq A_n$

$K = A_n$. Mi basta far vedere che i 3 cicli sono in K

$\sigma = (a\ b\ c) \in A_n$

$\overset{\shortparallel}{(a\ b)(b\ c)} = \overbrace{(a\ b)(d\ e)}\,\overbrace{(b\ c)(d\ e)} \in K$ $\square$

per questa scrittura mi servono almeno 5 elementi

Se $n = 4$?

$K = \{ (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), e \} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

↳ non è tutto A_4 perché $|A_4| = 4!/2 = 12$

$\sigma \in S_n$

Allora $Z_{S_n}(\sigma) < A_n \iff \sigma$ è prodotto di cicli dispari disgiunti, tutti di lunghezza diversa

NB! vanno considerati anche i cicli di lunghezza 1 $\Rightarrow$ non ci possono essere due punti fissi o più

$\sigma = \sigma_1 \cdots \sigma_k$ prodotto di cicli disgiunti

$\sigma_i \in Z(\sigma)$

$Z(\sigma) < A_n \Rightarrow \sigma$ non ha cicli di lungh. pari

σ_i, σ_j cicli dispari della stessa lungh.

$\sigma_i = (a_1 \cdots a_\ell)$

$\sigma_j = (b_1 \cdots b_\ell)$

$\tau \sigma_i \tau^{-1} = \sigma_j$

$\tau = (a_1 b_1)(a_2 b_2) \cdots (a_\ell b_\ell) \notin A_n$

$\tau(\sigma_i \sigma_j)\tau^{-1} = \sigma_i \sigma_j$

e commuta con tutti gli altri σ_k $k \neq i, j$

$\tau \in Z(\sigma)$ $\tau \notin A_n$ (ciò dimostra $\Rightarrow$)

$\Leftarrow$ $\sigma = \sigma_1 \cdots \sigma_k$ σ_i cicli di lungh. dispari, tutte diverse
$\ell_1 \cdots \ell_k$ lungh.

$$|Z(\sigma)| = |S_n| / |C(\sigma)|$$

$$|C(\sigma)| = \binom{n}{\ell}(\ell_1 - 1)! \cdots \binom{n-\ell_1-\cdots-\ell_k}{\ell_k}(\ell_k - 1)! =$$

Oss $\ell_1 + \dots + \ell_k = n$

$$= \frac{n(n-1) \cdots (n-\ell_1+1)}{\ell_1!}(\ell_1 - 1)! \frac{(n-\ell_1)\cdots(n-\ell_1-\ell_2+1)}{}(\ell_2-1)! \cdots$$

$$= \frac{n!}{\ell_1 \ell_2 \cdots \ell_k} \Rightarrow |Z_{S_n}(\sigma)| = \frac{n!}{\frac{n!}{\prod \ell_i}} = \prod \ell_i \qquad |Z_{S_n}(\sigma) \cap A_n| = \begin{cases} |Z_{S_n}(\sigma)| \\ \cancel{\frac{1}{2}|Z_{S_n}(\sigma)|} \end{cases}$$

impossibile perché $|Z_{S_n}(\sigma)|$ è dispari

Ricordiamo in S_5 l'unica classe tale che $Z(\sigma) < A_5$ è quella del 5 ciclo

Sia $\sigma \in A_n$

$C_{A_n}(\sigma) = C_{S_n}(\sigma) \Leftrightarrow Z(\sigma) \not\subset A_n$

e se $Z(\sigma) \subset A_n$ vale che

$C_{S_n}(\sigma) = C_{A_n}(\sigma) \sqcup C_{A_n}(\tau\sigma\tau^{-1})$ τ trasposizione

$$|C_{S_n}(\sigma)| = |S_n| / |Z_{S_n}(\sigma)| = \frac{n!}{|Z_{S_n}(\sigma)|}$$

$$|C_{A_n}(\sigma)| = |A_n| / |Z_{A_n}(\sigma)| = \frac{n!}{2|Z_{S_n}(\sigma) \cap A_n|}$$

$C_{A_n}(\sigma) \subset C_{S_n}(\sigma)$

Vale l'uguaglianza $\Leftrightarrow 2|Z_{S_n}(\sigma) \cap A_n| = |Z_{S_n}(\sigma)|$

$$\Leftrightarrow \left| Z_{S_n}(\sigma) / Z_{S_n}(\sigma) \cap A_n \right| = 2$$

Ho dimostrato $C_{S_n}(\sigma) = C_{A_n}(\sigma) \Rightarrow Z(\sigma) \not\subset A_n$

Viceversa, se $\exists\, \tau \in Z_{S_n}(\sigma) \setminus A_n$

vuol dire che $\left| Z_{S_n}(\sigma) / Z_{S_n}(\sigma) \cap A_n \right| \geq 2$

$\Rightarrow Cl_{A_n}(\sigma) \geq Cl_{S_n}(\sigma) \Rightarrow Cl_{A_n}(\sigma) = Cl_{S_n}(\sigma)$

$|Cl_{S_n}(\sigma)| = 2|Cl_{A_n}(\sigma)|$ Prendo τ trasposizione

$\tau\sigma\tau^{-1} \in Cl_{S_n}(\sigma)$

$Cl_{S_n}(\sigma) = Cl_{A_n}(\sigma) \sqcup Cl_{A_n}(\tau\sigma\tau^{-1})$

$g \in S_n \Rightarrow$ o $g \in A_n$ o $g\tau \in A_n$

$g\sigma g^{-1} \in Cl_{A_n}(\sigma) \leftarrow$ se $g \in A_n$

$\underbrace{g\tau\tau\sigma\tau^{-1}\tau^{-1}g^{-1}}_{= g\sigma g^{-1}} \in Cl_{A_n}(\tau\sigma\tau^{-1}) \leftarrow$ se $g\tau \in A_n$ $\square$

- A_5 è semplice

Un gruppo G si dice SEMPLICE se gli unici sottogruppi normali sono $\{e\}$ e G

OSS $N \triangleleft A_n$ allora N è unione di classi di coniugio

A_5 è unione delle classi dei seguenti elementi

	cardinalità:
e	1
$(12)(34)$	15
(123)	20
(12345)	12
(21345)	12
	60

per quanto osservato nell'esercizio 5

$N \triangleleft A_5$ $e \in N$

$\Rightarrow N =$ unione di classi tra cui $Cl(e)$

$|N| \mid 60$

$|N| \in \{\cancel{1}\ \underbrace{\cancel{2}\ \cancel{3}\ \cancel{4}\ \cancel{5}\ \cancel{6}\ \cancel{10}\ \cancel{12}}_{\text{troppo piccoli, la classe più piccola ha cardinalità 12}}\ 15\ 20\ 30\ \cancel{60}\}$

Per gli altri si verifica manualmente che gli unici divisori di 60 che sono somma di 1 e di un sottoinsieme di $\{12, 12, 15, 20\}$ sono 1 e 60 $\Rightarrow A_5$ semplice

OSS A_4 non è semplice

$K = Cl(e) \cup Cl((12)(34)) \triangleleft A_4$

$|K| = 4 \qquad |A_4| = 24/2 = 12$

ESERCIZIO 3

Gli unici sgr normali di S_n sono $\{e\}$, A_n e S_n

Soluzione: $N \triangleleft S_n \quad N \neq \{e\}$

$\exists \sigma \in N \mid \sigma \neq e$

τ trasposizione $\qquad \tau\sigma\tau^{-1} \in N$

$$\Rightarrow \underbrace{\tau\sigma\tau^{-1}\sigma^{-1}}_{[\tau,\sigma]} \in N$$

$$\tau\sigma\tau^{-1}\sigma^{-1} = \tau \cdot (\sigma\tau\sigma^{-1}) = (a\ b)(c\ d)$$

il coniugato di una trasposizione è una trasposizione

In N c'è il prodotto di due trasposizioni

- Se sono disgiunte, allora N contiene $\langle (i\,j)(k\,l) \mid i,j,k,l$ distinti$\rangle$

  Se $n \geq 5$, $A_n \subseteq N \Rightarrow N = A_n \vee N = S_n$

- Se $|\{a\,b\} \cap \{c\,d\}| = 1$, allora $(a\,b)(c\,d)$ è un 3-ciclo

  $\langle (i\,j\,k) \mid i,j,k$ distinti$\rangle \subseteq N \Rightarrow A_n \subseteq N \Rightarrow N = A_n \vee N = S_n$

- Se $\{a\,b\} = \{c\,d\}$ $\quad \tau$ e σ commutano

  A meno di cambiare τ, posso prendere τ che non commuta con $\sigma \Rightarrow$ posso ricondurmi agli altri due casi

OSS • $n \geq 3$

allora $Z(S_n) = \{e\}$ e $S_n = \langle (i\,j) \mid i \neq j \rangle$

$\sigma \neq e \Rightarrow$ posso trovare τ trasposizione tale che $[\tau\sigma] \neq e$

- $n = 2$

  $S_n \cong C_2$ ✓

- $n = 3$

  conosciamo tutti i sgr di S_3 ✓

- $n = 4$

  l'unica possibilità che manca è

  $$N = \langle (i\,j)(k\,l) \rangle \triangleleft S_4$$
  $$\cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

ESERCIZIO A_n semplice $(n \geq 5)$ — si può dimostrare come con A_5

- Supponiamo che A_6 sia semplice

Prendo $n \geq 7$

$\{e\} \neq N \trianglelefteq A_n \qquad \underset{\underset{e}{\neq}}{\sigma} \in N$

$Z(A_n) = \{e\} \Rightarrow$ posso trovare τ 3-ciclo $\mid [\tau\, \sigma] \neq e$

$[\tau\,\sigma] = (\tau \sigma \tau^{-1}) \sigma^{-1} = \tau(\sigma \tau^{-1} \sigma^{-1})$ ↳ prodotto di due 3-cicli

$x = \tau(\sigma\tau^{-1}\sigma^{-1})$
muove al più 6 elementi,

allora $\exists\, K < A_n$ con $x \in K$ ↗ gruppo alterno del gruppo che muove 6 elementi, fra cui tutti quelli di x

$K \cong A_6$

$N \cap K \neq \{e\}$, ↳ per esempio c'è σ

$N \cap K \trianglelefteq K$ (perché $N \trianglelefteq A_n$) $\Rightarrow N = K$ perché K è semplice.

$\Rightarrow N$ contiene un 3-ciclo $\Rightarrow N = A_n$ $\square$

$\Rightarrow$ dato che è normale contiene tutta la classe di coniugio di un 3 ciclo $\Rightarrow$
$\Rightarrow$ contiene tutti i generatori di A_n

29/10/2024
Del Corso

Classificazione dei gruppi di ordine 8

abeliano $p=2$:
- $\mathbb{Z}_{p^3}$
- $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$
- $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

non abeliani:
- D_4
- $Q \rightarrow$ quaternioni

$Q = \langle i\, j \mid i^2 = j^2 = -1 \quad ij = -ji \rangle$

$Q = \{1, -1, i, -i, j, -j, \underset{k}{ij}, \underset{-k}{ji}\}$

$$\boxed{\operatorname{ord} x^K = \frac{\operatorname{ord} x}{(\operatorname{ord} x, K)}}$$

È un p-gruppo $\Rightarrow$ se è non abeliano vale necessariamente
$|Z(G)| = 2 \Rightarrow Z(Q) = \{\pm 1\}$ (non può essere $|Z(G)| = 4$ altrimenti $G/Z(G)$ sarebbe ciclico)

$(ij)^2 = ijij = -jiij = -j(-1)j = j^2 = -1 \Rightarrow ij$ ha ordine 4

(Tutti gli elementi esclusi 1 e -1 hanno ord 4) $\Rightarrow$

$\Rightarrow$ tutti i sgr sono normali

G abeliano $\Rightarrow$ Teo di struttura

Supponiamo G non abeliano $\Rightarrow \exists a \in G \mid o(a) = 4$

ESERCIZIO
ogni gruppo con elementi di solo ord 2 è abeliano
$\hookrightarrow a, b \in G$ $ab \neq ba$ $aba^{-1}b^{-1} \neq e$ $(ab)^2 = e$

$\langle a \rangle$ è normale (indice minimo)

$G/\langle a \rangle = \{ \langle a \rangle, b\langle a \rangle \}$

$(b\langle a \rangle)^2 = b^2\langle a \rangle = \langle a \rangle$ $b^2 = a, a^3 \Rightarrow$ $\Rightarrow o(b) = 8$

$b^2 \in \langle a \rangle = \{1, \cancel{a}, a^2, \cancel{a^3}\}$ (ogni volta che aggiungo un elemento a un sgr. massimale genero tutto)

$b^2 = \begin{cases} 1 \\ a^2 \end{cases}$ $G = \langle a, b \rangle$

Caso $b^2 = 1$

normalità + il coniugio conserva l'ordine (perché è omo. iniettivo)

$a^4 = b^2 = 1$ $bab^{-1} = \begin{cases} \cancel{a} \to \text{commuterebbero} \\ a^3 \end{cases}$

$$\begin{array}{ccc} G & \xleftrightarrow{\varphi} & D_4 \\ a & \longmapsto & r \\ b & \longmapsto & s \end{array}$$

Relazioni da verificare: $a^4 = 1$, $b^4 = 1$, $bab^{-1} = a^3$

come faccio a sapere che non ce ne sono altre da controllare?

Vado da D_4 a G perché so che D_4 è definito da (queste relazioni dato che ho 8 elementi non possono esserci altre relazioni indipendenti

φ è un isomorfismo

Caso $b^2 = a^2$

ord $b = 4$
$bab^{-1} = a^3$

$ab = b^{-1}a^3b^2 =$
$= b^3a^3b^2$

$$\begin{array}{ccc} Q & \xrightarrow{\varphi} & G \\ i & \longmapsto & a \\ j & \longmapsto & b \end{array}$$

Questo assegnamento rispetta le relazioni? Se sì, si estende in modo unico a omomorfismo

$i^4 = j^4 = 1$

$i^2 = j^2$ $ij = -ji$

$\varphi(i)^4 = a^4 = 1$ $\varphi(j)^4 = b^4 = 1$
$\varphi(i)^2 = a^2 = \varphi(j)^2 = b^2$ $a(\underbrace{a^3ba^3}_{b}) = ba^3 = \varphi(j)\varphi(i)^{-1} = \varphi(j)\varphi(-i) = \varphi(-ji)$

$\varphi(ij) = \varphi(i)\varphi(j) = ab = a^2ba = \varphi(-i)\varphi(j)\varphi(i) = \varphi(-ji)$

Cerco il minimo n tale che $Q \hookrightarrow S_n$

$n = 8$ Cayley $G \to S(G)$ $G = \{g_1 \cdots g_n\}$
$g \longmapsto \varphi_g : G \to G$
$g_i \longmapsto gg_i$
$(g_i \ gg_i \ g^2g_i \ \cdots \ g^{d-1}g_i)$ ord g

$8 \mid n! \Rightarrow n \geq 4$

$D_4 \subseteq S_4 \to D_4$ è un 2-Sylow

Se fosse $Q \subseteq S_4$ sarebbe un 2-Sylow e

avrei $D_4 \cong Q$ (sono tutti coniugati tra di loro) ↯

S_5 ha gli stessi 2-sylow di S_4

$\Rightarrow n \geq 6$

Consideriamo S_6

$D_4 = \langle (1\,2\,3\,4), (12)(34) \rangle$

il 2-Sylow di S_6 sarà $D_4 \times \mathbb{Z}_2$ verificando le hp. del teo di prodotto diretto $P_2 = D_4 \langle (5\,6) \rangle$

$\mathbb{Z}_2 = \langle (5,6) \rangle$

normale nel 2-Sylow perché ha indice due

ci sono solo 2 elementi di ord 4 $\Rightarrow$ non può contenere Q

I 2-Sylow di S_7 sono isomorfi a quello di S_6

$\Rightarrow$ l'$n=8$ dato da Cayley è il migliore

G gruppo, $|G| = 2d$, d dispari $\Rightarrow \exists H \trianglelefteq G, |H| = d$

Cayley: $G \overset{\varphi}{\hookrightarrow} S(G) \cong S_{2d}$

$G \overset{\varphi}{\hookrightarrow} S_{2d} \xrightarrow{\pi} S_{2d}/_{A_{2d}} = \{\pm 1\}$ $\qquad G \xrightarrow{\sim} H$

$H = \varphi(G)$

$\pi(H) < S_{2d}/A_{2d}$

$\operatorname{Ker} \pi|_H = H \cap A_{2d}$

$\pi(H) = H/_{H \cap A_{2d}}$ $\qquad [H : (H \cap A_{2d})] = \begin{cases} 1 \\ 2 \end{cases}$

Claim: $K = H \cap A_{2d}$

$H \neq H \cap A_{2d}$

Tramite l'immersione di Cayley un elemento di ordine 2

va in un prodotto di d trasposizioni $\Rightarrow$ H ha un elemento

dispari. $\Rightarrow$ $|H \cap A_{2d}| = d$, è normale in S_{2d} in quanto ker di π $\Rightarrow \varphi^{-1}(H \cap A_{2d})$ ha ordine d ed è normale in G. □

$|G| = 2 \cdot 5 \cdot 3 = 2d \quad d = 15 \Rightarrow \exists H \trianglelefteq G \quad |H| = 15 \quad H = \langle x \rangle \cong \mathbb{Z}_{15}$

Per Cauchy $\exists y \in G \mid \text{ord}\, y = 2$

$K = \langle y \rangle \Rightarrow G = HK$ (perche' H era massimale)

$H \cap K = \{e\}$

$H \triangleleft G$

$\Rightarrow G \cong H \rtimes_\varphi K$

$\varphi : K \to \text{Aut}(H) \cong \text{Aut}(\mathbb{Z}_{15}) \cong \mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^* \cong$

$y \mapsto$ id φ_b φ_a φ_c $\cong \mathbb{Z}_2 \times \mathbb{Z}_4$

↳ andrà in un elemento di ord 2

di elementi di ord 2 che trovo in $\mathbb{Z}_2 \times \mathbb{Z}_4$

$\varphi_a : x \mapsto x^a$

$\varphi_b : x \mapsto x^b$

$\varphi_c : x \mapsto x^c$

$\varphi \in \text{Aut}(H)$
$\varphi^2 = id$

$\varphi(x) = x^i \quad (i, 15) = 1$
$\varphi^2(x) = x^{i^2} \quad i^2 \equiv 1 \ (15)$

$\begin{cases} i^2 \equiv 1 & (3) \\ i^2 \equiv 1 & (5) \end{cases} \quad \begin{cases} i \equiv \pm 1 & (3) \\ i \equiv \pm 1 & (5) \end{cases}$

$\Rightarrow i = 1, -1, 4, -4$

mi da $\mathbb{Z}/30\mathbb{Z}$

$id = \varphi_1$
$\varphi_a = \varphi_{-1}$
$\varphi_b = \varphi_4$
$\varphi_c = \varphi_{-4}$

$\Rightarrow$ ha al più 4 gruppi

$\varphi_{-1}(x) = yxy^{-1} = x^{-1} \Rightarrow$ ottengo D_{15}

$\varphi_4(x) = yxy^{-1} = x^4 \Rightarrow D_5 \times \mathbb{Z}_3$ (fissa un elemento di ordine 3 che è nel centro)

$\varphi_{-4}(x) = yxy^{-1} = x^{-4} \Rightarrow D_3 \times \mathbb{Z}_5$

why?

↑ il suo centro non ha un elemento di ordine 3

RICHIAMI SUGLI ANELLI

Def. $(A, +, \circ)$

- $(A,+)$ è un gruppo abeliano
- $\circ$ è un'operazione associativa su A
- $a(b+c) = ab + ac$
  $(b+c)a = ba + ca \quad \forall\, a,b,c \in A$

Un anello si dice COMMUTATIVO se $\circ$ è commutativa

A si dice anello con unità se $\exists\, 1 \in A \mid 1 \cdot a = a \cdot 1 = a \ \forall a \in A$

Esempi:

interi di Gauss

$\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{Q}[i], \mathbb{Z}[i]$

$\mathbb{Z}/n\mathbb{Z}$, $M_{n \times n}(\mathbb{C})$, $2\mathbb{Z}$

non abeliano

Se G è un gruppo abeliano, $End(G) = Hom(G,G)$ è un anello con somma $(f+g)(x) = f(x) + g(x)$ e composizione.

Def. $(A, +, \circ)$ si dice CAMPO se $(A \setminus \{0\}, \circ)$ è un gruppo abeliano

Def. A anello

0 è un divisore di 0

$x \in A$ si dice DIVISORE DI ZERO se $\exists\, y \in A,\ y \neq 0 \mid xy = yx = 0$

$x \in A$ si dice NILPOTENTE se $\exists\, n \in \mathbb{N} \mid x^n = 0$

$x \in A$ si dice INVERTIBILE se $\exists\, y \in A \mid xy = yx = 1$

con identità

Def. A commutativo con 1 si dice DOMINIO DI INTEGRITÀ se

$\mathcal{D}_A = \{x \in A \mid x \text{ è divisore di } 0\} = \{0\}$

$A^* = \{x \in A \mid x \text{ è inv}\}$

Esercizio: calcolare $\mathcal{D}_A$ e A^* per $A = \mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_n \times \mathbb{Z}_m$

Proposizione A comm. con 1

(i) $(A^*, \circ)$ gruppo abeliano

(ii) $A^* \cap \mathcal{D}_A = \emptyset$

(iii) $|A| < +\infty \Rightarrow A = A^* \cup \mathcal{D}_A$

$\bar{a} \in \mathbb{Z}_n \quad (a,n) = d > 1 \qquad \bar{a}\,\underset{\neq 0}{\overline{\tfrac{n}{d}}} = 0$

DIM

(i) facile

(ii) Supponiamo $\exists x \in A^* \cap \mathcal{D}_A \quad \exists y \mid xy = yx = 1$

$\exists \underset{\neq 0}{z} \mid xz = zx = 0$

$$\begin{aligned} zxy &= z(xy) = z \\ \shortparallel & \\ ((zx)y) &= 0 \cdot y = 0 \end{aligned} \Rightarrow z = 0 \;\lightning$$

(iii) $x \in A \setminus \mathcal{D}$ th: x invertibile

$\varphi_x : A \to A$ $\quad \varphi_x$ omomorfismo di gruppi
$a \mapsto xa$

$\ker \varphi_x = \{y \in A \mid xy = 0\} = \{0\}$

φ_x iniettivo $+ |A| < +\infty \Rightarrow \varphi_x$ suriettivo $\Rightarrow$

$\Rightarrow 1 \in \operatorname{Im} \varphi_x \Rightarrow \exists a \in A \mid xa = 1 \Rightarrow x \in A^*$

Corollario Ogni dominio di integrità finito è un campo

Def. $B \subset A$ è sottoanello $\Leftrightarrow$ $(B,+) < (A,+)$ e B è chiuso rispetto a $\cdot$

$I \subset A$ è IDEALE $\Leftrightarrow$ $(I,+) < (A,+)$ e $\forall a \in A \quad aI \subseteq I,\ Ia \subseteq I$

A commutativo, con 1
I ideale $\Leftrightarrow \begin{cases} \cdot\ I \neq \emptyset \\ \cdot\ \forall x,y \in I \Rightarrow x+y \in I \\ \cdot\ \forall a \in A \quad ax \in I \quad \forall x \in I \end{cases}$

Chi sono gli ideali di $\mathbb{Z}$?

Li cerco tra i sgr. $\{n\mathbb{Z}\}_{n \geq 0}$

Tutti di questi sono ideali (hanno la prop. di assorbimento)

- $\{0\}, A$ sono sempre ideali di A

A commutativo con unità, $S \subseteq A$, $S \neq \emptyset$

$(S) = \left\{ \sum_{i=1}^{n} a_i s_i \mid n \in \mathbb{N},\ a_i \in A,\ s_i \in S \right\} \Rightarrow$ ideale generato da S

↳ Es: verificare che è un ideale di A

$$(S) = \bigcap_{\substack{I \subseteq A \text{ ideale} \\ S \subseteq I}} I$$

$\supseteq$ (S) fa parte dell' intersezione $\Rightarrow$ $(S) \supseteq \bigcap I$

$\subseteq$ $\forall x \in (S) \Rightarrow x \in I$ dove $S \subset I$, I ideale di A

$$x = \sum_{i=1}^{n} a_i s_i \in I$$

$S = \{x\}$
$(x) = xA \qquad (x) = \left\{ \sum_{i=1}^{n} a_i x = x\left(\sum_i a_i\right) \right\}$

Operazioni tra ideali

A anello commutativo con unità, I e J ideali di A

- $I \cup J$ in generale non è un ideale
- $I \cap J$ è un ideale
- $I + J = \{ i + j \mid i \in I, j \in J \} = (I \cup J)$ generato dall' unione
- $IJ = (\{ij \mid i \in I \ j \in J\})$
- $\sqrt{I} = \{ x \in A \mid \exists n \in \mathbb{N} \mid x^n \in I \}$
- $\sqrt{0} = \mathcal{N} = \{ x \in A \mid x$ è nilpotente $\}$
- $(I : J) = \{ x \in A \mid xJ \subset I \} \qquad (10\mathbb{Z} : 12\mathbb{Z}) = 5\mathbb{Z}$

$H \rtimes_\varphi K \qquad H \rtimes_\psi K \qquad \varphi, \psi : K \to Aut(H)$
$\qquad\qquad\qquad\qquad\qquad\qquad k \mapsto \varphi_k, \psi_k$

Proposizione: se $\exists \alpha \in Aut(H)$ $\beta \in Aut(K)$ tali che

$$\alpha \circ \varphi_k \circ \alpha^{-1} = \psi_{\beta(k)} \quad \forall k \in K$$

$\Rightarrow H \rtimes_\varphi K \cong H \rtimes_\psi K$

DIM $F : H \rtimes_\varphi K \longrightarrow H \rtimes_\psi K$

$(h\ k) \longmapsto (\alpha(h), \beta(k))$ è un isomorfismo

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & Aut(H) \quad f \\ \beta \downarrow & & \downarrow \\ K & \xrightarrow[\psi]{} & Aut(H) \quad \alpha f \alpha^{-1} \end{array}$$

$(\alpha(h)\psi_{\beta(k)}(\alpha(x)), \beta(ky))$

$F((hk)(xy)) \overset{?}{=} F((hk))F((xy)) = (\alpha(h), \beta(k))(\alpha(x), \beta(y))$

$F((h\varphi_K(x), Ky)) = (\alpha(h\varphi_K(x)), \beta(Ky))$

Voglio dire che $\alpha(h\varphi_K(x)) = \alpha(h)\psi_{\beta(K)}(\alpha(x))$

$\cancel{h}\varphi_K(x) = \cancel{h}\,\alpha^{-1}\left(\psi_{\beta(K)}(\alpha(x))\right) \quad \forall x$

$\varphi_K = \alpha^{-1}\psi_{\beta(K)}\alpha$

$$\mathrm{Aut}(H\times K) \xleftarrow{\Theta} \mathrm{Aut}(H)\times \mathrm{Aut}(K)$$

$$\vartheta_{(f,g)} \longleftarrow (f,g)$$

$\vartheta_{(f,g)}(x,y) = (f(x), g(y))$

In generale questa mappa non è suriettiva

(ES $\mathrm{Aut}(\mathbb{Z}_2\times\mathbb{Z}_2) \cong S_3$ ma $\mathrm{Aut}(\mathbb{Z}_2) = \{id\}$)

Θ omo. iniettivo

Θ suriettivo $\Longleftrightarrow$ H e K caratteristici in $H\times K$

($\Rightarrow$) $\forall \phi \in \mathrm{Aut}(H\times K) \Rightarrow \phi = \Theta(f,g)$ $\quad f\in\mathrm{Aut}(H)$, $g\in\mathrm{Aut}(K)$

$\phi(H\times\{e\}) \subset H\times\{e\}$

$\overset{\shortparallel}{\Theta}(f,g)(h, e) = (f(h), g(e)) = (f(h), e) \in H\times\{e\}$

($\Leftarrow$) $\forall \phi \in \mathrm{Aut}(H\times K)$ $\exists f\in\mathrm{Aut}(H)$ $g\in\mathrm{Aut}(K)$

tale che $\phi = \Theta(f,g)$

$\underset{\underset{f}{\shortparallel}}{\phi|_H} \in \mathrm{Aut}(H)$ $\qquad \underset{\underset{g}{\shortparallel}}{\phi|_K} \in \mathrm{Aut}(K)$

Esercizio: $(|H|, |K|) = 1 \Rightarrow$ H e K caratteristici in $H\times K$

G NON abeliano $|G| = p^3$

Allora
- $|Z(G)| = p$ ✓
- $[G,G] \overset{?}{=} Z(G)$
- Calcolare # di classi di coniugio di G

~~più grande~~ più piccolo sgr. tale che il quoziente è comm.

(cioè G/G' è il più grande quoziente commutativo)

$\downarrow$

$[G,G] = G'$ (derivato)

$\left|G/Z(G)\right| = p^2 \Rightarrow$ abeliano

allora $G' \subset Z(G)$

$\not=$

$\{e\}$ perché G NON è abeliano. Allora per cardinalità

$G' = Z(G)$

$$|G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} |G| / |Z_G(x)|$$

$$p^3 = p + |R \setminus Z(G)| \, p$$

$\Rightarrow$ # di classi di coniugio $\Rightarrow p^2 + p - 1$

Classificare a meno di isomorfismo i G tali che $|G| = 5^2 \cdot 13$

$$\begin{matrix} n_5 \equiv 1 \ (5) & n_5 \mid 13 \\ n_{13} \equiv 1 \ (13) & n_{13} \mid 25 \end{matrix} \Rightarrow \begin{matrix} n_5 = 1 \\ n_{13} = 1 \end{matrix}$$

$$\Rightarrow G = P_5 \times P_{13}$$

$P_5 = \mathbb{Z}_{25}$ oppure $\mathbb{Z}_5 \times \mathbb{Z}_5$, $\quad P_{13} \cong \mathbb{Z}_{13}$

$|G| = 5^2 \cdot 11$, c'è un gruppo non abeliano di questo ordine?

$$n_{11} \equiv 1 \ (11) \Rightarrow n_{11} = 1$$

$$n_5 \equiv 1 \ (5) \Rightarrow n_5 = \begin{cases} 1 \\ 11 \end{cases}$$

$$P_{11} \rtimes P_5, \quad P_5 = \mathbb{Z}_5 \times \mathbb{Z}_5 \text{ oppure } \mathbb{Z}_{25}$$

$$\mathbb{Z}_{25} \longrightarrow \mathrm{Aut}(\mathbb{Z}_{11}) \cong \mathbb{Z}_{10}$$

$$\bar{1} \longmapsto \varphi_i : \bar{1} \longmapsto \bar{i}$$

$$\varphi_i^5(1) = i^5 \equiv 1 \ (11) \qquad i^{10} \equiv 1$$

$$i = 4$$

04/11/2024
Patino

A_n semplice (2ª dim.)

