Dipartimento
di Matematica
Università di Pisa

APPUNTI DEL CORSO DI

ALGEBRA I

A cura di Chiara Di Sano
c.disano1@studenti.unipi.it

Rielaborazione delle lezioni dei prof.
G. Gaiffi
V. Melani
F. G. Callegaro
A.A. 2021-2022

29 - 09 - 21 Lezione 1 Prof. Gaiffi

RICEVIMENTO: ore 18:00 GIOVEDÌ

Azione di gruppo su un insieme

Def Sia X un insieme, G un gruppo, un'azione di G su X è una funzione $G \times X \longrightarrow X$

$$(g, x) \mapsto g \cdot x$$

ESEMPIO: $(123) \cdot 1 = 2$

$\underbrace{(12)(123)}_{(1)(23)(23)} \cdot 1 = 1$

$(1)(23)(23) \cdot 1 = 1$

che soddisfa due proprietà

1) $e \cdot x = x \quad \forall x \in X$

2) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

Azioni famose

elem. del gruppo

- Il coniugio: $X = G$, $g \cdot x = g x g^{-1}$ è una azione?

Verifica: $e x = e x e^{-1} = x$ OK

$$\begin{array}{ccc} (g_1 g_2) x & \overset{?}{=} & g_1 (g_2 x) \\ \| & & \| \\ g_1 g_2 x (g_1 g_2)^{-1} & & g_1 \cdot g_2 x g_2^{-1} \\ \| & & \| \\ g_1 g_2 x g_2^{-1} g_1^{-1} & = & g_1 g_2 x g_2^{-1} g_1^{-1} \end{array}$$ OK

- Azione sui laterali: Prendo $H < G$, $G/H = X$ A PRIORI È UN INSIEME

è gruppo $\Leftrightarrow$ H è normale

$g \cdot kH = gkH$ verificate che è una "buona azione"

Def Sia G gruppo che agisce su X, diremo orbita di $x \in X$

$\mathrm{orb}(x) = \{ g \cdot x \mid g \in G \}$ e diremo stabilizzatore di x

$G \geq \mathrm{Stab}(x) = \{ g \in G \mid g \cdot x = x \}$

$\downarrow$

è un sottogruppo ma NON è normale

Lemma $\mathrm{Stab}(x) < G$. $g_1, g_2 \in \mathrm{Stab}(x)$, $(g_1 g_2) \cdot x = g_1 (g_2 x) =$

$= g_1 x = x$

$g \in \mathrm{Stab}(x)$ $\quad g \cdot x = x$. Applico g^{-1}

$g^{-1}(g x) = (g^{-1} g) x = g^{-1} x = x \qquad g^{-1} \in \mathrm{Stab}(x)$

□

Teorema Sia G che agisce su X $G \curvearrowright X$

Sia $x \in X$. Esiste una funzione bigettiva $G/\mathrm{Stab}(x) \leftrightarrow \mathrm{orb}(x)$

INSIEME

Verificate che non dipende dal rappresentante

$\bar{g}\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x) \Leftrightarrow \bar{g} = gh$ con $h \in \mathrm{Stab}(x)$ $g\,\mathrm{Stab}(x) \to gx$

$g^{-1}\bar{g} \in \mathrm{Stab}(x)$ $\bar{g}\,\mathrm{Stab}(x) \to \bar{g}x = (gh)x = g(hx) = gx$

Surgettiva: $g_1 \in \mathrm{orb}(x)$ prendo $g_1\mathrm{Stab}(x) \mapsto g_1 x$

Iniettiva:

$$\begin{tikzcd} g_1\,\mathrm{Stab}(x) \arrow[dr] & \\ & \underbrace{g_1 x = g_2 x} \\ g_2\,\mathrm{Stab}(x) \arrow[ur] & \end{tikzcd}$$

$$\underset{(g_2^{-1}g_1)x}{\underset{\parallel}{g_2^{-1}(g_1x)}} = \underset{x}{\underset{\parallel}{g_2^{-1}(g_2x)}}$$

→ cioè $g_2^{-1}g_1 \in \mathrm{Stab}(x)$ quindi $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$

Proposizione Le orbite costituiscono una partizione di X

Dim $y \in X$ appartiene almeno ad un'orbita: $\mathrm{orb}(y)$

Ora mostriamo che se $x \in \mathrm{orb}(y)$ allora $\mathrm{orb}(x) = \mathrm{orb}(y)$

$\boxed{x \in \mathrm{orb}(y)}$ significa che esiste $g \in G$ tale che $g \cdot y = x$.

Applico g^{-1}: $\underbrace{g^{-1}(gy)} = \underbrace{g^{-1}x}$

$y = g^{-1}x$ → cioè $y \in \mathrm{orb}(x)$ → $\mathrm{orb}(y) \subseteq \mathrm{orb}(x)$

ricavo $\mathrm{orb}(x) \subseteq \mathrm{orb}(y)$

□

Teorema $$|X| = \sum_{O_i \text{ orbita}} |O_i| = \sum_{\substack{O_i \text{ orbita} \\ \text{rappresentata} \\ \text{da } X_i}} \left| G/\mathrm{Stab}(x_i) \right| = \sum_{\substack{O_i \text{ orbite} \\ \text{rappr. da } x_i}} \frac{|G|}{|\mathrm{Stab}(x_i)|}$$

Caliamo il tutto nell'esempio della famosa azione di G su sé stesso: $G = X$, sia $x \in G$, $\mathrm{orb}(x) = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$ si chiama ANCHE classe di coniugio di x.

ES $x \in S_7$ $x = (1\,2)(3\,4)(5\,6\,7)$

$\mathrm{orb}(x)$?

$\tau x \tau^{-1} = (\tau(1), \tau(2))(\tau(3), \tau(4))(\tau(5), \tau(6), \tau(7))$

tutti quelli della forma (,)(,)(, ,)

E a Stab(x) che nome diamo?

$$\text{Stab}(x) = \}g \in G \text{ tc } gx = x\{$$
$$= \}g \in G \text{ tc } gxg^{-1} = x\{$$
$$= \}g \in G \text{ tc } gx = xg\{$$

$C(x)$

Stab(x) si chiama anche centralizzatore (in questo caso) o centralizzatore di x ed è il più grande sgruppo H di G tale che $x \in Z(H)$

Il teorema diventa (in questo caso) $|G| = \sum_{\substack{\text{classi di}\\ \text{coniugio}\\ \text{rappr. da } g_i}} \frac{|G|}{|C(g_i)|}$

Prop Sia $|G| = p^n$ con p primo allora $Z(G) \neq \}e\{$.

$|G| = \sum \frac{|G|}{|C(g_i)|}$ $\qquad p^n = ?$

$$|C(g_i)| = \begin{cases} p^n & \text{e } g_i \in Z(G) \\ \underbrace{|C(g_i)|}_{p^{n_i}} \underset{\neq}{\mid} p^n & \text{e } g_i \notin Z(G) \end{cases}$$

p^{n_i} con $n_i < n$

$p^n = |Z(G)| + \sum_{n_i < n} \frac{p^n}{p^{n_i}}$ → Scopro dunque che $p \mid Z(G) \rightarrow Z(G) \neq \}e\{$

Corollario Se $|G| = p^2$ allora G è abeliano

Dim Per il Teo $|Z(G)| = \begin{cases} p \\ p^2 \end{cases}$ → prendo $a \in G \setminus Z(G)$. Penso a $C(a)$, di sicuro $C(a) \supseteq Z(G)$. Inoltre $a \in C(a)$ ma $a \notin Z(G)$. Allora $C(a) \supsetneq Z(G)$. Per ragioni di cardinalità sarebbe allora $|C(a)| = p^2 \Rightarrow a \in Z(G)$ ↯

Teorema di Cauchy

Sia G gruppo finito e sia p primo tale che $p \mid |G|$. Allora esiste un elemento di ordine p. (dimostrazione: domani)

Esercizio Trovare tutti i sottogruppi di ordine 12 di S_5

Sia H un sottogruppo di ordine 12, $H < S_5$, $X = \}1, 2, 3, 4, 5\{$

H agisce su X. Per Cauchy so che esiste in H un elemento di ordine 3, ossia un 3-ciclo (a, b, c). orb$(a) = \}a, b, c, \ldots ?\}$

Dunque esiste un'orbita di cardinalità ≥ 3 $\quad 12 \nmid 6$

$|X| =$
- $3+1+1$ → H agisce solo su 3 elementi e ne lascia fissi 2 $\Rightarrow H < S_3$ }
- $3+2$ → $S_3 \times S_2$ $\quad \# = 12 \rightarrow$ OK
- $4+1$
- ~~5~~ la cardinalità dell'orbita deve dividere la cardinalità di H

$$|\operatorname{orb}(x)| = \frac{|G|}{|\operatorname{Stab}(x)|}$$

30 - 09 - 21 $\qquad$ Lezione 2 $\qquad$ Prof. Gaiffi

Riprendiamo l'esercizio.

Le permutazioni nel caso $3+2$ possono essere al massimo $3! \cdot 2!$

Deve essere un sottogruppo del tipo $K_1 \times K_2$ con $|K_1 \times K_2| = 12$ e con $K_1 \simeq S_3$ e $K_2 \simeq S_2$ → Tutti e soli gli H che hanno orbite $3+2$ sono di questo tipo. Quanti sono tali H? Sono $\binom{5}{3} = \frac{5 \cdot 4}{2} = 10$.

Ci chiediamo se sono tutti coniugati fra loro.

Esempio: $H_1 \longleftrightarrow \overbrace{\{1,2,3\}\ \{4,5\}}^{\text{orbite}} \qquad H_2 \longleftrightarrow \overbrace{\{1,2,5\}\{3,4\}}^{\text{orbite}}$

$\sigma :$
$1 \longrightarrow 1$
$2 \longrightarrow 2$
$3 \longrightarrow 5$
$4 \longrightarrow 3$
$5 \longrightarrow 4$

$\sigma^{-1} H_2 \sigma \overset{?}{=} H_1$ $\quad$ cosa fa? esempio 1: $\underbrace{\sigma^{-1} \underbrace{\overset{H_2}{\overset{\in}{h}} \underbrace{\sigma(3)}_{5}}_{1 \vee 2 \vee 5}}_{1 \vee 2 \vee 3}$

esempio 2: $\underbrace{\sigma^{-1} \underbrace{h \underbrace{\sigma(4)}_{3}}_{3 \vee 4}}_{4 \vee 5}$

SONO TUTTI CONIUGATI FRA LORO

Def Dato G gruppo e $H < G$. Il normalizzatore di H in G indicato con $N(H)$ è il più grande (per inclusione) sottogruppo di G che contiene H e in cui H è sgruppo normale.

Oss $N(H)$ esiste perché H contiene H e $H \triangleleft H$. Possiamo mostrare che ne esiste uno max.

Esempio Sia H un sgruppo di ordine 12 in S_3 di quelli discussi sopra

$H = K_1 \times K_2 \simeq S_3 \times S_2$ chi è $N(H)$?

Sia $X = \}$ tutti i coniugati di $H \{$, S_5 agisce per coniugio su X

$\sigma \in S_5 \qquad H \quad gHg^{-1} \qquad \sigma \cdot H = \sigma H \sigma^{-1}$

perché sono tutti coniugati

Abbiamo visto che c'è un'unica orbita, in altre parole $X = orb(H)$

Allora ricordo che $|orb(H)| = \frac{|S_5|}{|Stab(H)|}$

$\sigma H \sigma^{-1} = H \longrightarrow Stab(H) = N(H) \Rightarrow |N(H)| = \frac{|S_5|}{|orb(H)|} = \frac{5 \cdot 4 \cdot 3 \cdot 2}{10} = 12$

Quindi $N(H) = H$.

Caso 4+1: Cos'è un'orbita da 1? Un elemento che lascia un'el. fisso.

Allora $H < S_4$

vedo S_4 in S_5 come il sgrp che permuta $\}1,2,3,4\{$ e lascia 5 fisso

Risulta che $H = A_4$. Verificare che i sgrp di $\# = 12$ in S_4 sono $\simeq A_4$.

I sgrp di #6 di S_4 sono tutti $\simeq S_3$. Verificare (anche con Cauchy)

Ricorda: $H < S_n$ allora $H < A_n$ oppure ha metà elementi dispari e metà pari.

Dim. Se $H < A_n \rightarrow$ ok

Se $H \nsubseteq A_n \Rightarrow \exists \tau \in H$ dispari.

$H \cap A_n \rightarrow H \cap (S_n \setminus A_n)$

$g \in H \mapsto \tau g \in H$

PARI DISPARI

Questa mappa possiede l'inversa:

$H \cap A_n \leftarrow H \cap (S_n \setminus A_n)$

$\tau^{-1} \gamma \leftarrow\!\shortmid \gamma$

Nota: τ^{-1} è dispari perché ha la stessa forma ciclica.

$H \cap A_4 < S_4$ con 6 elem. ma abbiamo visto che sono tutti isomorfi a S_3 che ha un po' di elem. pari e un po' dispari $\rightarrow$ ASSURDO

Conclusione I sgrp di S_5 di # 12 con orbite 4+1 sono isomorfi ad A_4, più precisamente sono di questo tipo: dati a, b, c, d

distinti in $\{1, -, 5\}$ il gruppo in questione è quello dato dalle perm. pari che permutano a, b, c, d. SONO 5 E CONIUGATI FRA LORO.

Sia H uno di esso. $H = A_4$ ossia permuto $\{1, -, 4\}$.

Come prima $|N(H)| = \dfrac{|S_5|}{|orb(H)|} = \dfrac{5!}{5} = 4! = 24$, $|H| = 12$ → è cresciuto

Dunque $N(H) = S_4$. (x es. Quali sono i sgrp di S_5 di # 24?)

IL TEOREMA DI CAUCHY

Teorema p primo, $p \mid |G|$. Allora G ha un elemento di ordine p.

Più precisamente le soluzioni $x^p = e$ in G sono in numero di Kp con $K \geq 1$.

Dim. $S = \{(a_1, a_2, -, a_{p-1}, a_p) \mid a_i \in G \quad a_1 \cdot \dots \cdot a_p = e\}$

$|S| = |G|^{p-1}$ (l'ultimo prodotto è "forzato")

Faccio agire su S il gruppo $\mathbb{Z}_p$ mediante la regola:

$[i] \cdot (a_1, a_2, \dots, a_p) = (a_{1+i}, \dots \quad)$

Es Verificare che sia un'azione (Oltre le proprietà, verificare che "cade" in S)

$$(a_1, a_2, \dots, a_p) \to (a_2, a_3, \dots, a_p, a_1) \overset{?}{\in} S \quad \to a_2 \cdot \dots \cdot a_1 \overset{?}{=} e$$

$a_1 a_2 \dots a_p = e$

$a_1^{-1}(a_1 \dots a_p) a_1 = a_1^{-1} e a_1$

$a_2 \dots a_p a_1 = e$

A noi interessano le p-uple $(a, a, \dots, a) \in S \quad a^p = e$

Guardiamo le equazioni delle orbite $|S| = |U| + \sum_{\text{altre orbite}} p$

$U = \{(a, a, \dots, a) \mid a^p = e\} \qquad |G|^{p-1} = |U| + pn$ con n intero ≥ 0

Quindi $p \mid |U|$, $|U| \geq 1$ perché c'è almeno $(e, \dots, e)$

Quindi $|U| = pK$ con $K \geq 1$.