Reminder: $N \triangleleft S_n \Rightarrow N = \{e\}, A_n, S_n$

DIM. $N \triangleleft A_n \quad N \neq \{e\}, A_n$

$\Rightarrow N$ non è normale in S_n

$N_{S_n}(N) = A_n$

$\forall \tau \notin A_n \quad \tau N \tau^{-1} \neq N$

Prendiamo τ trasposizione

$c_\tau : A_n \xrightarrow{\sim} A_n \qquad N \triangleleft A_n \Rightarrow \tau N \tau^{-1} \triangleleft A_n$

$\rightarrow N \cap \tau N \tau^{-1} \triangleleft A_n$

Infatti $A_n < N_{S_n}(N \cap \tau N \tau^{-1}) \ni \tau$

contiene sia A_n che una trasposizione τ

$\Rightarrow N_{S_n}(N \cap \tau N \tau^{-1}) = S_n$

$N \cap \tau N \tau^{-1} = \{e\}$

$N(\tau N \tau^{-1}) < A_n$ perché $N \triangleleft A_n$, inoltre è normale in S_n

Se $g \in A_n$, vale $g(n \tau n' \tau^{-1}) g^{-1} = \underbrace{g n g^{-1}}_{\in N} \underbrace{g \tau n' \tau^{-1} g^{-1}}_{\in \tau N \tau^{-1}} \in N \tau N \tau^{-1}$

Prendiamo τ trasposizione

$\tau n \overset{\tau^{-1}}{\tau} N \cancel{\tau^{-1}} \cancel{\tau^{-1}} = \tau N \tau^{-1} \cdot N = N \cdot \tau N \tau^{-1}$

$\Rightarrow \tau, A_n \in N_{S_n}(N \tau N \tau^{-1}) \Rightarrow N \tau N \tau^{-1} \triangleleft S_n \Rightarrow N \tau N \tau^{-1} = A_n$

$|\underbrace{N \tau N \tau^{-1}}_{\text{stessa card. di } N}| = |N|^2 = n!/2$ non ha sol.

$\Rightarrow |N|$ è pari

$\Rightarrow N$ ha un elemento σ di ordine 2

$\exists\ \tau$ trasposizione che commuta con $\sigma \Rightarrow \sigma \in N \cap \tau N \tau^{-1}$ ↯

ESERCIZIO 1

Struttura dei 2-Sylow e dei 3-Sylow in S_4

P 2-Sylow di $S_4 \Rightarrow |P| = 8$

$\exists$ sgr di $S_4 \cong D_4 \qquad \langle (1\,2\,3\,4), (1\,2)(3\,4) \rangle < S_4$

$\cong D_4$ è un 2-Sylow

P 3-Sylow in S_9

$|P| = 3^4 = 81$

$\tau_1 = (1\ 2\ 3) \quad \tau_2 = (4\ 5\ 6) \quad \tau_3 = (7\ 8\ 9)$

$H = \langle \tau_1, \tau_2, \tau_3 \rangle \cong (\mathbb{Z}/3\mathbb{Z})^3$

$\exists$ un 3-Sylow P che contiene H e $H \triangleleft P$

$\Rightarrow P = \langle H, \sigma \rangle$ dove $\sigma \in N_{S_9}(H) \setminus H$

es. $\sigma = (4\,7\,1)(2\,5\,8)(3\,6\,9)$

$$\sigma\tau_1\sigma^{-1} = \tau_2$$
$$\sigma\tau_2\sigma^{-1} = \tau_3$$
$$\sigma\tau_3\sigma^{-1} = \tau_1$$

$P = \langle H, \sigma \rangle \cong H \rtimes \langle \sigma \rangle \cong (\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}_3$

$\varphi(\bar{1})^{r} = \overset{(x\,y\,z)}{} \ (x\ y\ z)$

Questo approccio funziona sempre per trovare il p-Sylow in S_{p^2}, p primo

ESERCIZIO 2

n_2 in S_5

dall'esercizio precedente so che i 2-Sylow di S_4 sono $\cong D_4$

$P \rightarrow$ 2-Sylow in S_5 $\Rightarrow P \cong D_4$

$D_4 = \langle r, s \rangle$ $\quad$ ord $r = 4$, ord $s = 2$, $srs = r^{-1}$

Sia Q un 2-Sylow $\Rightarrow \exists\, r \in Q \mid o(r) = 4$ $\quad$ r è un 4-ciclo

$$\#\, 4\text{-cicli} = \binom{5}{4} \frac{4!}{4} = 5 \cdot 3! = 30 \cdot 6$$

Q deve avere s di ord 2 che normalizza $\langle r \rangle$

$$srs^{-1} = r^{-1}$$
$$srs^{-1} = r^3$$

Se $srs^{-1} = r \Rightarrow s \in Z(r) = \langle r \rangle$

Se $srs^{-1} = r^3$ $\quad$ $r = (1\ 2\ 3\ 4)$, $r^3 (1\ 4\ 3\ 2)$ $\Rightarrow$ Una possibile $s_0 = (2\,4)$

$$srs^{-1} = r^3 \Rightarrow s_0 s r s^{-1} s_0^{-1} = s_0 r^3 s_0^{-1} = r$$

$S_0 s \in Z(r) \Rightarrow s \in S_0 Z(r)$

$N(\langle r\rangle) = Z(r) \cup S_0 Z(r) \Rightarrow$ è un 2-Sylow

Siano Q, Q' due 2-Sylow

Sono uguali SSE il gruppo generato dagli elementi di ordine 4 sono uguali.

Contrare i 2-Sylow $\equiv$ contare i sgr ciclici di ord 4

r, r' 4 cicli $\quad \langle r\rangle = \langle r'\rangle \iff r' = r^k$ con $(k,2)=1$

$\iff k = 1$ o 3

$\Rightarrow n_2 = 15$

ESERCIZIO 3

$|G| = p \cdot q \cdot r \qquad p<q<r$

$\Rightarrow$ Uno dei Sylow è normale (per cui un gruppo di questa cardinalità non è mai semplice)

j-Sylow normale $\iff n_j = 1$

Supponiamo $n_p, n_q, n_r > 1$

$n_r = \cancel{1}, \cancel{p}, \cancel{q}, pq$ ← + piccoli di r

$n_r \equiv 1\ (r) \qquad n_q \equiv 1\ (q)$

$n_p \equiv 1\ (p)$

$n_p = \cancel{1}, q, r, qr$

$n_q = \cancel{1}, \cancel{p}, r, pr$

$\Rightarrow \begin{array}{l} n_r = pq \\ n_p \geq q \\ n_q \geq r \end{array}$ → gli r-Sylow si intersecano trivialmente (r primo) e ognuno ha $r-1$ elementi di ord. r

$\Rightarrow pq(r-1)$ el. di ord r

Ho $\geq q(p-1)$ el. di ord. p

Ho $\geq r(q-1)$ el. di ord q

el. neutro

$pqr \geq pq(r-1) + q(p-1) + r(q-1) + 1$

$0 \geq \cancel{-pq} + \cancel{qp} - q + rq - r + 1$

$r(q-1) \leq q-1$ ↯

ESERCIZIO: Vale sempre $n_r = 1$

ESERCIZIO 4

Classificazione gruppi di ordine $4p$, $p \equiv 3(4)$ e $p \geq 5$ (primo)

$n_p = 1, \cancel{2}, \cancel{4} \qquad n_p \equiv 1\ (p) \Rightarrow n_p = 1$ il p-Sylow è unico e normale

$p \geq 5$

Q è il 2-Sylow

$$G = PQ = P \rtimes Q \; \begin{cases} \mathbb{Z}_4 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \end{cases}$$

- Assumiamo $Q \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$

$\left.\begin{array}{l} \varphi(1,0) = \pm 1 \\ \varphi(0,1) = \pm 1 \end{array}\right\}$ notazione moltiplicativa

$\varphi(1,0) = \varphi(0,1) = 1 \Rightarrow G = P \times Q = \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}_2$

$\varphi(1,0) = 1 \quad \varphi(0\,1) = -1 \Rightarrow G \cong D_p \times \mathbb{Z}_2$

↳ e analogamente scambiando ± 1

$\varphi(1,0) = \varphi(0,1) = -1 \Rightarrow \varphi(1,1) = 1$

A meno di cambiare base di $\mathbb{Z}_2 \times \mathbb{Z}_2$ posso prendere come generatori $(1,\cancel{0}^{\,1})$ e $(0,1) \Rightarrow G \cong D_p \times \mathbb{Z}_2$

- Assumiamo $Q \cong \mathbb{Z}/4\mathbb{Z}$

$\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}_p^*$

$\varphi(1) = 1 \to G \cong \mathbb{Z}/4p\mathbb{Z}$

$\varphi(1) = -1 \to G = \langle x, y \mid x^{2p}, y^4, yxy^{-1} = x^{-1} \rangle$, $y^2 = x^p$

gruppo diciclico

per $p = 2 \quad G \cong Q_8$

ESERCIZIO 4

$|G| = 45 = 3^2 \cdot 5 \Rightarrow G$ abeliano

$n_3 \equiv 1 \ (3) \quad n_3 \mid 5 \quad \to n_3 = 1$

$n_5 \equiv 1 \ (5) \quad n_5 \mid 9 \quad \to n_5 = 1$

$\Rightarrow G \cong \underset{\text{3-Sylow}}{P} \times \underset{\text{5-Sylow}}{Q} \Rightarrow G$ abeliano

ESERCIZIO

Classificare i gruppi di ordine $66 = 2 \cdot 3 \cdot 11$

$n_{11} = 1 \Rightarrow P_{11}$ normale

$P_{11}P_3 = P_3 P_{11} \trianglelefteq G$ (indice 2) $\qquad 3 \nmid 11 - 1 \Rightarrow P_3P_{11}$ ciclico $\cong \mathbb{Z}_{33}$

$G \cong P_{11}P_3 \rtimes P_2 \cong \mathbb{Z}_{33} \rtimes_{\varphi} \mathbb{Z}_2$

$\varphi : \mathbb{Z}_2 \to \mathbb{Z}_{33}^*$

$\mathbb{Z}_{11}^* \times \mathbb{Z}_3^*$

$\varphi(1) = (\pm 1, \pm 1)$

$\varphi(1) = (1\ 1) \Rightarrow G$ è abeliano $\Rightarrow G$ è ciclico

$\varphi(1) = (1\ -1) \Rightarrow G \cong \mathbb{Z}_{11} \times D_3$ $\longrightarrow$ P_{11} commuta con P_3 e $P_2 \Rightarrow P_{11}$ centrale

$P_2 < N(P_3)$

$G = P_{11}P_3P_2 =$

$= P_{11} \times (P_3P_2) \cong$

$\mathbb{Z}_{11} \times D_3$

$\varphi(1) = (-1\ 1) \Rightarrow G \cong D_{11} \times \mathbb{Z}_3$

$\varphi(1) = (-1\ -1) \Rightarrow G \cong D_{33}$

↳ -1 di $\mathbb{Z}_{33}^*$

Devo anche verificare che tutti i gruppi elencati non sono isomorfi tra loro

$\mathbb{Z}_{66}$, $D_{11} \times \mathbb{Z}_3$, D_{33}, $D_3 \times \mathbb{Z}_{11}$

- $\mathbb{Z}_{66}$: unico ciclico
- $D_{11} \times \mathbb{Z}_3$: 11 el. di ordine 2
- D_{33}: 33 el. di ordine 2
- $D_3 \times \mathbb{Z}_{11}$: 3 el. di ordine 2

$\Rightarrow$ NON isomorfi

ESERCIZIO 2

Non esistono gruppi semplici di ordine 84

$84 = 2^2 \cdot 3 \cdot 7$

$n_7 = 1\ \cancel{2}\ \cancel{4}\ \cancel{3}\ \cancel{6}\ \cancel{12} \Rightarrow P_7$ normale

$\Rightarrow$ non può essere semplice

05/11/2024
Del Corso

Def. A, B anelli con 1

$\phi : A \to B$ omo di anelli

- $\phi(a_1 + a_2) = \phi(a_1) + \phi(a_2)$ → implica $\phi(0) = 0$
- $\phi(a_1 a_2) = \phi(a_1)\phi(a_2)$ → implica $\phi(1) = 1$? NO
- $\phi(1_A) = 1_B$

$\phi(a) = \phi(1_A a) = \phi(1_A)\phi(a)$

$\phi(a)(1_B - \phi(1_A)) = 0 \quad \forall a$

↳ potrebbe essere un divisore di zero $\neq 0$

$A \quad I \subseteq A$

$(A/I, +) \quad \{a + I\}_{a \in A}$

↳ normale perché un anello è anche un gr. abeliano

$(a+I)(b+I) := ab + I$

Buona definizione:

$a+x, \ x \in I \qquad (a+x+I)(b+y+I) =$
$b+y, \ y \in I \qquad = ab + bx + ay + xy + I = ab + I$

assorbimento

$(A/_I, +, \cdot)$ è un anello (commutativo con identità se A lo è)

Abbiamo definito il prodotto di classi in modo che

$\pi: A \to A/_I$ sia un omo. di anelli

$\pi(a_1+a_2) = \pi(a_1) + \pi(a_2)$
$\pi(a_1 a_2) = \pi(a_1)\pi(a_2)$

Proposizione: gli ideali di A sono tutti e soli i nuclei degli omomorfismi definiti su A

DIM. $I \subseteq A$ ideale

$\Rightarrow I = \ker \pi_I$

Viceversa, $\phi: A \to B$ omo di anelli

$\ker \phi$ è un ideale di A

- È un sgr (già noto)
- Resta da vedere che $\forall a \in A, \ \forall x \in \ker \varphi \Rightarrow ax \in \ker \phi$, $xa \in \ker \phi$

$\phi(ax) = \phi(a)\phi(x) = 0 \qquad (\phi(xa)$ analogo$)$

TEOREMA DI OMOMORFISMO

$\phi: A \to B$ omo di anelli

$I \subseteq A, \quad I \subseteq \ker \phi$

$\Rightarrow \exists! \ \overline{\phi}: A/_I \to B$ t.c.
omo di anelli

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\pi_I"'] \arrow[dr, phantom, "\circlearrowleft"] & B \\ A/_I \arrow[ur, "\overline{\phi}"'] & \end{tikzcd}$$

tale che il diagramma commuta

Risulta $\phi(A) = \overline{\phi}(A/_I) \qquad \ker \overline{\phi} = \ker \phi /_I$

DIM. Dallo stesso teo. sui gruppi, so che $\exists! \ \overline{\phi}$ omo di GRUPPI che rispetta le hp.

Devo far vedere che $\overline{\phi}$ è anche (nelle nostre hp.)

omomorfismo di anelli.

$\bar{\Phi}(\pi_I(a)) = \phi(a)$

$\bar{\Phi}(a+I) = \phi(a)$

$\bar{\Phi}$ ben definita e omo. di gruppi

$\bar{\Phi}((a+I)(b+I)) = \bar{\Phi}(ab+I) = \phi(ab)$

$\bar{\Phi}(a+I)\bar{\Phi}(b+I) = \phi(a)\phi(b)$ $\square$

Corollario (II teo di omomorfismo)

$I \subseteq J \subseteq A$ ideali

(Gli ideali sono sempre sottogruppi normali)

$$\frac{A/I}{J/I} \cong A/J$$ isomorfismo di anelli

Corollario (III teo di omomorfismo)

$I, J \subseteq A$ ideali

$$\frac{I+J}{I} \cong J/_{I\cap J}$$

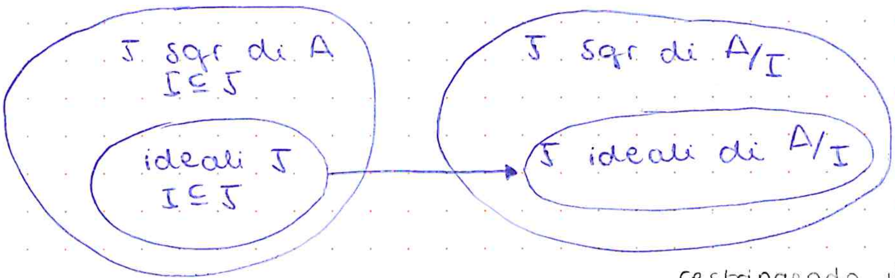
TEOREMA DI CORRISPONDENZA

$\pi_I : A \to A/I$ A anello, I ideale di A

↳ induce una corrispondenza biunivoca tra gli ideali di A/I e gli ideali di A che contengono I

Sappiamo già $\left\{ \begin{matrix} \text{ideali} \\ \text{sgr di A che} \\ \text{contengono I} \end{matrix} \right\} \longleftrightarrow \left\{ \mathcal{J} \subseteq A/I \text{ sgr ideali} \right\}$

$J \longmapsto \pi_I(J) = J/I$



Restringo la mappa agli ideali di A che contengono I

Devo far vedere che:

restringendo il dominio agli ideali anche in immagine ottengo solo ideali

- $f(J) = J/I$ è un ideale di A/I (ottengo effettivamente ideali)
- $\forall\, \mathcal{J} \subseteq A/I$ ideale, $\exists\, J \subseteq A$ ideale $\mid I \subseteq J$ t.c. $\pi_I(J) = J/I = \mathcal{J}$ (suriettività)

l'iniettività ce l'ho già dal teorema sui gruppi

LEMMA $\phi: A \to B$ omo di anelli

(i) $\forall J \subseteq B$ ideale $\phi^{-1}(J)$ ideale di A

(ii) Se ϕ è suriettivo $\forall J \subseteq A$ ideale di A

$\phi(J)$ è ideale di B

DIM (ii) $\forall b \in B \quad b\phi(J) \subseteq \phi(J)$

$b = \phi(a) \quad \phi(a)\phi(J) = \phi(aJ) \subseteq \phi(J)$

Esempio:

ϕ non suriettivo $\not\Rightarrow$ (ii)

$i: \mathbb{Z} \hookrightarrow \mathbb{Q}$
$n \mapsto n$

$I = 2\mathbb{Z} \quad i(2\mathbb{Z}) = 2\mathbb{Z}$

$2\mathbb{Z}$ non è un ideale di $\mathbb{Q}$ ($\mathbb{Q}$ campo $\Rightarrow$ ha solo ideali banali)

TEOREMA CINESE PER ANELLI

A anello commutativo con 1 $\quad I, J \subseteq A$ ideali

$$f: A \to A/_I \times A/_J$$
$$a \mapsto (a+I, a+J) \quad \text{omo di anelli}$$

$\ker f = I \cap J$
f surgettiva $\iff I + J = A$

OSS | $I + J = (I, J) = \{ i + j \mid i \in I, j \in J \}$

Se $I + J = A = (1)$
$I \cap J = IJ$

Corollario: $\mathbb{Z}/_{mn\mathbb{Z}} \cong \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \iff (m,n) = 1$

$A = \mathbb{Z} \quad I = m\mathbb{Z} \quad J = n\mathbb{Z}$

$\ker f = m\mathbb{Z} \cap n\mathbb{Z} \quad \mathbb{Z}/_{m\mathbb{Z} \cap n\mathbb{Z}} \hookrightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$ ed è surg $\iff I + J = A$

$m\mathbb{Z} + n\mathbb{Z} = (1)$

DIM. f omo (ovvio)

$\ker f = \{ a \in A \mid f(a) = (a+I, a+J) = (I, J) \} =$

$= \{ a \in A \mid a + I = I, a + J = J \} = \{ a \cap A \mid a \in I \cap J \}$

$(\Leftarrow)$ $I+J=A$ $\quad 1 = i+j \quad \begin{matrix} i\in I \\ j \in J \end{matrix}$

f surgettiva $\quad \forall (a+I, b+J) \quad \exists x \in A$ t.c.

$f(x) = (x+I, x+J) = (a+I, b+J)$

$x = \overset{I}{bi} + \overset{J}{aj}$

$\Rightarrow f(x) = (\cancel{bi}+aj+I, \; bi+\cancel{aj}+J)$

$aj = a(1-i)$

$\Rightarrow aj + I = a + I$

potrei fare lo stesso ragionamento con b, oppure $\quad x \equiv b \; (J)$?

$x = bi + aj \equiv \underset{\substack{\parallel \\ b}}{bi} \quad (J)$

$(\Rightarrow)$

f surgettiva $\Rightarrow I+J=A$

$\exists x \in A \quad f(x) = (I, 1+J)$

~~$\exists y \in A \quad f(y) = (1+I, J)$~~ non serve

$x \equiv 0 \; (I)$
$x \equiv 1 \; (J)$

$x \in I \quad j = x-1 \in J$

$1 = \underset{\substack{\cap \\ I}}{x} - \underset{\substack{\cap \\ J}}{j}$

Esercizio

- S_6 non contiene sgr abeliani di ordine 20
- $\exists H < S_6 \quad |H| = 20$
- S_6 contiene sgr di ordine 40? E di ordine 80?

1) $\left.\begin{matrix} \mathbb{Z}_{20} \\ \mathbb{Z}_{10} \times \mathbb{Z}_2 \end{matrix}\right\}$ possibili sgr. abeliani di ordine 20

↳ hanno entrambi un elemento di ordine 10 ma S_6 non ha elementi di ord 10

↑ va giustificato per bene

2) $|H| = 20 \Rightarrow H \cong P_5 \rtimes P_2$

$\langle (1\,2\,3\,4\,5) \rangle$
(a meno di rienumerare)

H deve normalizzare $P_5 \Rightarrow$ deve essere contenuto nel normalizzatore di un 5-ciclo $\quad H < N_{S_6}(P_5)$

non può essere $c=0$ perché il coniugio è un automorfismo quindi mantiene l'ordine

$$\overset{\text{WLOG}}{P_5} = \langle (1\,2\,\overset{\sigma}{\overset{\shortparallel}{3}}\,4\,5)\rangle \qquad N_{S_6}(\langle\sigma\rangle) = \{\rho \in S^6 \mid \rho\sigma\rho^{-1} = \sigma^i \; i = 1,\dots,4\}$$

l'eq. $\rho\sigma\rho^{-1} = \sigma^i$ è risolubile $\forall i = 1,\dots,4$ (stessa scomposizione in cicli disgiunti)

$\rho_1, \rho_2, \rho_3, \rho_4$ soluzioni per $i = 1,\dots,4$ rispettivamente

se $r \in Z(P_6)$ $\quad P_i r$ sol. di $\rho\sigma\rho^{-1} = \sigma^i$

$$\rho_i = r \qquad \rho_i\sigma\rho_i^{-1} = r\sigma r^{-1} \Rightarrow r \in \rho_i Z(\langle\sigma\rangle)$$

$$\rho_i^{-1} r \in Z(\langle\sigma\rangle)$$

$$Z_{S_6}(\langle\sigma\rangle) = \langle\sigma\rangle \qquad |N_{S_6}(\langle\sigma\rangle)| = 4 \cdot |Z(\langle\sigma\rangle)| = 20$$

2) $|K| = 40 \Rightarrow$ il 5-Sylow di K è normale in K
$\downarrow$ generato da un 5-ciclo

allora non può esistere perché il normalizzatore del sgr generato da un 5-ciclo ha solo 20 elementi

3) $|H| = 80 \rightarrow$ il 5-Sylow non è necessariamente normale

$$H \cap A_6 = \begin{cases} 40 & \text{NO sarebbe un sgr anche di } S_6 \\ 80 & \text{NO } 80 \nmid \frac{6!}{2} \end{cases}$$

06/11/2024
Patino

ESERCIZIO 7

$|G| = 80 \Rightarrow G$ non semplice

$80 = 16 \cdot 5 = 2^4 \cdot 5$

Supponiamo che G sia semplice

$n_2 = 5$

$n_5 = 16$

G agisce per coniugio sull'insieme dei 2-Sylow

$\rightsquigarrow \varphi : G \rightarrow S_5$ omo ma $80 \nmid 5! = 120$

(Assurdo perché ho trovato un sgr. normale non banale ma avevo supposto G semplice)

$\Rightarrow \operatorname{Ker}\varphi \neq \{e\}$ e $\operatorname{Ker}\varphi \neq G$ $\qquad \operatorname{Ker}\varphi \trianglelefteq G$

$\downarrow$

l'azione di G sui 2-Sylow è transitiva, $\operatorname{Ker}\varphi$ ha indice ≥ 5

$\operatorname{Ker}\varphi < \operatorname{Stab} x \quad \forall x \in \{1,\dots,5\}$

la cardinalità dell'orbita è pari all'indice dello Stab.

ESERCIZIO 8

$G \circlearrowleft X$, G finito

transitiva $(\forall x,y \in X \ \exists g \in G \mid gx = y)$

- $Stab_G(x) = \{g \in G \mid gx = x\}$ è coniugato a $Stab_G(y)$ $\forall x,y \in X$

$\exists g \mid gx = y$ $\quad Stab_G(gx) \supset g\,Stab_G(x)g^{-1}$

Se $s \in Stab(x)$ $\quad gsg^{-1}(gx) = gsx = gx$

$x = g^{-1}gx \Rightarrow Stab(x) \supset g^{-1}Stab(gx)g$

$\Updownarrow$

$g\,Stab(x)g^{-1} \supset Stab(gx)$

$\Rightarrow Stab(x) = g\,Stab(gx)g^{-1}$

Non serve che l'azione sia transitiva ma solo che x e y siano nella stessa orbita

- G finito $\exists g \in G \mid gx \neq x \ \forall x \in X$
  $|X| \geq 2$

esiste un elemento di G che non stabilizza nessun elemento di X

$\downarrow$

$\Updownarrow$

$g \notin Stab(x) \ \forall x \in X$

Stab(x) ha indice $|X| \geq 2 \Rightarrow$ sgr proprio

$\Updownarrow$

$g \notin \bigcup_{x \in X} Stab(x) = \bigcup_{g \in G} g\,Stab(x)g^{-1}$

perché abbiamo visto nel punto precedente che gli stabilizzatori sono tutti coniugati

Ricordiamo $H \lneq G$ $\quad |G| < \infty$

- $G \neq \bigcup_{g \in G} gHg^{-1}$ $\quad$ Quindi $\exists g \in G \setminus \bigcup_{g \in G} g\,Stab(x)g^{-1}$

ESERCIZIO 9

Def. $G \circlearrowleft X$ si dice doppiamente transitiva se $\forall (x,y) \neq (z,w)$ coppie in X $\quad x \neq y, \ z \neq w \quad \exists g \in G \mid \begin{array}{l} gx = z \\ gy = w \end{array}$

$|X| \geq 3$ TFAE:

(i) $G \circlearrowleft X$ è doppiamente transitiva

(ii) $G \circlearrowleft X \times X$ (definita come $g(x,y) = (gx, gy)$) ha esattamente due orbite

(iii) $\forall x \in X$ $\quad Stab(x) \circlearrowleft X \setminus \{x\}$ è transitiva

(iv) $G \circlearrowleft X$ è transitiva e $\exists x_0 \mid Stab(x_0) \circlearrowleft X \setminus \{x_0\}$ è transitiva

(i) $\Rightarrow$ (ii)

$\Delta = \{(x,x) \mid x \in X\} \subset X \times X$

$g(\Delta) = \Delta$

Δ è un'orbita se $G \circlearrowleft X$ è transitiva

Dimostriamolo: $x,y \in X$, $\exists z \in X$ $z \neq x,y$

(x,z) (y,z)

$\exists g \mid gx = y$, $gz = z$

Δ unica orbita $(x,x), (y,y) \in \Delta$, $\exists g \mid (gx, gx) = (y,y)$

$(X \times X) \setminus \Delta$ è unica orbita per def. di doppiamente transitivo.

(ii) $\Rightarrow$ (i) $g(\Delta) \subset \Delta$ Quindi se $X \times X$ ha due orbite, queste devono essere Δ e $(X \times X) \setminus \Delta$

↳ è un orbita $\Rightarrow G \circlearrowleft X$ doppiamente transitiva

(i) $\Rightarrow$ (iii) $y,z \in X \setminus \{x\}$

$\exists g \mid g(x,y) = (x,z)$ cioè $gx = x$, $gy = z$ $\Rightarrow g \in Stab(x)$

(iii) $\Rightarrow$ (iv)

$\exists x_0$ è chiaro.

Devo dimostrare che $G \circlearrowleft X$ è transitiva.

Prendo y,z. Se $y,z \in X \setminus \{x\}$ $\exists g \in Stab(x) \subset G \mid gy = z$

Devo considerare il caso $y = x$, $z \neq x$

$\exists t \neq x,z$ $\exists g \in Stab(t) \mid gy = z$

↳ prendo un terzo elemento $\neq$ da entrambi e applico la (iii) a questo

(iv) $\Rightarrow$ (i)

$(x,y), (z,w)$ con $x \neq y$, $z \neq w$

$\exists g \in G \mid gx = x_0$ $g(x,y) = (x_0, gy)$ $gy \neq x_0$

$\exists h \in G \mid hz = x_0$ $h(z,w) = (x_0, hw)$ $hw \neq x_0$

$\exists r \in Stab(x_0) \mid rgy = hw$

$h^{-1} rg(x,y) = (z,w)$ $\square$

ESERCIZIO 10

$G \circlearrowleft X \quad S = Stab(x) \quad x \in X \quad |X| \geq 3$
$S < H < G$

1. $H \circlearrowleft X$ non è transitiva

2. S sgr proprio massimale se $G \circlearrowleft X$ dopp. trans.

1. Prendiamo $g \in G \quad gx \in X$

Se $H \circlearrowleft X$ è transitiva, $\exists h \in H \mid hgx = x$

$\Rightarrow hg \in S \Rightarrow g \in h^{-1} S \subset H$

$\Rightarrow G = H$ $\lightning$

2. S non massimale $\Rightarrow \exists H$ con $S \lneq H \lneq G$

L'azione di H non è transitiva

Sappiamo che $S \circlearrowleft X \setminus \{x\}$ trans.

$X \setminus \{x\}$ è contenuto in un'unica H orbita

$\Rightarrow H$ ha due orbite $\{x\}$, $X \setminus \{x\} \Rightarrow H = S$ $\lightning$

- $S_n \circlearrowleft \{1, \dots, n\}$ è doppiamente transitiva?