□

IL TEOREMA DI CAYLEY

Teorema • Sia G gruppo che agisce su X.

Dato $g \in G$ chiamo $\phi_g : \begin{array}{l} X \to X \\ x \mapsto g x \end{array}$

Vale che:

- ϕ_g è BIGETTIVA
- $\Gamma : G \longrightarrow Big(X)$ è un OMOMORFISMO DI GRUPPI
  $g \mapsto \phi_g$

Dim Sulle dispense

ϕ_g è bigettiva perché esiste $\phi_{g^{-1}}$

$$\Gamma(g_1 g_2) = \Gamma(g_1) \circ \Gamma(g_2)$$

$$\overset{\text{def}}{=} \phi_{g_1 g_2} \qquad \overset{}{=} \phi_{g_1} \circ \phi_{g_2}$$

$$\phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x$$

$$\phi_{g_1} \circ \phi_{g_2}(x) = \phi_{g_1}(\phi_{g_2}(x))$$

$$= \phi_{g_1}(g_2 \cdot x)$$

$$= g_1 \cdot (g_2 \cdot x)$$

Teorema di Cayley

Sia G gruppo finito con n elementi. Allora G è isomorfo ad un sottogruppo di S_n.

Dim G agisce su G per moltiplicazione a sinistra. $G \circlearrowright G$

Per il teorema precedente, $\Gamma : G \to Big(G) \simeq S_n$

$$g_1 \mapsto \phi_{g_1}$$

$$g_2 \mapsto \phi_{g_2}$$

Se fosse $\phi_{g_1} = \phi_{g_2}$. Applicandole ad e:

$$\phi_{g_1}(e) = \phi_{g_2}(e) \Leftrightarrow g_1 e = g_2 e \Leftrightarrow g_1 = g_2 \Leftrightarrow \Gamma \text{ è iniettiva.}$$

$\square$

Se $G = S_n$ il teorema dice che $S_n \hookrightarrow Big(S_n) \simeq S_{n!}$

$\sigma \in S_n$ $\quad orb(\sigma)$ $\Big\}$ ottengo la stessa orbita o ne ottengo una più piccola? → Esercizio nelle dispense

$g \sigma g^{-1}$ solo con g pari

Teorema Sia G gruppo finito e $H < G$ tc $|G/H| = p$ primo

Se p è il più piccolo primo che divide $|G|$ allora $H \triangleleft G$.

Dim Usiamo la famosa azione sui laterali.

$X = G/H$ (adesso so solo che è un insieme)

G agisce così: $g \in G \quad xH \in G/H \quad g \cdot xH = gxH$

Per il **Teorema** • ho un OMOMORFISMO $\Gamma : G \to Big(G/H) \simeq S_{|G/H|}$

Strategia: mostreremo che $H = Ker\, \Gamma$

Inclusione facile: Vale che $Ker\, \Gamma \subseteq H$ perché se $K \in Ker\, \Gamma$, $K \mapsto \phi_K$

$$\phi_K : G/H \longrightarrow G/H$$
$$xH \longmapsto xKH$$

$K \in Ker\, \Gamma$ implica che $\phi_K =$ identità. In particolare $\underset{KH}{\underset{\|}{\phi_K(H)}} = H$

$KH = H$ è vera $\iff$ $K \in H$

VERO OGNI VOLTA CHE È IN BALLO L'AZIONE SUI LATERALI.

Guardare $\supseteq$ (dispense).

01-10-21 Lezione 3 Prof. Melani

Esempi di azioni: 1) G agisce su sé stesso per coniugio

2) $H < G$ $\quad G$ agisce sui laterali

1bis) $G = S_n$: $\sigma \tau \in S_n$ $\quad \tau \sigma \tau^{-1}$ ⇝ la dec. in cicli disgiunti è la stessa di σ

↳ dimostrarla per es.

Siano $\sigma_1, \sigma_2 \in S_n$ con la stessa decomposizione in cicli disgiunti, allora σ_1 e σ_2 sono coniugati cioè $\exists \tau$ tc $\tau \sigma_1 \tau^{-1} = \sigma_2$

L'azione del coniugio mi dà una partizione di S_n in orbite.

Idea: "costruire" τ → $\sigma_1 = (123)(45)(67)$, $\sigma_2 = (812)(37)(45)$

$\tau = ?$ $\quad \tau\sigma_1\tau^{-1} = \sigma_2$

$\tau\sigma_1\tau^{-1} = (\tau(1), \tau(2), \tau(3))(\tau(4), \tau(5))(\tau(6), \tau(7)) = \sigma_2$

$\tau(1) = 8$, $\tau(2) = 1$, $\tau(3) = 2$, $\tau(4) = 3$, $\tau(5) = 7$, $\tau(6) = 4$, $\tau(5) = 5$

Esercizio 2.3.1

$(123) \in S_n \quad n \geq 3$ $\quad$ Chi è il $\overbrace{\text{centralizzante}}^{\{\tau \in S_n \,:\, \tau\sigma\tau^{-1} = \sigma \ \forall \sigma \in S_n\}}$ di (123)?

$$|\mathrm{Stab}(123)| = |S_n| / |\mathrm{orb}(123)|$$

$|\{3\text{-cicli di } S_n\}| = ?$ $\quad 2 \cdot \binom{n}{3}$ deriva dal fatto che $(123) = (231) = (312)$

$$\Rightarrow |C((123))| = \frac{n!}{\binom{n}{3} \cdot 2} = 3(n-3)!$$

$\left|\text{Elementi di } S_n \text{ che non toccano } (123)\right| = (n-3)!$ $\qquad \overset{\mathrm{id}}{\overset{\shortparallel}{(123)(132)}} \in C((123))$

- ho i σ che non toccano 123
- ho $(123)\sigma$ con σ che non toccano 123
- ho $(132)\sigma$ con σ " " " "

Esercizio: descrivere il centralizzatore di $(12)(34)$ in S_5

Esercizio: descrivere la classe di coniugio di (123) in A_4

$$\{\sigma(123)\sigma^{-1}, \ \sigma \in A_4\} \subseteq \{\sigma(123)\sigma^{-1}, \ \sigma \in S_4\}$$

$C_{S_n}((123)) = \{e, (123), (132)\} \subset A_n$

$|C_{S_n}((123))| = 3 \qquad |\mathrm{orb}_{A_4}(123)| = |A_4|/3 = 4$

esercizio: trovare questi 4 elementi

In generale: Per quali $\sigma \in A_n$ $\mathrm{orb}_{A_n}(\sigma) = \mathrm{orb}_{S_n}(\sigma)$? (esercizio 2.3.7)

Se σ non tocca due elementi i, j, allora (i, j) commuta con σ, non posso avere due punti fissi, ne ho o 1 o 0.

Se uno dei cicli (es. τ) nella dec. di σ è dispari, allora τ commuta con σ.

Def: Un gruppo G si dice semplice se gli unici suoi sgruppi normali sono $\{e\}$ e G.

Esempi e controes.:

- $\mathbb{Z}_n$ è semplice? Solo se n è primo
- Gruppi abeliani di # non primo non sono semplici
- S_n $n \geq 3$ non è semplice
- A_4 non è semplice, $A_3 \simeq \mathbb{Z}_3$ è semplice

Teorema: A_n è semplice $\forall n \geq 5$

06-10-2021 Lezione 4 Prof. Gaiffi

Teorema Sia G gruppo finito e $H < G$ tc $|G/H| = p$ primo

Se p è il più piccolo primo che divide $|G|$ allora $H \triangleleft G$.

Dim. Già vista $\Gamma : G \to Big(G/H)$

IDEA: dimostrare che $\operatorname{Ker}\Gamma = H$

Si era notato che $\operatorname{Ker}\Gamma \subseteq H$.

Mostriamo adesso che $H \subseteq \operatorname{Ker}\Gamma$. Notiamo che $Big(G/H) \cong S_p$.

Dunque $\operatorname{Im}\Gamma < S_p$ (completarla per esercizio).

I TEOREMI DI SYLOW

Teorema (Sylow I)

Sia G gruppo finito e p primo tale che $p \mid |G|$. Sia $p^b \mid |G|$ e $p^{b+1} \nmid |G|$ con $b \geq 1$. Allora per ogni a con $0 \leq a \leq b$ esiste in G un sottogruppo di cardinalità p^a.

Dim. Per $a = 0$ banale. Sia $1 \leq a \leq b$ $|G| = p^b m$ con m primo con p

$$X = \} \underbrace{L}_{\hookrightarrow \text{ sottoinsieme}} \subseteq G \mid |L| = p^a \{ \rightsquigarrow |X| = \binom{p^b m}{p^a} = \frac{(p^b m)!}{(p^a)!(p^b m - p^a)!} =$$

$$= \frac{(p^b m)(p^b m - 1)\cdots(p^b m - p^a + 1)}{p^a (p^a - 1) \cdots 2 \cdot 1}$$

$$\frac{p^b m}{p^a} = p^{b-a} \cdot m$$

si osserva poi che se $p^k \mid p^b m - i$ allora $p^k \mid p^a - i$ e viceversa.

Per esempio: se $p^k \mid p^a - i$ innanzitutto $k \leq a$ e allora $p^k s = p^a - i \to i = p^a - p^k s$ da cui $p^k \mid i$ ma allora $p^k \mid p^a m - i$

Risulta quindi che la massima potenza di p che divide $|X|$ è p^{b-a}.

Come faccio agire G su X ?

$$L \in X$$

$$g \in G$$

$g \cdot L = gL$ che ha ancora p^a elementi e dunque appartiene ad X

Chiamiamo $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_k$ le orbite di questa azione.

$$\mathcal{L}_1 = orb(L_1)$$

$$\vdots$$

$$\mathcal{L}_k = orb(L_k)$$

$$|X| = \sum_{i=1}^{k} |\mathcal{L}_i| = \sum_{i=1}^{k} |orb(L_i)|$$

Non è possibile che p^{b-a+1} divida tutti gli $|orb(L_i)|$.

Sia j tale che $p^{b-a+1} \nmid |orb(L_j)|$

$$|orb(L_j)| = \frac{|G|}{|Stab(L_j)|} = \frac{p^b m}{|Stab(L_j)|}$$

$$|Stab(L_j)| = \frac{p^b m}{\boxed{|orb(L_j)|}}$$ → la massima potenza di p che lo divide è minore o uguale a p^{b-a}

Di sicuro $p^a \mid |Stab(L_j)|$. Ora mostriamo che $p^a = |Stab(L_j)|$

Consideriamo infatti la funzione:

$$\text{gruppo} \to Stab(L_j) \longrightarrow L_j \to \text{insieme}$$

$$\gamma \longmapsto \gamma e$$

↳ $\in L_j$ perché $\gamma \in Stab(L_j)$

} iniettiva

$$\gamma_1 e = \gamma_2 e \Leftrightarrow \gamma_1 = \gamma_2$$

Quindi $|Stab(L_j)| \leq |L_j| = p^a$.

Quindi $p^a \mid |Stab(L_j)| \leq p^a \Rightarrow |Stab(L_j)| = p^a$.

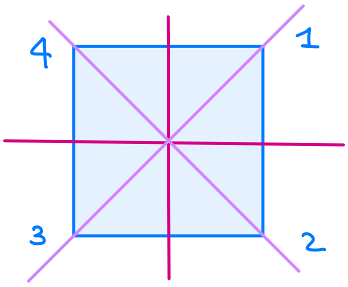
□

Def. Nelle ipotesi sopra, un sottogruppo $K < G$ con $|K| = p^b$ si dice un p-Sylow.

Esempio (dal passato) Trovare qualche 2-Sylow in S_4.

$|S_4| = 24 \qquad 2^3 | 24$ ma $2^4 \nmid 24$.

Cerchiamo dunque sgruppi di ordine 8.



D_4 gruppo delle simmetrie del quadrato ha 8 elementi e si identifica con un sgruppo di S_4.

rotazione di 180° $\in Z(D_4)$

$D_4 = \} e, \underline{(1,4)(2,3)}, (1,3)(2,4), \underline{(1,2)(3,4)}, (1,2,3,4), (4,3,2,1),$

$(1,3), (2,4) \{$

D_4 è un 2-Sylow di S_4. ⊛ $|4\text{-cicli}(S_4)| = 6 = \frac{24}{4}$

Numerando diversamente i vertici del quadrato si ottengono in tutto 3 2-Sylow K_1, K_2, K_3 tutti isomorfi a D_4.

Teorema (Sylow II) Sia G come sopra. Sia H un p-Sylow e $K < G$ con $|K| = p^a$. Allora:

1) esiste $g \in G$ tc $K \subseteq gHg^{-1}$

2) Se anche K è p-Sylow allora esiste $g \in G$ tc $K = gHg^{-1}$

Dim. 2) segue da 1) immediatamente

Faremo agire K sull'insieme $X = G/H$

$k \in K \qquad gH \qquad k \cdot gH = kgH$

X viene partizionato in orbite, g_1H, g_2H, g_3H siano rappresent. delle orbite. L'equazione delle orbite dice

$|G/H| = \sum_{i=1}^{r} |orb(g_iH)| = \sum_{i=1}^{r} \frac{|K|}{|Stab(gH)|} = \sum_{i=1}^{r} p^{a_i}$. Osservo che $|G/H| = m$ è primo con p perché H è un p-Sylow. Allora almeno uno degli a_i deve essere $= 0$. Supponiamo dunque che $a_j = 0$ per qualche j.

Allora $\text{orb}(g_j H) = \{g_j H\}$

Vedremo che $K < g_j H g_j^{-1}$. Infatti: $\forall k \in K$ e $\forall h \in H$ esiste $h^{-1} \in H$ tale che $K g_j h = g_j h'$ (perché $K g_j H = g_j H$).

Dunque $k = g_j h' h^{-1} g_j^{-1}$. Dato che k era un qualunque elemento di K ho dimostrato che $K < g_j H g_j^{-1}$

□

Def. Dato $H < G$ il normalizzatore $N(H)$ di H in G è

$$N(H) = \{g \in G \mid g H g^{-1} = H\}$$

Oss:
- $N(H)$ è sgruppo di G.
- $N(H)$ è il più grande (per inclusione) sgruppo di G in cui H è normale.

Corollario: Sia G come sopra. Sia n_p il numero dei p-Sylow di G. Allora $n_p = \dfrac{|G|}{|N(H)|}$ dove H è un qualunque p-Sylow. (in part. $n_p \mid |G|$).

Dim. Preso H p-Sylow, $X = \{p\text{-Sylow di } G\}$

G agisce su X per coniugio. Per Sylow II c'è un'unica orbita.

$|\text{orb}(H)| = \dfrac{|G|}{|\text{Stab}(H)|}$ ma $\text{Stab}(H) = N(H)$ per definizione.

l'azione è il coniugio. $n_p = |X| = |\text{orb}(X)| = \dfrac{|G|}{|N(H)|}$

□

Torniamo all'esempio dei 2-Sylow di S_4.

Dunque K_1, K_2, K_3 sono coniugati fra loro e si potrebbe già dimostrare che sono tutti e soli i 2-Sylow.

Teorema (Sylow III)

Sia G come sopra. Il numero n_p dei p-Sylow soddisfa $n_p \equiv 1 \ (p)$

Dim. dispense

Ancora sui 2-Sylow di S_4. Cosa so di n_2?

$n_2 \mid 24$ per cor. Sylow II. $n_2 \equiv 1 \ (2)$

$n_2 = $ 1 → conosco già K_1, K_2, K_3 → NO
 ③

Rileggiamo l'omo da S_4 a S_3. Faccio agire S_4 per coniugio sui 2-Sylow. Ho un omomorfismo $\Gamma: S_4 \to S_3$
$\sigma \mapsto$ permutazioni K_1, K_2, K_3
per vedere che è surg. ci aiuta SII?

→ Va fatto il conto. Il $\ker \Gamma = $ Klein.

07-10-2021 Lezione 5 Prof. Melani

Teorema: A_n è semplice $\forall n \geq 5$

Idea: $H \triangleleft A_n$, $H \neq \{e\}$ → si dimostra che $H = A_n$

Prop: I 3-cicli generano A_n

Dim: Equivale a dimostrare che ogni permutazione pari è generata da un 3-ciclo. (In particolare vedo che prodotti di un n° pari di trasposiz. possono essere scritti come 3-cicli o prod. di 3-cicli)

$H < A_n$, H contiene tutti i 3-cicli. Vorrei dire che H contiene tutte le permutazioni del tipo $(1\,2)(1\,3) = (1\,3\,2)$ → è già un 3-ciclo OK

Ma cerco anche del tipo $\overbrace{(12)(34)}^{\in H} = \overbrace{(12)\underbrace{(23)(23)}_{=e}(34)}^{\in H} = (2\,1\,3)(3\,2\,4) \in H$ OK
$\Longrightarrow A_n = H$

Dim. (teorema) Sia $H \triangleleft A_n$, $H \neq \{e\}$

Voglio $H = A_n$, quindi **voglio** che H contenga tutti i 3-cicli

Voglio che H contenga un 3-ciclo → se ne contiene uno allora li ha tutti

Oss: Per $n \geq 5$, ho almeno 2 punti fissi (Guardare i casi più semplici)

Vediamo cosa succede in A_5: $H \triangleleft A_5$, $H \neq \{e\}$. Prendiamo $\sigma \in H$, $\sigma \neq e$

$\sigma = $
- $(1\,2\,3)$ 3-ciclo OK
- $(12)(34)$ 2-ciclo + 2-ciclo ↓
- $(1\,2\,3\,4\,5)$ 5-ciclo x es.

} permutazioni **PARI**

$$\tau(12)(34)\tau^{-1} = \underbrace{(\tau(1), \tau(2))(\tau(3), \tau(4))}_{\text{Voglio trovare } \tau \text{ tc questo sia un 3 ciclo}}$$ → ma τ è big → sarà sempre un 2-2-ciclo

ES $(12)(34) \cdot (34)(15) = \underbrace{(12)(15)}_{\text{3-ciclo}} \overset{?}{\in} H$ So solo che $(12)(34) \in H$ e i suoi coniugati per trasposizioni pari

$\tau = (23145)$ Voglio trovare una permutazione pari "speciale"

$\tau(12)(34)\tau^{-1} = (43)(15) \in H$ perché H è normale

Quindi $\underbrace{(12)(34)\cdot(43)(15)}_{3\text{-ciclo}} \in H \Rightarrow A_5$ è semplice

Un altro modo di dimostrarlo è studiare le classi di coniugio

Idea: usare l'induzione

Voglio dimostrare il teorema generale per induzione su n.

Lemma: $n \geq 5$, $\sigma \in A_n$, $\sigma \neq id$. Allora σ ha un coniugato σ' tale che

$\sigma(i) = \sigma'(i)$ per qualche $i \in \{1, \dots, n\}$

Dim: Sia ℓ la lunghezza massima dei cicli che compaiono in una decomposizione di σ in cicli disgiunti.

$\sigma = (12\dots\ell)\underset{\substack{\uparrow \\ \text{disgiunta}}}{\,}\tau$ (a meno di riordinare)

Se $\ell \geq 3$, coniugo σ per (345), trovo $\sigma' = (124)\tau' \to \sigma(1) = \sigma'(1)$

Se $\ell = 2$? Esercizio

A_n agisce su $\{1, 2, \dots, n\}$ $\quad H_i = Stab(i) < A_n$

Ricorda: I sgrp normali sono chiusi per coniugio

Oss: $H_i \simeq A_{i-1}$ per hp induttiva H_i è semplice

Prendiamo $N \triangleleft A_n$, $N \neq \{e\}$.

Sia $\sigma \in N$, $\sigma \neq id \Rightarrow \exists\, \sigma' \neq \sigma$, σ' coniugato a σ, $\sigma(i) = \sigma'(i)$ per qualche i

$\Rightarrow \sigma' \in N$ perché N è normale

$\rightsquigarrow \underset{\in N}{\sigma'} \cdot \underset{\in N}{\sigma^{-1}} \in N \cap H_i$ Quindi $N \cap H_i < H_i$, $N \cap H_i \neq \{e\}$ perché $\sigma' \neq \sigma$ $\rightsquigarrow \sigma' \cdot \sigma^{-1} \neq id$

In realtà $N \cap H_i \triangleleft H_i$ perché $N \triangleleft A_n$.

$\Rightarrow N \cap H_i = H_i$ perché H_i semplice.

Cioè $H_i \subseteq N \rightsquigarrow N$ contiene un 3-ciclo $\Rightarrow$ contiene tutti i 3-cicli.

"Cose da portare a casa":
- I 3-cicli generano A_n
- Sporcatevi le mani (provate tante strade)
- Rassegnazione

Esercizio: G gruppo con $|G| = 148$. Allora G non è semplice.

$148 = 4 \cdot 37$ $\qquad n_{37} = \#$ sgrp di 37 elementi

$n_{37} \mid 148$, $n_{37} \equiv 1 \ (37) \Rightarrow n_{37} = 1$

Equivale a dire che l'unico sottogruppo di 37 elementi è normale

(perché è stabile per coniugio ⇝ tutti i p-Sylow sono coniugati tra loro)

Quindi G non è semplice.

Esercizio: Sia G un gruppo con $|G| = 72$. Allora G non è semplice.

$72 = 2^3 \cdot 3^2$ ⇝ $n_3 = \#$ sgruppi di 9 elementi

$n_3 \mid 72$, $n_3 \equiv 1 \ (3)$ ⇝ $n_3 = \begin{cases} 1 & \text{ok} \to \text{come prima} \\ 4 \end{cases}$ $\qquad$ **Oss**: $n_3 = \frac{|G|}{|N(P)|}$

Idea: se $n_3 = 4$ sappiamo che G agisce sull'insieme di 3-Sylow

⇝ $G \to S_4$ omomorfismo ⇝ Il nucleo è normale e non è banale per cardinalità

Esercizio: Sia G un gruppo con $|G| = p^2 q$ $\quad p, q$ due primi distinti,

allora G non è semplice.

08-10-2021 Lezione 6 Prof. Gaiffi

① Cerchiamo sgrp di ordine 30 in S_5

Sia H un tale sgrp.

S_5 agisce su S_5/H

$\sigma \circ \tau H = \sigma\tau H$ (azione sui laterali)

Dunque ho un omomorfismo: $S_5 \longrightarrow \mathrm{Big}(S_5/H) = S_4$ $\qquad 4 = \frac{120}{30}$

$\mathrm{Ker}\,\Gamma \neq \{e\}$ per ragioni di cardinalità

- DA UNA PROPRIETÀ GENERALE di questa azione sappiamo che $\mathrm{Ker}\,\Gamma \subseteq H$
- $\mathrm{Ker}\,\Gamma \triangleleft S_5$

$$\mathrm{Ker}\,\Gamma \begin{cases} \{e\} & \underline{\text{NO}} \quad \text{visto prima} \\ A_5 & \underline{\text{NO}} \quad \overset{60}{\overset{\shortparallel}{|A_5|}} \nmid 30 \\ S_5 & \underline{\text{NO}} \quad \text{se } H \text{ sgrp proprio di } G \Rightarrow \mathrm{Ker}\,\Gamma \neq G \end{cases}$$

Vediamo perché:

$K \trianglelefteq S_5$

- $K < A_5$
  - $K = \{e\}$
  - $K = A_5$

  (A_5 è semplice)
- $|K \cap A_5| = |K \cap S_5 \setminus A_5|$ → gruppo formato da metà permutazioni dispari e metà permutazioni pari

  $K \cap A_5 \trianglelefteq A_5$

  $K \cap A_5$
  - $\{e\}$ <u>NO</u> ⟶ K in tal caso avrebbe 2 elementi, ed un elemento dispari di ordine 2. Si vede subito che $K \ntrianglelefteq S_5$
  - A_5 <u>SI</u> ↳ $K = S_5$

Abbiamo praticamente dimostrato la proposizione:

<u>Prop</u>: Se $n \geq 5$, gli unici sgrp normali di S_n sono $\{e\}, A_n, S_n$

In complesso abbiamo ottenuto un assurdo: non esistono sgruppi di ordine 30

<u>Nota</u>: Con lo stesso argomento si dimostra che non esistono sgruppi di 40 elementi in S_5.

<u>Prop</u>: Sia $n \geq 5$. Allora in S_n non esistono sgruppi di indice K, con $2 < K < n$

② Sottogruppi di ordine 15. Sia H un tale sgruppo. Ogni $h \in H$ è PARI.

Per Lagrange $h^{15} = e$. Applicando l'omomorfismo

$$sgn : S_5 \longrightarrow \{-1, 1\}$$

$$sgn(h)^{15} = 1 \quad \text{dunque} \quad sgn(h) = 1.$$

Dunque $H < A_5$. Considero l'azione di A_5 su A_5/H. Ho un omo

$\Gamma : A_5 \longrightarrow Big(A_5/H) = S_4 \qquad \frac{60}{15} = 4$

Per la semplicità di A_5

$\operatorname{Ker} \Gamma =$
- $\{e\}$ <u>NO</u> perché Γ sarebbe iniettiva e $|A_5| = 60$, $|S_5| = 120$
- A_5 <u>NO</u> per i soliti motivi validi per l'azione sui laterali

③ Sgruppi di ordine 5 → quelli generati dai 5-cicli

I 5-cicli sono 24. In ogni sgruppo di ordine 5 ce ne sono 4, del tipo

$\sigma = (1, 2, 3, 4, 5)$, σ^2, σ^3, σ^4

Allora ci sono 6 sgruppi di ordine 5.

$H_1 \qquad H_2$

$\exists g$ tc $gH_1g^{-1} = H_2$

$$\begin{array}{l} H_1 = ((1,2,3,4,5)) \\ \qquad\;\; \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ H_2 = ((1,3,4,5,2)) \end{array}$$

$g(1) = 1 \quad g(2) = 3 \quad g(3) = 4 \quad g(4) = 5 \quad g(5) = 2$

$g^{-1}Hg = H_1$

Oppure si poteva notare che i sgrp di ordine 5 sono i 5-Sylow e dunque tutti coniugati per Sylow II. Se S_5 agisce sui sgrp di ordine 5 forma un'orbita O.

$6 = |O| = \frac{|S_5|}{|N(H)|}$ dove H è un qualunque sgruppo di ordine 5.

$$|N(H)| = \frac{120}{6} = 20$$

Sappiamo che $H = ((12345))$ **NOTO** che $(1243)\overset{\sigma}{\overset{\shortparallel}{(12345)}}(3421) = (12345)^2$

$(1243)\sigma^2(3421) = (1243)\sigma(5421)(1243)\sigma(3421) = \sigma^2\sigma^2$

Dunque $(1243) \in N(H)$.

Dunque $N(H) = \underbrace{((12345), (1243))}_{L}$ sgruppo generato. Vediamo perché:

$L < N(H)$ ma L ha ordine multiplo di 20, perché contiene un elemento di ordine 4 e un elemento di ordine 5.

ma $|N(H)| = 20$ allora vale $L = N(H)$.

④ Sottogruppi di ordine 10

Sia H un tale sottogruppo. Per Cauchy contiene un elemento σ di ordine 5 ossia un 5-ciclo, e un elemento g di ordine 2.

Supponiamo che $g = (a,b)$.

Di sicuro una potenza di σ è del tipo $(a\,b\,c\,d\,e)$

$(a\,b\,c\,d\,e)(a\,b) = (a\,c\,d\,e)$ ASSURDO perché ha ordine 4 e $4 \nmid 10$.

Quindi $g = (\ ,\ )(\ ,\ )$. A meno di rinumerare prendiamo $\sigma = (12345)$

A meno di coniugare per σ posso supporre che $g = (\ ,\ )(\ ,\ )(5)$.

Ho 3 casi possibili e verifico che:

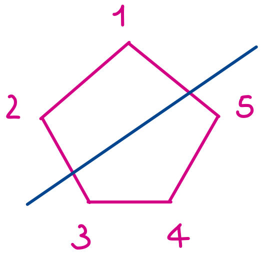
$(1\,2\,3\,4\,5)(1\,2)(3\,4) = (1\,3\,5)$ NO perché $3 \nmid 10$

$(1\,2\,3\,4\,5)(1\,3)(2\,4) = (1\,4\,3\,2\,5)$

noto che $(1\,4\,3\,2\,5) \notin \langle(1\,2\,3\,4\,5)\rangle$

Perché in H c'è un solo 5-Sylow.

Invece l'ultima funziona:



$(1,4)(2,3)$

Si tratta di una presentazione di $D_5 < S_5$.

I sgruppi di ordine 10 sono tutti e soli quelli prodotti così, $\langle \sigma, g \rangle$.