$\cup$
$Stab(1) = S_{n-1} \circlearrowleft \{2, \dots, n\}$ transitivamente

$\Rightarrow Stab(1)$ sgr massimale $\hookrightarrow \Rightarrow S_n \circlearrowleft \{1, \dots, n\}$ doppiamente transitiva per il punto (iv) dell'esercizio 9

- $A_n \circlearrowleft \{1, \dots, n\}$

$Stab(1) \cong A_{n-1} \circlearrowleft \{2, \dots, n\}$ transitivamente (se $n-1 \geq 3$)

$A_{n-1} < A_n$ sgr massimale

- $GL_2(\mathbb{Z}/p\mathbb{Z}) \circlearrowleft (\mathbb{Z}/p\mathbb{Z})^2$

$GL_2(\mathbb{Z}/p\mathbb{Z}) \circlearrowleft$ ssp. vettoriali 1-dimensionali di $(\mathbb{Z}/p)^2$

L'azione è dopp. transitiva perché ogni base di $(\mathbb{Z}/p)^2$ può andare in ogni altra base

$x = \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle$ $\quad Stab(x) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} < GL_2(\mathbb{Z}/p\mathbb{Z})$ massimale

$\cap$

$(\mathbb{Z}/p)^2$

in dimensione maggiore $\left\{ \left[\begin{array}{c|c} * & \\ 0 & \\ \vdots & \\ 0 & \end{array} \right] \right\} < GL_n(\mathbb{K})$

PROP:

$SL_2(\mathbb{F}_p) / \{\pm id\}$ è un gr semplice $(p \geq 4)$

$\|=$

$\{A \in GL_2(\mathbb{F}_p) \mid \det A = 1\}$

$G \circlearrowleft G$ per coniugio

$\varphi : G \to Aut(G)$
$\quad g \mapsto c_g$

$Ker\varphi = Z(G)$

$Imm\varphi \cong Inn(G)$

$Z(S_n) = \{e\}$ se $n \geq 3$

$Inn(S_n) \cong S_n$

TEO $n \geq 3$, $n \neq 6$

$\quad Inn(S_n) = Aut(S_n)$

Cosa succede se $n = 6$?

- Quanti sono i 5-Sylow di S_5?

$\quad 4! = \#$ 5-cicli $\quad \frac{4!}{4} = 6 = n_5$

$S_5 \circlearrowleft \{5\text{-Sylow}\}$ coniugio $\rightsquigarrow \varphi : S_5 \to S_6$
transitivo $\qquad\qquad$ omomorfismo esotico

$\varphi(S_5)$ agisce transitivamente su $\{1, \ldots, 6\}$

φ è iniettivo

$Ker\varphi$ ha indice ≥ 6 (perché l'azione è transitiva)

$\ker\psi \triangleleft S_5 \Rightarrow \ker\psi = \{e\}$

$\left| S_6 / \psi(S_5) \right| = 6$

$S_6 \circlearrowleft S_6/\psi(S_5)$ data dalla moltiplicazione a sinistra

$(g_1(g_2\psi(S_5)) = g_1 g_2 \psi(S_5))$

$\varphi : S_6 \to S\left(S_6/\psi(S_5)\right) \cong S_6$

$S_6/\underbrace{\psi(S_5)}_{= H} = \{H, g_2H, g_3H, \dots, g_6H\}$

se φ iniettivo:

$\rho \circ \varphi \in \mathrm{Aut}(S_6)$

$\ker\varphi$ ha indice ≥ 6 (azione transitiva)

$\Rightarrow \ker\varphi = \{e\}$

$\Rightarrow \varphi$ isomorfismo $\Rightarrow \rho \circ \varphi \in \mathrm{Aut}(S_6)$

Voglio mostrare $\rho \circ \varphi \notin \mathrm{Inn}(S_6)$

Chi è $\rho \circ \varphi(H)$?

$\varphi(H) = \mathrm{Stab}(H) \Rightarrow \quad \rho \circ \varphi(H) = \mathrm{Stab}(1)$

Ma $g\,\mathrm{Stab}(1)\,g^{-1} = \mathrm{Stab}(g(1))$

$\Rightarrow$ Non può valere $\rho \circ \psi = c_g$, perché

$\rho \circ \varphi(H) = \mathrm{Stab}(x)$

$\Rightarrow c_g^{-1}(\mathrm{Stab}(1)) = H$, ma $c_g^{-1}(\mathrm{Stab}(1)) = \mathrm{Stab}(g^{-1}(1))$ ↯

H agisce transitivamente ma $\mathrm{Stab}(g^{-1}(1))$ no

$\Rightarrow H \neq \mathrm{Stab}(g^{-1}(1))$

---

p, q primi distinti

$|G| = p^k$, $|H| = q^h$ $\quad \varphi, \psi : H \to \mathrm{Aut}(G)$

$\underbrace{G \rtimes_\varphi H}_{= K} \cong \underbrace{G' \rtimes_\psi H'}_{= K'} \Rightarrow \ker\varphi \cong \ker\psi$

DIM. G è un p-Sylow in K. $G \triangleleft K \Rightarrow n_p = 1$

G' p-Sylow in K' $G' \triangleleft K' \Rightarrow n_p = 1$

$\sigma(G)$ p-Sylow $\Rightarrow \sigma(G) = G'$

$\sigma(H)$ q-Sylow $\exists g \in K' \mid g\sigma(H)g^{-1} = H'$

$\ker\varphi = H \cap Z(G)$

$\sigma(\ker\varphi) = \sigma(H) \cap \sigma(Z(G)) = \sigma(H) \cap Z(G')$

$G' \triangleleft K' \Rightarrow Z(G') \triangleleft K'$

perche' se $x \in Z(G')$ $hxh^{-1}g' = hxg''h^{-1} = g'hxh^{-1}$

$$\underset{hg''h^{-1}\,g' \in G'}{\overset{\shortparallel}{}}$$

$g\sigma(\ker\varphi)g^{-1} = g\sigma(H)g^{-1} \cap Z(G') = H' \cap Z(G') = \ker\psi$

$c_g \circ \sigma$ $\ker\varphi \xrightarrow{\sim} \ker\psi$ $\square$

11/11/2024
Patimo

ES. 2

A anello commutativo con unità

I, J ideali

→ 1) $IJ \subset I\cap J$
→ 2) $\sqrt{IJ} = \sqrt{I\cap J} = \sqrt{I}\cap\sqrt{J}$
→ 3) $\sqrt{\sqrt{I}} = \sqrt{I}$

1) $x \in IJ$
$x = ab \quad a\in I,\ b\in J$

Per la prop. di assorbimento $\begin{matrix} ab\in I \\ ab\in J\end{matrix} \Rightarrow \overset{x}{\overset{\shortparallel}{ab}} \in I\cap J$

$\Rightarrow IJ \subset I\cap J$

Non vale l'altra inclusione

$I=(2) \qquad IJ=(8)$
$J=(4) \qquad I\cap J=(4)$

2) • $IJ \subset I\cap J \Rightarrow \sqrt{IJ} \subset \sqrt{I\cap J}$

$x\in\sqrt{I\cap J} \Rightarrow \exists n \mid x^n \in I\cap J$

$x^{2n} = x^n\cdot x^n \in (I\cap J)(I\cap J) \subset IJ$

$\Rightarrow \sqrt{I\cap J} \subset \sqrt{IJ}$

• th: $\sqrt{I\cap J} = \sqrt{I}\cap\sqrt{J}$

$\subseteq$ $x\in\sqrt{I\cap J}\quad \exists n\mid x^n \in I\cap J \;{}^{\subset I}_{\subset J}$

$\Rightarrow x \in \sqrt{I}\cap\sqrt{J}$

$\supseteq$ $x \in \sqrt{I}\cap\sqrt{J} \quad \Rightarrow \begin{matrix}\exists n\mid x^n\in I\\ \exists m\mid x^m \in J\end{matrix}$

$x^{n+m} \in \sqrt{I\cap J}$

↳ appartiene sia a I che J per assorbimento

3) $\sqrt{\sqrt{I}} = \sqrt{I}$

$\supseteq$ $I \subset\sqrt{I} \Rightarrow \sqrt{I}\subset\sqrt{\sqrt{I}}$

$\subseteq$ $x\in\sqrt{\sqrt{I}} \Rightarrow \exists n\mid x^n\in\sqrt{I} \Rightarrow \exists m \mid \underset{x^{n\cdot m}}{\underset{\shortparallel}{(x^n)^m}} \in I$

allora $x\in\sqrt{I}$

□

→ 4) $I+J = \underset{(1)}{\underset{\shortparallel}{A}} \Rightarrow IJ = I\cap J$
⊂→ questa inclusione vale sempre

② $I+J=(1) \Rightarrow 1 = a+b \quad a\in I,\ b \in J$

Prendo $x \in I\cap J \quad x = x\cdot 1 = x(a+b) = \underset{JI}{\underset{\cap}{xa}} + \underset{IJ}{\underset{\cap}{xb}} \in IJ$

ES. $A = \mathbb{F}_5[x]$

$I = (x^2+1) \quad J = (x^3-1)$

$I\cap J = ?, \quad IJ = ? \quad I+J=?$

$IJ = (\{a(x^2+1)b(x^3-1) \mid ab \in A\}) = ((x^2+1)(x^3-1))$

$I+J = \{f \in \mathbb{F}_5[x] \mid f = a+b \quad a\in I,\ b\in J\}$

$f = a'(x^2+1) + b'(x^3-1)$

<u>OSS</u> K ideale $K = (f,g)$

Facendo la divisione con resto:

$g = qf + r \quad \deg(r) < \deg(f) \Rightarrow K = (f,g) = (f,r)$

$I+J = (x^2+1, x^3-1) = (x^2+1, x+1) = (x+1, 2) = (1)$

$x^3-1 = x(x^2+1)-(x+1) \qquad x^2+1 = x(x+1) - x+1 \qquad (x+1, x-1)$

dall' osservazione

perché 2 nel mio anello è invertibile

$\Rightarrow I\cap J = IJ = ((x^2+1)(x^3-1))$

<u>OSS</u> $a \in I \wedge a$ invertibile $\Rightarrow I = (1)$

$\exists b \mid ba = \underset{I}{\underset{\cap}{1}}$

ES. $A = \mathbb{Q}[x,y]$

$I = (x-1, y-1) \quad J = (1-xy)$

Tesi: I massimale, J primo ma non massimale

non esistono ideali propri di A che lo contengono strettamente

$\Updownarrow$

$A/_I$ è un campo (dal teo. di corrispondenza)

<u>OSS</u> A anello <u>COMMUTATIVO</u> è un campo se tutti i suoi elementi $\neq 0$ sono invertibili.

$\Rightarrow a \in A \quad (a) = A$ se $a \neq 0 \Rightarrow$ gli unici ideali sono (0) e A

Viceversa, se (0) e A sono gli unici ideali, dato $a \in A, a \neq 0$

$(a) = A \Rightarrow 1 \in (a) \Rightarrow 1 = ab$

per cui tutti gli elementi $\neq 0$ sono invertibili $\Rightarrow A$ campo.

$$\left\{ \begin{array}{c} \text{Ideali di} \\ A/_I \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Ideali di } A \\ \text{che contengono} \\ I \end{array} \right\}$$

$$J/_I \longleftarrow J$$

I massimale $\Leftrightarrow A/_I$ campo

Tornando all'esercizio:

Cerco $\varphi : \mathbb{Q}[x,y] \longrightarrow \mathbb{K}$ campo, $\varphi \neq 0$

tale che $\operatorname{Ker}\varphi = I$, cioè $\mathbb{Q}[x,y]/_I \cong \mathbb{K}$

$\mathbb{K} = \mathbb{Q} \qquad \underset{\text{omo di anelli}}{\underbrace{\varphi(f) = f(1,1)}}$

$\varphi(fg) = fg(1,1) = f(1,1)g(1,1) = \varphi(f)\varphi(g)$
$\varphi(f+g) = \varphi(f) + \varphi(g)$

È suriettivo (basta guardare i polinomi costanti)

$I \subseteq \operatorname{Ker}\varphi$

Vale anche $\operatorname{Ker}\varphi \subseteq I$?

$f \in \operatorname{Ker}\varphi \qquad f(x,y) = \sum a_{mn} x^m y^n = \sum_n q_n(x) y^n \in K[x][y]$

$$q_n(x) = \sum_m a_{mn} x^m$$

Faccio la divisione con resto

$f(x,y) = q(x,y)(x-1) + r(y)$

Come? $q_n(x) = q_n(x)(x-1) + r_n \quad \forall n \qquad r_n \in \mathbb{Q}$

$\Rightarrow f(x,y) = q(x,y)(x-1) + r(y)$ dove $q(x,y) = \sum q_n(x) y^n$
$r(y) = \sum r_n y^n$

$f \in \operatorname{Ker}\varphi \Rightarrow f(1,1) = 0 \Rightarrow q(1,1)\cdot 0 + r(1) = 0 \Rightarrow y-1 \mid r(y)$

$r(y) = (y-1)p(y)$

$\Rightarrow \operatorname{Ker}\varphi \subset I$

I è massimale e $J \subset I$ perché $J \subset \operatorname{Ker}\varphi = I$

in generale, K campo

$I(x_1 - a_1, \dots, x_n - a_n) \subset K[x_1 \dots x_n]$

$K[x_1 \dots x_n]/I \xrightarrow{\varphi} K$

$\varphi(f) = f(a_1, \dots, a_n)$

$q \in I \iff q(a_1, \dots, a_n) = 0$

—

J non è massimale $J \subset I$, $J \neq I$

$p \in J$ $p(x,y) = (1-xy)q(x,y)$

$\forall a \in \mathbb{Q}^*$ $p(a, 1/a) = 0$

Ma $q(x,y) = x-1 \in I$ $q(2, 1/2) = 1 \neq 0 \Rightarrow q \notin J$

—

Studiamo $G = SL_2(\mathbb{F}_5) = \{M \in M_{2\times 2}(\mathbb{F}_5) \mid \det M = 1\}$

Obiettivo: $SL_2(\mathbb{F}_5)/\{\pm id\} \cong A_5$

$|G| = ?$

$|GL_2(\mathbb{F}_5)| = (5^2-1)(5^2-5) = 24 \cdot 20$

$\det : GL_2(\mathbb{F}_5) \to \mathbb{F}_5^*$ $\Rightarrow$ det morfismo di gruppi

$A \mapsto \det A$

$\downarrow$

omo.

per Binet

$SL_2(\mathbb{F}_5) = \mathrm{Ker}(\det)$ $\left| GL_2(\mathbb{F}_5) / SL_2(\mathbb{F}_5) \right| = |\mathbb{F}_5^*| = 4$

$\Rightarrow |SL_2(\mathbb{F}_5)| = 120 = 2^3 \cdot 3 \cdot 5$

Che struttura hanno i 2-Sylow di $SL_2(\mathbb{F}_5)$?

Gruppi di ordine 8:

$\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, Q_8

Chi sono gli elementi di ordine 2 in $SL_2(\mathbb{F}_5)$?

$x \in SL_2(\mathbb{F}_5)$ $x^2 = id$ $\Rightarrow$ il polinomio minimo di x divide $(\lambda+1)(\lambda-1)$

$\Downarrow$

x diagonalizzabile

$\exists\, g \in GL_2(\mathbb{F}_5) \mid gxg^{-1}$ diagonale

con autovalori 1 e -1

perché $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ è centrale

$\det(gxg^{-1}) = 1 \Rightarrow gxg^{-1} = \begin{pmatrix}-1&0\\0&-1\end{pmatrix} \Rightarrow x = \begin{pmatrix}-1&0\\0&-1\end{pmatrix}$

$\cancel{\mathbb{Z}/4 \times \mathbb{Z}_2}$, $\cancel{(\mathbb{Z}/2\mathbb{Z})^3}$, $\cancel{D_4}$ $\leftarrow$ $\exists!$ elemento di ordine 2

Chi sono gli elementi di ordine 4?

$A \in SL_2(\mathbb{F}_5)$ $\quad A^4 = id \Rightarrow$ pol. minimo di A divide

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

$\Downarrow$

A diagonalizzabile

gAg^{-1} diagonale con autoval. ± 1 e ± 2

gAg^{-1} ha det 1

$\Rightarrow gAg^{-1} = \cancel{\begin{pmatrix}1&\\&1\end{pmatrix}}, \cancel{\begin{pmatrix}-1&\\&-1\end{pmatrix}}, \underbrace{\begin{pmatrix}2&\\&-2\end{pmatrix}, \begin{pmatrix}-2&\\&2\end{pmatrix}}_{\text{elementi di ordine 4}}$

<u>OSS</u> $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}2&\\&-2\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}-2&\\&2\end{pmatrix}$

$\Rightarrow$ Tutti gli el. di ord. 4 appartengono alla stessa classe di coniugio in $GL_2(\mathbb{F}_5)$ di $\begin{pmatrix}+2&0\\0&-2\end{pmatrix}$

Quanti sono gli el. di ord 4?

È l'indice di $Z_{GL_2(\mathbb{F}_5)}\left(\begin{pmatrix}2&0\\0&-2\end{pmatrix}\right)$

$= \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} \mid a=b=0\right\}$ ↗ si calcola a mano

$=$ matrici diagonali invertibili

$\Rightarrow \left| Z_{GL_2(\mathbb{F}_5)}\left(\begin{pmatrix}2&\\&-2\end{pmatrix}\right)\right| = 4^2 = 16$

$\Rightarrow \mathcal{C}\left(\begin{pmatrix}2&\\&-2\end{pmatrix}\right) = 30$

$\cap$

$SL_2(\mathbb{F}_5)$

$Z_{SL_2} = Z_{GL_2} \cap SL_2 =$ matrici diagonali in SL_2

$\Downarrow$

ha 4 elementi (scelgo il primo el. come voglio e il secondo come suo inverso)

$$\Rightarrow \quad Cl_{GL_2}\left(\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}\right) = Cl_{SL_2}\left(\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}\right)$$

$\Rightarrow$ il 2-Sylow è isomorfo a Q_8

Quanti sono questi 2-Sylow?

$$n_2 = \cancel{1}, \cancel{3}, 5, 15$$

In Q_8 ci sono 6 elementi di ordine 8 $\Rightarrow n_2 \neq 1 \quad n_2 \neq 3$

P_1, P_2 2-Sylow in $SL_2(\mathbb{F}_5)$

$x \in P_1 \cap P_2 \quad ord(x) = 4 \quad \Rightarrow P_1 = P_2$

Infatti $P_1 = N(x)$

$$\underset{\text{in } SL_2}{N}\begin{pmatrix} 2 & \\ & -2 \end{pmatrix} = \left\{ g \in L_2 \mid g\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}g^{-1} = \underbrace{\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}}_{\text{centralizzatore}} \circ \underbrace{\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}^3}_{= \begin{pmatrix} -2 & \\ & 2 \end{pmatrix}} \right\} =$$

$$= Z_{SL_2}\begin{pmatrix} 2 & \\ & -2 \end{pmatrix} \cup \left\{ g \mid g\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}g^{-1} = \begin{pmatrix} -2 & \\ & 2 \end{pmatrix} \right\}$$

$$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{= g}\begin{pmatrix} 2 & \\ & -2 \end{pmatrix} = \begin{pmatrix} -2 & \\ & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff a = d = 0$$

$\Rightarrow \left|N_{SL_2}\begin{pmatrix} 2 & \\ & -2 \end{pmatrix}\right| = 8 \rightarrow$ è ~~un~~ il 2-Sylow che contiene x

Ricapitolando:

- 30 el. di ord 4
- ogni 2-Sylow ne contiene 6
- 2-Sylow distinti non hanno el. di ord 4 in comune

$\Big\} \Rightarrow n_2 = 5$

$\varphi : SL_2(\mathbb{F}_5) \longrightarrow S_5$ coniugio dei 2-Sylow

$$\Rightarrow \quad SL_2(\mathbb{F}_5) / \{\pm id\} \cong A_5$$

$I \subseteq A$ ideale $\rightarrow$ banale se $I = 0$
$\rightarrow$ proprio se $I \subsetneq A$

<u>OSS</u>

I è proprio $\iff I \cap A^* = \emptyset$

Contronominale: $I \cap A^* \neq \emptyset \iff I = A$

$I = A \iff 1 \in I$

$1 \in I \implies I \cap A^* \neq \emptyset$

assorbimento

$I \cap A^* \neq \emptyset$ allora sia $z \in I \cap A^*$, $z^{-1} \in A \implies zz^{-1} = 1 \in I$

Def. $I \subsetneq A$ si dice **PRIMO** se

$xy \in I \implies x \in I \vee y \in I$
$x, y \in A$

Def. $I \subsetneq A$ si dice **MASSIMALE** se $\forall J \subseteq A$ |

$I \subseteq J \subseteq A \implies J = \begin{cases} I \\ A \end{cases}$

Proposizione $I \subsetneq A$

(i) I è primo $\iff A/I$ è un dominio

(ii) I è massimale $\iff A/I$ è un campo

(Corollario: I massimale $\implies I$ primo)

DIM.

(i) I è primo SSE $(\forall x, y \in A \quad xy \in I \implies x \in I \vee y \in I)$

A/I dominio SSE $\forall x, y \in A \ (x+I)(y+I) = I \iff x + I = I \vee y + I = I$

$xy + I = I \quad xy \in I \implies x \in I \vee y \in I$

(ii) I massimale $\iff A/I$ ha come unici ideali $(\bar{0})$ e $(\bar{1}) = A/I$

corrispondenza

$\iff A/I$ è un campo

$\implies$ sia $\bar{x} \in A/I \quad \bar{x} \neq 0 \implies (\bar{x}) = A/I = (\bar{1})$

allora $\exists \bar{a} \in A/I$ | $\bar{x}\bar{a} = \bar{1} \implies \bar{x}$ invertibile

$\Leftarrow$ facile

---

confrontabile con tutti gli elementi

$(\mathcal{F}, \leq)$ insieme partialmente ordinato

$X \subseteq \mathcal{F}$, $M \in \mathcal{F}$ maggiorante per X se $\forall a \in X$, $a \leq M$

$A \in \mathcal{F}$ è un elemento massimale di X se (non deve essere necessariamente confrontabile con tutti)

$A \in X$ e $\forall B \in X \quad A \leq B \Rightarrow A = B$

$A \in \mathcal{F}$ è un massimo per $\mathcal{F}$ (La differenza tra maggiorante e massimo è che il massimo deve stare nell'insieme considerato, un maggiorante non per forza)

$\forall B \in \mathcal{F} \quad B \leq A$

Una CATENA di $\mathcal{F}$ è un sottoinsieme di $\mathcal{F}$ totalmente ordinato

$(\mathcal{F}, \leq)$ si dice INDUTTIVO se ogni catena di $\mathcal{F}$ ammette un maggiorante in $\mathcal{F}$

LEMMA DI ZORN

$(\mathcal{F}, \leq)$ part. ordinato $\quad \mathcal{F} \neq \emptyset$

$\mathcal{F}$ induttivo $\Rightarrow$ $\mathcal{F}$ ammette elementi massimali

Esempio:

$\mathcal{F}$ = ideali propri di A, $\subseteq$

$\mathcal{F} \neq \emptyset \qquad \mathcal{C} = \{I_i\}_{i \in \hat{I}}$ catena $\forall i,j \in \hat{I} \quad I_i \subseteq I_j \vee I_j \subseteq I_i$

$I = \bigcup_{i \in \hat{I}} I_i$ è un ideale $\qquad I \supseteq I_i \quad \forall i \in \hat{I}$

$I \in \mathcal{F}$ se $1 \in I = \bigcup I_i \Rightarrow \exists i \mid 1 \in I_i$

$\Rightarrow$ Ogni anello ammette ideali massimali

Proposizione (i): ogni ideale proprio di A è contenuto in un ideale massimale

(ii): ogni elemento non invertibile di A è contenuto in un ideale massimale

DIM (i) $\Rightarrow$ (ii) $\quad x \in A \setminus A^* \Rightarrow (x) \subsetneq A \underset{(i)}{\Rightarrow} (ii)$

(i) $I \subsetneq A \quad$ Tesi: $\exists M$ ideale massimale di $A \mid I \subseteq M$

$\mathcal{F} = \{J \subseteq A \mid I \subseteq J\} \qquad (\mathcal{F}, \subseteq)$ poset (insieme parzialmente ordinato) $\quad I \in \mathcal{F} \Rightarrow \mathcal{F} \neq \emptyset$

$\mathcal{F}$ induttivo $\quad \mathcal{C} = \{I_i\}_{i \in \hat{I}}$ catena $\quad \mathcal{C} \subseteq \mathcal{F}$

$J = \bigcup_{i \in \hat{I}} I_i \qquad J \subseteq A$ ideale $\qquad J \supseteq I$ ovvio

J è proprio perché l'unione di id. propri è propria

$\Rightarrow J \in \mathcal{F}$

J maggiorante in $\mathcal{F}$ per $\mathcal{C}$.

Per il lemma di Zorn $\mathcal{F}$ ammette elementi massimali

$\Rightarrow \exists M \in \mathcal{F}$ elemento massimale di $\mathcal{F}$

$I \subseteq M \subsetneq A$

↳ voglio far vedere che è un ideale massimale di A

Sia $L \subsetneq A \mid M \subseteq L \Rightarrow I \subseteq L \Rightarrow L \in \mathcal{F} \Rightarrow L = M$ perché M massimale in $\mathcal{F}$.

Proposizione

$\pi : A \to A/I$

Nella corrispondenza tra ideali di A/I e ideali di A che contengono I si conservano ideali primi e ideali massimali.

DIM. $I \subseteq J \subseteq A \qquad J \mapsto \pi_J(J) = J/I$

$$A/J \cong {}^{A/I}\!/_{J/I} \quad \text{(2° teo. di omomorfismo)}$$

J massimale $\Rightarrow A/J$ campo $\Rightarrow {}^{A/I}\!/_{J/I}$ campo $\Rightarrow$

$\Rightarrow J/I$ massimale

Anello delle frazioni di un dominio

A (comm. con 1) dominio

$S \subset A \quad \left.\begin{array}{l} 0 \notin S \\ 1 \in S \\ \forall s,t \in S \Rightarrow st \in S \end{array}\right] \Rightarrow S$ è una PARTE MOLTIPLICATIVA di A

Esempio: $S = A \setminus \{0\}$

$S = \{x^n\}_{n \geq 0} \quad x \in A,\ x \neq 0$

$S^{-1}A = \left\{ \frac{a}{s} \mid a \in A, s \in S \right\} /_{\sim} \qquad \frac{a}{s} \sim \frac{b}{t} \iff at = bs$

$S \times A /_{\sim}$ dove $(s,a) \sim (t,b) \iff at = bs$ e chiamo frazioni le classi di equivalenza

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Sono ben definite?

$\frac{a}{s} = \frac{a'}{s'}$ $\quad \frac{b}{t} = \frac{b'}{t'}$

$$\frac{a'}{s'} + \frac{b'}{t'} = \frac{a't' + b's'}{s't'} \overset{?}{=} \frac{at+bs}{st}$$

$$\Updownarrow$$

$$st(a't' + b's') = s't'(at + bs)$$

$$\underbrace{sa'}_{s'a}tt' + \underbrace{tb'}_{bt'}ss' = s't'at + s't'bs \quad \checkmark$$

Idem per il prodotto

TEOREMA $(S^{-1}A, +, \cdot)$ è un anello commutativo con identità ed è un dominio

$\frac{0}{1}$, $\frac{1}{1}$, $\quad \frac{a}{s} \cdot \frac{b}{t} = \frac{0}{1}$ $\quad ab \cdot 1 = 0 \cdot st = 0 \Rightarrow a = 0 \vee b = 0$
poiché A è un dominio

Esempio: $A = \mathbb{Z}$ $\quad S = \{10^n\}_{n \geq 0}$

$$S^{-1}A = \left\{ \frac{a}{10^n} \;\middle|\; a \in \mathbb{Z} \;\; n \geq 0 \right\}$$

$(S^{-1}A)^* = ?$

$\frac{a}{s} \cdot \frac{b}{t} = \frac{1}{1}$ $\quad ab = st \in S$

Prop:

$$(S^{-1}A)^* = \left\{ \frac{a}{s} \;\middle|\; \exists b \in A \mid ab \in S \right\}$$

$\supseteq$ $\cancel{\frac{a}{s} \in S^{-1}A^* \Leftrightarrow \frac{a}{1} \in S^{-1}A^*}$ $\quad \exists b \mid ab \in S \Rightarrow \frac{sb}{ab} \in S^{-1}A$

$\cancel{\frac{b}{ab} \cdot \frac{a}{1} = \frac{ab}{ab} = 1}$ $\quad$ e si verifica che $\frac{a}{s} \cdot \frac{sb}{ab} = \frac{1}{1}$

$\Rightarrow \frac{a}{s} \in (S^{-1}A)^*$

$\subseteq$ $\frac{a}{s} \in (S^{-1}A)^* \Rightarrow \exists \frac{a'}{s'} \mid \frac{aa'}{ss'} = \frac{1}{1} \Rightarrow aa' = ss' \in S \Rightarrow aa' \in S$ $\quad \square$

Proposizione $f: A \to S^{-1}A$ è un omo. iniettivo
$a \longmapsto a/1$

Proposizione $S = A \setminus \{0\}$

$S^{-1}A$ è un campo (campo dei quozienti di A)

il campo dei quozienti è il più piccolo campo che contiene A

DIM. S p.m. di A
(parte moltiplicativa)

$\frac{a}{s} \in S^{-1}A \setminus \{0\}$ $\quad \frac{s}{a} \in S^{-1}A \Rightarrow \frac{a}{s}$ invertibile $\quad S^{-1}A$ campo
perché sia s che a sono elementi di A

K campo. $A \subseteq K \Rightarrow \forall s \in A \quad s \neq 0 \quad (\forall s \in S)$
$\frac{1}{s} \in K \quad a \in A \quad a \in K, \frac{1}{s} \in K$
$\frac{a}{s} \in K \quad \forall \begin{smallmatrix} a \in A \\ s \in S \end{smallmatrix} \Rightarrow S^{-1}A \subseteq K$

Esempio

- $K[x]$ campo dei quozienti: $K(x) = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f, g \in K[x], g(x) \neq 0 \right\}$

  ↑ anello delle funzioni razionali

- A dominio $P \subset A$ ideale primo

  $A_P = S^{-1}A$ con $S = A \setminus P \to$ è una parte moltiplicativa

  $\forall s, t \in S \Rightarrow st \in S$
  $\forall s, t \notin P \Rightarrow st \notin P$ $\Updownarrow$ P primo

  A_P è un anello locale, cioè ammette un unico ideale massimale, cioè $(P)A_P$
  ↳ cioè l'ideale (P) visto dentro A_P

  $f: A \to A_P$
  $a \mapsto a/1$

  $(P)A_P = (f(P))$

Def. A dominio si dice DOMINIO EUCLIDEO (ED) se ammette una funzione grado $d: A \setminus \{0\} \to \mathbb{N}$

(1) $\forall x, y \in A \setminus \{0\} \quad d(x) \leq d(xy)$

(2) $\forall x \in A \quad y \in A \setminus \{0\} \quad \exists q, r$ t.c. $x = qy + r \quad \begin{cases} r = 0 \\ d(r) < d(y) \end{cases}$

Esempio:

- $(\mathbb{Z}, |\cdot|)$
- $(K[x], \deg)$
- $(K[[x]], d)$ $\quad \sum_{i \geq n_0} a_i x^i \quad a_{n_0} \neq 0$
  $\downarrow d$
  n_0
- $(\mathbb{Z}[i], N)$ $\quad N(a+ib) = a^2 + b^2$

Proposizione Gli elementi di grado minimo di A sono gli elementi di A^*

A ED $\Rightarrow A$ PID

$\mathbb{C}[x,x^{-1}]$ può essere ottenuto localizzando $\mathbb{C}[x]$ in

$S = \{x^k \mid k \geq 1\}$

cioè $S^{-1}\mathbb{C}[x] \cong \mathbb{C}[x,x^{-1}]$

ES4 A dominio, $S \subset A$ parte moltiplicativa

1) Dimostriamo che gli ideali di $S^{-1}A$ sono tutti della forma $S^{-1}I$, con I ideale di A

<u>OSS</u> I ideale di $A \Rightarrow S^{-1}I$ ideale di $S^{-1}A$

$$S^{-1}I = \left\{\frac{a}{b} \mid a \in I, b \in S\right\}$$

Infatti: $\frac{r}{s} \in S^{-1}A$ $\frac{a}{b} \in S^{-1}I \Rightarrow \frac{ra}{bs} \in S^{-1}I$ perché $ra \in I$

Se $\frac{a}{b}, \frac{c}{d} \in S^{-1}I$ $b,d \in S$, $a,c \in I$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in S^{-1}I \qquad ad+bc \in I$$

J ideale di $S^{-1}A$. Cerco I ideale $J = S^{-1}I$

Scelgo $I = J \cap A$

Devo far vedere che I è un ideale e che $S^{-1}I = J$

- I ideale: $\frac{a}{1} \in J \cap A \Rightarrow \frac{ba}{1} \in J \cap A$ perché $\frac{ba}{1} \in A$ e $b \cdot \frac{a}{1} = \frac{b}{1} \cdot \frac{a}{1} \in J$

$\frac{a}{1}, \frac{b}{1} \in J \cap A \Rightarrow \frac{a}{1} + \frac{b}{1} \in J \cap A$

$S^{-1}I = J$?