C'è una bigezione tra

$$\text{sgruppi di ordine } 5 \longleftrightarrow \text{sgruppi di ordine } 10$$

Dunque ci sono 6 sgruppi di ordine 10. $\frac{5!}{20} = 6$

Sia H un tale sgruppo. Allora $|N(H)| = 20$ perché sono un'unica orbita (stesso argomento). Sia H di ordine 10 e sia σ un 5-ciclo in H.

$$\langle\sigma\rangle \subseteq H$$

Sia $g \in N(H)$. Dico che $g \in N(\langle\sigma\rangle)$, $gHg^{-1} = H$, $\overbrace{g\langle\sigma\rangle g^{-1}}^{\text{sgr di ordine 5}} \subseteq H$

$g\langle\sigma\rangle g^{-1} = \langle\sigma\rangle$.

FATTO GENERALE: $K < H < G$, K è l'unico sgrp di ordine m in H, allora

$N(H) \subseteq N(K)$, $gHg^{-1} = H$, $gKg^{-1} \subseteq H$, $gKg^{-1} = K$

Nel nostro caso:

$N(H) \subseteq N(\langle\sigma\rangle)$ studiato al passo precedente

↑ per ragioni di # è un =

⑤ Sgruppi di ordine 20 di S_5. Sia H un tale sgruppo. Se fosse $H < A_5$ allora

$\Gamma : A_5 \to \text{Big}(A_5/H) \cong S_3$

$$\begin{tikzcd} & \{e\} \ \ \text{NO} \\ \operatorname{Ker}\Gamma = \arrow[ur, dash] \arrow[dr, dash] & \\ & A_5 \ \ \text{NO} \end{tikzcd}$$

Allora deve valere che $|H \cap A_5| = 10$. Mostriamo che $H = N(H \cap A_5)$ questo ci permette di dire che H è del tipo visto ai passi ③ e ④ ossia H è del tipo: $H = \langle (1,2,3,4,5), (1,2,4,3) \rangle$

dato che $H \cap A_5 \trianglelefteq H$ vale $N(H \cap A_5) \geq H$

per motivi di ordine vale =

Studiamo da VICINO: $H = \langle (12345)(1243) \rangle$. Quanti sono i 5-Sylow?

$n_5 \mid 20$ e $n_5 \equiv 1\ (5)$ dunque $n_5 = 1$.

Dunque $\langle (12345) \rangle \trianglelefteq H$ lo sapevamo dal passo ③

Poi c'è il sgruppo $K = \langle (1243) \rangle$ che è $\cong \mathbb{Z}_4$

$L \cap K \overset{?}{=} \{e\}$

$LK = \{ek \mid e \in L, k \in K\}$

$|LK| = 20$ allora $LK = H$

Ma quindi $H \cong \underset{\mathbb{Z}_5 \times \mathbb{Z}_4 \cong \mathbb{Z}_{20}}{\underset{\cong}{L \times K}}$? NO!

$$\begin{tikzcd} & H & \\ L \arrow[ur, phantom, "\subset"] & & K \arrow[ul, phantom, "\supset"] \\ \mathbb{Z}_5 \arrow[u, phantom, "\cong"] & & \mathbb{Z}_4 \arrow[u, phantom, "\cong"] \end{tikzcd}$$

LK $\quad e_1 k_1$ $\quad L \trianglelefteq H$

$\quad\quad e_2 k_2$

$e_1 k_1 e_2 k_2 \overset{?}{=} e_1 \overbrace{k_1 e_2 k_1^{-1}}^{\in L} k_1 k_2 = e_1 (k_1 e_2 k_1^{-1}) k_1 k_2$

Oss: Sia H di ordine 20. Chi è $N(H)$? I sgrp di ordine 20 sono tutti coniugati e sono 6, allora $|N(H)| = \frac{120}{6} = 20$ allora $N(H) = H$.

Al punto ③, c'era l'azione di S_5 sui sgruppi di ordine 5.

I sgruppi di ordine 20 sono gli $\mathrm{Stab}(x)$ con x nell'unica ORBITA.

Prop: Sia G gruppo che agisce su X insieme. Siano $x, y \in O$ orbita. Allora $\mathrm{Stab}(x)$ e $\mathrm{Stab}(y)$ sono coniugati.

Dim. se $\overset{\to\ \exists \text{ perché } x,y \in O}{g} \cdot x = y$ allora vale $g^{-1}\,\mathrm{Stab}(y)\,g \overset{\to \text{ segue analogamente}}{\overset{\supseteq}{\subseteq}} \mathrm{Stab}(x)$

13-10-21 Lezione 7 Prof. Melani

Esempio $GL_n(\underset{\hookrightarrow \text{ campo}}{\mathbb{K}})$ gruppo potenzialmente infinito

$GL_n(\underset{\mathbb{Z}/p\mathbb{Z}}{\underset{\shortparallel}{F_p}})$ gruppo finito

① Quanti elementi ha $GL_n(F_p)$?

Sono le trasformazioni lineari invertibili da $F_p^n \longrightarrow F_p^n$

$\underbrace{(p^n-1)}_{\text{scelte per il 1° vett.}}\underbrace{(p^n-p)}_{\text{2° vett.}}(\dots)$

Equivale a mandare una base (prendiamo la base can.) in sé stessa tale che la funzione sia lineare e invertibile. Per il 1° el ho p^n elt meno lo zero, il 2°...

② Studiare i p-Sylow in $GL_n(F_p)$

Esercizi ① Sia G gruppo con $|G| = 40$. Dim. che G non è semplice.

$40 = 5 \cdot 8 = 5 \cdot 2^3$

$$\begin{cases} n_5 \equiv 1 \ (5) \\ n_5 \mid 40 \end{cases} \Rightarrow n_5 = 1 \quad \underline{\text{ok}}$$

$$\begin{cases} n_2 \equiv 1 \ (2) \\ n_2 \mid 40 \end{cases} \Rightarrow n_2 = \begin{cases} 1 \\ 5 \end{cases}$$

② Sia G gruppo semplice con $|G| = n$ non primo.

Sia p un primo che divide n. Allora $n \leq n_p!$

G agisce sull'insieme dei suoi p-Sylow. Questa azione corrisponde ad un omo di gruppi: $\varphi: G \longrightarrow S_n \Rightarrow \operatorname{Im}\varphi < S_n$ $\quad \operatorname{Im}\varphi \cong G/\operatorname{Ker}\varphi$ $\begin{cases} \{e\} \rightarrow \operatorname{Im}\varphi = S_n \\ G \rightarrow \underline{\operatorname{Im}\varphi = \{e\}} \end{cases}$

perché G è semplice e $\operatorname{Ker}\varphi \trianglelefteq G$

è assurdo!

Quindi $\operatorname{Im}\varphi = S_n \Rightarrow n \leq n_p!$

③ G gruppo, $|G| = 24$, dimostrare che G non è semplice.

$24 = 3 \cdot 8 = 3 \cdot 2^3$

$$\begin{cases} n_3 \equiv 1 \ (3) \\ n_3 \mid 24 \end{cases} = \begin{cases} 1 \\ 4 \end{cases}$$

$|G| = 24 \leq n_3!$ se G è semplice.

$$\begin{cases} n_2 \equiv 1 \ (2) \\ n_2 \mid 24 \end{cases} \Rightarrow n_2 = \begin{cases} 1 \\ 3 \end{cases}$$

Se G fosse semplice avrei $24 \leq n_2!$ ASSURDO

④ Sia $|G|$ gruppo con $|G| = 56$. Mostrare che G non è semplice.

$56 = 2^3 \cdot 7$

$$\begin{cases} n_7 \equiv 1 \ (7) \\ n_7 \mid 56 \end{cases} \Rightarrow n_7 = \begin{cases} 1 \\ 8 \end{cases} \qquad \begin{cases} n_2 \equiv 1 \ (2) \\ n_2 \mid 56 \end{cases} \Rightarrow n = \begin{cases} 1 \\ 7 \end{cases}$$

Supponiamo $n_7 = 8$, qualunque 7-Sylow hanno intersezione $\{e\}$.

$P, Q < G$ 7-Sylow $P \cap Q < P$, $P \cap Q < Q$

Quanti elementi di ordine 7 ci sono in G? $48 = \overset{\#\text{ sgrp di 7 elem}}{8} \cdot \overset{\#\text{ elem di ordine 7 in ogni sgruppo}}{6}$

Restano fuori 8 elementi, che quindi formano l'unico 2-Sylow ⇒ che è normale

⑤ Sia G gruppo semplice con $|G| = n$. Dimostrare che se n è pari, allora $4 \mid n$.

Pista: prendiamo $H < G$ un 2-Sylow, e supponiamo $H = \langle h \rangle$.

Voglio interpretare h come una permutazione dispari. Trovare un'azione e un morfismo Γ associato. (Non banale)

⑥ Mettere tutto insieme e dimostrare che non esistano gruppi semplici diversi dai gruppi di ordine p con ordine < 60.

⑦ Mostrare che A_5 è l'unico gruppo semplice di ordine 60 (a meno di iso)

~ o ~

G gruppo, $G \xrightarrow{\varphi} S_{|G|} = \mathrm{Big}(G) \supseteq \mathrm{Aut}(G)$

$\varphi(g_1 g_2)(x) = \varphi(g_1)(\varphi(g_2)(x))$

$\varphi(g)(xy) = \varphi(g)(x)\varphi(g)(y)$

$gxyg^{-1} = gxg^{-1}gyg^{-1}$ ✓ → L'azione per coniugio è un'azione per automorfismi

$$\begin{tikzcd} G \arrow[r] \arrow[dr] & S_{|G|} \arrow[d, phantom, "\vee"] \\ & \mathrm{Aut}(G) \end{tikzcd}$$

Voglio studiare $\mathrm{Aut}(S_n)$

$\psi: S_n \to \mathrm{Aut}(S_n)$ è iniettivo? $\Updownarrow$ c'è una copia di S_n in $\mathrm{Aut}(S_n)$?

$\sigma \mapsto C_\sigma : S_n \to S_n$

$\tau \mapsto \sigma\tau\sigma^{-1}$

$\sigma \in \ker \psi \iff \sigma \in Z(S_n) = \}e\{$

↳ per $n \geq 3$ ⟶ Quindi ψ è un'immersione!

Teorema $\mathrm{Aut}(S_n) \simeq S_n$ $n > 2$, $n \neq 6$

14-10-2021 Lezione 8 Prof. Gaiffi

Prodotti Semidiretti

Sia G gruppo, siano $M < G$, $N < G$.

In generale non è vero che $MN < G$.

In S_3 $M = \}e, (1,2)\{$, $N = \}e, (1,3)\{ \rightsquigarrow MN = \}e, (1,3), (1,2), (1,2)(1,3)\{$

$\boxed{MN \not< S_3}$

Lemma: Sia $M \triangleleft G$ e $N < G$. Allora $MN < G$.

Dim. Verifichiamo per es. che è chiuso per $\cdot$.

$m, m_1 \in M$ $n, n_1 \in N$

$m n m_1 n_1 = m n m_1 n^{-1} n n_1 = m \underbrace{n m_1 n^{-1}}_{\in M \text{ perché } M \triangleleft G} n n_1 \in MN$

Lemma Se $M \triangleleft G$, $N \triangleleft G$ e vale anche $M \cap N = \}e\{$.

Allora $\forall m \in M$, $\forall n \in N$ vale $mn = nm$.

Oss In questo caso dunque $MN < G$ e $MN \cong M \times N$

COSTRUZIONE DI UN PRODOTTO SEMIDIRETTO

Siano H, K gruppi e sia $\tau: K \to \mathrm{Aut}(H)$ omomorfismo.

Considero sull'insieme $H \times K$ il seguente prodotto:

$(h, k)(\bar{h}, \bar{k}) = (h\tau(k)(\bar{h}), k\bar{k})$

Prima: $m \underbrace{n m_1 n^{-1}} n n_1$

$m\, c(n)(m_1)\, n n_1$

$M \triangleleft G$

Def: Chiamo $H \rtimes_\tau K$ il gruppo definito qui sopra.

(Prodotto semidiretto di H e K rispetto a τ)

① ESERCIZIO: Dimostrare che è un gruppo

② $H \times \{e_K\} = \{(h, e_K) \mid h \in H\}$ è sgrp di $H \rtimes_\tau K$ ed è $\cong H$

$\uparrow$ identità di K

$$(h_1, e_K)(h_2, e_K) = (h_1 \tau(e_K)(h_2), e_K) = (h_1 h_2, e_K)$$

$$\tau : K \to Aut(H)$$
$$e_K \to Id$$

$$\psi : H \to H \times \{e_K\}$$
$$h \mapsto (h, e_K)$$ è un ISO.

Esercizio. $H \times \{e_K\} \trianglelefteq H \rtimes_\tau K$

(l'inverso di $(\bar{h}, \bar{k})$ è $(\tau(\bar{k}^{-1})(\bar{h}^{-1}), \bar{k}^{-1})$)

$$(\bar{h}, \bar{k})(h, e_K)(\tau(\bar{k}^{-1})(\bar{h}^{-1})), \bar{k}^{-1}) \overset{?}{=} (\qquad , e_K)$$

Oss: $\{e_H\} \times K$ è sgruppo di $H \rtimes_\tau K$

Teorema Sia G gruppo. Sia $H \trianglelefteq G$ e $K < G$. Sia $H \cap K = \{e\}$ e sia $G = HK$

(Nei sgruppi G di ordine 20 in S_5 accadeva proprio questo, avevamo

$H = \langle(1,2,3,4,5)\rangle$ $K = \langle(1,2,4,3)\rangle$ $H \cap K = \{e\}$; $|HK| = 20 \Rightarrow HK = G$)

Allora $G \cong H \rtimes_{C_G} K$ dove $C_G : K \to Aut(H)$

$k \to$ automorfismo tale che

$\forall h \in H$, $h \to khk^{-1}$

Dim: Considero $\vartheta : HK \to H \rtimes_{C_G} K$
$$hk \to (h, k)$$

completare per esercizio

Esempio: Classifichiamo i gruppi di ordine 6.

Sia G un gruppo di ordine 6. Sia N_2 un 2-Sylow, N_3 un 3-Sylow.

$n_3 = 1$ (equiv. N_3 ha indice 2) $\Rightarrow N_3 \trianglelefteq G$.

Inoltre $N_3 \cap N_2 = \{e\}$ e $|N_3 N_2| = \dfrac{|N_3||N_2|}{|N_3 \cap N_2|} = 3 \cdot 2 = 6$ cioè $N_3 N_2 = G$

Allora per il Teorema ho che $G \cong N_3 \rtimes_{C_G} N_2$

$C_G : N_2 \to \mathrm{Aut}(N_3)$ chi è C_G?