$\subseteq$ $S^{-1}I = \left\{\frac{a}{s} \mid a \in I, s \in S\right\} \subset J$ perché $\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} \in J$

$\supseteq$ $\frac{a}{b} \in J$ con $a \in A$, $b \in S$ $\frac{b}{1} \cdot \frac{a}{b} = \frac{a}{1} \in J \cap A \Rightarrow \frac{a}{b} \in S^{-1}I$

$$\begin{Bmatrix}\text{ideali} \\ \text{di } S^{-1}A\end{Bmatrix} \underset{S^{-1}I \leftarrow I}{\overset{J \mapsto J\cap A}{\rightleftarrows}} \begin{Bmatrix}\text{ideali} \\ \text{di } A\end{Bmatrix}$$

CONTROESEMPIO

$\mathbb{C}[x,x^{-1}] = S^{-1}\mathbb{C}[x]$ $S = \{x^k\}$

$S^{-1}(x(x+1)) = S^{-1}((x+1))$

Queste operazioni NON sono una l'inversa dell'altra.

I ideale di A con $I \cap S \neq \emptyset$ allora $1 \in S^{-1}I \Rightarrow S^{-1}I = S^{-1}A$

$$\begin{Bmatrix}\text{ideali primi} \\ \text{di } S^{-1}A\end{Bmatrix} \rightleftarrows \begin{Bmatrix}\text{ideali primi di} \\ A \text{ con } P \cap S = \emptyset\end{Bmatrix}$$

④

$(2z^2-1) \subset \ker\varphi$ ma $(2t^2-1)$ è massimale $\Rightarrow \ker\varphi = (2t^2-1)$

REMINDER: se A è PID (per esempio A euclideo)

allora ogni ideale primo $\neq 0$ è massimale

K campo $\Rightarrow K[x]$ è PID (è anche euclideo)

$\mathbb{Q}[x,y]$ $J = (1-xy)$ è primo ma non massimale

non PID

$(I = (x)$ è anche primo ma non massimale$)$

$\mathbb{Q}[x,y]/_{(x)} \cong \mathbb{Q}[y]$

Ricordiamo anche I primo $\Longleftrightarrow A/_I$ dominio

$(1-xy) \subsetneq (x-1, y-1)$ $\quad y(x-1)+(y-1) = xy-1$

$\hookrightarrow (1-xy)$ non è massimale

$\mathbb{Q}[x,y]/_{(1-xy)}$ è un dominio?

$\varphi : \mathbb{Q}[x,y] \to \mathbb{Q}[x,x^{-1}] = \boxed{\left\{ \sum_{i=-n}^{n} a_i x^i \mid a_i \in \mathbb{Q} \right\} \text{ "POLINOMI DI LAURENT"}}$

$\varphi(f(x,y)) := f(x,x^{-1})$

Si verifica che φ è omo di anelli

$\varphi(fg) = f(x,x^{-1})\, g(x,x^{-1}) = \varphi(f)\varphi(g)$

$\ker\varphi = ?$

$\varphi(1-xy) = 0 \Rightarrow (1-xy) \subset \ker\varphi$

Sia ora $p \in \ker\varphi$

$p(x,x^{-1}) = 0 \qquad p(x,y) = \sum a_{n,m} x^n y^m$

$p(x,x^{-1}) = \sum a_{n,m} x^{n-m} =$ raccolgo le potenze uguali

$= \sum_d \left(\sum_n a_{n,n-d}\right) \underline{\underline{x^d}} = 0 \Longleftrightarrow \sum_n a_{n,n-d} = 0 \ \forall d$

$p(x,y) = \sum_{m,n} a_{n,m} x^{n-m} (xy)^m \overset{m=n-d}{=} \sum_d \sum_n a_{n,n-d}\, x^d (xy)^{n-d} =$

non dipende da n

$= \sum_d x^d \left(\sum_n a_{n,n-d} (xy)^{n-d} \right)$

OSS $f(z) = \sum b_n z^n$ se $\sum b_n = 0$, $f(1) = 0 \Rightarrow z-1 \mid f(z)$

$xy-1 \mid \sum a_{n,n-d} (xy)^{n-d} \ \forall d \Rightarrow xy-1 \mid p(x,y)$

$\Rightarrow \ker\varphi = (1-xy)$

(1)

18/11/2024
Patimo

ES.1

1) A dominio di integrità finito $\Rightarrow$ A campo

$x \in A \setminus \{0\}$

$\cdot x : A \to A$

moltiplicazione per x

A dominio $\Rightarrow$ $ax = 0$ SSE $a = 0$ $\Rightarrow$ $(\cdot x)$ è iniettiva
$(\cdot x)$ suriettiva

$\Rightarrow 1 \in Im(\cdot x)$ cioè $\exists b \mid b \cdot x = 1$

2) $|A| = p$ primo $\Rightarrow$ A campo

$(A, +)$ gruppo abeliano

$(A, +) \cong \mathbb{Z}/p\mathbb{Z} = \langle 1 \rangle$

Voglio far vedere $\mathbb{F}_p \cong A$

$\varphi : \mathbb{Z} \to \mathbb{F}_p$ $\to$ omo di anelli

$n \mapsto \bar{n}$ $\quad$ $Ker\varphi \cong p\mathbb{Z} \Rightarrow \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$

Similmente $\psi : \mathbb{Z} \to A$
$n \mapsto n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ volte}}$

ψ omo di anelli suriettivo (perché A è generato da 1)

$A \cong \mathbb{Z}/Ker\psi \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$

OSS con lo stesso argomento $(A, +) \cong \mathbb{Z}/n\mathbb{Z}$ come gruppo

allora $A \cong (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ come anello

CLASSIFICARE GLI ANELLI CON 4 ELEMENTI

$(A, +) \cong \mathbb{Z}_4 \lor \mathbb{Z}_2 \times \mathbb{Z}_2 \Rightarrow$

$\Downarrow$

$(A, +, \cdot) \cong \mathbb{Z}/4\mathbb{Z}$ come anello

$\langle 1 \rangle \cong \mathbb{Z}_2$ (come gruppo)

$\langle 1 \rangle$ è un sottoanello
$\langle 1 \rangle \cong \mathbb{Z}_2$ come anello

A è uno spazio vettoriale su $\langle 1 \rangle \cong \mathbb{F}_2$ di dim 2

$A = \langle 1 \rangle \cup \langle 1 \rangle x \qquad x \notin \langle 1 \rangle$

Possiamo costruire un omomorfismo di anelli

③

$\mathbb{F}_2[x]/(x^2-1) = \mathbb{F}_2[x]/(x-1)^2 \cong \mathbb{F}_2[y]/(y^2)$

BONUS la stessa classificazione vale per $|A| = p^2$

ES.3 $\mathbb{Q}[x,y]/(x-y,\ x^3+y^3-x)$

Scrivere A come prodotto di campi

$I = (x-y)$

$J = (x^3+y^3-x)$

$\mathbb{Q}[x,y]/_{I+J} \cong \mathbb{Q}[x,y]/I \Big/ {}^{I+J}/_I$

• Chi è $\mathbb{Q}[x,y]/(x-y)$?

Voglio mostrare $\mathbb{Q}[x,y]/(x-y) \cong \mathbb{Q}[z]$

$f: \mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[z]$

$p(x,y) \longmapsto p(z,z)$

$I \subset K$ ideali

$A/K \cong A/I \big/ K/I$

$(x-y) \subset \ker f$ (banale)

Per l'altra inclusione:

$f: A \to B$ con $\ker f = I$, $B \cong A/I$

$f(K) \cong K/I$

$f: K \to f(K)$

$A/K \cong A/I \big/ f(K)$

$p(x,y) = \sum a_{n,m} x^n y^m$ con $p(z,z) = 0$

$p(z,z) = \sum a_{nm} z^{n+m} = 0$

$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1}) \Rightarrow x^n - y^n \equiv 0 \mod (x-y)$

$x^n \equiv y^n \mod (x-y)$

$\Downarrow$

$p(x,y) \equiv \sum a_{n,m} y^n y^m \pmod{x-y}$

$\equiv 0 \pmod{x-y}$

$\Rightarrow (x-y) \mid p(x,y) \Rightarrow \ker f \subset (x-y)$

Quindi $\ker f = (x-y)$

$\mathbb{Q}[x,y]/_{I+J} \cong \mathbb{Q}[z]/_{f(I+J)} = \mathbb{Q}[x]/_{f(J)} = \mathbb{Q}[z]/_{f(x^3+y^3-x)} =$

$= \mathbb{Q}[z]/(2z^3-z) \cong \underbrace{\mathbb{Q}[z]/(z) \times \mathbb{Q}[z]/(2z^2-1)}_{\text{campi}}$

Più esplicitamente $\mathbb{Q}[z]/(2z^2-1) \cong \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

$\varphi: \mathbb{Q}[z] \to \mathbb{Q}(\sqrt{2})$

$z \mapsto 1/\sqrt{2}$

(2)

$\varphi: \mathbb{F}_2[x] \to A$
$\quad x \mapsto a$

(*)

→ sto usando la proprietà universale dell'anello di polinomi

S, R anelli, $f: R \to S$ omo di anelli

Fissiamo $s \in S$

$\exists!\ \bar{f}: R[x] \to S$ omo di anelli t.c.

$\bar{f}(r) = f(r) \quad \forall r \in R$
$\bar{f}(x) = s$

DIM definisco $\bar{f}(\sum_n r_n x^n) = \sum_n f(r_n) s^n$ e verifico che è l'unico omo con le prop. richieste

(*) φ è suriettivo $A \cong \mathbb{F}_2[x]/\mathrm{Ker}\,\varphi$

Se $b = a^2 \quad \varphi(x^2) = b$

$b = 0, 1, a, a+1 \qquad (|A| = 4)$

$b = 0 \to x^2 \in \mathrm{Ker}\,\varphi$

$$\left|\mathbb{F}_2[x]/(x^2)\right| = 4 \Rightarrow A \cong \mathbb{F}_2[x]/(x^2)$$

$b = 1 \Rightarrow A \cong \mathbb{F}_2[x]/(x^2-1)$

$b = a \Rightarrow A \cong \mathbb{F}_2[x]/(x^2-x)$

$b = a+1 \Rightarrow A \cong \mathbb{F}_2[x]/(x^2+x+1)$

↳ irriducibile su $\mathbb{F}_2$
⇓

$$\mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$$

$x^2 - x = \underbrace{x(x-1)}_{\text{coprimi}} \overset{\text{teo. cinese}}{\Rightarrow} \mathbb{F}_2/(x^2-1) \cong \mathbb{F}_2[x]/(x) \times \mathbb{F}_2[x]/(x-1) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$

(che non è un campo per cui non può essere isomorfo al precedente)

$\mathbb{F}_2[x]/(x^2)$ non è un campo
⇓
$\exists a \mid a^2 = 0$ (per cui non è isomorfo a $\mathbb{F}_2 \times \mathbb{F}_2$ che non ha elementi nilpotenti)

19/11/2024
Del Corso

Sia A un dominio di integrità

Def. $a, b \in A$, $b \neq 0$

allora $b | a$ se $\exists c \in A$ tale che $a = bc$

OSS $b | a \iff (a) \subseteq (b)$

Def. $a, b \in A$ si dicono associati se vale una delle seguenti condizioni equivalenti (si scrive $a \sim b$)

(i) $\exists u \in A^* \mid b = au$

(ii) $b | a \wedge a | b$

(iii) $(a) = (b)$

(ii) $\Rightarrow$ (i) $\quad$ $b | a \Rightarrow a = bc$ $\quad$ $a = adc$
$a | b \Rightarrow b = ad$ $\quad$ $a(1 - dc) = 0 \Rightarrow dc = 1$

Def. $x \in A \setminus (A^* \cup \{0\})$ si dice primo se $\forall z, y \in A$

$x | yz \Rightarrow x | y \vee x | z$

x si dice irriducibile se $x = ab$ con $a, b \in A \Rightarrow$

$\Rightarrow a \in A^* \vee b \in A^*$

Proposizione A dominio

1) x primo $\Rightarrow x$ irriducibile

2) x primo $\iff (x)$ è un ideale primo

3) x irriducibile $\iff (x)$ è massimale nella classe degli ideali principali di A

non necessariamente in tutto A

DIM. 1) Uguale a quella su $\mathbb{Z}$

2) Già vista

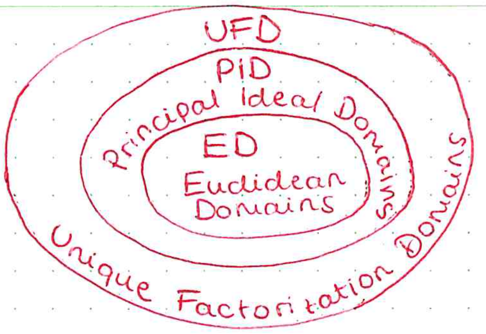
3) $(\Rightarrow)$ $(x) \subseteq (y) \subsetneq A$ $\quad \exists a \in A \mid x = ya$

$\Rightarrow y \in A^* \vee a \in A^* \Rightarrow (x) = (y)$

NO, altrimenti sarebbe $(y) = A$

$(\Leftarrow)$ $x = ab$ e supponiamo $a \notin A^*$

$(x) \subseteq (a) \subsetneq A$
$\Rightarrow (x) = (a) \Rightarrow x \sim a \Rightarrow b \in A^*$



- le serie formali di potenze $K[[x]] = \{\sum_{i \geq n_0} a_i x^i \mid n_0 \in \mathbb{Z}, a_i \in K\}$ sono un ED (la funz. grado manda ogni serie nel grado del monomio di grado minore che compare)
- Ogni campo è un ED (il grado di ogni elemento non nullo è 1)

Proposizione A è PID $\Rightarrow$ gli ideali primi di A sono $\{0\}$ e gli ideali massimali

DIM. $\{0\}$ è primo $\Leftrightarrow$ A è un dominio

e gli ideali massimali sono primi in ogni anello

Sia $P \subseteq A$ ideale primo, $P \neq \{0\}$

$P = (x)$ x primo $\Rightarrow$ x irriducibile $\Rightarrow$

$\Rightarrow$ (x) massimale nella classe degli ideali principali

(cioè tutti in questo caso perché A è PID) $\square$

Domini euclidei, PID e UFD

Dati $a, b \in A$ dominio euclideo, con l'Algoritmo di Euclide posso calcolare $d = (a,b)$ e $x_0, y_0 \in A \mid ax_0 + by_0 = d$

Def. In un PID d è detto MCD tra a e b se $(d) = (a,b)$ (non è unico ma lo è a meno di associati)

Def. A dominio si dice a fattorizzazione unica (UFD) se $\forall x \in A$ $x \notin A^*$, $x \neq 0$, x si scrive in modo "unico" come prodotto di irriducibili

a meno di moltiplicazione per invertibili e ordine dei fattori

Proposizione Sia A un UFD

$a, b \in A$ non entrambi nulli. Allora esiste un massimo comune divisore tra a e b, $d = \prod$ "fattori comuni con minimo esponente"

nel senso classico del termine

In questo caso il MCD non coincide con il generatore dell' ideale (a,b).

$d = MCD(a,b)$
$(a,b) \subseteq (d)$

Esempio $\quad \mathbb{Z}[x] \quad MCD(2,x) = 1$ ma $1 \notin (2,x)$

$\downarrow$

se per assurdo appartenesse a I

$$1 = 2p(x) + xq(x)$$

valuto in $x = 0$

$$1 = 2p(0) \Rightarrow 1 \text{ è pari } \lightning$$

Teorema di caratterizzazione degli UFD

A dominio, sono fatti equivalenti:

① A è UFD

② Valgono le due seguenti considerazioni
(i) Ogni elemento irriducibile di A è primo
(ii) Ogni catena discendente di divisibilità è stazionaria

$$\{x_i\}_{i \geq 1} \subseteq A \qquad x_{i+1} \mid x_i \ \forall i \geq 1 \qquad \exists n_0 \mid \forall n \geq n_0 \ x_n \sim x_{n_0}$$

la (i) è equivalente a richiedere l'unicità della fattorizzazione, la (ii) è equivalente a richiedere che ogni catena ascendente di ideali principali è stazionaria

$$\{x_i\}_{i \geq 1} \subseteq A \qquad (x_i) \subseteq (x_{i+1}) \qquad \exists n_0 \mid (x_n) = (x_{n_0}) \ \forall n \geq n_0$$

Esempio:

① $A = K[\{\sqrt[n]{x}\}_{n \geq 1}]$

$\{x^{\frac{1}{2n}}\}_{n \geq 1} \qquad x^{\frac{1}{2(n+1)}} \mid x^{\frac{1}{2n}} \quad \forall n \in \mathbb{N} \setminus \{0\} \longrightarrow$ non vale la (ii)

$x^{\frac{1}{2n}} = x^{\frac{1}{2(n+1)}} \cdot x^{\frac{1}{2n(n+1)}}$

② $A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

2 è irriducibile ma non primo $\longrightarrow$ non vale (i)

$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ supponiamo cioè di averlo scomposto

$\downarrow$ N (norma)

$4 = (a^2 + 5b^2)(c^2 + 5d^2)$

4 si scompone come $4 \cdot 1$ o 2×2

↳ posso escluderla perché avrei un invertibile nella fattorizzazione di 2

$a^2+5b^2=4$
$c^2+5d^2=1 \Rightarrow d=0 \quad c=\pm 1 \Rightarrow \boxed{2 \text{ irriducibile}}$

$a^2+5b^2=2 \Rightarrow b=0 \quad a^2=2$ ↯

$2 | 6 \qquad 6=(1+\sqrt{-5})(1-\sqrt{-5})$ ma $2 \nmid (1\pm\sqrt{-5}) \Rightarrow \boxed{2 \text{ NON primo}}$

se facessi vedere che questi fattori sono irriducibili e lo sono anche 2 e 3 $(6=2\cdot 3)$ avrei dimostrato la non unicità della fattorizzazione

TEOREMA A PID $\Rightarrow$ A UFD

(i) Ogni irriducibile è primo, infatti:

$x \in A$ irriducibile $\Rightarrow (x)$ massimale $\Rightarrow (x)$ primo $\Rightarrow x$ primo

(ii) $I_k=(x_k) \quad I_k \subseteq I_{k+1} \quad \forall k \geq 1$

$I=\bigcup_{k\geq 1} I_k$ è un ideale di A $\Rightarrow$ è principale $I=(x)$

$\Rightarrow \exists n_0 \mid x \in I_{n_0} \subseteq I=(x) \Rightarrow I=I_{n_0}$

$I_{n_0} \subseteq I_n \subseteq I \quad \forall n \geq n_0 \Rightarrow I_n=I \quad \forall n \geq n_0$

Queste due osservazioni e il teorema di caratterizzazione degli UFD mi permettono di concludere che ogni PID è UFD □

Teorema A è UFD $\Rightarrow A[x]$ è UFD

Corollario A è UFD $\Rightarrow A[x_1 \cdots x_n]$ è UFD

LEMMA DI GAUSS Se A è UFD e $f,g \in A[x]$ allora $c(fg)=c(f)c(g)$

Se $f=\sum_{i=1}^{n} a_i x^i \Rightarrow c(f)=MCD(a_1,\dots,a_n)$

$c(f)\sim 1 \Rightarrow f$ si dice PRIMITIVO , $f=c(f)f'$, dove f' è un pol. primitivo

DIM. Caso 1: $c(f)=c(g)=1$

Se per assurdo valesse $c(fg)\not\sim 1 \Rightarrow \exists p$ primo t.c. $p | c(fg)$

$P=(p)$ è un ideale primo di A

$\pi: A[x] \to A/p[x]$ è un omomorfismo di anelli
$\sum a_i x^i \mapsto \sum \bar{a}_i x^i$

$\pi(fg) = \pi(f)\pi(g)$ ↯ ($\frac{A[x]}{P}$ è un dominio)
$\overset{\shortparallel}{0}$ $\quad\overset{\neq}{0}$ $\quad\overset{\neq}{0}$

Caso generale:

$f = c(f)f'$ $\quad$ f' e g' primitivi
$g = c(g)g'$

$fg = c(f)c(g)\underbrace{f'g'}$

primitivo grazie al caso precedente

$c(fg) = c(f)c(g)$ $\square$

Corollario 1 | A UFD, $f, g \in A[x]$, f primitivo

Se $f | g$ in $\underset{\substack{\uparrow \\ \text{campo delle} \\ \text{frazioni di } A}}{K[x]}$ $\Rightarrow$ $f | g$ in $A[x]$

DIM. $g = fh$ $\quad h \in K[x]$

$\exists d \in A \mid \underbrace{dh}_{\substack{\shortparallel \\ h_1 \text{ (primitivo)}}} \in A[x]$

$dg = fh_1$

$c(dg) = dc(g) = c(fh_1) = c(f)\overset{\substack{1 \\ \shortparallel}}{c(h_1)}$

$d | c(f) \Rightarrow g = fh = \underbrace{f'dh}$ $\quad dh \in A[x]$
$\quad f' \in A[x]$ $\square$

Corollario 2 | $f \in A[x]$ $\quad f = gh$ $\quad g, h \in K[x]$

$\deg g \geq 1$ $\quad \deg h \geq 1$

$\Rightarrow \exists \delta \in K^*$ t.c. $g_1 = \delta g$ $\quad g_1, h_1 \in A[x]$
$h_1 = \delta^{-1} h$

$f = g_1 h_1$ in $A[x]$

DIM. $f = gh$ in $K[x]$

$\exists d \in A$ $\quad g_1 = dg \in A[x]$

$f = \underset{\substack{\cap \\ A[x]}}{(dg)}\underset{\substack{\cap \\ A[x]}}{(d^{-1}h)} = g_1'(d^{-1}h)c(g_1) \Rightarrow h_1 = \underset{\substack{\cap \\ A[x]}}{(d^{-1}h)c(g_1)}$

g_1' ↳ primitivo

per il corollario precedente $\square$

Corollario $f \in A[x]$ primitivo è irriducibile in $A[x]$ $\Longleftrightarrow$

$\Longleftrightarrow$ è irriducibile in $K[x]$

Criterio di Eisenstein

A è UFD, $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$

e P ideale primo t.c.
(i) $a_n \notin P$
(ii) $a_i \in P \quad \forall i \in \{0, 1, \dots, n-1\}$
(iii) $a_0 \notin P^2$

$\Rightarrow f$ irriducibile in $K[x]$

20/11/2024
Del Corso

$K \subset L$ campi L/K ← sottocampo di L

Def.
$\alpha \in L$ si dice algebrico su K se $\exists f(x) \in K[x]$ $f(x) \neq 0$ tale che $f(\alpha) = 0$

α si dice trascendente su K se non è algebrico su K

$K \subset L$ $\alpha \in L$

omomorfismo di valutazione in α

$$\varphi_\alpha : K[x] \to L \quad p(x) \mapsto p(\alpha)$$ è omomorfismo di anelli

$\mathrm{Im}\,\varphi_\alpha =: K[\alpha]$ $\varphi_\alpha : K[x] \twoheadrightarrow K[\alpha] = \{p(\alpha) \mid p(x) \in K[x]\}$

Dal I teo. di omo:

$$\begin{tikzcd} K[x] \arrow[r, "\varphi_\alpha"] \arrow[d, "\pi"] & K[\alpha] \\ K[x]/\ker\varphi_\alpha \arrow[ur, "\cong"] & \end{tikzcd}$$

$\ker\varphi_\alpha$ è un ideale di $K[x]$ (ED) $\Rightarrow$
$\Rightarrow$ è principale $\ker\varphi_\alpha = (f(x))$
$K[\alpha] \subseteq L \Rightarrow K[\alpha]$ dominio $\Rightarrow$
$K[\alpha] \cong K[x]/\ker\varphi_\alpha$

$\Rightarrow \ker\varphi_\alpha$ primo
- $\{0\} \to \alpha$ trascendente
- ideale massimale di $K[x]$

perché gli ideali primi di un PID sono $\{0\}$ e i massimali

$\ker\varphi_\alpha = (\mu_\alpha(x))$

irriducibile perché genera un ideale massimale
lo scelgo monico e lo chiamo POLINOMIO MINIMO DI α SU K

$\mu_{\alpha,K}(x)$ è l'unico generatore monico di $\ker\varphi_\alpha$

$K[\alpha] \cong K[x]$ se α è trascendente su K

$K[\alpha] \cong K[x]/(\mu_\alpha(x))$ è un campo perché $(\mu_\alpha(x))$ massimale

$\alpha \longleftrightarrow \bar{x}$

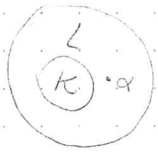
$K[\alpha] = K(\alpha) := \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p, q \in K[x]\ q \neq 0 \right\}$

perché è un campo

spazio vettoriale di dimensione $\deg \mu_\alpha(x)$ con base $1, \bar{x}, \dots, \bar{x}^{\deg \mu_\alpha - 1}$

$\Rightarrow K[\alpha]$ ha base $1, \alpha, \dots, \alpha^{\deg \mu_\alpha - 1}$

Proposizione $K \subseteq L$ $\quad \alpha \in L$ algebrico su K



$K[\alpha] = K(\alpha)$ è un campo

$[K(\alpha):K] := \dim_K K(\alpha) = \deg \mu_\alpha = n$ (come sp. vettoriale)

$\{1, \alpha, \dots, \alpha^{n-1}\}$ è una K-base di $K(\alpha)$

$L/K \quad [L:K] = \dim_K L$

L/K è finita se $[L:K] < +\infty$

Proprietà del grado (estensioni finite)

TORRI

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array} \qquad K \subseteq F \subseteq L$$

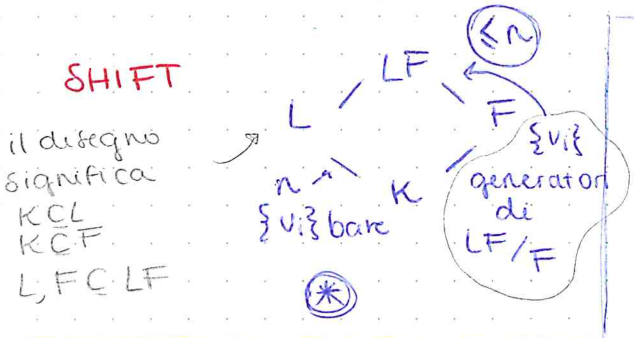
$[L:K] = [L:F] \cdot [F:K]$

(L/K finita $\Leftrightarrow$ L/F e F/K finite)

$\{v_i\}_{i=1}^m$ K-base di F e $\{w_j\}_{j=1}^n$ F-base di L

$\Rightarrow \{v_i w_j\}_{i=1}^{j=1,\dots,n}$ è una K-base di L

SHIFT



$K \subseteq L$ campo

$S \subseteq L$ sottoinsieme

$K(S) = \bigcap_{\substack{M \subseteq L \\ K, S \subseteq M}} M$ (sottocampo di L) $\rightarrow$ più piccolo sottocampo di L che contiene sia S che K

(L/K algebrica se $\forall \alpha \in L$, α è algebrico su K)

$$K(S) = \left\{ \frac{p(s_1, \dots, s_r)}{q(s_1, \dots, s_r)} \;\middle|\; r \in \mathbb{N} \quad p, q \in K[x_1, \dots, x_r] \quad q(s_1, \dots, s_r) \neq 0, \; s_i \in S \right\}$$

esercizio: verificare che le due def. sono uguali

$LF = L(F) = F(L)$ $\rightarrow$ il più piccolo campo che li contiene entrambi)

α, β alg. su K

$K(\alpha, \beta) = \left\{ \frac{p(\alpha,\beta)}{q(\alpha,\beta)} \;\middle|\; q(x,y), p(x,y) \in K[x,y], \; q \neq 0 \right\}$ $= K[\alpha, \beta]$

$K[\alpha, \beta] = \{ p(\alpha, \beta) \mid p(x,y) \in K[x,y] \}$

perché $K[\alpha,\beta] = K[\alpha][\beta] \overset{\alpha \text{ algebrico}}{=} K(\alpha)[\beta] \overset{\beta \text{ algebrico}}{=} K(\alpha)(\beta) = K(\alpha, \beta)$

$$K(\alpha,\beta) = \underbrace{K(\alpha)}_{L}\underbrace{K(\beta)}_{F}$$

$$L(F) = K(\alpha)(K(\beta)) = K(\alpha)(\beta)$$

✱ → DIMOSTRAZIONE DEL TEO. DI SHIFT (pensava lo avessimo visto ad aritmetica quindi non si capisce niente)

$\alpha \in LF = F(L) \qquad \alpha = p(\ell_1, \dots, \ell_k) \quad \ell_i \in L$

$\ell_j = \sum_i a_{ji} v_i \quad a_{ji} \in K$

α polinomio con coeff. in F valutato nei v_i

α generato su F da $\{v_1, \dots, v_n\}$

$L = K(v_1, \dots, v_n) = \langle v_1, \dots, v_n \rangle_L$ ↳ span

dim. alternativa

$FL = \cancel{F(K(v_1,\dots,v_n))}$

$\shortparallel$

$F(L) = F(\langle v_1, \dots, v_n \rangle_K) = \langle v_1, \dots, v_n \rangle_F$ $\square$

$\underset{K}{\mathbb{Q}}(\sqrt[3]{2}, \underset{\text{radice 3ª dell' unità}}{\zeta_3}) = \underset{K'}{\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})}$

⊇ $\zeta^3\sqrt{2},\ \zeta^{2\,3}\sqrt{2} \in K$

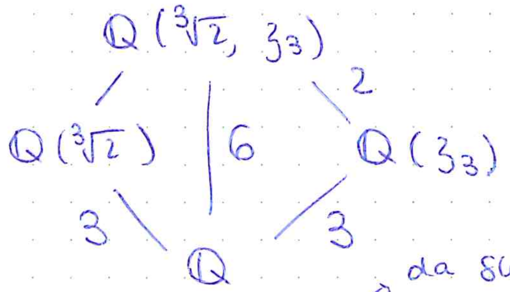
$\mathbb{Q} \subset K$ $\Rightarrow K \supseteq K'$

⊆ $\sqrt[3]{2} \in K'$

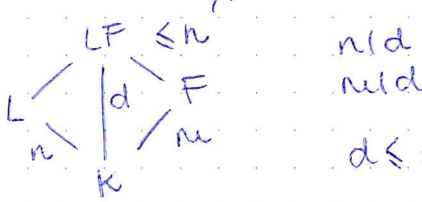
$\zeta_3 = \zeta_3 \frac{\sqrt[3]{2}}{\sqrt[3]{2}} \in K'$ $\Rightarrow K \subseteq K'$

$\mathbb{Q} \subset K'$

allora sono uguali



Composizione:



$n \mid d \Rightarrow [n,m] \mid d$

$m \mid d$

$d \leq nm$

$\to K(\alpha_1,\dots,\alpha_n)K(\beta_1,\dots,\beta_m) = K(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_m)$

$\to K(\alpha,\beta) = K(\alpha)(\beta)$

Proposizione L/K finita $\Rightarrow$ L/K è algebrico

DIM. $\alpha \in L$ e devo mostrare che α è algebrico su K.

$$\left[\begin{array}{ll} p(x) = \sum_{i=1}^{n} a_i x^i \neq 0 \\ p(\alpha) = 0 & \sum_{i=1}^{n} a_i \alpha^i = 0 \end{array}\right]$$

$[L:K] = n < +\infty$ $\quad \{\alpha^i\}_{i\geq 0} \subseteq L$ $\quad \underbrace{1, \alpha, \dots, \alpha^n}_{n+1 \text{ el.}}$ $\Rightarrow$ lin. dipendenti su K

$\Rightarrow \exists\, a_0, \dots, a_n$ in K non tutti nulli

t.c. $\sum_i a_i \alpha^i = 0$

$\Downarrow$

$p(x) = \sum_i a_i x^i$ è non nullo e $p(\alpha) = 0$

$\Rightarrow \alpha$ algebrica su K

Il viceversa è falso, non tutte le estensioni algebriche sono finite

Prop. L/K $\quad A = \{\alpha \in L \mid \alpha \text{ è alg. su } K\}$

$\Rightarrow$ A campo (est. alg di K)

DIM. $K \subset A$

$\alpha, \beta \in A \Rightarrow \underbrace{\alpha+\beta,\ \alpha\beta,\ -\alpha,\ \beta^{-1}}_{K(\alpha,\beta)} \in A$ $\quad$ se $\beta \neq 0$

Osservo che $K(\alpha,\beta)/K$ è finita

$[K(\alpha,\beta):K] = [K(\alpha)(\beta):K(\alpha)][K(\alpha):K]$

$\qquad\qquad\qquad\qquad\qquad\qquad\downarrow$ finita $\qquad\qquad \downarrow$ finita

(le estensioni semplici (di un solo el) sono algebriche $\Leftrightarrow$ sono finite

$\Rightarrow [K(\alpha,\beta):K]$ finita $\Rightarrow$ $K(\alpha,\beta)/K$ è algebrica

$\underbrace{K(\alpha,\beta)}_{\text{è alg. su } K} \subset L$ $\Rightarrow K(\alpha,\beta) \subseteq A$ $\quad$ A è un campo

Esempio di est. algebrica non finita

$\mathbb{Q} \subset \mathbb{C}$

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è alg. su } \mathbb{Q}\}$

$\sqrt[n]{2} \in \overline{\mathbb{Q}}$ $\quad x^n - 2 \rightarrow$ irriducibile $\forall n$ per Eisenstein

$\overline{\mathbb{Q}}/\mathbb{Q}$ algebrica. Dico che $[\overline{\mathbb{Q}} : \mathbb{Q}] = +\infty$

Supponiamo $[\overline{\mathbb{Q}} : \mathbb{Q}] = d$

$\sqrt[d+1]{2} \in \overline{\mathbb{Q}}$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[d+1]{2}) \subseteq \overline{\mathbb{Q}}$ $\quad \lightning$

$d+1 \qquad d$

$x^{d+1} - 2$ irriducibile per Eisenstein $\Rightarrow$ è il polinomio minimo

Def. Ω campo si dice alg. chiuso se ogni polinomio $f(x) \in \Omega[x]$ $f(x)$ non costante ammette radice in Ω

Es. il teo. fondamentale dell'algebra dice che $\mathbb{C}$ è algebricamente chiuso

<u>OSS</u> Ω alg. chiuso $f(x) \in \Omega[x] \setminus \Omega$

$\deg f = n \quad f(x) = \lambda(x - \alpha_1) \cdots (x - \alpha_n) \quad \alpha_i \in \Omega$

$\lambda \in \Omega$

Def. K campo $\Omega \supseteq K$ è una chiusura alg. di K se
- Ω alg. chiuso
- Ω/K è algebrica

Esempi: $\mathbb{C}$ è una chiusura algebrica di $\mathbb{R}$

$\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[x]/(x^2+1)$

ma non è una chiusura algebrica di $\mathbb{Q}$

TEO (Esistenza e "unicità" della chiusura algebrica)

Sia K campo, allora esiste sempre la sua chiusura algebrica

Inoltre due chiusure algebriche di K, Ω e Ω' sono isomorfe $\varphi: \Omega \to \Omega'$ $\varphi|_K = id$

Esempio: $\overline{\mathbb{Q}}$ (con la definizione di prima) è una chiusura algebrica di $\mathbb{Q}$) è quello che voglio dimostrare

- $\overline{\mathbb{Q}}/\mathbb{Q}$ è algebrica (per definizione)

- $\overline{\mathbb{Q}}$ alg. chiuso

$f(x) \in \overline{\mathbb{Q}}[x] \setminus \overline{\mathbb{Q}}$

$f(x) \in \mathbb{C}[x] \Rightarrow \exists \alpha \in \mathbb{C} \quad f(\alpha) = 0$

$\mathbb{C}$ alg. chiuso

Tesi: $\alpha \in \overline{\mathbb{Q}}$

$f(x) = \sum_i a_i x^i \qquad \mathbb{Q}(a_0, \dots, a_n) \subseteq \overline{\mathbb{Q}}$

Lemma $\alpha_1, \dots, \alpha_n \in L \quad K \subset L \quad \alpha_1, \dots, \alpha_n$ alg. su K

$\Rightarrow K(\alpha_1, \dots, \alpha_n)/K$ è finita

"una estensione finitamente generata, generata da elementi algebrici è finita".

DIM. Induzione su n

$n = 1 \quad K[\alpha]/K$ (è finita, ha grado quello del pol minimo di α su K)

$n-1 \Rightarrow n$

$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$

$[K(\alpha_1, \dots, \alpha_{n-1}) : K] < +\infty$ per ip. induttiva

$K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$
| $\to$ semplice e alg $\Rightarrow < +\infty$
$K(\alpha_1, \dots, \alpha_{n-1})$
| $< +\infty$
K

$\Rightarrow$ concludo per torri

$\mathbb{Q} \subset \mathbb{Q}(a_0, \dots, a_n) \subset \mathbb{Q}(a_0, \dots, a_n)(\alpha)$

$\mathbb{Q} \subset L \subset L(\alpha)$

finita (lemma) — semplice e alg. perché $f(x) \in L[x]$ $\to$ finita

Per torri $L(\alpha)/\mathbb{Q}$ è finita $\Rightarrow$ è alg. $\Rightarrow$ α è alg. su $\mathbb{Q}$ $\Rightarrow$

$\Rightarrow \alpha \in \overline{\mathbb{Q}}$

25/11/2024
Patino

Prima parte - correzione errori compitini
(ho fatto la foto alla lavagna)

A anello, S parte moltiplicativa

$$\begin{tikzcd} \left\{\begin{matrix}\text{ideali in} \\ S^{-1}A\end{matrix}\right\} \arrow[r, bend left, "\phi"] & \left\{\begin{matrix}\text{ideali} \\ \text{di } A\end{matrix}\right\} \arrow[l, bend left, "\psi"] \end{tikzcd}$$

$J \mapsto J \cap A$

$S^{-1}I \leftarrow I$

Se J è un ideale di $S^{-1}A$ allora dato $I = J \cap A$ vale

$J = S^{-1}I = S^{-1}(J \cap A)$

$\subseteq$ prendo $\frac{x}{a} \in S^{-1}I$ con $x \in I$, $a \in S$

$\frac{1}{a} \cdot \frac{x}{1} \in S^{-1}A(J) \subset J$

$\supseteq$ $\frac{x}{a} \in J$, con $x \in A$, $a \in S$. Allora $x = \underset{\uparrow A}{\frac{a}{1}} \cdot \underset{\uparrow J}{\frac{x}{a}} \in J \cap A = I$

$\frac{x}{a} \in S^{-1}I$ $\quad$ $1 \in S$ per def. di parte moltiplicativa

Quindi $\psi \circ \phi = id$ (l'altra composizione non è l'identità, a meno che non si considerino solo gli ideali primi)

$$\left\{\begin{matrix}\text{ideali} \\ \text{primi di} \\ S^{-1}A\end{matrix}\right\} \rightleftarrows \left\{\begin{matrix}\text{ideali primi } P \text{ di } A \\ \text{con} \\ P \cap S = \emptyset\end{matrix}\right\}$$

P primo $\Rightarrow$ $S^{-1}P$ primo:

$\frac{x}{a}, \frac{y}{b} \in S^{-1}A$ con $\frac{x}{a}\frac{y}{b} \in S^{-1}P$ allora $\exists\, p \in P, s \in S$ t.c.

$\frac{xy}{ab} = \frac{p}{s} \Rightarrow xys \in P \Rightarrow xy \in P \Rightarrow x \in P \vee y \in P \Rightarrow$

$\Rightarrow \frac{x}{a} \in S^{-1}P \vee \frac{y}{b} \in S^{-1}P$

Vogliamo dimostrare che se P primo e $P \cap S = \emptyset$ $S^{-1}P \cap A = P$

$\supseteq$ $P \subset A$ $P \subset S^{-1}P$

$\subseteq$ $\frac{p}{s} = t$ $p \in P$, $s \in S$, $t \in A$

$\Rightarrow st \in P \Rightarrow t \in P \Rightarrow \frac{p}{s} = t \in P$.

Quindi otteniamo la bigezione di prima.

ES 2 ① Classificare gli ideali di $\mathbb{Z}_{(2)} = \{ \underbrace{(\mathbb{Z} \setminus (2))^{-1}}_{} \mathbb{Z} \} =$

è una parte moltiplicativa perché è il complementare di un ideale primo

$= \left\{ \frac{a}{b} \mid \begin{matrix} a \in \mathbb{Z} \\ b \in \mathbb{Z} \setminus (2) \end{matrix} \right\} \subset \mathbb{Q}$

(2) è l'unico ideale primo di $\mathbb{Z}_{(2)}$

Sappiamo che tutti gli ideali di $\mathbb{Z}_{(2)}$, sono nella forma $S^{-1}I$, con I ideale di $\mathbb{Z}$

$\quad\quad\quad\quad\quad\quad\quad\quad \overset{\shortparallel}{S^{-1}(n)}$ per qualche $n \in \mathbb{Z}$

OSS: p primo dispari t.c. $p \mid n$

$S^{-1}(n) \ni \frac{n}{p} \rightarrow S^{-1}(n) = S^{-1}\left(\frac{n}{p}\right)$

Quindi tutti gli ideali sono della forma

$$S^{-1}(2^k) = \left\{ \frac{2^k a}{b} \quad \begin{matrix} a \in \mathbb{Z} \\ b \text{ dispari} \end{matrix} \right\} \text{ o } (0) = \{0\}$$

② Consideriamo l'immersione naturale $i: \mathbb{Z} \rightarrow \mathbb{Z}_{(2)}$

ideale generato dall'immagine di I

Dato $I \subset \mathbb{Z}$ ideale di $\mathbb{Z}$ descrivere $\langle i(I) \rangle$. $I = (n)$ per qualche $n \in \mathbb{Z}$ $\langle i(I) \rangle = S^{-1}I$ e $S^{-1}(I) = S^{-1}(2^k)$ dove $n = 2^k d$ con d dispari.

③ Descrivere $\langle i(I) \rangle \cap \mathbb{Z}$: $\langle i(I) \rangle = S^{-1}(2^k)$

$S^{-1}(2^k) \cap \mathbb{Z} = (2^k)$. Se $I = (0)$, $\langle i(I) \rangle = 0$ e $S^{-1}(0) \cap \mathbb{Z} = (0)$

ES 3 Classificare gli ideali massimali di $\mathbb{Z}[x]$

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}/p\mathbb{Z}\,[x] \qquad \frac{\mathbb{Z}/p\mathbb{Z}\,[x]}{(x)} \cong \mathbb{Z}/p\mathbb{Z} \rightarrow \text{campo}$$

$$\mathbb{Z}[x]/_{(p,x)} \cong \frac{\mathbb{Z}[x]/_{(p)}}{(p,x)/_{(p)}} \cong \mathbb{Z}/_{p\mathbb{Z}}[x]/_{(x)} \cong \mathbb{Z}/_{p\mathbb{Z}}$$ è un campo

$\Rightarrow (p,x)$ è massimale

<u>OSS</u> (p,x) non è principale, quindi $\mathbb{Z}[x]$ non è PID.
Infatti se $(p,x) = (f)$ avrei $f|p$ e $f|x$ ma p e x non hanno fattori in comune.

LEMMA A anello, I ideale di A $\quad A[x]/_{I[x]} \cong A/_I[x]$

<u>DIM</u>. $\varphi : A[x] \to A/_I[x]$

$$a_0 + a_1x + \dots + a_nx^n \mapsto \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n$$

φ omo. di anelli suriettivo.

$\operatorname{Ker}\varphi = \{ b_0 + b_1x + \dots + b_nx^n \mid b_i \in I \} = (I)$ $\square$

Supponiamo che M sia un ideale massimale di $\mathbb{Z}[x]$ con $p \in M$ per qualche primo $p \in \mathbb{Z}$. Quindi $(p) \subset M$ e

$$\mathbb{Z}[x]/_M \cong \frac{\mathbb{Z}[x]/_{(p)}}{M/_{(p)}} \cong \frac{\mathbb{Z}/_{p\mathbb{Z}}[x]}{J}$$

Con J ideale ed essendo $\mathbb{Z}/_{p\mathbb{Z}}[x]$ PID
$J = (f)$ con $f \in \mathbb{Z}/_{p\mathbb{Z}}[x]$ e dato che il quoziente è un campo f deve essere un irriducibile.
Quindi $M/_{(p)} = (f) \Rightarrow M = (p, \hat{f})$ con

$$\hat{f} = f \mod (p)$$

$\pi : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}[x] \cong \mathbb{Z}[x]/(p)$

$J = \pi(M) \cong M/(p) \Rightarrow M = \pi^{-1}(J)$ (perché $M \supset \operatorname{Ker}\pi$)

Ma $J = (f)$, quindi $M = \pi^{-1}(f) = (\hat{f}) + \operatorname{Ker}\pi = (\hat{f}, p)$

con $\pi(\hat{f}) = f$

Supponiamo che M sia massimale in $\mathbb{Z}[x]$ e che $M \cap \mathbb{Z} = \{0\}$

Prendiamo $S = \mathbb{Z} \setminus \{0\}$ $\quad S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$

$\mathbb{Q}[x]$ è PID. M massimale e $M \cap S = \emptyset \Rightarrow S^{-1}M = (f)$ con f irriducibile in $\mathbb{Q}[x]$

$M = S^{-1}M \cap \mathbb{Z}[x]$

Ricordiamo: LEMMA DI GAUSS

Siano $q_1, q_2 \in \mathbb{Z}[x]$ primitivi (cioè il MCD dei coefficienti è 1), allora anche il prodotto è primitivo

$S^{-1}M = (f)$ $\qquad M = (f) \cap \mathbb{Z}[x]$

$\exists q \in \mathbb{Q} \mid qf \in \mathbb{Z}[x]$ è primitivo

CLAIM: $M = (qf)$

$\supseteq$ Vale perché $(qf) \subset (f) \cap \mathbb{Z}[x]$

$\subseteq$ Prendiamo $gf \in (f) \cap \mathbb{Z}[x]$ con $g \in \mathbb{Q}[x]$

$\exists q'$ t.c. $gq' \in \mathbb{Z}[x]$ primitivo

Quindi $\underset{\substack{\| \\ (qf)(gq')}}{qfgq'} \in \mathbb{Z}[x]$ primitivo, ma $gf \in \mathbb{Z}[x]$

$\Rightarrow \frac{1}{qq'} \in \mathbb{Z} \Rightarrow gf = \underset{\substack{\cap \\ \mathbb{Z}}}{\frac{1}{qq'}} \underset{\substack{\cap \\ \mathbb{Z}[x]}}{(q'g)}(qf) \in (qf)$ di $\mathbb{Z}[x]$ $\square$

Ricapitolando

M massimale in $\mathbb{Z}[x]$, $M \cap \mathbb{Z} = \{0\} \Rightarrow M = (f)$ con $f \in \mathbb{Z}[x]$

Voglio far vedere che (f) non può non essere massimale.

Infatti, se $p \in \mathbb{Z}$ primo con $p \nmid$ leading term (f)

voglio $(f) \subsetneq (p, f) \subsetneq \mathbb{Z}[x]$

OK! Perché $p \notin (f)$ se $\deg(f) \geq 1$

$\mathbb{Z}[x]/(p,f) = \mathbb{Z}/p\mathbb{Z}[x]/(\bar{f})$ $\quad \deg(\bar{f}) = \deg f$, quindi $\mathbb{Z}/p\mathbb{Z}[x] \neq (\bar{f})$

cioè (p,f) è proprio in $\mathbb{Z}[x]$. $\square$

ES 5 $\quad \mathbb{Z}[\sqrt{-5}] = R$ non è un UFD

$\quad \| $

$\mathbb{Z}[x]/(x^2+5)$

R è un dominio perché $R \subseteq \mathbb{C}$

$z \in \mathbb{C} \quad N(z) = z\bar{z} \in \mathbb{R}_{\geq 0} \quad N(zw) = N(z)N(w)$

$z = a+ib \Rightarrow N(z) = a^2+b^2$

$\mathbb{Z}[\sqrt{-5}] = \{ a+b\sqrt{-5} \mid a,b \in \mathbb{Z} \}$

$N(a+b\sqrt{-5}) = a^2+5b^2 \in \mathbb{Z}^+$

<u>OSS</u> $\hat{a} \in R^* \Rightarrow \underset{\substack{\| \\ a^2+5b^2}}{N(\hat{a})} \mid N(1) = 1$

$\Rightarrow b=0 \wedge a = \pm 1$

Voglio dire che 2 e 3 sono irriducibili in R

Se $2 = xy$, con $x,y \notin R^*$

allora $\underset{\substack{\| \\ 4}}{N(2)} = N(x)N(y) \Rightarrow N(x) = N(y) = 2$

Ma $a^2+5b^2 = 2$ non ha soluzione

Analogamente si dimostra che 3 è irriducibile

($a^2+5b^2 = 3$ non ha soluzione)

$\Rightarrow$ (2) e (3) sono massimali tra gli ideali principali

Sono massimali in $\mathbb{Z}[\sqrt{-5}]$?

Lo sono SSE quozientati per (x^2+5) mi danno un ideale massimale di $\mathbb{Z}[x]/(x^2+5)$

$\updownarrow$ per corrispondenza

$(2,x^2+5)$ e $(3,x^2+5)$ sono massimali in $\mathbb{Z}[x]$

Consideriamo $(2,x^2+5)$

$x^2+5 = x^2+1 = (x+1)^2$ non è irriducibile

$(2,x^2+5) \subset (2,x+1) = M$ è massimale (per l'es. precedente)

$\widehat{N} = M/(x^2+5) = (2,x+1)$ in $\mathbb{Z}[x]/(x^2+5)$

$\widehat{N}^2 = (4,(x+1)^2, 2(x+1)) = (4, \underset{\substack{\| \\ -5}}{x^2}+2x+1, 2x+2) = (4, 2x-4, 2x+2) =$

$= (4,6,2x+2) = (2)$

$\underset{\substack{\| \\ \sqrt{-5}+1}}{x+1}, \underset{\substack{\| \\ \sqrt{-5}-1}}{x-1} \in \widehat{N} \qquad (x+1)(x-1) \in N^2 = (2)$

$\qquad \underset{\substack{\| \\ x^2-1 = -6}}{}$

$6 = 2 \cdot 3 = (1+x)(1-x)$, visto che $\overset{\text{norma}}{N(1-x)} = 6$ e non è divisibile né da $N(2)$ né $N(3)$.

26/11/2024
Del Corso

Def. K campo $f(x) \in K[x]$ $\deg f \geq 1$ ($= n$)

$\overline{K}$ chiusura alg. di K

$\{\alpha_1, \dots, \alpha_n\} \subseteq \overline{K}$ radici di f

Allora si dice CAMPO DI SPEZZAMENTO di f su K

$$K \subseteq K(\alpha_1, \dots, \alpha_n) \subseteq \overline{K}$$

OSS. Il campo di spezzamento di f su K è univocamente definito una volta fissata una chiusura algebrica.

$\mathcal{F} = \{f_i\}_{i \in \Lambda}$ $f_i \in K[x]$ $\forall i \in \Lambda$

$\overline{K} \supseteq \{\alpha_i\}_{i=1,\dots,n_i}$ radici di f_i

Chiamo campo di spezzamento di $\mathcal{F}$ su K il sottocampo

$$K \subseteq K(\{\alpha_{ij}\} \mid i \in \Lambda, \ j = 1, \dots, n_i) \subseteq \overline{K}$$

Esempio:

$\mathbb{Q}$ $\mathcal{F} = \{x^n - 1 \mid n \geq 1\}$

Il campo di sp. di $\mathcal{F}$ su $\mathbb{Q}$ è $\mathbb{Q}^{ab}$

Es. 1

$K = \mathbb{Q}$ $x^2 - 2$

$\downarrow$ c. di spezzamento

$\mathbb{Q}(\sqrt{2})$

Es. 2

$K = \mathbb{Q}$ $f(x) = x^3 - 2$

$$\downarrow$$

$$\underset{\overline{K}}{\mathbb{Q}(\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2})} \overset{\subseteq,\ \supseteq}{=} \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

$\hookrightarrow$ questo campo ha grado 6 su $\mathbb{Q}$

$$\begin{tikzcd}
 & \overline{K} \arrow[dl, dash, "\leq 2"'] \arrow[dr, dash, "\leq 3"] \arrow[dd, dash, "d"] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Es. 3 $\mathbb{Q}$ $f_n(x) = x^n - 1$

$C_n = \{ \zeta_n^i \}_{i=1,\dots,n}$ $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

$\cap\mathbb{C}^*$ radici n-esime dell'unità

(sono anche un sottogruppo di $\mathbb{C}^*$)

C_n gruppo ciclico di ordine n

Criterio della derivata

$f \in K[x]$. f ha radici multiple in $\overline{K}$ $\iff$ $(f, f') \neq 1$

hanno una radice in comune

DIM. $f(x) = (x-\alpha)\, q(x)$ $\overline{K}[x]$

($\Leftarrow$) $f'(x) = q(x) + (x-\alpha) q'(x)$

$0 = f'(\alpha) = q(\alpha) + \cancel{(\alpha-\alpha)} q'(\alpha) \implies q(\alpha) = 0$

$(x-\alpha) \mid q(x) = (x-\alpha) h(x)$

$\implies f(x) = (x-\alpha)^2 h(x)$

($\Rightarrow$) $f(x) = (x-\alpha)^i q(x)$ $i \geq 2$

$f'(x) = i(x-\alpha)^{i-1} q(x) + (x-\alpha)^i q'(x)$

$f'(\alpha) = 0$

$\implies (f, f') \neq 1$

Corollario $f \in K[x]$ irriducibile, f ha fattori multipli $\iff$ $f'(x) = 0$

DIM. f irriducibile di grado n

$\deg f' \leq n-1$ $(f, f') = \begin{cases} 1 & \text{No, per il criterio della derivata} \\ f \end{cases}$

$\deg f > \deg f' \implies f' = 0$

Conseguente:

- Se $\operatorname{char} K = 0$ ogni polinomio irriducibile di $K[x]$ ha radici distinte.
- Se $\operatorname{char} K = p$ esistono polinomi irriducibili con radici multiple

Es: $K = \mathbb{F}_p(t)$ $f \in K[x]$

campo delle frazioni di $\mathbb{F}_p[t]$

$f(x) = x^p - t$

$\partial f/\partial x = 0$ $(p x^{p-1} = 0)$

ha derivata nulla, ora devo dimostrare che $x^p - t$ è irriducibile in $\mathbb{F}_p[t][x]$

$f(x)$ irriducibile in $\underbrace{\mathbb{F}_p[t]}_{A}[x]$ per Eisenstein, infatti...

VERIFICA DELLE HP. DI EISENSTEIN

A è ED $\Rightarrow$ UFD.

$p = (t)$ è un primo di A $\Rightarrow$ f è irriducibile in $K[X]$ per il lemma di Gauss.
$\hookrightarrow A/_{(t)} \cong \mathbb{F}_p$ (campo)

Esercizio: $K = \mathbb{F}_p$ $f \in K[X]$ ha derivata $0 \iff f(x) = (g(x))^p$

$f_n(x) = x^n - 1$

$f_n'(x) = nx^{n-1}$ $(f_n, f_n') = 1$

$C_n = \{\zeta_n^i\}_{i=1,\dots,n}$ $|C_n| = n$

$C_n \cong \mathbb{Z}/_{n\mathbb{Z}}$ ha $\varphi(n)$ generatori, cioè i ζ_n^i con $(i,n) = 1$

c. di spezzamento di $f_n/_{\mathbb{Q}}$

$\mathbb{Q}(\zeta_n^i \mid i = 1, \dots, n) = \mathbb{Q}(\zeta_n)$ $\Phi_n(x) =$ polinomi di ζ_n

CAMPI FINITI

1) F campo finito $\operatorname{char} F = p$ primo

2) $|F| = p^n$ $\mathbb{F}_p \subset F$ $\dim_{\mathbb{F}_p} F = [F : \mathbb{F}_p] = n < +\infty$

Se $v_1, \dots, v_n$ è una $\mathbb{F}_p$-base $\Rightarrow F = \{\underbrace{a_1 v_1 + \dots + a_n v_n}_{\text{sono } p^n \text{ el. distinti}} \mid a_i \in \mathbb{F}_p\}$

$\Rightarrow F \cong (\mathbb{F}_p)^n$ come sp. vettoriale su $\mathbb{F}_p$

Teorema $\forall p$ primo e $\forall n \geq 1$ esiste un unico campo F con $|F| = p^n$ all'interno di una fissata chiusura algebrica di $\mathbb{F}_p$.

DIM. $\mathbb{F}_p \subseteq F \subseteq \overline{\mathbb{F}_p}$

Se F esiste allora F^* ha card. $p^n - 1$

Gli elementi di F^* sono radici di $x^{p^n-1} - 1$ in $\overline{\mathbb{F}_p}$

$\forall \alpha \in F^*$ $\alpha^{p^n-1} = 1$

gli el. di F sono tutti radici di $x(x^{p^n-1} - 1) = x^{p^n} - x$

Questi elementi sono p^n tutti distinti

(per il criterio della derivata $p^n x^{p^n-1} - 1 = f'(x)$)
non è nulla $\Rightarrow$ NON ci sono fattori multipli

$F = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\}$
$\hookrightarrow$ ha p^n elementi

F è l'unico candidato, verifichiamo che è un campo.