Studio adesso tutti i possibili omomorfismi:

$\{1,-1\} = \mathbb{Z}_3 \setminus \{0\}$

$\tau : N_3 \to \mathrm{Aut}(N_3)$, $N_3 \cong \mathbb{Z}_3$, $N_2 \cong \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_3) \cong \overset{\shortparallel}{\mathbb{Z}_3^*} \cong \mathbb{Z}_2$

Sto dunque studiando (a meno di isomorfismi) i possibili OMOMORFISMI:

$\tau : \mathbb{Z}_2 \to \mathbb{Z}_2$ In totale ho due omomorfismi

$1 \mapsto \{0, 1\}$

$\tau_1 : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3) = \{Id, -Id\}$

$1 \mapsto Id$

$\tau_2 : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$

$1 \mapsto -Id$

Esistono AL MASSIMO due gruppi di ordine 6 perché

- sappiamo che un tale gruppo è del tipo $\mathbb{Z}_3 \rtimes_\tau \mathbb{Z}_2$
- sappiamo che di τ di quel tipo ossia $\tau : S_3 \to \mathrm{Aut}(\mathbb{Z}_3)$ ne esistono 2

Ma ne conosciamo due di gruppi di # 6. $\underset{\text{abeliano}}{\mathbb{Z}_6}$ e $\underset{\text{non abeliano}}{S_3}$

Dunque deve essere $\mathbb{Z}_3 \rtimes_{\tau_1} \mathbb{Z}_2 \enclose{circle}{\cong} \mathbb{Z}_6$

$\mathbb{Z}_3 \rtimes_{\tau_2} \mathbb{Z}_2 \cong S_3$

$\to \tau_1$ infatti è banale : $\tau_1(1) = Id$

$(a,b)(c,d) = (a\,\tau_1(b)(c), bd)$

$= (ac, b,d)$

$\Rightarrow \mathbb{Z}_3 \rtimes_{\tau_1} \mathbb{Z}_2 = \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$

S_3 . $H = \langle(1,2,3)\rangle$, $K = \langle(1,2)\rangle$

$S_3 = HK \cong H \rtimes_{\substack{\text{coniugio}\\ \text{in } S_3}} K$

$\tau : K \to \mathrm{Aut}(H)$

$(1,2) \mapsto$ automorfismo di H che manda ogni elemento nell'inverso $\to$ es: $(1,2)(1,2,3)(1,2) = (1,3,2)$

$= (1,2,3)^{-1}$

Esercizio (Wreath product = prodotto intrecciato)

$H = \mathbb{Z}_3 \times \mathbb{Z}_3$, $K = \mathbb{Z}_2$, $H \rtimes K$. Sia $\tau : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$

$1 \mapsto$ scambi di coordinate

Prendiamo $a = \big(\overset{\mathbb{Z}_3 \times \mathbb{Z}_3}{\overset{\rotatebox{90}{$\in$}}{(0,0)}} , \overset{\mathbb{Z}_2}{\overset{\rotatebox{90}{$\in$}}{1}} \big) \in H \rtimes_\tau K$, $b = ((1,0),1) \in H \rtimes_\tau K$

$aba^{-1} \overset{?}{=} ((0,0),1)((0,0),1) = ((0,0) + \tau(1)((1,0)), 1+1)((0,0),1) = ((0,1), \underset{\substack{\uparrow\\ \text{siamo in } \mathbb{Z}_2}}{0})((0,0),1) =$

$= ((0,1) + \tau(\overset{\swarrow \text{id}}{0})(0,0), 0+1) = ((0,1),1) \neq ((1,0),1) = b$

Il gruppo $\mathbb{Z}_3 \times \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ non è commutativo.

15/10/21 Lezione 9 Prof. Gaiffi

Proposizione Dati H e K gruppi siano τ_1 e $\tau_2 \cdot K \to Aut(H)$ due omo.

Se esistono $\alpha \in Aut(H)$ e $\beta \in Aut(K)$ tali che $\alpha \circ \tau_2(k) \circ \alpha^{-1} = \tau_1(\beta(k))$ $\forall k \in K$ allora $H \rtimes_{\tau_1} K \cong H \rtimes_{\tau_2} K$

Dim. $\vartheta: H \rtimes_{\tau_1} K \to H \rtimes_{\tau_2} K$
$(h, k) \mapsto (\alpha(h), \beta(k))$ è l'isomorfismo (verificare).

Esempio Classificazione dei gruppi di cardinalità pq con p e q PRIMI.

Prop Sia $p>q$. Se $q \nmid p-1$ esiste (a meno di iso) un solo gruppo di cardinalità pq ed è $\mathbb{Z}_{pq}$.

Se $q \mid p-1$ esistono esattamente due gruppi di ordine pq: $\mathbb{Z}_{pq}$ e l'altro è non abeliano.

Dim. Sia G gruppo con $|G|=pq$.

Sia N_p un p-Sylow, N_q un q-Sylow. Si nota subito che $N_p \trianglelefteq G$ visto che ha indice q, il più piccolo primo che divide l'ordine del gruppo.

$N_p N_q = G$ per ragioni di cardinalità. ($N_p \cap N_q = \{e\}$)

$$|N_p N_q| = \frac{|N_p||N_q|}{|N_p \cap N_q|} = p \cdot q. \quad \text{Allora} \quad G \cong N_p \rtimes_{\tau_G} N_q$$

$$N_p \cong \mathbb{Z}_p$$

$$N_q \cong \mathbb{Z}_q$$

Studio tutti i possibili $\tau: \mathbb{Z}_q \to Aut(\mathbb{Z}_p)$.

$Aut(\mathbb{Z}_p) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$.

Se $q \nmid p-1$ allora $\tau: \mathbb{Z}_q \longrightarrow \overset{Id}{Aut(\mathbb{Z}_p)} \cong \overset{0}{\mathbb{Z}_{p-1}}$

$1 \longmapsto$ NON CI SONO ELEMENTI DI ORDINE q

Quindi l'immagine di 1 è Id di $Aut(\mathbb{Z}_p)$ ovvero 0 di $\mathbb{Z}_{p-1}$.

Segue anche che $\tau(i) = Id$ $\forall i \in \mathbb{Z}_q$

Quindi $\mathbb{Z}_p \rtimes_\tau \mathbb{Z}_q$ coincide col prodotto diretto $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

Se $q \mid p-1$

$$\tau : \mathbb{Z}_q \longrightarrow \mathbb{Z}_{p-1} \quad \leftarrow \text{ADDITIVO}$$

$$\begin{tikzcd}
1 \arrow[r] \arrow[dr, "\tau_1"] \arrow[ddr, "\tau_2"] \arrow[dddr] \arrow[ddddr, "\tau_{q-1}"'] & 0 \quad \text{questo produce } \mathbb{Z}_p \times \mathbb{Z}_q \\
& \frac{p-1}{q} \\
& 2\frac{p-1}{q} \\
& \dots \\
& (q-1)\frac{p-1}{q}
\end{tikzcd}$$

Mostriamo usando il lemma che:

$$\mathbb{Z}_p \rtimes_{\tau_1} \mathbb{Z}_q \cong \mathbb{Z}_p \rtimes_{\tau_2} \mathbb{Z}_q \cong \dots \cong \mathbb{Z}_p \rtimes_{\tau_{q-1}} \mathbb{Z}_q$$

Per ogni $i = 1, 2, \dots, q-1$ scelgo $\beta_i \in \mathrm{Aut}(\mathbb{Z}_q)$ definito da $\beta_i(1) = i$.

Ricordo che $\mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_q^*$ e la mappa era

$$\begin{array}{ccc} \mathrm{Aut}(\mathbb{Z}_q) & & \mathbb{Z}_q^* \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ 1 \to i & \leftrightarrow & i \\ \quad\ \uparrow & & \\ \quad\ \neq 0 & & \end{array}$$

Affermo che $\tau_i(1) = \tau_1(\beta_i(1))$.

Infatti $\tau_i(1) = i\frac{p-1}{q}$, $\tau_1(\beta_i(1)) = \tau_1(i) = i\frac{p-1}{q}$, $\tau_1(1) = \frac{p-1}{q}$.

Dunque $\tau_1 \circ \beta_i$ e τ_i coincidono su tutto $\mathbb{Z}_q$, perché coincidono su 1 che è un generatore di $\mathbb{Z}_q$. Per il lemma $\mathbb{Z}_p \rtimes_{\tau_1} \mathbb{Z}_q \cong \mathbb{Z}_p \rtimes_{\tau_i} \mathbb{Z}_q$ $\forall i$.

Dunque ci sono (a meno di iso) al massimo due gruppi di $\#\, pq$:

$$\mathbb{Z}_p \times \mathbb{Z}_q \quad \text{e} \quad \mathbb{Z}_p \rtimes_{\tau_1} \mathbb{Z}_q$$

Per mostrare che NON sono iso mostriamo che $\mathbb{Z}_p \rtimes_{\tau_1} \mathbb{Z}_q$ NON è ABELIANO.

Sia $a \in \mathbb{Z}_p$, sia $b \in \mathbb{Z}_q$.

$(a,b)(0,b) = (a + \tau_1(b)(0), 2b) = (a, 2b)$

$(0,b)(a,b) = (0 + \tau_1(b)(a), 2b) = (\tau_1(b)(a), 2b)$

Scelgo b tale che $\tau_1(b) \neq Id$. (τ_1 non era l'OMOMORFISMO BANALE).

$\tau_1(b) \neq Id$ significa che $\exists$ un elemento che non viene mandato in se stesso da $\tau_1(b)$. Prendo $a =$ questo elemento $\tau(b)(a) \neq a$.

Dunque $\mathbb{Z}_p \rtimes_{\tau_1} \mathbb{Z}_q$ non è commutativo.

Nota: Si poteva anche osservare che se $G = \mathbb{Z}_p \rtimes_{\tau_1} \mathbb{Z}_q$ fosse stato abeliano allora τ_1 avrebbe descritto il coniugio in G che è l'identità e dunque τ_1 sarebbe stato l'omomorfismo banale, ASSURDO

GRUPPI DI ORDINE 12

Sia G gruppo di ordine 12. Sia N_2 un 2-Sylow $|N_2| = 4$ e sia N_3 un 3-Sylow $|N_3| = 3$.

$$n_2 = \begin{cases} 1 \\ 3 \end{cases} \qquad\qquad n_3 = \begin{cases} 1 \\ 4 \end{cases}$$

Casi: $n_2 = 1$ Allora $N_2 \triangleleft G$ e per i soliti motivi $G \cong N_2 \rtimes N_3$

$$N_2 \cong \begin{cases} \mathbb{Z}_4 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \end{cases}$$

Studiamo la situazione $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$

$$Aut(\mathbb{Z}_4) \cong \mathbb{Z}_4^* \cong \mathbb{Z}_2$$

$$\tau : \mathbb{Z}_3 \to \mathbb{Z}_2$$
$$1 \mapsto 0$$

è l'unico possibile per motivi di ordine

Abbiamo dunque solamente $\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$

Studiamo adesso il caso $N_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

$$Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong GL(2, \mathbb{Z}_2)$$

$$\underset{\text{modi}}{(2^2-1)} \; \underset{\text{modi}}{(2^2-2)}$$

$$|GL(2, \mathbb{Z}_2)| = 3 \cdot 2 = 6$$

$GL(2, \mathbb{Z}_3)$ non è abeliano e dunque $GL(2, \mathbb{Z}_2) \cong S_3$.

Dato che sappiamo che esiste (a meno di iso) un solo gruppo non abeliano di cardinalità 6.

Nota: $\mathbb{Z}_2 \times \mathbb{Z}_2$ è generato da $(1,0)$ e $(0,1)$.

Un automorfismo è un cambio di base. le basi sono tutte e sole le coppie a, b dove $a \neq b$, e a e $b \in X = \}(1,0), (0,1), (1,1)\{$.

Questo identifica i cambi di base con le permutazioni di X.

Cambiare base significa prendere due elementi a, b e mandarli in $a', b' \in X$. Questo crea una permutazione inviando il terzo elemento c in c')

$$\tau : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$$

$$\begin{tikzcd} 1 \arrow[r] \arrow[dr, "\tau_1"] \arrow[ddr, "\tau_2"'] & e \\ & (1 2 3) \\ & (1 2 3)^2 = (1 3 2) \end{tikzcd}$$

questo dà $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$

per ragioni di ordine deve essere un 3-ciclo

Ora osservo che $\tau_1 \circ \beta = \tau_2$ dove $\beta \in \mathrm{Aut}(\mathbb{Z}_3)$
$\beta(1) = 2$

Infatti $\tau_1(\beta(1)) = \tau_1(2) = (1,2,3)^2$ dunque $\tau_1 \circ \beta = \tau_2$.

Potevo anche prendere $\alpha \in S_3$ tale che $\alpha (1 3 2) \alpha^{-1} = (1 2 3) \to \alpha = (2 3)$

Allora $\alpha \circ \tau_2(1) \circ \alpha^{-1} = \tau_1(1)$

$$\alpha (1 3 2) \alpha^{-1} = (1 2 3)$$

Dunque applico il lemma e deduco che c'è un solo gruppo del tipo $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3$ ossia in cui il 2-Sylow è normale ed è $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Dato che conosciamo A_4 è lui. Abbiamo terminato i casi in cui il 2-Sylow è normale.

Sia dunque adesso $n_2 = 3$

Allora $n_3 = 1$. Perché?

Se $n_3 = 4$ avrei 8 elementi di ordine 3 e resterebbero 4 non di ordine 3, che costituirebbero l'unico 2-Sylow. ASSURDO perché allora $n_2 = 1$.

Sia dunque adesso $n_2 = 3$. Allora $n_3 = 1$. Perché?

Dunque $n_2 = 3$ e $n_3 = 1$. Allora $G \cong N_3 \rtimes N_2$.

L'ANALISI SI DIRAMA IN DUE CASI:

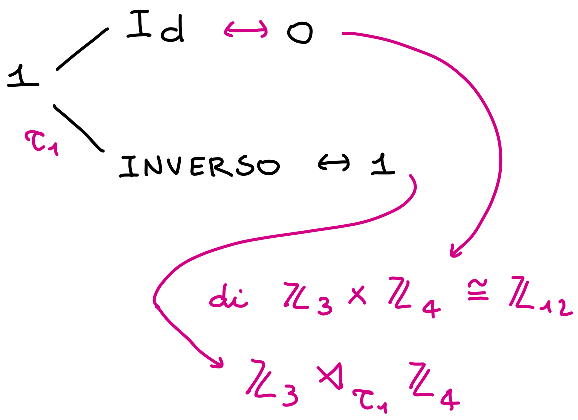
Ⓐ $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$

oppure

Ⓑ $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$

Analizziamo il primo caso:

Ⓐ $\tau : \mathbb{Z}_4 \longrightarrow \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$



$(a,b)(c,d) = (a + \tau_1(b)(c),\ b + d) = (a + (-1)^b c,\ b + d)$

Un modello per questo si trova per esempio dentro $SL(2, \mathbb{C})$.