$0,1 \in F$ — da verificare che sono in F (esercitio)

$\alpha, \beta \in F$ $\quad \alpha+\beta \quad \alpha\beta \quad \alpha^{-1} \quad -\alpha$

$$(\alpha+\beta)^{p^n} \underset{\uparrow}{=} \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$$

binomio di Newton

F lo chiamo $\mathbb{F}_{p^n} \neq (\mathbb{F}_p)^n$ ← sp. vettoriale

non è neanche un dominio

Esempio $\quad \mathbb{F}_4 = \{\alpha \in \overline{\mathbb{F}_2} \mid \alpha^4 = \alpha\}$

$x^2+1+x \in \mathbb{F}_2[x]$ irrid.

$$\mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, \bar{x}, \bar{x}+1\}$$

$\mathbb{F}_{p^n}$ è il campo di spettamento su $\mathbb{F}_p$ del polinomio $x^{p^n}-x$ $\quad (x^{p^n-1}-1)$

Teorema $\quad K$ campo $\quad G < K^*$

Se $|G| < +\infty$ allora è ciclico

("Ogni sottogruppo moltiplicativo FINITO di un campo è ciclico)

DIM. $\quad |G| = n$

$\forall g \in G \quad g^n = 1 \qquad f_d(x) = x^d - 1 \in K[x]$ ha al più d radici in K

$\Rightarrow$ Ha al più d radici in G

$G_d = \{\alpha \in G \mid \alpha^d - 1 = 0\} \qquad |G_d| \leq d$

$K_d = |\{\alpha \in G \mid \text{ord}\,\alpha = d\}|$ analog. G_d $\qquad$ Se $d \nmid n \Rightarrow K_d = 0$; $\quad d \mid n \Rightarrow K_d = 0$ oppure > 0

$>0 \Downarrow$ $\exists\, g \in G$ con $\text{ord}\, g = d$

$\langle g \rangle \subseteq G_d$ allora

varrebbe l'uguaglianza per cardinalità

$|\langle g \rangle| = d = |G_d| \Rightarrow \langle g \rangle = G_d$

$K_d = \varphi(d) \Leftarrow$

perché ho scoperto che G_d è ciclico

$$n = |G| = \sum_{d \mid n} K_d \leq \sum_{d \mid n} \varphi(d) = n$$

$\Downarrow$ $=$

Allora $K_n = \varphi(n) \Rightarrow$ in $G \ \exists$ un el. di ord. $n \Rightarrow G$ è ciclico. $\square$

Corollario 1 $\mathbb{F}_{p^n}^*$ è ciclico

Corollario 2 $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ (cioè è estensione semplice)

$\alpha \in \mathbb{F}_p(\alpha) \Rightarrow \langle\alpha\rangle \subseteq \mathbb{F}_p(\alpha)$

DIM. $\mathbb{F}_{p^n}^* = \langle\alpha\rangle \quad \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n} \Rightarrow \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$

OSS. Non è vero che $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \not\Rightarrow \langle\alpha\rangle = \mathbb{F}_{p^n}^*$

Corollario 3 $\forall p$ e $\forall n$ $\exists$ polinomi irriducibili di $\mathbb{F}_p[x]$ di grado n

DIM. $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \quad [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n = \deg \mu_\alpha$

Esempio: $\mathbb{F}_{p^{12}}$

$$\begin{tikzcd}[arrows=dash]
 & & \mathbb{F}_{p^{12}} \arrow[d, "2"] \arrow[dll, "3"'] & \\
\mathbb{F}_{p^4} \arrow[dr, "2"'] & & \mathbb{F}_{p^6} \arrow[dl, "3"'] \arrow[dr, "2"] & \\
 & \mathbb{F}_{p^2} \arrow[dr, "2"'] & & \mathbb{F}_{p^3} \arrow[dl, "3"] \\
 & & \mathbb{F}_p &
\end{tikzcd}$$

Prop. $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$

DIM. ($\Rightarrow$) $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ Per torri $n \mid m$

$\underbrace{\mathbb{F}_p \subseteq \mathbb{F}_{p^n}}_{n}$, $\underbrace{\mathbb{F}_p \subseteq \cdots \subseteq \mathbb{F}_{p^m}}_{m}$

($\Leftarrow$) $n \mid m \quad n = \lambda m$

$p^m \equiv 1 \ (p^m - 1)$

$p^{\lambda m} \equiv 1 \ (p^m - 1) \Rightarrow p^m - 1 \mid p^n - 1$

$\Rightarrow \mathbb{F}_{p^m}^* \subseteq \mathbb{F}_{p^n}^*$ (✱)

✱ $\alpha \in \mathbb{F}_{p^m}^* \iff \alpha^{p^m - 1} = 1$ ma

$p^{n-1} = a(p^m - 1) \Rightarrow$

$\Rightarrow \alpha^{a(p^m-1)} = 1$

$\alpha^{a(p^m-1)} = \alpha^{p^n - 1} \Rightarrow \alpha \in \mathbb{F}_n^*$

$\alpha \in \overline{\mathbb{F}_p}$ dato che soddisfa $x^{p^n} - x = 0$

Sia

f irriducibile di grado n in $\mathbb{F}_p[x] \qquad \{\alpha_1, \dots, \alpha_n\} \in \overline{\mathbb{F}_p}$ radici di f

$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha_1) \cong \mathbb{F}_p[x]/(f(x))$

$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha_2) = \dots = \mathbb{F}_p(\alpha_n)$

Esercizio: # di polinomi irriducibili di deg. 10 in $\mathbb{F}_p$

$\mathbb{F}_{p^{10}}$

$\mathbb{F}_p$ $\mathbb{F}_{p^2}$ $\mathbb{F}_{p^5}$

Gli el. che hanno pol. minimo di deg 10 sono quelli

di $\mathbb{F}_{p^{10}} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^5})$

Sono $p^{10} - (p^2 + p^5 - p) = n_{10}$

Il # cercato è $\frac{n_{10}}{10}$ (ogni pol. ha 10 radici distinte)

27/11/2024
Del Corso

f irriducibile di grado n (irriducibile su $\mathbb{F}_{p^m}$)

$f \in \mathbb{F}_{p^m}$ $\Rightarrow$ il campo di spezzamento di f su $\mathbb{F}_{p^m}$ è $\mathbb{F}_{p^m}(\alpha) = \mathbb{F}_{p^{mn}}$

$$mn \left(\begin{array}{c} \mathbb{F}_{p^m}(\alpha) \\ | - n \\ \mathbb{F}_{p^m} \\ | - m \\ \mathbb{F}_p \end{array} \right. \qquad \forall \alpha \text{ radice di } f$$

CAMPI DI SPEZZAMENTO SU $\mathbb{F}_q$ $(q = p^m)$

$f \in \mathbb{F}_q[x]$ $f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}$ f_i irriducibile in $\mathbb{F}_q[x]$

$\deg f_i = d_i$

$\Rightarrow$ il c. di spezzamento di f su $\mathbb{F}_q$ è $\mathbb{F}_{q^d}$ $d = \text{mcm}[d_i, i = 1, \dots, r]$

DIM. (1) Il c. di spezzamento di f su $\mathbb{F}_q$ è il composto dei c. di spezzamento degli f_i su $\mathbb{F}_q$ $K(\alpha)K(\beta) = K(\alpha, \beta)$

(2) Il c. di spett. di f_i è $\mathbb{F}_{q^{d_i}}$ $\rightarrow$ (f_i ha il pol. irriducibile su $\mathbb{F}_q$ di deg d_i)

(3) $\mathbb{F}_{q^{d_1}} \cdots \mathbb{F}_{q^{d_r}} = \mathbb{F}_{q^c}$ $\mathbb{F}_{q^{d_i}} \subset \mathbb{F}_{q^c} \Rightarrow d_i | c \ \forall i \Rightarrow$
$\Rightarrow d | c$

$\mathbb{F}_{q^c}$ è la più piccola estensione di $\mathbb{F}_q$ che contiene tutte le radici di f

" " " di f_i $\forall i = 1, \dots, r$, cioè che contiene tutti gli $\mathbb{F}_{q^{d_i}}$ $\Rightarrow c = d$ $\square$

Campo di spezzamento di $x^n - 1$ su $\mathbb{F}_p$

$n = p^a m \qquad (m, p) = 1$

$x^{p^a m} - 1 = (x^m - 1)^{p^a} \qquad (x^p = 1 \Rightarrow x^p - 1 = 0 \Rightarrow (x-1)^p = 0 \Rightarrow x = 1)$

$G_n = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^n = 1\} = G_m = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^m = 1\} \leftarrow x^m - 1$

$\{\text{radici di } x^n - 1\} = \{\text{radici di } x^m - 1\}$

$|G_m| = m$

$(f_m(x) = x^m - 1, \quad f'(x) = m x^{m-1} \neq 0$
$(f, f') = 1) \qquad p \nmid m$

Il c. di spezzamento di f_n (analog. f_m) su $\mathbb{F}_p$ è $\mathbb{F}_p(G_m)$

$G_m < \overline{\mathbb{F}_p} \qquad \begin{matrix}\alpha^m = 1 \\ \beta^m = 1\end{matrix} \Rightarrow (\alpha\beta)^m = 1$

↳ è ciclico

$\mathbb{F}_p(G_m) = \mathbb{F}_{p^d}$, chi è d?

in G_m non c'è lo zero

d è il minimo tale che $G_m \subset \mathbb{F}_{p^d}^*$

$\{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^d - 1} = 1\}$

$\{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^m = 1\}$

Vale "<" $\Leftrightarrow$ SSE $m \mid p^d - 1$

$\Leftarrow$ $m \mid p^d - 1 \quad \alpha \in G_m \Rightarrow \alpha^m = 1 \Rightarrow \alpha^{me} = 1 \Rightarrow \alpha^{p^d - 1} = 1 \Rightarrow \alpha \in \mathbb{F}_{p^d}^*$

$\Rightarrow$ $G_m < \mathbb{F}_{p^d}^* \Rightarrow m = |G_m| \mid p^d - 1 = |\mathbb{F}_{p^d}^*|$

$d = \min\{k \mid m \mid p^k - 1\}$ ← divide

$ = \min\{k \mid p^k \equiv 1 \ (m)\} = \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^*} p$

TEOREMA

$n = p^a m \qquad (m, p) = 1$

Il c. di spezzamento di $x^n - 1$ su $\mathbb{F}_p$ (coincide sul c. di spezzamento di $x^m - 1$ su $\mathbb{F}_p$) è $\mathbb{F}_{p^d}$ $\quad d = \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^*} p$

Esempio:

$f_7(x) = x^7 - 1$ in $\mathbb{F}_5, \mathbb{F}_{11}$

$\mathbb{F}_5 \to m = 7 \quad p = 5 \quad 5^k \equiv 1 \ (7) \quad k = 6 \Rightarrow$ il c. di spezzamento è $\mathbb{F}_{p^6}$

voglio cercare la fattorizzazione $f_7(x)$. So che il MCM dei gradi dei fattori irriducibili è 6

$x^7 \equiv 1 \ (5)$

$\underset{\overset{\shortparallel}{x}}{x^5} x^2 \equiv 1 \ (5) \Rightarrow x^3 \equiv 1 \ (5) \Rightarrow$ l'unica sol. è 1

↳ in $\mathbb{Z}_5^*$ non ci sono el. di ord 3

$x^7 - 1 = (x-1)(x^6 + x^5 + \dots + x + 1)$

↑ se fosse riducibile avrebbe un termine di deg 1 nella fattorizzazione (perché il MCM dei gradi dovrebbe essere 6) diverso da $(x-1)$ (valutato in 1 non fa 0)

Su $\mathbb{F}_{11}$:

il c. di spezzamento è $\mathbb{F}_{11^d}$, calcolo d

$11^d \equiv 1 \ (7)$

$4^d \equiv 1 \ (7) \Rightarrow d = 3$

Cerco le radici in $\mathbb{F}_{11}$ di $x^7 \equiv 1 \ (11)$

↳ ha ordine 1 o 7

$\mathbb{Z}_{11}^*$ ha $\varphi(11) = 10$ el. $\Rightarrow$ non ha el. di ord 7 $\Rightarrow x \equiv 1 \ (11)$

$x^7 - 1 = (x-1)(\underbrace{x^6 + x^5 + \dots + x + 1}_{3+3})$

Esempio: $x^8 - 1$ su $\mathbb{F}_p$

$p = 2 \Rightarrow x^8 - 1 = (x-1)^8$

$p > 2$ c. di spezzamento su $\mathbb{F}_p$ $\quad p^k \equiv 1 \ (8)$ $\begin{cases} k=1 & p \equiv 1 \ (8) \\ k=2 & p \not\equiv 1 \ (8) \end{cases}$

$x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x+1)(x-1)(x^2+1)(x^4+1)$

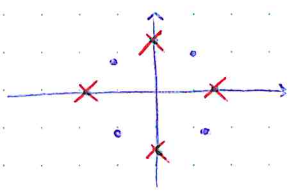
↓ irriducibile in $\mathbb{Z}[x]$

ma su $\mathbb{Z}_p[x]$, x^4+1 è sempre riducibile

(perché abbiamo visto che i fattori irriducibili hanno grado 1 o 2)

↳ possibili valori di k

Radici in $\mathbb{C}[x]$:



(radici ottave dalle quali tolgo le radici quarte)

Sui campi finiti tutti i polinomi che non hanno 0 come radice sono prodotti di polinomi ciclotomici (ogni elemento $\neq 0$ in un campo finito è radice dell'unità).

$K \to \overline{K}$

$\mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$

(ogni omomorfismo non banale sui campi è iniettivo, perché i campi hanno solo ideali banali)

$q \mapsto q$ se $q \in \mathbb{Q}$

$\sqrt[3]{2} \mapsto \sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$

$\downarrow$

perché queste sono tutte e sole le possibili immagini?

$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/(x^3-2)$

$\varphi_\beta : \mathbb{Q}[x] \to \overline{\mathbb{Q}}$

$x \mapsto \beta$ (β qualsiasi)

$\mathbb{Q}[x]/(x^3-2)$

voglio che passi al quoziente

$\ker \varphi_\beta = \{ p(x) \in \mathbb{Q}[x] \mid p(\beta) = 0 \}$

$(x^3-2) \subset \ker\varphi_\beta \Rightarrow \beta^3 - 2 = 0 \Rightarrow \beta$ deve essere una radice 3^a di 2

$K \quad \alpha \in \overline{K}$

$\varphi : K(\alpha) \to \overline{K} \qquad \varphi|_K = id$

$\varphi_\beta : \quad K[x] \to \overline{K}$

$x \mapsto \beta$

$p(x) \to p(\beta)$

$$\begin{tikzcd} K[x] \arrow[r, "\varphi_\beta"] \arrow[d, "\pi"'] & \overline{K} \\ K(\alpha) \cong K[x]/(\mu_\alpha(x)) \arrow[ur, dashed] & \end{tikzcd}$$

$(\mu_\alpha(x)) \subseteq \ker\varphi_\beta = \{ p(x) \in K[x] \mid p(\beta) = 0 \}$

$\Updownarrow$

$\mu_\alpha(\beta) = 0$

$\varphi : K(\alpha) \to \overline{K} \qquad \varphi|_K = id$

$\alpha \mapsto \beta \to$ radice di μ_α

$\#\varphi = \#$ radici distinte di μ_α in $\overline{K} = \deg \mu_\alpha$

$\hookrightarrow$ nei nostri casi

K campo $\quad \alpha, \beta \in \overline{K}$

α e β sono coniugati su K $\iff$ $\mu_\alpha|_K = \mu_\beta|_K$

sono radici dello stesso polinomio irriducibile su K

Generalizzando:

$\alpha \in \overline{K}$

$\psi : K \to \overline{K}$

$\varphi : K(\alpha) \to \overline{K} \qquad \varphi|_K = \psi \qquad$ (nel caso precedente $\psi = id$)

$$K(\alpha) \cong K[x]/(\mu_\alpha(x))$$

pol. minimo di α su K

$$\begin{aligned} \varphi_\beta : K[x] &\to \overline{K} \\ x &\mapsto \beta \\ k &\mapsto \psi(k) \\ p(x) &\mapsto (\psi p)(\beta) \end{aligned}$$

elemento di K

Passa al quotiente modulo $\mu_\alpha(x) \iff \mu_\alpha(x) \in \ker \varphi_\beta$

$$\ker \varphi_\beta = \{ p(x) \mid (\psi p)(\beta) = 0 \}$$

$(\psi p)(\beta) = 0 \iff \beta$ è radice di $(\psi \mu_\alpha)(x)$

$\# \varphi = \#$ radici distinte di $(\psi \mu_\alpha)(x) =$

$= \#$ radici distinte di $\mu_\alpha(x)$

Tralasciamo il "distinte", consideriamo che lo siano sempre.

$\deg \mu_\alpha = \deg(\psi \mu_\alpha) \Rightarrow$ hanno lo stesso $\#$ di radici

ψ manda num. diversi da 0 in num $\neq 0$ $\Rightarrow$ il termine di testa non si annulla

Proposizione $\quad K$ campo, $\alpha \in \overline{K} \qquad \mu_\alpha$ pol. di α / K

$n = \deg \mu_\alpha$

$\psi : K \to \overline{K}$

ψ si estende in n modi ad un omomorfismo

$\varphi : K(\alpha) \to \overline{K}$ t.c. $\varphi|_K = \psi$

Se $(\psi\mu_\alpha)(x) = (x-\beta_1)\cdots(x-\beta_n)$

$\varphi_1,\dots,\varphi_n$ sono definiti da $\varphi|_K = id$

$\varphi_i(\alpha) = \beta_i$

TEOREMA

E/K $\quad [E:K] = n$

$\forall\ \psi : K \hookrightarrow \overline{K}$ immersione

$\exists$ esattamente n estensioni ad E

$\varphi_1,\dots,\varphi_n : E \to \overline{K}$

$\varphi_i|_K = \psi \qquad i=1,\dots,n$

DIM. $\quad E = K(\alpha_1,\dots,\alpha_d)$

Per induzione su d

$d=1 \quad E = K(\alpha) \leftarrow$ è la prop.

$d-1$

$E = F(\alpha_d) \qquad F = K(\alpha_1,\dots,\alpha_{d-1})$

$\underbrace{K \underset{m}{\subseteq} F \underset{e}{\subseteq} E}_{n} \qquad n = me$

$$\begin{array}{l} E = F(\alpha_d) \\ \mid e \\ F = K(\alpha_1,\dots,\alpha_{d-1}) \\ \mid m \\ K \end{array}$$

$$\varphi_1 \begin{cases} \tilde{\varphi}_{11} \\ \vdots \\ \tilde{\varphi}_{1e} \end{cases} \quad \cdots \quad \varphi_m \begin{cases} \\ \\ \end{cases}$$

$\{\tilde{\varphi}_{ij}\}$ $\quad \begin{array}{l} j = 1,\dots,m \\ i = 1,\dots,e \end{array}$

Esempio: $\mathbb{Q}(\zeta_p)$ p primo

$\mu_{\zeta_p}(x) = \dfrac{x^p-1}{x-1} = x^{p-1} + \dots + x + 1$ è irriducibile

$\uparrow$

$\Phi_p(x+1)$ è p-Eisenstein

$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg \Phi_p(x) = p-1$

$\mathbb{Q}(\zeta_p) \hookrightarrow \overline{\mathbb{Q}}$

$\zeta_p \longmapsto \zeta_p^i \qquad 0 < i < p$

$\varphi_i\, \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta_p) \qquad ij \equiv 1\ (p)$

Def. F/K algebrico, si dice estensione NORMALE se

$\forall \varphi: F \to \overline{K}$ $\quad \varphi|_K = id$

si ha $\varphi(F) = F$

Esempi:

→ $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è normale

→ $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ normale

→ $K(\sqrt{a})/K$ normale

02/12/2024
Patimo

ES1 R UFD, $a \neq 0$

campo delle frazioni di R

$q \in Quot(R)$, se $\exists\ n \mid q^n \in R \Rightarrow q \in R$

$q = \frac{a}{b}$ con $a, b \in R$ a, b non hanno fattori irriducibili in comune

$q^n = \frac{a^n}{b^n} = t \in R \iff a^n = tb^n$

$a = u_a p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $u_a \in R^*$ p_i irriducibile

$b = u_b\, p_1^{\beta_1} \cdots p_k^{\beta_k}$ (se p_i non compare prendo $\alpha_i, \tau_i, \beta_i = 0$)

$t = u_t\, p_1^{\tau_1} \cdots p_k^{\tau_k}$

$\Rightarrow \forall i \quad p_i^{n\alpha_i} = p_i^{\tau_i + n\beta_i}$

$\Rightarrow n\alpha_i = \tau_i + n\beta_i \qquad n \mid \tau_i \quad \exists\ \tau_i' \in \mathbb{N}$ con $\tau_i = n\tau_i'$

$q = \frac{a}{b} = \frac{u_a}{u_b} p_1^{\alpha_1 - \beta_1} \cdots p_k^{\alpha_k - \beta_k}$

$n\tau_i' = n(\alpha_i - \beta_i) \Rightarrow \alpha_i - \beta_i = \tau_i'$

$\Rightarrow q = \frac{u_a}{u_b} p_1^{\tau_1'} \cdots p_k^{\tau_k'} \in R$

R UFD

$R/(a)$ è un dominio $\iff$ a è irriducibile

"$\Rightarrow$" Supponiamo per assurdo a riducibile

$a = bc \quad b, c \notin R^* \qquad \underset{\overset{\shortparallel}{0 \text{ in } R/(a)}}{\bar{a}} = \bar{b}\bar{c} \Rightarrow \bar{b} = 0$ o $\bar{c} = 0$

$\bar{b} = 0 \Rightarrow b \in (a) \Rightarrow a \mid b \quad \exists\ \beta \in R$ con $\beta = b$

$a = bc = a\beta c \Rightarrow a(1 - \beta c) = 0$

$\underset{0}{\overset{\shortparallel}{}} \Rightarrow c \in R^*$ ↯

$\bar{c} = 0$ simile

"$\Leftarrow$" a irriducibile

Supponiamo $R/(a)$ NON dominio

$\exists\ b, c \in R/(a) \quad b, c \neq 0 \quad bc = 0$

Prendo $\hat{b}$ con $\bar{\hat{b}} = b$ e $\hat{c}$ con $\bar{\hat{c}} = c$

$\hat{b}\hat{c} \in (a) \Rightarrow \exists k$ con $ak = \hat{b}\hat{c}$

a irriducibile $\Rightarrow a | \hat{b}$ o $a | \hat{c} \Rightarrow b = 0$ o $c = 0$ $\lightning$

ES 3

R anello, $K \subset R$ campo. Se $\dim_K R < +\infty$ e R dominio

$\Rightarrow$ R campo

DIM. $\quad a \in R \quad (\cdot a) : R \to R$
$x \mapsto a \cdot x$

$(\cdot a)$ suriettiva $\Leftrightarrow$ iniettiva $\Leftrightarrow a \neq 0$

$\Updownarrow$

$\exists b$ con $ba = 1 \Leftrightarrow a \in R^*$ $\quad \square$

ES 4 $\quad$ K campo $\quad K(x) = \mathrm{Quot}(K[x])$

$a \in K(x)$ è algebrico su K $\Rightarrow a \in K$

DIM $\quad a = \frac{f(x)}{g(x)} \quad f, g \in K[x], \ g \neq 0$

Se a è alg. $\exists\, p \in K[y] \ | \ p(a) = 0$, $p \neq 0$

$$p(y) = \sum_{i=0}^{n} p_i y^i$$

$$p(a) = 0 = \sum p_i \frac{f(x)^i}{g(x)^i} = 0$$

$$\Rightarrow \underbrace{\sum_{i=0}^{n} p_i f(x)^i g(x)^{n-i}}_{t(x)} = 0$$

- $\underset{n}{\deg f} \neq \underset{n'}{\deg g} \quad \deg t = n \max(n, n') \neq 0 \Rightarrow t \neq 0$

- $\deg f = \deg q$

$f(x) = q\,q(x) + r(x) \qquad \deg(r) < \deg(q)$

$\frac{f}{q} = q + \frac{r}{q} \qquad \frac{f}{q}$ alg. $\Leftrightarrow \frac{r}{q}$ alg.

Se $r \neq 0$, $\frac{r}{q}$ non è alg. per il punto precedente

$a = \frac{f}{q}$ alg $\Rightarrow f = qq$ con $q \in K \Rightarrow a \in K$ $\square$

ES 2

ELEMENTI NILPOTENTI

R anello commutativo con unità,

$\sqrt{0} = \bigcap_{P \text{ ideale primo}} P = \bigcap_{M \text{ ideali massimali}} M$

$\subseteq$

P primo $0 \in P$

$x \in \sqrt{0} \Rightarrow \exists n \mid x^n = 0 \Rightarrow x^n \in P \Rightarrow x \in P$

$\sqrt{0} \subset P \;\; \forall P \Rightarrow \sqrt{0} \subset \bigcap_{\text{primi}} P$

$\supseteq$ Se $x \notin \sqrt{0} \Rightarrow$ allora $\exists P$ primo $\mid x \notin P$

Mi basta trovare un ideale massimale che non contiene x

Prendo $\{I \text{ ideali} \mid x^n \notin I \;\forall n\} \neq \emptyset$ (contiene (0))

Zorn: prendo in questo insieme un ideale massimale

(le ip. di Zorn sono di facile verifica)

Sia Q un ideale massimale rispetto all'inclusione,

voglio verificare sia primo

Supponiamo Q non primo $\Rightarrow \exists a, b \in R \setminus Q \mid ab \in Q$

$\langle Q, a\rangle \supsetneq Q \Rightarrow \langle Q, a\rangle \notin S \Rightarrow \exists n \mid x^n \in \langle Q, a\rangle$

Stessa cosa per $\langle Q, b\rangle$, $\exists m \mid x^m \in \langle Q, b\rangle$

$\langle Q, a\rangle = \{q + ra \mid q \in Q, r \in R\}$

$x^n = q + ra$
$x^m = q' + r'b$

$$x^{n+m} = (q+ra)(q'+r'b) = \underbrace{qq' + raq' + qr'b}_{\in \mathbb{Q}} + \underbrace{rr'ab}_{\in \mathbb{Q}} \in \mathbb{Q}$$

ES 5 K campo $\operatorname{char} K \neq 2$ $a,b \in K$

$$K(\sqrt{a}) = K(\sqrt{b}) \iff \frac{a}{b} \in (K^*)^2$$

$(\Leftarrow)$ $\frac{a}{b} = t^2 \iff a = bt^2 \iff \sqrt{a} = \pm t\sqrt{b}$
$t \in K$

$$\Rightarrow K(\sqrt{a}) \subset K(\sqrt{b})$$

$$\sqrt{b} = \pm \frac{1}{t}\sqrt{a}$$

$$\Rightarrow K(\sqrt{a}) = K(\sqrt{b})$$

$(\Rightarrow)$ $[K(\sqrt{a}) : K] = [K(\sqrt{b}) : K]$

il grado divide 2 perché $x^2 - a$ è multiplo di $\mu_{\sqrt{a}}$

Se $[K(\sqrt{a}) : K] = 1 \Rightarrow \sqrt{a} \in K^* \Rightarrow a \in (K^*)^2$

$\sqrt{b} \in (K^*)^2$ (analogo)

$$\Rightarrow \frac{a}{b} \in (K^*)^2$$

Se $[K(a) : K] = 2$

$K(\sqrt{a}) = \{x + y\sqrt{a} \mid x,y \in K\}$

$\sqrt{b} \in K[\sqrt{a}) \Rightarrow \sqrt{b} = x + y\sqrt{a}$

$\Rightarrow b = x^2 + y^2 a + \underbrace{2xy\sqrt{a}}_{\in K}$

$\sqrt{a} \notin K$ se $[K(\sqrt{a}) : K] = 2 \Rightarrow$ $2xy = 0 \Rightarrow x = 0 \vee y = 0$

$\sqrt{b} = x$ $\vee$ $\sqrt{b} = y\sqrt{a} \Rightarrow \frac{a}{b} = \frac{1}{y^2} \in (K^*)^2$ $\square$

NO, $\sqrt{b} \notin K$

<u>OSS</u> Se $\operatorname{char} K = 2$ la prop. non vale

ES 6 p, q primi distinti

$K = \mathbb{Q}(\sqrt{p} + \sqrt{q})$

(i) $\sqrt{p} \in K$

(ii) $[K:\mathbb{Q}]$ normale

(iii) Contare le immersioni $K \hookrightarrow \overline{\mathbb{Q}}$

$\mathbb{Q}(\sqrt{p}+\sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p},\sqrt{q})$

$\mathbb{Q}(\sqrt{q}) \neq \mathbb{Q}(\sqrt{p})$

$$\begin{array}{ccc} & & \mathbb{Q}(\sqrt{p},\sqrt{q}) \\ & {}^{2}\nearrow & \\ \mathbb{Q}(\sqrt{p}) & & \Big| \, 4 \\ & {}_{2}\searrow & \\ & & \mathbb{Q} \end{array}$$

Ricordiamo L/K normale se $\forall \varphi: L \to \overline{K}$ che fissa K vale $\varphi(L)=L$

$\mathbb{Q}(\sqrt{p},\sqrt{q})$ è normale

$\varphi: \mathbb{Q}(\sqrt{p},\sqrt{q}) \hookrightarrow \overline{\mathbb{Q}}$

$\varphi(\sqrt{p}) = \pm\sqrt{p}$

$\varphi(\sqrt{q}) = \pm\sqrt{q}$

$\Rightarrow \varphi(\mathbb{Q}(\sqrt{p},\sqrt{q})) = \mathbb{Q}(\sqrt{p},\sqrt{q})$

$\sqrt{p}$ è radice di x^2-p in $\mathbb{Q}[x]$ $\varphi(\sqrt{p})$ è radice di $\varphi(x^2-p) = x^2-p$
$\Rightarrow \varphi(\sqrt{p}) = \pm\sqrt{p}$

So anche quali sono le 4 immersioni di $\mathbb{Q}(\sqrt{p},\sqrt{q})$ in $\overline{\mathbb{Q}}$

$\sqrt{p}+\sqrt{q} \mapsto \pm\sqrt{p}\pm\sqrt{q}$

↳ questi 4 elementi sono tutti distinti

$\pm\sqrt{p}\pm\sqrt{q}$ sono tutte radici di $\mu_{\sqrt{p}+\sqrt{q}} \Rightarrow \deg \mu_{\sqrt{p}+\sqrt{q}} \geq 4$

ma il grado è esattamente 4 perché $\sqrt{p}+\sqrt{q} \in \mathbb{Q}(\sqrt{p},\sqrt{q})$
↓
ha deg. 4 su $\mathbb{Q}$

$\Rightarrow \mathbb{Q}(\sqrt{p}+\sqrt{q}) = \mathbb{Q}(\sqrt{p},\sqrt{q}) \Rightarrow \sqrt{p} \in \mathbb{Q}(\sqrt{p}+\sqrt{q})$

Questo conclude tutti i punti

ES7 K campo, $f, q \in K[x]$ irriducibili

$\deg f = m$, $\deg q = n$ $\quad (m,n)=1$

Presa α radice di f, q è irriducibile su $K(\alpha)$

q irriducibile su K $\iff$ $\forall \beta$ radice di q vale $[K(\beta):K]=n$

$$\begin{tikzcd}
 & K(\alpha,\beta) \arrow[dl, dash] \arrow[dr, dash] & \\
K(\alpha) \arrow[dr, dash, "m"'] & & K(\beta) \arrow[dl, dash, "n"] \\
 & K &
\end{tikzcd}$$

Shift

$n, m \mid [K(\alpha,\beta):K] \implies mn \mid [K(\alpha,\beta):K] \leq mn$

$\implies \deg \mu_\beta^{(K(\alpha))} = [K(\alpha,\beta):K(\alpha)]$

$\mu_\beta^{(K(\alpha))} \mid \mu_\beta^{(K)} = q \quad *$

$\implies [K(\alpha,\beta):K] = mn$

$\deg \mu_\beta^{(K(\alpha))} = [K(\alpha,\beta), K(\alpha)] = n \implies$ dalla divisibilità $*$ $\mu_\beta^{K(\alpha)} = \lambda q$

con $\lambda \in K$

Quindi q è un polinomio minimo su $K(\alpha)$

perciò è irriducibile. $\square$

ES9 Calcolare il grado del Campo di spezzamento L di $x^4-5 = f(x)$ su $\mathbb{Q}$

Radici $\sqrt[4]{5}$, $-\sqrt[4]{5}$, $i\sqrt[4]{5}$, $-i\sqrt[4]{5}$ $= \mathbb{Q}(\sqrt[4]{5}\, i^k \mid k=0,1,2,3)$

$L = \mathbb{Q}(\sqrt[4]{5}, i\sqrt[4]{5}) = \mathbb{Q}(\sqrt[4]{5}, i)$ questa doppia inclusione va mostrata!