$x = (1, 0)$

$y = (0, 1)$

$x = \begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix}$ $\qquad \omega = e^{\frac{2\pi}{3} i}$

$y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

Il gruppo $(x, y) \subseteq SL(2, \mathbb{C})$. Vale la relazione $yxy^{-1} = x^{-1}$.

$\uparrow$

il sottogruppo di $GL(2, \mathbb{C})$ dato
dalle matrici $\det = 1$.

Resta il secondo caso:

Ⓑ $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ (PROSEGUIREMO)

20-10-2021 Lezione 10 Prof. Melani

G gruppo $\rightsquigarrow$ $Aut(G)$ gruppo degli automorfismi di G $\quad Aut(G) \subseteq Big(G)$

$g \in G \quad C_g : G \to G$, $x \mapsto gxg^{-1}$ $\qquad S_n \hookrightarrow Aut(S_n)$

Teorema: $Aut(S_n) \simeq S_n \quad n>2, n \neq 6$

Idee della dim:

① $\varphi \in Aut(S_n)$, $x \in S_n$ di ordine 2 $\Rightarrow$ $\varphi(x)$ ha ancora ordine 2

$(\varphi(x)^2 = \varphi(x)\varphi(x) = \varphi(x^2) = \varphi(e) = e)$

② $\varphi \in Aut(S_n)$, $x, y \in S_n$ coniugati fra loro $\Rightarrow$ $\varphi(x)$ e $\varphi(y)$ sono coniugati

(se $gxg^{-1} = y$, allora $\varphi(gxg^{-1}) = \varphi(y)$, cioè $\varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(y)$)

③ $\varphi \in Aut(S_n)$

φ permuta le classi di coniugio degli elementi di ordine 2

$\Gamma_K :=$ classe di coniugio dei K 2-cicli in S_n

$$\#\Gamma_K = \frac{1}{K!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2(K-1)}{2}$$

Lemma: Se $n \neq 6$ allora $\#\Gamma_K \neq \#\Gamma_1 \quad \forall K>1$

Conseguenza Se $n \neq 6$, $\varphi(\Gamma_1) = \Gamma_1$, cioè φ manda trasposizioni in trasposiz.

Esercizio: dimostrare il lemma

Domanda: Se $\varphi \in Aut(S_n)$ manda trasposizioni in trasposizioni

è vero che $\varphi = C_g$ per qualche $g \in S_n$?

Risposta: Sì! Infatti: supponiamo $\varphi(12) = (ab)$ e prendiamo $i \neq 1,2$.

Allora $(12)(1i)$ è un 3-ciclo e dunque $\varphi((12)(1i)) = \varphi(12)\varphi(1i) = (ab)\varphi(1i)$ è un 3-ciclo.

Posso quindi supporre $\varphi(1i) = (ac)$ con $c \neq a, b$

Affermo: $\forall j \neq 1$, $\exists\, d \neq a$ tc $\varphi(1j) = (ad)$

→ per $j = 2, i$ lo so già

→ $\varphi((1j)(12))$ è un 3-ciclo, voglio escludere la possibilità che $\varphi(1j) = (bf)$

Idea: Supponiamo $j \neq 2, i$, $\varphi((1j)(1i)) = (bf)(ac)$ è un 3-ciclo $\Rightarrow f = c$?

$(ab)(ac)(ab) = (bc) = (bf)$

$\varphi(12)\varphi(1i)\varphi(12) = \varphi(1j)$

$\varphi((12)(1i)(12)) = \varphi(1j)$

$\varphi(2i) = \varphi(1j)$ ASSURDO

esercizio: Concludere la dimostrazione del teorema

Idea: $g(1) = a$ $g(j) = d$ $j \neq 1$

Gruppi di ordine 8

- ordine degli elementi di $G = \left\{ \begin{array}{l} \cancel{1} \\ 2 \\ 4 \\ 8 \Rightarrow \text{G ciclico} \quad G \simeq \mathbb{Z}/8\mathbb{Z} \end{array} \right.$

Pensiamo invece al massimo ordine.

- Se maxord = 2:

$x^2 = e$ $\forall x \in G$, cioè $x = x^{-1}$ $\forall x \in G$. Ma allora G è abeliano;

$x, y \in G \Rightarrow xy \in G$ $\quad (xy)^2 = e \Rightarrow xyxy = e = e \cdot e = x^2 y^2$
↳ G gruppo

esercizio: In questo caso $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

- Se maxord = 4:

Sia $x \in G$ di ordine 4, e sia $H = \langle x \rangle$ il sgruppo generato da x.

$H \triangleleft G$ perché di indice 2. $H = \}e, x, x^2, x^3\{$

Idea: Prendiamo $y \in G \setminus H$ con $\text{ord}(y) = 2$, $K = \}e, y\{ < G$

$G = \}e, x, x^2, x^3, y, xy, x^2y, x^3y\{ \rightsquigarrow G \simeq H \rtimes_{\varphi} K$ chi è yxy^{-1}?

$\varphi : K \to \text{Aut}(H)$ $\quad \varphi : \mathbb{Z}/2\mathbb{Z} \to \text{Aut}\left(\mathbb{Z}/4\mathbb{Z}\right) \simeq \mathbb{Z}/2\mathbb{Z}$

Se l'azione è banale, $G \simeq H \times K \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Altrimenti $yxy^{-1} = x^3$ $\quad G \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_4$
↖ esercizio

Domanda: Ma perché esiste un elemento di ordine 2 fuori da H?
(pensarci per esercizio)

21-10-2021 Lezione 11 Prof. Gaiffi

Finiamo la classificazione dei gruppi di ordine 12

Nella lezione 9 era rimasto da analizzare il caso $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$

$\tau : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_3^* = \}1, -1\{ \cong \mathbb{Z}_2$

$$\left.\begin{aligned} a &= (1,0) \\ b &= (0,1) \end{aligned}\right\} \text{generatori}$$

Per dire chi è τ devo indicare $\tau(a)$ e $\tau(b)$

Se $\begin{aligned} a &\longmapsto 0 \\ b &\longmapsto 0 \end{aligned}$ ho il prodotto diretto: $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$

$\tau_1 :$ $a \longmapsto 0$
$b \longmapsto 1$
$(a+b \longmapsto 1)$

$\tau_2 :$ $a \longmapsto 1$
$b \longmapsto 0$
$(a+b \longmapsto 1)$

$\tau_3 :$ $a \longmapsto 1$
$b \longmapsto 1$
$(a+b \longmapsto 2 = 0)$

In realtà $\mathbb{Z}_3 \rtimes_{\tau_1} (\quad) \cong \mathbb{Z}_3 \rtimes_{\tau_2} (\quad) \cong \mathbb{Z}_3 \rtimes_{\tau_3} (\quad)$

$\alpha \circ \tau_2(k) \circ \alpha^{-1} = \tau_1(\beta)$ $\alpha \in \mathrm{Aut}(\mathbb{Z}_3)$ $\beta \in \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$

Scelgo $\alpha = \mathrm{Id}$ (tanto non mi aiuta) e β il cambio di base che scambia a e b.

Per il caso τ_2 e τ_3 basta scegliere β come il cambio di base che manda a in a e b in a+b.

Il gruppo trovato è $D_6 = \}r, s \mid r^6 = e\ ,\ s^2 = e \quad srs = r^{-1}\{$

$r^6 = \mathrm{Id}$ $\langle r \rangle$, $\langle r^2 \rangle$ $\}e, r^3, \overset{\text{simmetria}}{s}, r^3 s\{$ è sgruppo iso a $\mathbb{Z}_2 \times \mathbb{Z}_2$

Dunque D_6 ha le caratteristiche richieste.

Domanda: $S_3 \times \mathbb{Z}_2$ quale gruppo è nella classificazione?

Prendo $H \leq S_3$ $H = ((123)) \rightsquigarrow H \times \}0\{ \lhd S_3 \times \mathbb{Z}_2 \rightsquigarrow$ il 3-Sylow è normale

$K \leq S_3$ $K = \}(12)\{$ $K \times \mathbb{Z}_2$ è un sgruppo di $S_3 \times \mathbb{Z}_2$ isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$

il gruppo $S_3 \times \mathbb{Z}_2$ non è COMMUTATIVO dunque $S_3 \times \mathbb{Z}_2 \cong D_6$.

Domanda: Siano S_3, $\mathbb{Z}_2$. Costruisco un τ omomorfismo:

$$\tau: \mathbb{Z}_2 \longrightarrow Aut(S_3) \simeq S_3 \qquad C_g \leftarrow g$$

$$1 \longmapsto (1,2)$$

Posso dunque fare $S_3 \rtimes_\tau \mathbb{Z}_2$: chi è ? NON è ABELIANO

A_4

gruppo diciclico Dic_3

D_6

$b = ((1,2),0) \in S_3 \rtimes_\tau \mathbb{Z}_2$

$b^2 = (e,0)$

$((1,2),0)((1,2),0) = ((1,2)\tau(0)(1,2), 0+0) = (e,0) \qquad \tau(0) = Id$

$g = (e,1) \qquad g^2 = (e,0)$

Sia $x = bg$, $x = \underset{b}{((12),0)}\underset{g}{(e,1)} = ((12),1) \notin S_3 \times \{0\}$

$x^2 = bgbg = bggb = bg^2b = beb = b^2 = e$. Infatti b e g commutano.

$gb = (e,1)((1,2),0) = (e\,\tau(1)(12), 1)$

Ma $\tau(1)$ è il CONIUGIO per (12) e quindi $(12)(12)(12) = (12)$

$gb = ((12),1) = bg$

Mostriamo che x commuta con $S_3 \times \{0\}$

$\langle x \rangle = K$ ha ordine 2. $S_3 \times \{0\} = H$ ha ordine 6.

$H \cap K = \{e\}$, $HK = S_3 \rtimes_\tau \mathbb{Z}_2$. Poiché x commuta con H, $HK \cong H \times K \cong S_3 \times \mathbb{Z}_2$

Per vedere che x commuta con $H = S_3 \times \{0\}$ basta vedere che:

- x commuta con $b = ((12),0)$ GIÀ VISTO
- x commuta con $a = ((123),0)$

$ax = ((123),0)((12),1)$

$xa = ((12),1)((123),0)$

in entrambi i casi il risultato è $((13),1)$

$xa = ((12)\tau(1)(123), 1+0) =$

$= (\cancel{(12)}\cancel{(12)}(123)(12), 1)$

$= ((13), 1)$

Oss: Con il lemma avrei mai potuto scoprire che $S_3 \times \mathbb{Z}_2 \cong S_3 \rtimes_{\tau_{BAN}} \mathbb{Z}_2$ e $S_3 \rtimes \mathbb{Z}_2$ sono isomorfi?

$$\begin{array}{rccl} \tau_{BAN}: & \mathbb{Z}_2 & \longrightarrow & S_3 \\ & 1 & \longmapsto & e \end{array}$$

$$\begin{array}{rccl} \tau: & \mathbb{Z}_2 & \longrightarrow & S_3 \\ & 1 & \longmapsto & (1,2) \end{array}$$

$\alpha\tau(1)\alpha^{-1} = \tau_{BAN}(\beta(1))$ $\quad \beta \in Aut(\mathbb{Z}_2) = \}Id\{$, β non aiuta

$\alpha \in Aut(S_3) \cong S_3$

Penso α come un elemento di S_3.

$$\tau(1) = (12)$$

$$\alpha(12)\alpha^{-1} = e$$

$$(\alpha(1), \alpha(2)) = e$$

IMPOSSIBILE

ESERCIZIO (Proposizione)

Sia p primo ≥ 3 e $\alpha \in \mathbb{Z} \geq 2$. Allora $(\mathbb{Z}_{p^\alpha})^* \cong \mathbb{Z}_{\varphi(p^\alpha)} = \mathbb{Z}_{p^{\alpha-1}(p-1)}$ quindi è ciclico.

Svolgimento:

Strategia: troviamo un elemento γ di ordine $p^{\alpha-1}$ e un elemento β di ordine $p-1$ allora $\gamma\beta$ avrà ordine $p^{\alpha-1}(p-1)$

PERCHÉ IL GRUPPO È ABELIANO E GLI ORDINI SONO PRIMI TRA LORO

e quindi $(\mathbb{Z}_{p^\alpha})^* = (\gamma\beta)$

Lemma: Sia $K \in \mathbb{N} \setminus \}0\{$ $\quad (1+p)^{p^K} = 1 + \lambda p^{K+1}$ con λ primo con p

Dim: PER INDUZIONE: Per $K=1$ $\quad (1+p)^p = 1 + \binom{p}{1}p + \binom{p}{2}p^2 + \quad + p^p =$

$$= 1 + p^2 + \underbrace{\binom{p}{2}p^2 + \quad + p^p}_{\text{sono divisi da } p^3}$$

$$= 1 + p^2[\underbrace{1 + \delta p \qquad}_{\lambda}]$$

$$= 1 + p^2\lambda \quad \text{con } MCD(\lambda, p) = 1$$

PASSO INDUTTIVO: $(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p = (1+\lambda p^{k+1})^p = 1 + \binom{p}{1}\lambda p^{k+1} + \binom{p}{2}(\lambda p^{k+1})^2 + \dots$

$$= 1 + \lambda p^{k+2} + \underbrace{\qquad\qquad\qquad\qquad}_{\text{diviso da } p^{k+3}}$$

$$= 1 + p^{k+2}[\overbrace{\lambda + pu}^{\lambda'}]$$ come volevamo, con $MCD(\lambda', p) = 1$

$\square$

<u>Nota</u>: abbiamo dimostrato che $1+p$ ha ORDINE $p^{\alpha-1}$ in $(\mathbb{Z}_{p^\alpha})^*$

$$(1+p)^{p^{\alpha-1}} \underset{\substack{\uparrow \\ \text{per lemma}}}{=} 1 + p^\alpha \lambda \equiv 1 \ (p^\alpha)$$

Inoltre se $r < \alpha - 1$ $\quad (1+p)^r \underset{\substack{\uparrow \\ \text{per lemma}}}{=} 1 + p^{r+1}\lambda' \not\equiv 1 \ (p^\alpha)$

Quindi $\gamma = (1+p)$

$$\psi : (\mathbb{Z}_{p^\alpha})^* \to (\mathbb{Z}_p)^* \cong \mathbb{Z}_{p-1}$$
$$[m]_{p^\alpha} \longmapsto [m]_p$$

ψ è OMOMORFISMO.

Sia $x \in \mathbb{Z}_p^*$ di ordine $p-1$. Sia $y \in (\mathbb{Z}_{p^\alpha})^*$ tale che $\psi(y) = x$

Che ordine ha y? Siccome x ha ordine $p-1$, allora y ha ordine un multiplo di $p-1$. Allora nel gruppo ciclico (y) trovo un elemento β di ordine esattamente $p-1$. (FINE DELL'ESERCIZIO)

<u>ESERCIZIO</u> (Proposizione):

Sia $\alpha \geq 3$, $(\mathbb{Z}_{2^\alpha})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ NON è ciclico

<u>LEMMA</u>: $\forall k \in \mathbb{N} \setminus \{0\}$ vale $5^{2^k} = 1 + \lambda 2^{k+2}$ con λ dispari. (Dim: Analoga, x es)

<u>Dim</u> (Prop.): $\quad \psi : (\mathbb{Z}_{2^\alpha})^* \to (\mathbb{Z}_4)^* \cong \{1, -1\} \cong \mathbb{Z}_2$

$$[b]_{2^\alpha} \to [b]_4$$

ψ è OMOMORFISMO SURGETTIVO

Ker ψ ha $\dfrac{\varphi(2^\alpha)}{2}$ elementi. $\varphi(2^\alpha) = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1}$ ossia $2^{\alpha-2}$ elementi.

<u>OSS</u>: $5 \in$ Ker ψ e nel lemma abbiamo dimostrato che l'ordine di 5 in $(\mathbb{Z}_{2^\alpha})^*$ è $2^{\alpha-2}$. Dunque Ker ψ è ciclico, generato da 5.

Dunque dentro $(\mathbb{Z}_{2^\alpha})^*$ lo $\ker\psi \cong \mathbb{Z}_{2^{\alpha-2}}$. $H=\{-1,1\}$, $\ker\psi \cap H = \{1\}$.

Per ragioni di cardinalità $\ker\psi \cdot H = (\mathbb{Z}_{2^\alpha})^*$.

Dunque $(\mathbb{Z}_{2^\alpha})^* \cong \ker\psi \times H \cong \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_2$.

ESERCIZIO Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, chi è $\mathrm{Aut}(\mathbb{Z}_n)$? E per quali n è ciclico?

22-10-2021 Lezione 12 Prof. Gaiffi

CLASSIFICAZIONE DEI GRUPPI ABELIANI FINITAMENTE GENERATI

Def. Un gruppo abeliano M si dice finitamente generato se esistono $m_1, m_2, \dots, m_n \in M$ tali che $\forall m \in M$ si può scrivere $m = a_1 m_1 + a_2 m_2 + \dots + a_n m_n \in M$ con $a_i \in \mathbb{Z}$.

↳ combinazione lineare

Si dice che $\{m_1, \dots, m_n\}$ è un INSIEME DI GENERATORI.

Esempio $(\mathbb{Q}, +)$ non è finitamente generato

Dim. Per assurdo, sia $\left\{\frac{r_1}{s_1}, \dots, \frac{r_n}{s_n}\right\}$ un insieme di generatori.

Sia p primo, posso scrivere $\frac{1}{p} = a_1 \frac{r_1}{s_1} + \dots + a_n \frac{r_1}{s_n}$; allora avrei $s_1 \cdot \ldots \cdot s_n = kp$ $k \in \mathbb{Z}$

Ma ciò è assurdo perché p è primo. ↯ □

Def Se A gruppo abeliano è isomorfo a $\mathbb{Z}^r$ per un $r \geq 1$ lo chiameremo:

"gruppo abeliano libero di rango r"

Nota: Vedremo più avanti che il rango è univocamente definito, dunque è una buona definizione.

SUCCESSIONI ESATTE DI GRUPPI ABELIANI

Esempio di successione esatta corta: A, B, C gruppi abeliani, f, g omomorfismi

$\{0\} \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \{0\}$ si dice che è esatta se:

$\ker f = \{0\}$

$\mathrm{Im}\, f = \ker g$

$\mathrm{Im}\, g = C$

Esempio:

$\{0\} \to \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_{p^2} \xrightarrow{g} \mathbb{Z}_p \to \{0\}$

$f([a]_p) = [pa]_{p^2}$

$g([b]_{p^2}) = [b]_p$

è esatta. Ma non è vero che $\mathbb{Z}_{p^2} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proposizione:

Data $\{0\} \to A \xrightarrow{\varphi} B \xrightarrow{g} \mathbb{Z} \to \{0\}$ successione esatta, allora vale $B \cong \underbrace{A \oplus \mathbb{Z}}_{A \times \mathbb{Z}}$

$$\begin{tikzcd} B \arrow[r, "g"] & \mathbb{Z} \arrow[l, dashed, bend left, "\psi"] \end{tikzcd}$$

l'esistenza di questa mappa fa funzionare la proposizione

Dim. Visto che g è surgettiva, $\exists b \in B$ tc $g(b)=1$. Costruisco l'OMOMORFISMO

$\psi: \mathbb{Z} \to B$
$1 \mapsto b$

NOTIAMO che $g\circ\psi(1) = g(b) = 1$ cioè $g\circ\psi: \mathbb{Z}\to\mathbb{Z}$ è l'IDENTITÀ.

Costruisco $\Gamma: A\times\mathbb{Z} \to B$
$(a,n) \mapsto \varphi(a) + \psi(n)$

(IMMEDIATO VERIFICARE CHE È OMOMORFISMO)

Γ surgettiva: Sia $b' \in B$. Considero $g(b') = m \in \mathbb{Z}$

$$\begin{tikzcd} B \arrow[r, "g"] & \mathbb{Z} \\ b' \arrow[r, mapsto] & m \arrow[l, bend left, "\psi"] \end{tikzcd}$$

$\psi(m) = mb$

Noto che $g(b') = g(\psi(m)) = m$. Dunque $g(b - mb) = 0$.

Dunque $b' - mb \in \operatorname{Ker} g$.

Ma $\operatorname{Ker} g = \operatorname{Im} f$ per l'ESATTEZZA. Allora $\exists a \in A$ tc $\varphi(a) = b' - mb$

$b' = \varphi(a) + mb = \varphi(a) + \psi(m)$

dunque $\Gamma((a,m)) = \varphi(a) + \psi(m) = b'$.

Γ iniettiva: x esercizio ☐

Esercizio Siano due successioni esatte orizzontali e supponiamo che esistano mappe di collegamento e che tutti i diagrammi commutino. $= M' \xrightarrow{\gamma g} N = M' \xrightarrow{f\delta} N$

Dimostriamo che se due fra f, g, h sono isomorfismi, allora anche l'altro è un isomorfismo.

NB: è importante che le mappe esistano

b=0 a=0

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "\gamma"] \arrow[d, "f", "ISO"'] & M \arrow[r, "\gamma'"] \arrow[d, "g"] & M'' \arrow[r] \arrow[d, "h"', "ISO"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "\delta"'] & N \arrow[r, "\delta'"'] & N'' \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} b \arrow[r] \arrow[d] & a \arrow[r] \arrow[d] & 0 \arrow[d] \\ 0 \arrow[r] & 0 \arrow[r] & 0 \end{tikzcd}$$

Nota

Step 1) $a \in M$, $g(a) = 0$
$\to \delta'(g(a)) = \delta'(0) = 0$
Considero il percorso:
$\gamma'(a) = * \Rightarrow * = 0$
$h(\gamma'(a)) = 0 \Rightarrow \gamma'(a) = 0$
ISOMORFISMO: manda 0 in 0

Step 2) $a \in \operatorname{Ker}\gamma'$ (per •)
esattezza
$a \in \operatorname{Im}(\gamma) \Rightarrow \exists b \in M'$ tc
$\gamma(b) = a \Rightarrow g(\gamma(b)) = g(a) = 0$
Considero il percorso:
$f(b) = *$ $\delta(*) \to 0$ iniettiva per l'esattezza
$\Rightarrow * = 0 \Rightarrow \delta(f(b)) = \delta(0) = 0 \Rightarrow f(b) = 0$
$b \in \operatorname{Ker}(f) = \{0\} \Rightarrow b = 0 \Rightarrow a = 0 \Rightarrow g$ ISO
ISO γ esatta

ES:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_p \arrow[r, "\gamma"] \arrow[d, equal, "Id"] & \mathbb{Z}_p \times \mathbb{Z}_p \arrow[r, "\gamma'"] \arrow[d, dashed, "\cancel{g}"] & \mathbb{Z}_p \arrow[r] \arrow[d, equal, "Id"] & 0 \\ 0 \arrow[r] & \mathbb{Z}_p \arrow[r] & \mathbb{Z}_{p^2} \arrow[r] & \mathbb{Z}_p \arrow[r] & 0 \end{tikzcd}$$

NON ESISTE

$\gamma(a) = (a,0)$
$\gamma'(c,d) = d$

IN QUESTO CASO $\nexists g$ CHE FA COMMUTARE! $\mathbb{Z}_p \times \mathbb{Z}_p \ncong \mathbb{Z}_{p^2}$

Prop. Sia $M < \mathbb{Z}^n$. Allora $M \cong \mathbb{Z}^r$ per un certo $0 \le r \le n$

"un s.gruppo di un $\underset{\overset{\wr\wr}{\mathbb{Z}^k}}{\text{gruppo abeliano libero}}$ è un gruppo abeliano libero oppure è $\{0\}$"

Dim: Per induzione su n.

PASSO BASE: Per $n=1$, $M < \mathbb{Z}$ allora

$$\underset{\underset{\text{visto ad Aritmetica}}{\downarrow}}{M} = \begin{cases} = \{0\} \\ = d\mathbb{Z} \cong \mathbb{Z} \text{ come gruppo abeliano} \end{cases}$$

PASSO INDUTTIVO:

Sia $n > 1$, $\pi : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ la proiezione sull'ultima coordinata.

$M < \mathbb{Z}^n$, $\pi|_M : M \longrightarrow \mathbb{Z}$

Caso 1)

Se vale $\operatorname{Im} \pi|_M = \{0\}$ allora $M \subseteq T = \{(a_1, a_2, \dots, a_{n-1}, 0) \mid a_1, \dots, a_{n-1} \in \mathbb{Z}\} \cong \mathbb{Z}^{n-1}$

Allora per IPOTESI INDUTTIVA so che $M \cong \mathbb{Z}^r$ con $0 \le r \le n-1$

Caso 2)

Se vale $\operatorname{Im} \pi|_M = d\mathbb{Z}$. $\{0\} \longrightarrow \ker \pi|_M \xrightarrow{i} M \xrightarrow{\pi} \overset{\overset{\mathbb{Z}}{\wr\wr}}{d\mathbb{Z}} \longrightarrow \{0\}$

Per la Proposizione precedente $M \cong \ker \pi|_M \times d\mathbb{Z}$
(la successione "spezza")

$\cong \ker \pi|_M \times \mathbb{Z}$

NB $\oplus = \times$

Noto che $\ker \pi|_M \subseteq T \cong \mathbb{Z}^{n-1}$.

Per hp induttiva $\ker \pi|_M \cong \mathbb{Z}^r$ con $0 \le r \le n-1$.

Quindi $M \cong \underset{\ker \pi|_M}{\underset{\wr\wr}{\mathbb{Z}^r}} \underset{\oplus}{\underset{\downarrow}{\times}} \underset{\operatorname{Im}\pi|_M}{\underset{\wr\wr}{\overset{\overset{\mathbb{Z}}{\wr\wr}}{\mathbb{Z}}}} \cong \mathbb{Z}^{r+1}$ $\quad 1 \le r+1 \le n$

$f: V \longrightarrow V$
$\operatorname{Im} f \oplus \ker f = V$

Torno alla classificazione:

Sia M gruppo abeliano finitamente generato. Siano $m_1, \dots, m_n$ generatori.

Considero:

$\phi : \mathbb{Z}^n \longrightarrow M$ OMOMORFISMO

$(a_1, \dots, a_n) \longmapsto a_1 m_1 + a_2 m_2 + \dots + a_n m_n$

ϕ è surgettiva perché $m_1, \dots, m_n$ sono generatori.

$\{0\} \rightarrow \ker \phi \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\phi} M \rightarrow \{0\}$. Per il 1° Teo di Omo $M \cong \mathbb{Z}^n / \ker \phi$.

$\ker \phi$ dalla proposizione precedente è $\cong \mathbb{Z}^r$ (sgrp di un grp ab libero)

Esempio: se $n=2$ e $\ker \phi = ((2,0),(0,3))$ $\quad M \cong \mathbb{Z}^2 / ((2,0),(0,3)) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

$\vartheta : \mathbb{Z}^2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

$(a,b) \mapsto ([a]_2, [b]_3)$

ϑ è omo surg. Chi è Ker ϑ? Ker $\vartheta = ((2,0),(0,3))$

$$\mathbb{Z}^2/_{\text{Ker}\,\vartheta} \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

Esercizio: Sia G un gruppo di ordine pqr con $p<q<r$ PRIMI.

Dimostrare che l'r-Sylow è NORMALE.

Dim. $n_r \mid pq \qquad n_r \equiv 1 \ (r)$

$$n_r = \begin{matrix} 1 \\ p \\ q \\ pq \end{matrix}$$

Se non fosse $n_r = 1$ allora $n_r = 1+rk$ con $k \geq 1$ cioè $\underbrace{n_r > r > q > p}$.

da questo escludo $n_r = p$ e $n_r = q$

↓

$n_r = pq$

Resterebbe solo il caso $n_r = pq$. Studio allora n_q:

$$\underbrace{n_q \mid pr \qquad n_q \equiv 1 \ (q)} \longrightarrow n_q = \begin{matrix} 1 \\ p \\ r \\ pr \end{matrix}$$

Se non fosse $n_q = 1$ sarebbe $n_q = 1 + sq$ con $k \geq 1$ e dunque $\underbrace{n_q > q > p}$.

da questo escludo $n_q = p$

Restano $n_q = \begin{matrix} r \\ pr \end{matrix}$

In G ci sarebbero come minimo $\overset{\#\,q\text{-Sylow}}{r}\underset{\#\text{el di ord } q \text{ in ogni } q\text{-Sylow}}{(q-1)}$ elementi di ordine q.

Allora in G complessivamente avrei:

$$\underbrace{pq(r-1)}_{\text{el. di ord. } r} + \underbrace{n_q(q-1)}_{\text{el. di ord. } q} \geq pq(r-1) + r(q-1) = pqr - \underbrace{pq + rq - r}$$

1 Noto che: $qr - pq - r > qr - \overset{>pq}{pr} - r$ $\quad r(q-p-1)$

2 $> \underbrace{pqr}_{|G|} + \underbrace{r(q-p-1)}_{\geq 0}$

e devo ancora aggiungere gli elementi di ordine p ↯

Sicuramente non va bene neanche $n_q = pr$ perché $pr > r$

Deve dunque essere $n_q = 1 \Rightarrow N_q \trianglelefteq G$

$G/_{N_q} = \overline{G}$ gruppo di $\# = pr \qquad \dfrac{|G|}{|N_q|} = \dfrac{pqr}{q} = pr$

In $\overline{G}$ esiste $\overline{H}$ r-Sylow ed è normale perché ha indice $\overset{\text{più piccolo primo che divide } |G|}{\overset{\shortparallel}{p}}$.