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[4]{5}, i) \arrow[dl, dash, "\leq 2 \\ 1 \text{ o } 2"'] \arrow[dr, dash, "\leq 4"] & \\
\mathbb{Q}(\sqrt[4]{5}) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

f è irriducibile per Eisenstein (per $p=5$)

Se fosse $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] = 1$ avrei l'uguaglianza ma ciò è imp. perchè uno è contenuti in $\mathbb{R}$ e uno no

$\Rightarrow [\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}] = 8$

03/12/2024
Patinno

ES 3 K campo $f \in K[x]$, $\deg f = n$

L c. di spezzamento di f

$[L:K] \mid n!$

DIM. (induzione)
$f \sim 1$ ✓ $L = K$ $1 \mid 1!$

Fisso n e suppongo per $m < n$ che valga la tesi

Se tutte le radici di f sono in K, allora $L = K$ ✓

- Assumiamo f irriducibile

Presa $\alpha \in \overline{K}$ radice di f, $[K(\alpha):K] = n$

$$\begin{tikzcd}[column sep=small, row sep=small] & L \\ K(\alpha) \arrow[ur, dash] \arrow[dr, dash, "n"'] & \\ & K \end{tikzcd}$$

L è c.d.s. di $\underset{\overset{\shortparallel}{q(x)}}{\dfrac{f(x)}{x-\alpha}}$ in $K(\alpha)$

$\deg q = n-1$

Per ip. induttiva si ha

$[L:K(\alpha)] \mid (n-1)!$ $[L:K] = n[L:K(\alpha)] \mid n!$

- Assumiamo f riducibile $f(x) = \underset{\text{di deg } n_1}{f_1(x)}\underset{\text{di deg } n_2}{f_2(x)}$ (strettam. positivi)

$L_1 :=$ c.d.s. di f_1 su K L posso pensarlo come c.d.s di f_2 su L_1

$$\begin{tikzcd}[column sep=small, row sep=small] & L \\ L_1 \arrow[ur, dash] \arrow[dr, dash] & \\ & K \end{tikzcd}$$

Per ip. induttiva so che $[L_1:K] \mid n_1!$ e $[L:L_1] \mid n_2!$

$[L:K] \mid n_1!\, n_2! \mid n!$ perché $\dfrac{n!}{n_1!\, n_2!} = \binom{n}{n_1} \in \mathbb{Z}$ □

ES. 9 $f(x) = x^3 + x + 1$ su $\mathbb{Q}$

f è irriducibile perché non ha radici in $\mathbb{Q}$

$f(1) = 3 \quad f(-1) = 1$

α radice di f, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

L c.d.s. di f

$$\begin{array}{rc}
 & L \\
1 \circ 2 \rightarrow & | \\
 & \mathbb{Q}_\alpha \\
 & |\ 3 \\
 & \mathbb{Q}
\end{array} \Bigg) K \qquad \text{con } K \mid 6 = 3!$$

f ha una radice in $\mathbb{R}$

$f'(x) = 3x^2 + 1 > 0 \Rightarrow f$ è monotona su $\mathbb{R}$

$\Rightarrow f$ ha un'unica radice reale e 2 complesse

$$\alpha, \underbrace{\beta, \overline{\beta}}_{\notin \mathbb{R}}$$

$\Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$

$\mathbb{Q}(\alpha)$ è contenuto in $\mathbb{R}$,
$\mathbb{Q}(\alpha, \beta)$ no

$f(x) = x^4 + 3x^2 + 1$ su $\mathbb{Q}$

f è irriducibile? f non ha radici in $\mathbb{Q}$

Vediamo se $f = (x^2 + ax + b)(x^2 + a'x + b')$

$$\begin{cases} bb' = 1 \\ ab' + ba' = 0 \\ a + a' = 0 \\ aa' + b + b' = 3 \end{cases} \quad \text{non ha soluzione} \quad \Rightarrow f \text{ irriducibile}$$

$g(y) = y^2 + 3y + 1 \qquad f(x) = g(x^2)$

le radici di g sono $\dfrac{-3 \pm \sqrt{5}}{2}$

$\Rightarrow$ le radici di f sono $\pm \sqrt{\dfrac{-3 \pm \sqrt{5}}{2}}$

$\alpha = \sqrt{\dfrac{-3 + \sqrt{5}}{2}} \qquad \beta = \sqrt{\dfrac{-3 - \sqrt{5}}{2}} \quad \Rightarrow$ le radici sono $\pm\alpha$ e $\pm\beta$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, vale $\beta \in \mathbb{Q}(\alpha)$?

$1 = \alpha^2\beta^2 \Rightarrow \alpha\beta = \pm 1 \Rightarrow \beta = \pm\frac{1}{\alpha} \in \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\alpha)$ è il c.d.s. di f (grado 4)

ES 10 $\boxed{\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}}$

Reminder: $\exists!$ campo con p^n elementi (in una fissata chiusura algebrica)

$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \Leftrightarrow n \mid m$

$\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$ dove penso $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ quando $n \mid m$

(se $x \in \bigcup \mathbb{F}_{p^n}$, allora $x \in \mathbb{F}_{p^{n_0}}$, ma allora $x \in \mathbb{F}_{p^{kn_0}}\ \forall k \in \mathbb{N}$)

se $x, y \in \bigcup \mathbb{F}_{p^n}$, $\exists n_0, m_0 \mid x \in \mathbb{F}_{p^{n_0}}, y \in \mathbb{F}_{p^{m_0}}$

$\Rightarrow x, y \in \mathbb{F}_{p^{n_0 m_0}} \Rightarrow$ posso definire $x+y$ e yx in

$\mathbb{F}_{p^{n_0 m_0}} \subset \bigcup \mathbb{F}_{p^n}$ ($\Rightarrow$ è effettivamente un campo)

Voglio dimostrare che $\bigcup \mathbb{F}_{p^n}$ è una chiusura algebrica di $\mathbb{F}_p$

$\bigcup \mathbb{F}_{p^n}$ è alg. perché se $x \in \bigcup \mathbb{F}_{p^n} \Rightarrow \exists n_0 \mid x \in \mathbb{F}_{p^{n_0}}$

$\Rightarrow x$ algebrico

estensione alg. di $\mathbb{F}_p$

Sia ora $f(x) \in \bigcup \mathbb{F}_{p^n}[x]$

$f(x) = \sum_{i=0}^{d} a_i x^i$

$\forall i\ \exists n_i \mid a_i \in \mathbb{F}_{p^{n_i}} \subset \mathbb{F}_{p^m}$ dove $m = \prod n_i$

$\Rightarrow f(x) \in \mathbb{F}_{p^m}[x]$

Una radice α di f ha grado al più d su $\mathbb{F}_{p^m}$

Quindi $\alpha \in \mathbb{F}_{p^{md}} \subset \bigcup \mathbb{F}_{p^n} \Rightarrow f$ ha una radice

$\Rightarrow \bigcup \mathbb{F}_n$ è alg. chiuso ed è quindi una chiusura alg. di $\mathbb{F}_p$

$\bigcup \mathbb{F}_n = \overline{\mathbb{F}_p}$

ES 11 K campo, $\alpha \in \overline{K}$

Voglio trovare il polinomio minimo di α^2 in funzione di $\mu_\alpha(x)$

$$K \subset K(\alpha^2) \overset{\deg 2}{\subset} K(\alpha)$$

$$\mu_\alpha^{K(\alpha^2)} \mid x^2 - \alpha^2$$

Supponiamo $[K(\alpha) : K(\alpha^2)] = 2$

$$\deg \mu_{\alpha^2} = \frac{1}{2} \deg \mu_\alpha^{\text{su } K}$$

$$\mu_{\alpha^2}(\alpha^2) = 0$$

$$g(x) = \mu_{\alpha^2}(x^2),\ g(\alpha) = \mu_{\alpha^2}(\alpha^2) = 0$$

$$\Rightarrow g = \mu_\alpha \qquad \mu_\alpha(x) = \mu_{\alpha^2}(x^2)$$

Quindi μ_α ha solo termini di grado pari

Vale anche il viceversa, se $\mu_\alpha(x)$ ha solo termini di grado pari, lo posso pensare come $p(x^2)$

$p(x)$ è un pol. con radice α^2.

$$\deg p = \frac{1}{2} \deg \mu_\alpha \Rightarrow p = \mu_{\alpha^2}$$

Supponiamo che $\mu_\alpha(x) = p(x^2) + x\, d(x^2)$ con $p, d \in K[x]$

$$\mu_{-\alpha}(x) = p(x^2) - x\, d(x^2)$$

$$\mu_\alpha(x)\mu_{-\alpha}(x) = p(x^2)^2 - x^2 d(x^2)^2 = g(x^2)$$

$$\deg g = \deg \mu_\alpha = \deg \mu_{-\alpha} \qquad \mu_{\alpha^2}(x^2) = \mu_\alpha(x)\mu_{-\alpha}(x)$$

$$g(\alpha^2) = \mu_\alpha(\alpha)\mu_{-\alpha}(+\alpha) = 0$$

$\Rightarrow$ g polinomio minimo di α^2

ES 12 ζ_n radice primitiva dell'unità su $\mathbb{Q}$

$\zeta_n \in \overline{\mathbb{Q}}$ è radice di $x^n - 1$

e non è radice di $x^m - 1$ $\forall m \mid n,\ m \neq n$.

Vogliamo studiare $\mathbb{Q}(\zeta_n) \supset \mathbb{Q}$

Quante sono le radici primitive?

ζ_n^k è anche radice di $x^n - 1$

$$(\zeta_n^k)^n = \zeta_n^{nk} = 1^k = 1$$

$\zeta_n^a = \zeta_n^b$ con $0 \leq a < b < n$

$\Rightarrow \zeta_n^{b-a} = 1$ $\lightning$ ζ_n primitiva

Quindi, $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ sono tutte le radici di

$x^n - 1$. Quali sono primitive?

$(k, n) = d > 1$

$(\zeta_n^k)^{n/d} = 1 \Rightarrow \zeta_n^k$ non primitiva

$(k, n) = 1$ $\exists h$ con $kh \equiv 1$ (n)

$(\zeta_n^k)^h = \zeta_n$

E se $(\zeta_n)^m = 1$ con $m < n$ avrei anche $\zeta_n^m = 1$ $\lightning$

Quindi ho $\varphi(n)$ radici primitive

$\mu_{\zeta_9}(x) = \dfrac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1$

è il polinomio minimo (ci si annulla ζ_9 e ha deg $6 = \varphi(9)$)

Voglio far vedere che $\mathbb{Q}(\zeta_n)$ è normale

$$\varphi: \mathbb{Q}(\zeta_n) \hookrightarrow \overline{\mathbb{Q}}$$

$\varphi(\zeta_n)$ è una radice di $x^n - 1$, quindi $\varphi(\zeta_n) = \zeta_n^k \in \mathbb{Q}(\zeta_n)$

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = ?$

$\overset{\shortparallel}{\varphi(n)}$ $\rightarrow$ voglio dimostrarlo

Chiamo f il pol. minimo di ζ_n. Supponiamo che $\exists (k, n) = 1$

t.c. ζ_n^k non sia radice di f

$f \mid x^n - 1$ $\quad x^n - 1 = f(x) q(x)$ con $q(\zeta^k) = 0$

$(f, q) = 1$ perché f irriducibile

$h(x) = g(x^k)$

$h(\zeta_n) = 0 \Rightarrow f \mid h$

$g(x^k) = f(x)\, q(x)$

Prendo $t = \mu_{\zeta^k}(x)$ $\quad f(x)t(x) \mid x^n - 1$

$(f, t) = 1$ (f irriducibile)

$h(x) = t(x^k)$

$h(\zeta_n) = 0 \Rightarrow f \mid h$

$t(x^k) = f(x)\, q(x)$

Posso assumere che tutti questi polinomi siano primitivi (dividono $x^n - 1$ che è primitivo)

Prendo p primo che divide k, $k = pk'$

Posso ridurre modulo p.

$t(x^{pk'}) = t_1(x^{k'})^p$ per qualche t_1 in $\mathbb{F}_p[x]$ di deg $\frac{1}{p} \cdot \deg t$

$t_1(x^{k'})^p = \overline{f(x)}\, \overline{q(x)}$

Supponiamo per ora $k' = 1$. Sia α radice di $\overline{f}$ $\quad \overset{\overline{\mathbb{F}_p}}{\Downarrow}$

$t_1(\alpha) = 0 \Rightarrow \alpha$ radice di t_1 e quindi di t su $\mathbb{F}_p$

Ma α è anche radice di f

E ho $tf \mid x^n - 1$

α radice doppia di $x^n - 1 \Rightarrow \underbrace{x^{n-1}}_{\text{derivata}} = 0$ ↯ $(p \nmid n)$

Ho trovato un assurdo

ζ_n ha pol. minimo f

p primo che non divide n $\quad f(\zeta_n^p) = 0$

Def.

L/K alg. si dice **NORMALE** se

$\forall \varphi \quad L \to \overline{K} \qquad \varphi|_K = id \Rightarrow \varphi(L) = L$

($\overline{K}$) coincide con $\overline{L}$

Proposizione L/K alg. TFAE

1) L/K è normale

2) $\forall f \in K[x]$ irriducibile su K, se f ha una radice in $L \Rightarrow$

$\Rightarrow f$ ha tutte le radici in L

3) L è il c. di sp. su K di una famiglia di polinomi di $K[x]$

DIM. Nel caso L/K finita

1 ⇒ 2

Sia $f \in K[x]$ irriducibile e $\alpha \in L$ una radice di f $\quad f(\alpha) = 0$

In $K[x] \quad f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \qquad \alpha_1 = \alpha$

$K \subseteq K(\alpha) \subseteq L$

HP implicita ⇒ char $K = 0$ o campo finito (in questo modo gli irriducibili hanno radici distinte)

Siano $\varphi_1, \dots, \varphi_n$ le immersioni di $K(\alpha)/K$

$\varphi_i(\alpha) = \alpha_i$ deve andare in una radice del polinomio minimo $\qquad \varphi_i|_K = id$

Per il teo. di estensione delle immersioni

$\forall i \quad \varphi_i$ si estende $\tilde{\varphi}_i : L \to \overline{K} \qquad \tilde{\varphi}_i|_{K(\alpha)} = \varphi_i$

$\tilde{\varphi}_i|_K = \varphi_i|_K \quad \Rightarrow \quad \tilde{\varphi}_i(L) = L \quad \Rightarrow \quad \tilde{\varphi}_i(\alpha) = \varphi_i(\alpha) = \alpha_i \in L$

2 ⇒ 3

$\mathcal{F} = \{\mu_\alpha(x) \in K[x] \mid \alpha \in L\}$ famiglia di tutti i pol. minimi

TESI: L è il c. di sp. di $\mathcal{F}$ su K

$L_0 :=$ c. di sp. di $\mathcal{F}$ su $L = K(\beta_{\alpha i} \mid \alpha \in L, i = 1, \dots, n_\alpha)$ tutte le radici di tutti i pol.

$\mu_\alpha(x) = \prod_{i=1}^{n_\alpha} (x - \beta_{\alpha i})$

$\beta_{\alpha 1} = \alpha \Rightarrow L \subseteq L_0$

Voglio dimostrare l'inclusione opposta. $K \subseteq L$

$\Rightarrow$ i $\beta_{\alpha i}$ sono in L?

Per la prop. 2. tutte le radici di μ_α sono in L

$$\beta_{\alpha i} \in L \ \forall \alpha \ \forall i \Rightarrow L_0 \subseteq L \Rightarrow L = L_0$$

3 => 1 Sia $\mathcal{F} = \{f_i(x) \in K[x]\}_{i \in I}$

L è c. di sp. su K di $\mathcal{F}$ $\qquad f_i = \prod_{j=1}^{n_i}(x - \alpha_{ij})$ in $\overline{K}$

$\overset{\shortparallel}{K}(\alpha_{ij} \mid i \in I, j = 1, \dots, n_i)$

Sia $\varphi : L \to \overline{K}$ $\qquad \varphi|_K = id$

$\varphi(\alpha_{ij}) = \underset{\substack{\uparrow \\ \text{stessa } i}}{\alpha_{ij'}} \in L \qquad \forall i, j \quad f(\alpha_{ij}) \in L$

(le immersioni permutano le radici dei pol. minimi)

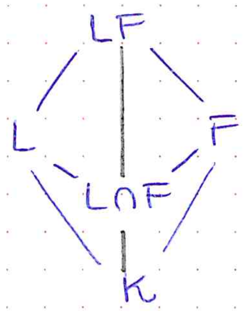
$$\varphi(L) = \varphi(K(\alpha_{ij} \mid \cdots)) = \varphi(K)(\varphi(\alpha_{ij}) \mid —)$$
$$= K(\alpha_{ij} \mid —) \subset L$$

$K^n \subset \underbrace{\varphi(L) \subseteq L}_{n}$ $\qquad [\varphi(L) : K] = \dim_K \varphi(L) \underset{\substack{| \\ \varphi \text{ è iniettiva}}}{=} \dim_K L = [L : K]$

PROPRIETÀ DELLE ESTENSIONI NORMALI

L/K F/K est. normali $\Rightarrow$ LF/K normale

$LF \cap F/K$ normale



LF/K normale $\Leftrightarrow \forall \varphi \ LF \to \overline{K}$

$\varphi|_K = id \quad \varphi(LF) = LF$

$\varphi(LF) = \varphi(L)\varphi(F) = LF$

$\varphi(L \cap F) = \varphi(L) \cap \varphi(F) = L \cap F$

TORRI (non vale)

$$\begin{array}{l} L \\ \mid \to \text{normale} \\ F \\ \mid \to \text{normale} \\ K \end{array}$$

non è detto sia normale

Esempio: $\mathbb{Q}(\sqrt[4]{2})$ | norm. $\mathbb{Q}(\sqrt{2})$ | norm. $\mathbb{Q}$ normale? NO

x^4-2

$\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$

$$\begin{array}{l} L \\ \mid \to \text{normale} \\ F \\ \mid \to \text{in generale non normale} \\ K \end{array}$$

norm.

Prop. L/K normale $\Rightarrow$ L/F normale

$\forall \varphi: L \to \overline{K}$ $\quad \varphi|_F = id \Rightarrow \varphi|_K = id$

$\Rightarrow \varphi(L) = L$

$L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

$$\begin{array}{l} L \\ \mid 2 \\ \mathbb{Q}(\sqrt[3]{2}) \\ \mid 3 \to \text{NON normale} \\ \mathbb{Q} \end{array} \qquad 6$$

x^3-2

SHIFT

\begin{tikzcd}
 & LF & \\
L \arrow[ur, dash] & & F \arrow[ul, dash, "norm"'] \\
 & K \arrow[ul, dash, "norm"] \arrow[ur, dash] &
\end{tikzcd}

$L, F \subseteq \overline{K}$

L/K normale $\Rightarrow$ LF/F normale

$\varphi: LF \to \overline{K}$ $\quad \varphi|_F = id$ $(\Rightarrow \varphi|_K = id)$

$\varphi(LF) = \varphi(L)\varphi(F) = LF$

$\hookrightarrow L/K$ normale

Gruppo di Galois

in realtà vale anche senza queste ip.

L/K finita e separabile $\quad$ ($\mathrm{char}\, K = 0$ oppure $|K| < +\infty$)

vale se i polinomi minimi hanno radici distinte

- L/K normale

Se $[L:K] = n$ $\exists\, \varphi_1, \dots, \varphi_n$ $L \to \overline{K}$ $\varphi_i|_K = id$ (sep.)

$\varphi_i(L) = L \quad \forall i$ (norm.) cioè che fissano puntualmente K

Le φ_i sono automorfismi su K di L

$\varphi_i \in Aut_K(L) = Gal(L/K)$

$|Gal(L/K)| = [L:K]$ ← È UN GRUPPO

Se L/K è norm. e sep. la chiamo "di Galois"

Proposizione $f(x) \in K[x]$ irriducibile $\deg f = n$

F c. di sp. di f su K $\Rightarrow Gal(F/K) \hookrightarrow S_n$

$$n \mid [F:K] \mid n!$$

vera anche quando f NON riducibile

DIM. f(x) ha deg. n

$f(x) = (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_n)$

$\underset{n}{K \subseteq K(\alpha_1)} \subseteq F = K(\alpha_1, \ldots, \alpha_n) \Rightarrow n \mid [F:K]$ (perché ho trovato una sottoestensione di deg. n)

$\hookrightarrow \mu_{\alpha_1} \mid f$ ma f irriducibile $\Rightarrow \mu_{\alpha_1} \sim f$

$[F:K] = |Gal(F/K)|$ se dimostro $Gal(L/K) \hookrightarrow S_n$

$|Gal(L/K)| \mid n!$

$\phi: Gal(F/K) \hookrightarrow S(\alpha_1 \ldots \alpha_n)$

$\varphi \longmapsto \varphi|_{\{\alpha_1 \ldots \alpha_n\}}$

ϕ è ben def. $\varphi(\alpha_i) = \alpha_j \Rightarrow \varphi(\{\alpha_1 \ldots \alpha_n\}) \subseteq \{\alpha_1 \cdots \alpha_n\}$

ϕ è omo ma da φ iniettiva ottengo l'uguaglianza

ϕ iniettivo

$Ker\,\phi = \{\varphi \in Gal(F/K) \mid \varphi(\alpha_i) = \alpha_i \ \forall i = 1, \ldots, n\}$

$F = K(\alpha_1, \ldots, \alpha_n)$

$\varphi|_K = id \quad \alpha_i \to \alpha_i \Rightarrow \varphi = id$

$Gal(F/K)$ agisce su $\{\alpha_1, \ldots, \alpha_n\}$ fedelmente e transitivamente

L'azione di $Gal(F/K)$ su $\{\alpha_1, \ldots, \alpha_n\}$ è TRANSITIVA

cioè $orb(\alpha_1) = \{\alpha_1, \ldots, \alpha_n\}$

l'unico elemento che fissa tutte le α_i è l'identità

DIM. $K \subseteq K(\alpha_1) \subseteq F = K(\alpha_1, \ldots, \alpha_n)$

$\varphi_i: \alpha_1 \to \alpha_i \quad \forall i$

$\forall i$ su $\hat{\varphi}_i$ est. di φ_i a F

$\hat{\varphi}_i(\alpha_i) = \alpha_i \qquad \hat{\varphi}_i \in Gal(F/K)$

Esercizi / esempi

$L/K \quad [L:K] = 2 \Rightarrow L/K$ norm. cioè data $\varphi : L \hookrightarrow \overline{K}$ t.c. $\varphi|_K = id \Rightarrow \varphi(L) = L$

$|Gal(F/K)| = 2$ (tutte le estensioni di grado 2 sono semplici)

$L = K(\sqrt{a})$ $\quad \begin{cases} id \\ \varphi(\sqrt{a}) = -\sqrt{a} \end{cases}$

$x^2 - a$

contiene

$Gal(F/K) \cong \mathbb{Z}/2\mathbb{Z}$

(estensione di deg p $\Rightarrow Gal(\ ) \cong \mathbb{Z}/p\mathbb{Z}$)

$f \in K[x]$ irriducibile di deg 3

F = c. di sp. di $f|_K$

$3 \mid [F:K] \mid 3!$

$3 \rightarrow Gal(F/K) \cong \mathbb{Z}/3\mathbb{Z}$

$6 \rightarrow Gal(F/K) \cong S_3$

$\downarrow$ es.

$\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \quad x^3 - 2$

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

$\varphi_i : \zeta_n \to \zeta_n^i \mapsto \bar{i}$

$(i, n) = 1$

(218 volume 1)

$f(x) = x^5 + x^2 - x + 4$

① c. di sp. su $\mathbb{F}_2$ e su $\mathbb{F}_3$

② c. di sp. su $\mathbb{F}_{3^k}$

$\mathbb{F}_2$ $\quad f(x) = x(x^4+x+1)$

↑ non ha radici e non si scompone in due term. di deg 2 perché l'unico irriducibile di deg 2 di $\mathbb{F}_2[x]$ è x^2+x+1 che al quadrato non fa questo

$\Rightarrow$ il c. di sp. è $\mathbb{F}_{2^4}$

$\mathbb{F}_3$ $\quad f(x) = x^5+x^2-x+1$

$= x(x^4-1)+(x^2+1) = (x^2+1)(x^3-x+1)$

irriducibili (al compito va giustificato)

$\Rightarrow$ il c. di sp. è $\mathbb{F}_{3^6}$

(2)

$\mathbb{F}_3(\alpha_1,\dots,\alpha_5) = \mathbb{F}_{3^6}$

$\mathbb{F}_{3^k}(\alpha_1,\dots,\alpha_5) = \mathbb{F}_{3^{kd}}$

Il c. di sp. è $\mathbb{F}_{3^{kd}}$ dove d è il minimo t.c.

$\alpha_1,\dots,\alpha_5 \in \mathbb{F}_{3^{kd}}$

$\Updownarrow$

$\mathbb{F}_{3^6} \subseteq \mathbb{F}_{3^{kd}}$ $\quad 6 \mid kd \iff \frac{6}{(6,k)} \mid d$

—

Fattorizzazione di x^3-a su $\mathbb{F}_p$ $\quad (p\neq 3,2)$, $a \neq 0$

$\mathbb{F}_p^* \xrightarrow{\varphi} \mathbb{F}_p^*$
$c \mapsto c^3$

$\mathbb{F}_p^*$ abeliani e ciclici

$\ker\varphi = \{c\in \mathbb{F}_p^* \mid c^3=1\}$ (elementi di ordine moltiplicativo 1 o 3)

$|\ker\varphi| = 1$ se $3 \nmid |\mathbb{F}_p^*| = p-1$

$|\ker\varphi| = 3$ se $3 \mid p-1$ ($\varphi(3) \neq$ identità)

$|\ker\varphi| = 1 \Rightarrow \varphi$ biiettiva $\Rightarrow$ trovo un'unica soluzione

$x^3-a = (x-c)\,q(x)$

↑ deg. 2

$|\mathrm{Ker}\,\varphi| = 3$

$a \in \mathrm{Imm}\,\varphi \Rightarrow (x^3 - a) = (x-c_1)(x-c_2)(x-c_3)$

$a \notin \mathrm{Imm}\,\varphi \Rightarrow x^3 - a$ irriducibile

09/12/2024
Patimo

ζ_n radice n-esima dell'unità su $\mathbb{Q}$

$\mathbb{Q}(\zeta_n)$ è normale su $\mathbb{Q}$

Se $\varphi : \mathbb{Q}(\zeta_n) \hookrightarrow \overline{\mathbb{Q}}$

allora $\varphi(\zeta_n) = \zeta_n^k$ per qualche k

φ iniettiva $\Rightarrow$ k coprimo con n, altrimenti trovo $m<n$
$(\zeta_n^k)^m = 1$

$\#$ immersioni $\leq$ $\#$ num. < di n coprimi con n $= \varphi(n)$

ζ_n radice primitiva $f = \mu_{\zeta_n}(x)$

$\Rightarrow \zeta_n^p$ è radice di $\mu_{\zeta_n}(x)$ se p è un primo che divide n

Tutti gli elementi della forma ζ_n^k con $(k,n)=1$ sono radici di $\mu_{\zeta_n}(x)$

$\deg \mu_{\zeta_n}(x) \geq \varphi(n)$ allora vale l'uguaglianza

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) = ?$ $\qquad \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^*$

$\Uparrow$

Gli automorfismi di $\mathbb{Q}(\zeta_n)$ sono definiti da $\varphi_k : \zeta_n \mapsto \zeta_n^k$
con $(k,n)=1$

$$\varphi_k \circ \varphi_{k'}(\zeta_n) = \varphi_k(\zeta_n^{k'}) = (\varphi_k(\zeta_n))^{k'} = \zeta_n^{kk'} = \varphi_{kk'}(\zeta_n)$$

ES. Studiare le sottoestensioni di $\mathbb{Q}(\zeta_{12})$

$\mathbb{Q}(\zeta_{12})/\mathbb{Q}$ è di Galois con gruppo $(\mathbb{Z}/12\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$$4\left(\begin{array}{c}\mathbb{Q}(\zeta_{12}) \\ | \\ L \\ | \\ \mathbb{Q}\end{array}\right.$$

sottoestensione propria

$\Rightarrow [L:\mathbb{Q}] = 2$

$\zeta_{12} = \cos(30°) + i\,\mathrm{sen}(30°) = \frac{\sqrt{3}}{2} + \frac{i}{2}$

$\mathbb{Q}(\sqrt{3}, i) \supset \mathbb{Q}(\zeta_{12})$ ma hanno entrambe grado 4 $\Rightarrow \mathbb{Q}(i,\sqrt{3}) = \mathbb{Q}(\zeta_{12})$

$\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ sono sottoestensioni

$\varphi \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_{12})/\mathbb{Q}\right)$ allora $\varphi(\sqrt{3}) = \pm\sqrt{3}$ e $\varphi(i) = \pm i$

Supponiamo che $L = \mathbb{Q}(\alpha)$ è un' estensione di grado 2 ($\Rightarrow$ normale)

$\alpha = a + b\sqrt{3} + ci + d\sqrt{-3}$ ← 4 elementi della base

$$\left.\begin{array}{l}\varphi_{+,+}(\alpha) = (a,b,c,d) \\ \varphi_{+,-}(\alpha) = (a,b,-c,-d) \\ \varphi_{-,+}(\alpha) = (a,-b,c,-d) \\ \varphi_{-,-}(\alpha) = (a,-b,-c,d)\end{array}\right\} \in \mathbb{Q}(\alpha)$$

$b \neq 0$ $\quad (a,b,c,d) + (a,b,-c,-d) = a + \sqrt{3}b \in \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3})$

$c \neq 0$ $\quad (a,b,c,d) + (a,-b,c,-d) = a + ic \in \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(i)$

$d \neq 0$ $\quad \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-3})$

Quindi ci sono solo queste 3 estensioni

ES. 2. $\alpha, \beta \in \overline{\mathbb{F}_p}$ $\quad [\mathbb{F}_p(\alpha):\mathbb{F}_p] = m$, $\quad [\mathbb{F}_p(\beta):\mathbb{F}_p] = n$ $\quad (m,n) = 1$

Tesi: $[\mathbb{F}_p(\alpha+\beta):\mathbb{F}_p] = mn$

L, K sono due campi finiti dentro $\overline{\mathbb{F}_p}$

$|L| = p^n, \ |K| = p^m$

allora $L < K \iff n \mid m$

$$\begin{tikzcd}
 & \mathbb{F}_p(\alpha,\beta) \arrow[dl, dash, "n"'] \arrow[dd, dash, "mn"] \arrow[dr, dash, "m"] \arrow[drr, dash] & & \\
\mathbb{F}_p(\alpha) \arrow[dr, dash, "m"'] & & \mathbb{F}_p(\beta) \arrow[dl, dash, "n"] & \mathbb{F}_p(\alpha+\beta) \arrow[dll, dash, "d"] \\
 & \mathbb{F}_p & &
\end{tikzcd}$$

Oss. $\mathbb{F}_p(\alpha,\beta) = \mathbb{F}_p(\alpha, \alpha+\beta) = \mathbb{F}_p(\beta, \alpha+\beta)$

Quindi $\mathbb{F}_p(\alpha,\beta) = \mathbb{F}_p(\alpha, \alpha+\beta)$ è la più piccola estensione che contiene α e $\alpha+\beta$

$\gamma, \delta \in \overline{\mathbb{F}_p}$

$$\begin{tikzcd}
 & \mathbb{F}_p(\gamma,\delta) \arrow[dl, dash] \arrow[dd, dash, "(c{,}d)"] \arrow[dr, dash] & \\
\mathbb{F}_p(\gamma) \arrow[dr, dash, "c"'] & & \mathbb{F}_p(\delta) \arrow[dl, dash, "d"] \\
 & \mathbb{F}_p &
\end{tikzcd}$$

$[\mathbb{F}_p(\gamma,\delta) : \mathbb{F}_p] = \text{mcm}(c,d)$

vale solo per i campi finiti perché c'è un unico sottocampo per ogni cardinalità

Sia $d = [\mathbb{F}_p(\alpha+\beta) : \mathbb{F}_p]$

$mn = \text{mcm}(d, m) = \text{mcm}(d, n)$

$m \mid d \wedge m \mid n$ e sappiamo che $d \mid mn$

$\Rightarrow d = mn$

ES. 3 $\quad x^4 + ax^2 + b$ irriducibile su $\mathbb{Q}$ — polinomio biquadratico

Sia L campo di spezzamento di f.

Studiare $\text{Gal}(L/\mathbb{Q})$

Le radici di f sono

$$\underbrace{\sqrt{\frac{-a+\sqrt{a^2-4b}}{2}}}_{=\alpha}, \ -\alpha, \ \underbrace{\sqrt{\frac{-a-\sqrt{a^2-4b}}{2}}}_{=\beta}, \ -\beta$$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

$\beta \in \mathbb{Q}(\alpha) \Rightarrow L = \mathbb{Q}(\alpha)$

il polinomio minimo di β su $\mathbb{Q}(\alpha)$ è $x^2 - \beta^2$ $\underset{\mathbb{Q}(\alpha)}{\in}$

$\beta \notin \mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] = 2$

$G \circlearrowleft X$ fedele, allora $G \hookrightarrow S_X$, $g \mapsto (g.)$

$$\frac{f(x)}{(x-\alpha)(x+\alpha)} \in \mathbb{Q}(\alpha)[x] \qquad L = \mathbb{Q}(\alpha,\beta)$$

$G \circlearrowleft X$ l'unico elemento che fissa tutto X è l'identità di G

$G = Gal(L/K)$

$|G| = 4 \circ 8$

$G \circlearrowleft \{\pm\alpha, \pm\beta\}$ l'azione è transitiva e fedele $(\alpha \underset{\varphi}{\mapsto} \alpha$ e $\beta \underset{\varphi}{\mapsto} \beta \Rightarrow \varphi = id)$

$|G| = 8 \Rightarrow G$ è un 2-Sylow di $S_4 \Rightarrow G \cong D_4$

$|G| = 4 \Rightarrow G \cong \mathbb{Z}/4\mathbb{Z}$ oppure $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

caso $\beta \notin \mathbb{Q}(\alpha)$

caso $\beta \in \mathbb{Q}(\alpha)$

$\langle$ 4-ciclo in $S_4 \rangle$ $\qquad$ $\langle$ doppie trasposizioni $\rangle$

$$f(x) = x^4 + a^2 x + b = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta) = x^4 - (\alpha^2+\beta^2)x + \alpha^2\beta^2$$

$$\Rightarrow b = \alpha^2\beta^2$$

Voglio dimostrare che

1) Se b è un quadrato in $\mathbb{Q}$ allora $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

2) Se b non è un quadrato, $b(a^2 - 4b) \in (\mathbb{Q})^2$ allora $G \cong \mathbb{Z}/4\mathbb{Z}$

3) altrimenti è D_4

$\sqrt{b} = \pm\alpha\beta \Rightarrow \sqrt{b} \in \mathbb{Q}(\alpha,\beta) = L$

$\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{a^2-4b}) = \mathbb{Q}(\beta^2)$

Oss. $\sqrt{a^2-4b} \notin \mathbb{Q}$ perché f è irriducibile

$\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{a^2-4b}) \iff b(a^2-4b)$ è un quadrato in $\mathbb{Q}$

Supponiamo b sia un quadrato

$$\alpha\beta = \pm\sqrt{b} \in \mathbb{Q}$$

Quindi $\beta \in \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\alpha)$ ha deg. 4 su $\mathbb{Q}$

Poiché $\sqrt{b} \in \mathbb{Q}$ $\qquad$ $\varphi \in Gal(L/K)$ fissa $\alpha\beta$

Se $g(\alpha) = \alpha$, $g(\beta) = \beta$

Se $g(\alpha) = \beta$, $g(\beta) = \alpha$

Se $g(\alpha) = -\beta$, $g(\beta) = -\alpha$

se $g(\alpha) = -\alpha$ $g(\beta) = -\beta$

b è un quadrato

$\Rightarrow$ non ho aut. di ordine 4

$\Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Sappiamo che $\sqrt{b} \notin \mathbb{Q}$, ma $\sqrt{b(a^2-4b)} \in \mathbb{Q}$

$\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{a^2-4b}) = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\beta^2)$

$\mathbb{Q}(\alpha)$ e $\mathbb{Q}(\beta)$ sono entrambe estensioni quadratiche

$\overset{\shortparallel}{\mathbb{Q}(\alpha^2)(\sqrt{\alpha^2})}$ $\quad \overset{\shortparallel}{\mathbb{Q}(\alpha^2)(\sqrt{\beta^2})}$

Sono uguali $\Leftrightarrow$ $\underbrace{\alpha^2\beta^2}_{= b}$ è un quadrato in $\mathbb{Q}(\alpha^2) - \mathbb{Q}(\sqrt{b})$

Ma b è un quadrato in $\mathbb{Q}(\sqrt{b}) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$

$\Rightarrow L = \mathbb{Q}(\alpha, \beta)$ ha deg. 4

$\mathbb{Q}(\sqrt{b})$ è una sottoestensione di $\mathbb{Q}(\alpha)$

$\exists g \in G$ t.c. $g(\sqrt{b}) = -\sqrt{b}$

$\alpha\beta = \pm\sqrt{b}$ $\quad g(\alpha\beta) = -\alpha\beta$

Voglio far vedere che $\operatorname{ord} g = 4$

G sottogruppo transitivo di $S_4 \Rightarrow g$ non ha punti fissi

$g(\alpha) = \alpha$ $\times$

$g(\alpha) = -\alpha \Rightarrow g(\beta) = -\beta$ $\times$

$g(\alpha) = \beta$ $\quad g(\beta) = -\alpha$ questa g ha ord. 4

$g(\alpha) = \beta$ $\quad g(\beta) = \alpha$

Se b e $b(a^2-4b)$ non sono quadrati, ho $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$

$\Rightarrow \mathbb{Q}(\alpha, \beta)$ ha deg. 8 $\Rightarrow G \cong D_4$

ES. 4 ζ_7 radice primitiva 7-ima di 1 su $\mathbb{Q}$

$\alpha = \zeta_7 + \zeta_7^{-1}$ $\quad\quad$ $Gal\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right)$

<u>OSS</u> $\zeta_7 + \zeta_7^{-1} \in \mathbb{R}$

$Gal\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right) \cong \mathbb{Z}_7^*$

$\varphi_i : (\zeta_7 \mapsto \zeta_7^i) \longleftrightarrow i$

$\varphi_i(\alpha) = \zeta_7^i + \zeta_7^{-i}$

<u>OSS</u> $\varphi_4(\alpha) = \varphi_3(\alpha)$

$\varphi_5(\alpha) = \varphi_2(\alpha)$

$\varphi_6(\alpha) = \varphi_1(\alpha)$

Ho 3 coniugati $\Rightarrow$ ho 3 immersioni di $\mathbb{Q}(\alpha)$ in $\overline{\mathbb{Q}}$

φ_1 fisso $\mathbb{Q}(\alpha)$

$\varphi_2(\alpha) = \zeta_7^2 + \zeta_7^{-2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$

$\varphi_3(\alpha) = \zeta_7^3 + \zeta_7^{-3} = \alpha^3 - 3\alpha \in \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\alpha)$ normale

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \Rightarrow Gal\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right) \cong \mathbb{Z}/3\mathbb{Z}$

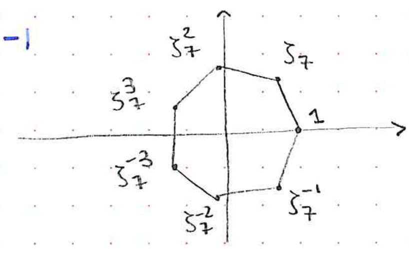
Il polinomio minimo di α ha grado 3

$$\alpha^3 = 3\alpha + \boxed{(\zeta_7^3 + \zeta_7^{-3})} = 3\alpha \boxed{-1 - \alpha - (\underbrace{\zeta_7^2 + \zeta_7^{-2}}_{\alpha^2 - 2})} =$$

$$= 2\alpha - 1 - \alpha^2 + 2$$

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$$

$$\mu_\alpha(x) = x^3 + x^2 - 2x - 1$$



sommate danno 0

10/12/2024
Patimo

ES. 5

Sia F un campo di caratteristica $p>0$

$f(x) = x^p - x - a$ con $a \in F$ e sia L il campo di spezzamento di f su F

Sia $\beta \in F$ una radice di f: $\beta^p - \beta = a$. Quali sono le altre soluzioni?

$f(\beta+1) = (\beta+1)^p - \beta - 1 - a = \beta^p + \cancel{1} - \beta - \cancel{1} - a = f(\beta) = 0$

Iterando lo stesso ragionamento ottengo che $\beta, \beta+1, \beta+2, \dots$

$\dots \beta + p - 1$ sono tutte radici di f.

Allora il campo di spezzamento è $F(\beta) = L$, inoltre essendo queste radici tutte distinte vale che L/F è un'estensione separabile

[**Def.** $F(\alpha)/F$ è separabile $\Longleftrightarrow$ α è separabile, cioè $\mu_\alpha(x)$ ha tutte radici distinte.]

L/F è normale $\Rightarrow$ L/F è di Galois.

Cerchiamo di capire chi è $Gal(L/F)$

Supponiamo che $\beta \notin F$, voglio far vedere che $f(x)$ è irriducibile. Supponiamo che non lo sia.

$\mu_\beta(x) \mid f(x)$ $\quad F(\beta)/F$ è di Galois

$G = Gal(F(\beta)/F) \ni g(\beta) = \beta + k$ per qualche k

$g(\beta) = \beta \Leftrightarrow g = id$. Se $F(\beta) \neq F$ $\exists g \neq id$ con $g(\beta) = \beta + k$ e $\beta + k$ radice di $\mu_\beta(x)$

$g^2(\beta) = g(\beta + k) = \beta + 2k$ che è una radice di μ_β

(Continuando ottengo tutti $\beta + i$). Poiché $(\beta, p) = 1$ ottengo che tutti i $\beta + i$ sono radici di μ_β $\Rightarrow \deg \mu_\beta = p \Rightarrow$

$\Rightarrow \mu_\beta = f$ e quindi f è irriducibile. Allora $\beta \notin F \Rightarrow$

$\Rightarrow Gal(F(\beta)/F) \cong \mathbb{Z}/p\mathbb{Z}$ (ha p elementi)

ES.6

$K \subset \mathbb{C}$ estensione di Galois di $\mathbb{Q}$

sia $\sigma: \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ allora σ induce un elemento in $Gal(K/\mathbb{Q})$ e $K^\sigma = \{x \in K \mid \sigma(x) = x\} = K \cap \mathbb{R}$

dimostrare che $[K:\mathbb{Q}]$ è dispari $\Rightarrow K \subset \mathbb{R}$

Solutione: $\sigma(z) = \bar{z}$, $\sigma(K) = K$ perchè $K/\mathbb{Q}$ è normale $\sigma|_K \in Gal(K/\mathbb{Q})$ inoltre $K^\sigma = K \cap \mathbb{R}$. Supponiamo che $[K:\mathbb{Q}]$ sia dispari. $\sigma|_K$ ha ordine che divide 2 $\Rightarrow \sigma|_K = id$

Quindi $K = K^\sigma = K \cap \mathbb{R} \Rightarrow K \subset \mathbb{R}$.

ES.7

Studiamo $\mathbb{C}(x^n) \subset \mathbb{C}(x)$, dimostriamo che è un' estensione con gruppo di Galois ciclico.

Solutione: $\mathbb{C}(x) = \mathbb{C}(x^n)[t]$ $\quad \mu_x(t) \mid t^n - x^n \in \mathbb{C}(x^n)[t]$

$t^n - x^n = (t-x)(t-\zeta_n x) \cdots (t - \zeta_n^{n-1} x)$ per cui vale che $\mathbb{C}(x)$ è il c.d.s. di $t^n - x^n$ su $\mathbb{C}(x^n)$ quindi normale $\mathbb{C}(x^n) \subset \mathbb{C}(x)$ è di Galois. Inoltre $[\mathbb{C}(x):\mathbb{C}(x^n)]$ è $\leq n$.

Sia $\sigma: \mathbb{C}(x) \to \mathbb{C}(x)$, $x \mapsto \zeta_n x$ " $\mathbb{C}(\zeta_n x)$

$\sigma \in Aut\, \mathbb{C}(x)$ e $\sigma|_{\mathbb{C}(x^n)} = id$ perciò $\sigma(x^n) = (\zeta_n x)^n = x^n$.

$\sigma \in Gal\left(\mathbb{C}(x)/\mathbb{C}(x^n)\right)$ $\quad ord(\sigma) = n \Rightarrow |\langle\sigma\rangle| = n \Rightarrow$

$|Gal(\quad)| \geq n$. Allora $\left|Gal\left(\mathbb{C}(x)/\mathbb{C}(x^n)\right)\right| = n$

$$Gal\left(\mathbb{C}(x)/\mathbb{C}(x^n)\right) \cong \langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$$

$\square$

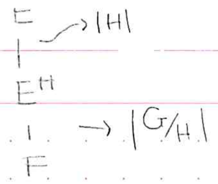
Teorema di corrispondenza di Galois

E/F estensione di Galois, $G = Gal(E/F)$ allora $\exists$ una bigez.

$$\left\{\begin{matrix}\text{sottogruppi}\\ \text{di } G\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}F \subset K \subset E\\ \text{sottoestensioni di}\\ \text{campi}\end{matrix}\right\} \quad \text{tramite}$$

$$H \mapsto E^H = \{x \in E \mid h(x) = x \ \forall h \in H\}$$

$$\{\varphi \in G \mid \varphi|_K = id\} \leftarrow K$$



- $[E^H : F] = |G/H|$, $[E : E^H] = |H|$
- La bigezione inverte le inclusioni, ovvero $H < H' \iff E^{H'} \subset E^H$
- E^H è normale su F se $H \triangleleft G$ e vale che $Gal(E^H/F) \cong G/H$

ESEMPIO: • sottogruppi di $\mathbb{Q}(\zeta_{12})$ su $\mathbb{Q}$

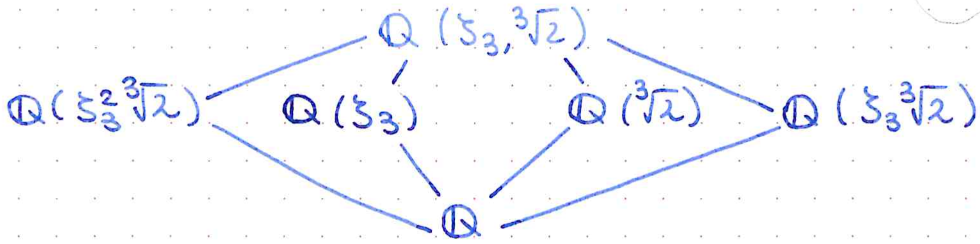
$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

ci sono 3 sottogruppi di ordine 2 (o indice 2)

$\Rightarrow$ 3 sottoestensioni di deg. 2 di $\mathbb{Q}(\zeta_{12})$: $\mathbb{Q}(i), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-3})$

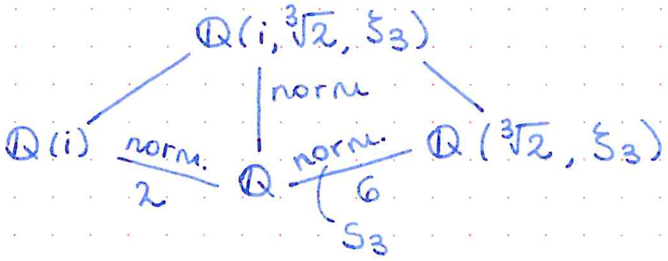
- Sottoestensioni di $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$
  ↳ c.d.s di x^3-2

$|G| = 6$ e G agisce fedelmente sulle radici di x^3-2, per cui $G \hookrightarrow S_3$. Per cardinalità $G \cong S_3$. Ci sono 3 sgr. di ord. 2 e indice 3 (non normali) generati dalle trasposizioni e 3 di ord 3 di indice 2 (normali) ?



Se $K = \mathbb{Q}(i, \sqrt[3]{2}, \zeta_3)$, vogliamo determinare tutti i campi $\mathbb{Q} \subset F \subset K$ con $[F:\mathbb{Q}] = 2$

$K/\mathbb{Q}$ è di Galois perché



$G = Gal(K/\mathbb{Q})$

$[K : \mathbb{Q}(\sqrt[3]{2}, \zeta_3)]$ ha grado 1 o 2

Ha grado 2 $\iff$

$i \in \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \iff \mathbb{Q}(i) < \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \iff$

$\iff \mathbb{Q}(i) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ ↯ $(\sqrt{i})(-3)$ non è un quadrato

Quindi $[K:\mathbb{Q}] = 12$

$K/\mathbb{Q}(i)$ è il c.d.s. di x^3-2 ha deg 6

$$\mathrm{Gal}(K/\mathbb{Q}(i)) \cong S_3 \qquad \mathrm{Gal}(K/\mathbb{Q}(\zeta_3,\sqrt[3]{2})) \cong \mathbb{Z}_2$$

$$H \trianglelefteq G \qquad\qquad H' \trianglelefteq G$$

sono estensioni normali

Vogliamo dire $G \cong H \times H'$. Mi serve dire che in questo caso $H \cap H' = \{e\} \iff K^{H\cap H'} = K$

Sappiamo che $K^{H\cap H'} \supset K^{H} = \mathbb{Q}(i)$ e $K^{H\cap H'} \supset K^{H'} = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$

$\Rightarrow K^{H\cap H'} \supset K \Rightarrow K^{H\cap H'} = K$ per cui vale che

$G \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$. Devo studiare i gruppi di ordine 6 in G. $T < G$ con $|T| = 6$. $\exists\, \sigma \in T$ di ordine 3 e gli unici sono $\sigma = \{((1\,2\,3),0)\}$ o $\{((1\,3\,2),0)\}$ quindi $\{((1\,2\,3),0)\} \in T$. $\exists\, \tau \in T$ di ordine 2

$T = \langle ((1\,2\,3),0), \tau \rangle \qquad \tau = \{e, 1\} \setminus \{\text{trasp}, 0\} \setminus \{\text{trasp}, 1\}$

$T \cong (1\,2\,3) \times \mathbb{Z}_2 \setminus S_3 \times \{0\} \setminus \{(\underset{S_3}{\sigma}, \mathrm{sgn}(\sigma))\}$

Ho quindi 3 estensioni di grado 2 su $\mathbb{Q}$

$\mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{3})$

$S_3 \times \{0\}$ $\quad (1\,2\,3) \times \mathbb{Z}_2$ $\quad \{(\sigma, \mathrm{sgn}(\sigma)) \mid \sigma \in S_3\}$

$q = p^n$ FORZAAA ♡

$\mathbb{F}_{q^d}/\mathbb{F}_q$ è sempre normale e sep. $\Rightarrow$ di Galois

$\varphi: \mathbb{F}_{q^d} \to \overline{\mathbb{F}_q}$ $\varphi|_{\mathbb{F}_q} = id$

$\varphi(\mathbb{F}_{q^d}) = \mathbb{F}_{q^d}$ (per unicità)

TEOREMA

$$Gal\left(\mathbb{F}_{q^d}/\mathbb{F}_q\right) = \langle \phi \rangle$$

dove $\phi: \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ AUTOMORFISMO DI FROBENIUS
$x \mapsto x^q$ $(q = p^n)$

DIM. $\left|Gal\left(\mathbb{F}_{q^d}/\mathbb{F}_q\right)\right| = d$

① $\phi \in Gal\left(\mathbb{F}_{q^d}/\mathbb{F}_q\right)$
② $\text{ord}\, \phi = d$ che mi da la tesi.

passi della dimostrazione:

① ϕ è un automorfismo
$\phi|_{\mathbb{F}_q} = id$ $x \in \mathbb{F}_q \overset{\text{def.}}{=} \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^q = \alpha\}$
(*) $\phi(x) = x^q = x$

② Sia $h = \text{ord}\, \phi$ $h \leq d$ (cardinalità di G)
$\phi^h(x) = x^{q^h} = x$ $\forall x \in \mathbb{F}_{q^d}$
$\Rightarrow h = d$ perché il polinomio
$x^{q^h} - x$ ha al più q^h radici in $\overline{\mathbb{F}_p}$

(*) È iniettivo (come tutti gli omo sui campi) e surg. per cardinalità

Dato che i q^d el. di $\mathbb{F}_{q^d}$ sono tutti radici
$\Rightarrow q^d \leq q^h \Rightarrow d \leq h \Rightarrow d = h$

ESEMPIO:

$Gal\left(\mathbb{F}_{p^{100}}/\mathbb{F}_p\right) = \langle \phi \rangle$ $\phi: x \mapsto x^p$
$\phi^2: x \mapsto x^{p^2}$

$Gal\left(\mathbb{F}_{p^{100}}/\mathbb{F}_{p^{20}}\right) = \langle \phi \rangle$ $\phi: x \mapsto x^{p^{20}}$

Teo. dell' elemento primitivo

L/K finita e separabile $\Rightarrow \exists\, \alpha \in L$ t.c. $L = K(\alpha)$

"Tutte le estensioni finite e separabili sono semplici"

ESEMPIO:

$\underset{L}{\overset{\shortparallel}{\mathbb{Q}(\sqrt{2},\sqrt{3})}}$ → deve essere generata da un elemento

$\alpha \in L$ $\quad \overbrace{\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq L}^{4}$

n

$\shortparallel$

di possibili immagini di α tramite le immersioni di L su $\mathbb{Q}$

↓

$[\mathbb{Q}(\alpha):\mathbb{Q}] = \#\{\varphi(\alpha) \mid \varphi \text{ immersione di } L/\mathbb{Q}\}$

$\shortparallel$

$\#\{\text{immersioni di } \mathbb{Q}(\alpha)/\mathbb{Q}\}$

$\varphi_{0,0} = id$

$\varphi_{1,0}: \quad \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3} \mapsto \sqrt{3}$

$\varphi_{0,1}: \quad \sqrt{2} \mapsto +\sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3}$

$\varphi_{1,1}: \quad \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3}$

$$\left.\begin{array}{l}
\sqrt{2}+\sqrt{3} \overset{\varphi_{0,0}}{\longmapsto} \sqrt{2}+\sqrt{3} \\
\sqrt{2}+\sqrt{3} \overset{\varphi_{1,0}}{\longmapsto} \sqrt{2}-\sqrt{3} \\
\sqrt{2}+\sqrt{3} \overset{\varphi_{0,1}}{\longmapsto} -\sqrt{2}+\sqrt{3} \\
\sqrt{2}+\sqrt{3} \overset{\varphi_{1,1}}{\longmapsto} -\sqrt{2}-\sqrt{3}
\end{array}\right\}$$

se sono tutte distinte il pol. minimo di $\sqrt{2}+\sqrt{3}$ ha deg (4)

(è almeno 4 ma so già che sono in una est. di deg 4)

DIM. $L = K(\alpha_1, \dots, \alpha_n)$ (finita $\Rightarrow$ fin. generata)

Caso K campo infinito

Per induzione su n

$n=2 \qquad L = K(\alpha,\beta) \overset{\text{tesi}}{=} K(\gamma)$

$[L:K] = d \qquad \varphi_1, \dots, \varphi_d : L \hookrightarrow \overline{K} \qquad \varphi_i|_K = id$

Cerco $r \in L$ $\quad [K(r):K] = d$

$\Rightarrow K(r) = L$

$$F(x) = \prod_{i<j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta))$$

$\deg F(x) \leq \binom{d}{2}$ $\qquad F(x) \not\equiv 0$

$\downarrow$

$\varphi_i(\alpha) + x\varphi_i(\beta) = \varphi_j(\alpha) + x\varphi_j(\beta)$

$\Rightarrow \begin{array}{l} \varphi_i(\alpha) = \varphi_j(\alpha) \\ \varphi_i(\beta) = \varphi_j(\beta) \end{array} \Rightarrow \varphi_i = \varphi_j$ ↯

$F(x) \in \overline{K}[x]$ $\qquad \Rightarrow F$ ammette un # finito di radici in $\overline{K}$

ma K infinito $\Rightarrow \exists\, p \in K$ t.c. $F(p) \neq 0$

$$F(t) = \prod_{i<j} (\varphi_i(\alpha) + t\varphi_i(\beta) - \varphi_j(\alpha) - t\varphi_j(\beta)) =$$

$$= \prod_{i<j} (\varphi_i(\alpha + t\beta) - \varphi_j(\alpha + t\beta))$$

$\varphi_i(\alpha + t\beta) \neq \varphi_j(\alpha + t\beta) \quad \forall i<j \Rightarrow \alpha + t\beta$ ha almeno d immagini distinte su $\overline{K}$

$\deg \mu_{\alpha + t\beta} \geq d \Rightarrow L = K(\alpha + t\beta)$

Caso K campo finito

$\Rightarrow L$ finito $\Rightarrow L^*$ ciclico $\quad L^* = \langle \alpha \rangle$ quindi $L = K(\alpha)$ $\square$

Teorema di corrispondenza di Galois

L/K finita di Galois

$$\mathcal{E} = \{F \mid K \subseteq F \subseteq L\} \leftrightarrow \mathcal{G} = \{H < \mathrm{Gal}(L/K)\}$$

$$F \xmapsto{\alpha} \mathrm{Gal}(L/F)$$

$$\{a \in L \mid h(a) = a \ \forall h \in H\} = L^H \xleftarrow{\beta} H, \quad L^H = \mathrm{Fix}(H)$$

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

Inoltre, L^H/K è normale $\Leftrightarrow H \trianglelefteq G$

In tal caso $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K) / \mathrm{Gal}(L/L^H)$

$$\begin{array}{l} L \\ | \\ L^H \\ | \; G/H \\ K \end{array} \Big) H \qquad \text{se } H \triangleleft G$$

(se c'è una sottoestensione non normale il gruppo di Galois non può essere abeliano)

LEMMA 1

L/M di Galois $\quad G = Gal(L/M) \quad H \leq G$

$$L^H = M \iff H = G$$

DIM.

$(\Leftarrow)$ $H = G$

$$L^G = \{ \alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G \}$$

Supponiamo $M \subsetneq L^G \subseteq L$

$[L^G : M] > 1$

$\exists \varphi : L^G \to \overline{M} \quad \varphi|_M = id$

$\varphi \neq id$

Sia $\hat{\varphi} : L \to \overline{M}$

$\hat{\varphi}|_L = \varphi$

$\Rightarrow \hat{\varphi} \in Gal(L/M)$

$\Rightarrow \hat{\varphi}(\alpha) = \alpha \quad \forall \alpha \in L^G \Rightarrow \varphi = id$ ↯

allora $L^G = M$

$(\Rightarrow)$ $\cdot L^H = M \underset{\text{tesi}}{\Rightarrow} H = G$

$L = M(\alpha)$

$$f(x) = \prod_{h \in H} (x - h(\alpha)) \in L[x]$$

$$\tau \in H \qquad \tau f(x) = \prod_{h \in H} (x - \tau h(\alpha)) = \prod_{h \in H} (x - h(\alpha)) = f(x)$$

$\Rightarrow f(x) \in L^H[x] = M[x]$

$f(\alpha) = 0 \Rightarrow \mu_{\alpha|M} \mid f(x)$

$$|G| = [\underset{\underset{M(\alpha)}{\shortparallel}}{L} : M] = \deg \mu_\alpha \leq \deg f(x) = \# H \leq \# G$$

$\Rightarrow$ sono tutte uguaglianze

$\square$

DIM. TEO. DI CORRISPONDENZA DI GALOIS

$\alpha(F) = \mathrm{Gal}(L/F) < \mathrm{Gal}(L/K)$ ✓

$H<G \quad \beta(H) = L^H \in \mathcal{E} \qquad K \subseteq L^H \subseteq L$ ✓

va verificato che è un campo (ovvio)

(i) $\alpha \circ \beta = id$
(ii) $\beta \circ \alpha = id$

(i) $\alpha \circ \beta(H) = \alpha(L^H) = \mathrm{Gal}(L/L^H) \overset{?}{=} H$; $\supset$ ✓ sono automorfismi di L/K e tutti fissano L^H

$\mathrm{Gal}(L/L^H) \subset H$?

Uso il lemma 1 con $L^H = M$

$\Rightarrow H = \mathrm{Gal}(L/M)$, $M = L^H$

(ii) $\beta \circ \alpha(F) = \beta(\mathrm{Gal}(L/F)) = L^{\mathrm{Gal}(L/F)} \underset{\text{lemma 1}}{=} F$ $\square$

lemma 2 L/K di Galois

$H < \mathrm{Gal}(L/K) \ni \sigma$

$L^{\sigma H \sigma^{-1}} = \sigma L^H$

$\sigma L^H = \{\sigma(\alpha) \mid \underbrace{h\alpha = \alpha \ \forall h \in H}_{\alpha \in L^H}\}$, $\alpha \in L$ $=$

$= \{\beta \in L \mid h\sigma^{-1}(\beta) = \sigma^{-1}(\beta) \ \forall h \in H\} = L^{\sigma H \sigma^{-1}}$
$\sigma h \sigma^{-1}(\beta) = \beta$ $\square$

$H \triangleleft G \iff \sigma H \sigma^{-1} = H \ \forall \sigma \in G \iff \sigma L^H = L^H \ \forall \sigma \in G \iff L^H/K$ è normale, $G = \mathrm{Gal}(L/K)$

$\forall \varphi : L^H \hookrightarrow \bar{K} \mid \varphi|_K = id$
$\varphi(L^H) = L^H$

Basta guardare solo quelle che sono nel gruppo di Galois perché ognuna si estende a un elemento di Gal

Proprietà

$H, S < \mathrm{Gal}(L/K)$ $\quad \bullet\ H \leq S \iff L^H \supseteq L^S$ $\quad \bullet\ L^{\langle S,H \rangle} = L^S \cap L^H$

$\bullet\ L^{H \cap S} = L^H L^S$

$H \triangleleft Gal(L/K)$

$Gal(L^H/K)$ $\quad res: Gal(L/K) \to Gal(L^H/K)$ (cerco un omo. con il giusto Ker)

$\sigma \mapsto \sigma|_{L^H}$

res è surgettiva per il teo. di estensione

(tutte le immersioni di L^H si estendono a L)

$Ker(res) = \{\sigma \in Gal(L/K) \mid \sigma|_{L^H} = id\} = Gal(L/L^H)$

$\square$