CONSIDERO $\pi: G \longrightarrow \overline{G} = G/N_q$ surgettiva, $\pi^{-1}(\overline{H}) < G$ e, come sappiamo dal Teorema di corrispondenza, $\pi^{-1}(\overline{H})$ ha rq elementi. Sappiamo anche che $\pi^{-1}(\overline{H}) \triangleleft G$.

Dentro $\pi^{-1}(\overline{H})$ c'è un r-Sylow R. Vale che $R \triangleleft \pi^{-1}(\overline{H})$ perché ha indice q. Inoltre, da Sylow II, sappiamo che è l'unico sottogruppo di $\pi^{-1}(\overline{H})$ di ordine r. Allora osservo che:

- $gRg^{-1} \subseteq \pi^{-1}(\overline{H})$ per la normalità di $\pi^{-1}(\overline{H})$ in G;
- $gRg^{-1} = R$ perché in $\pi^{-1}(\overline{H})$ ho un unico sottogruppo di ordine r.

In conclusione, abbiamo dimostrato che $\forall g \in G \quad gRg^{-1} = R$, cioè $\underbrace{R \triangleleft G}_{\downarrow}$. ASSURDO ↯ (eravamo nel caso $n_r = pq$)

se $K \triangleleft H$ e $H \triangleleft G$ non è detto che $K \triangleleft G$ (esempio: $G = S_4$, $H = \text{Klein}$, $K = \{e, (12)\}$)

ma se K è caratteristico in H e $H \triangleleft G$, allora vale $K \triangleleft G$.

Ricordiamo a tal proposito che un sottogruppo M di un gruppo L si dice caratteristico se $\forall \varphi \in \text{Aut}(L) \ \varphi(M) = M$.

"VIAGGIO NEI GRUPPI DI ORDINE 24"

Capitolo 1: Se $n_2 \neq 1$ e $n_3 \neq 1$, allora $G \cong S_4$. Infatti $n_3 \mid 8$ e $n_3 \equiv 1 \ (3)$ $\Rightarrow$ visto che $n_3 \neq 1$, vale $n_3 = 4$. Sia $X = \{P_1, P_2, P_3, P_4\}$ l'insieme dei 3-Sylow: G agisce su X per coniugio. $\longrightarrow$ $G \times X \longrightarrow X$, $(g, P_i) \longmapsto gP_ig^{-1}$

$\Gamma.\ G \longrightarrow \text{Big}(X) \cong S_4$, basta osservare che Γ è iniettivo:

$g \longmapsto e$ devo studiare questi g per capire chi è $\text{Ker}\,\Gamma$

Sono i g tali che ho $gP_1g^{-1} = P_1$, $gP_2g^{-1} = P_2$ e così via

$\text{Ker}\,\Gamma = \bigcap_{i=1}^{4} N(P_i)$. $\Rightarrow g \in \text{Ker}\,\Gamma \Leftrightarrow g \in N(P_1) \cap \ldots \cap N(P_2)$

Per Sylow II, $|N(P_1)| = |N(P_2)| = |N(P_3)| = |N(P_4)| = \dfrac{|G|}{\underset{n_3}{\overset{\parallel}{4}}} = 6 \Rightarrow \#\text{Ker}\,\Gamma \mid 6$.

↳ sono tutti coniugati

↳ #orb $\Rightarrow$ c'è un'unica orbita

27-10-2021 Lezione 13 Prof. Gaiffi

Ricapitoliamo: M gruppo abeliano finit. generato, $m_1, m_2, \ldots, m_n$

$\Phi: \mathbb{Z}^n \longrightarrow M$

$(a_1, a_n) \longmapsto a_1m_1 + a_2m_2 + \ldots + a_nm_n$

surgettivo

$0 \to \text{Ker}\,\Phi \xrightarrow{i} \mathbb{Z}^n \to M \to 0$

$M \cong \mathbb{Z}^n / \underset{\text{gruppo abeliano libero}}{\text{Ker}\,\Phi}$

Esempio Sia $n=3$

$$\operatorname{Ker}\varphi = \operatorname{Span}_{\mathbb{Z}}\left(\begin{pmatrix}2\\4\\2\end{pmatrix}, \begin{pmatrix}0\\4\\4\end{pmatrix}, \begin{pmatrix}0\\2\\8\end{pmatrix}\right)$$

$$\begin{pmatrix}2&0&0\\4&4&2\\2&4&8\end{pmatrix}$$

Voglio fare una mossa di riga intera su questa matrice

se $\det M = \pm 1$
$\Rightarrow$ M a coef. in $\mathbb{Z}$
+ M invertibile

$$\begin{pmatrix}1\\0\\0\end{pmatrix} \begin{pmatrix}0\\1\\0\end{pmatrix} \begin{pmatrix}0\\0\\1\end{pmatrix}$$

Base canonica

Fare una mossa di riga INTERA corrisponde a moltipeicare a sinistra per una matrice invertibile a coefficienti interi (e con inversa a coefficienti interi).

Cambiamenti di base

esempi:

$$\begin{pmatrix}1 & & 7\\ & \ddots & \\ & & 1\end{pmatrix}$$

$$\begin{pmatrix}1 &&&&& \\ &1&&&& \\ &&0&1&& \\ &&1&0&& \\ &&&&1& \\ &&&&&1\end{pmatrix}$$

$$\begin{pmatrix}1 &&&&& \\ &1&&&& \\ &&-1&&& \\ &&&1&& \\ &&&&1& \\ &&&&&1\end{pmatrix}$$

Cambiamenti di base (in arrivo)
⇕
Fare mosse di riga intere

Cambiamento di base (in partenza)
⇕
Fare mosse di colonne intere

$\mathbb{Z}_3 \to \mathbb{Z}_3$

$$\begin{pmatrix}2&0&0\\4&4&2\\2&4&8\end{pmatrix} \xrightarrow{\substack{R_2 \leftrightarrow R_2-2R_1 \\ R_3 \leftrightarrow R_3-R_1}} \begin{pmatrix}2&0&0\\0&4&2\\0&4&8\end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix}2&0&0\\0&2&4\\0&8&4\end{pmatrix} \xrightarrow{C_3 \leftrightarrow C_3-2C_2} \begin{pmatrix}2&0&0\\0&2&0\\0&8&-12\end{pmatrix} \xrightarrow[R_3 \leftrightarrow -R_3]{R_3 \leftrightarrow R_3-4R_2} \begin{pmatrix}2&0&0\\0&2&0\\0&0&12\end{pmatrix}$$

Dunque nella nuova base di $\mathbb{Z}^3$ in arrivo,

$\operatorname{Ker}\phi = \operatorname{Span}_{\mathbb{Z}}\left(\begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\0\\12\end{pmatrix}\right)$. Dunque $M \cong \mathbb{Z}^3/\operatorname{Ker}\phi \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$

Teorema Data una matrice L $t \times s$ e coefficienti interi di rango h è possibile attraverso una sequenza di mosse intere di riga o di colonna, trasformarla nelle matrici L' tale che

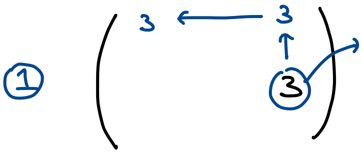
$L'_{ij} = 0$ se $i \neq j$ e poi $L'_{ii} > 0$ se $i \leq h$

diagonale

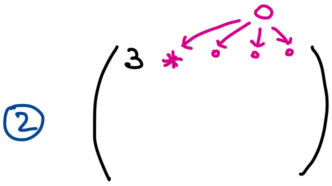
$L'_{ii} = 0$ se $i > h$ → mantiene il rango

$L'_{11} = \mathrm{MCD}(L_{ij})$ ⟶ $L'_{11} \mid L'_{22} \mid L'_{33} \mid \dots \mid L'_{hh}$

Traccia della dimostrazione:

①


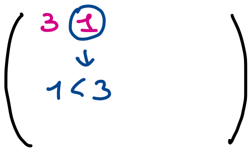
numero più piccolo

②


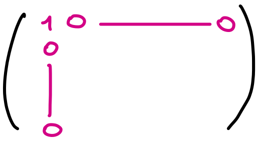
ho due casi:

- $3 \mid *$ ⇒ sostituisco $*$ con 0 (tramite mosse di Gauss)
- $3 \nmid *$ ⇒ $* = 3q + r$ ⇒ sostituisco $*$ con r

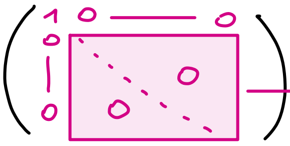
↓ esempio: $* = 7$



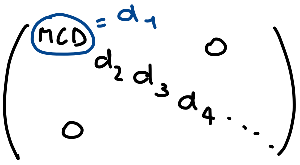
Avevamo che 3 era il minimo dei coef. della matrice, ma abbiamo trovato $r = 1 < 3$ dunque ripeto il passo ① e pongo 1 in pos. 1, 1



- $1 \nmid 3$ ⇒ dovrei procedere come prima ma $1 \mid 3$
- $1 \mid 3$ ⇒ faccio mosse di Gauss per ottere 0 al posto di 3



agisco sulla sottomatrice iterando il procedimento e per hp induttiva so che la stmat. è a coef. in $\mathbb{Z}$



$d_2 \mid d_3 \mid \quad \mid d_n$ e $d_1 \mid d_2$ ottengo la matrice cercata

Si chiama FORMA DI SMITH di una matrice a coefficienti in $\mathbb{Z}$.

Teorema

Sia M gruppo abeliano finitamente generato

a) Vale che $M \cong \overset{\text{parte libera}}{\mathbb{Z}^K}$ con $K \geq 0$ oppure $M \cong \mathbb{Z}^K \oplus \overset{\text{parte di torsione}}{\boxed{\bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}}}$ dove $K \geq 0$,

d_i INTERI ≥ 2 e se $i<j$ vale che $d_i \mid d_j$ ⇒ $d_1 = \text{MCD}(d_i)$

esempio:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathbb{Z}^5 / \overset{\text{generato dallo Span delle colonne}}{\text{Ker}\,\phi} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}^2$$

$\mathbb{Z}^5 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}$ OMOMORFISMO

$$(a_1, -, a_5) \mapsto ([a_1]_2, [a_2]_4, [a_3]_4, a_4, a_5)$$

b) I numeri $k, d_1, \ , d_r$ SONO UNIVOCAMENTE DETERMINATI

a) Dimostrato con FN di Smith

b) Da dimostrare

La parte $\bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$ può essere presentata anche in un altro modo.

Esempio: $6 = 2 \cdot 3$ $12 = 2^2 \cdot 3$ $48 = 2^4 \cdot 3$

$$\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{48}$$
$$\downarrow$$
$$\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{16} \times \mathbb{Z}_3}_{\text{p-Sylow}}$$
$$\downarrow$$
$$(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{16}) \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)$$

Nota Un gruppo abeliano finito è prodotto dei suoi p-Sylow.

Esempio di una presentazione di un 5-Sylow:

$$\mathbb{Z}_{5^2} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_{5^3} \times \mathbb{Z}_{5^7}$$

ESEMPIO $(\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_{7^2} \times \mathbb{Z}_{7^3}) \times (\mathbb{Z}_{11^4} \times \mathbb{Z}_{11^6})$ scrittura in p-Sylow

$$\Downarrow$$

$$\mathbb{Z}_2 \times \mathbb{Z}_{2^2 \cdot 7^2 \cdot 11^4} \times \mathbb{Z}_{2^2 \cdot 7^3 \cdot 11^6}$$

1) prendo i più grandi
2) prendo i "medi"
3) prendo i più piccoli

$$\Downarrow$$

$$\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{7^2} \times \mathbb{Z}_{11^4} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{7^3} \times \mathbb{Z}_{11^6}$$ scrittura in parte di torsione

Per dimostrare la parte b del teorema basta dimostrare:

Lemma Sia A un gruppo abeliano finito di ordine p^a con p primo e $a \geq 1$. Supponiamo che $A \cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times .. \times \mathbb{Z}_{p^{\alpha_j}}$ con $1 \leq \alpha_1 \leq \ldots \leq \alpha_j$ e anche che $A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \ldots \times \mathbb{Z}_{p^{\beta_h}}$ con $1 \leq \beta_1 \leq \beta_2 \leq \ldots \leq \beta_h$.

Allora $j = h$ e $\alpha_i = \beta_i$ $\forall i = 1, -, h$.

Dim Contando gli elementi di ordine $\leq p$ deduco subito che $j = h$. ↗ Nella 1^a ho p^{α_j}, nella seconda p^{β_h} ↘

$$A \cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times .. \times \mathbb{Z}_{p^{\alpha_u}} \times \ldots \times \mathbb{Z}_{p^{\alpha_h}} \qquad A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \ldots \times \mathbb{Z}_{p^{\beta_u}} \times \ldots \times \mathbb{Z}_{p^{\beta_h}}$$

Supponiamo che u sia il minimo tc $\beta_u \neq \alpha_u$. (Per esempio $\alpha_u > \beta_u$)

Considero il sottogruppo di A dato da $p^{\beta_u} A$.

$$p^{\beta_u} a_1 + p^{\beta_u} a_2 = p^{\beta_u}(a_1 + a_2)$$

$$H \cong 0 \times 0 \times \dots \times \mathbb{Z}_{p^{\alpha_u - \beta_u}} \times \dots \times \mathbb{Z}_{p^{\alpha_h - \beta_u}}$$

$$H \cong 0 \times 0 \times \dots \times \mathbb{Z}_{p^{\beta_h - \beta_u}}$$

Si ottiene un assurdo contando gli elementi di ordine $\leq p$ di H.

K (= rango) è unico:

$$A \cong \mathbb{Z}^K \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

$$A \cong \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{c_i}$$

ϕ iso: $\mathbb{Z}^K \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \to \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{c_i}$

PRIMA OSSERVAZIONE: $\mathbb{Z}^K \hookrightarrow \mathbb{Z}^K \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \xrightarrow{\phi} \mathbb{Z}^s \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \xrightarrow{\pi} \mathbb{Z}^s$ (FINIRE DALLE DISPENSE)

Riprendiamo dalla scorsa volta:

$|\text{Ker}\,\Gamma|$ deve dividere 6

- Se fosse $|\text{Ker}\,\Gamma| = 3$

sempre nei gruppi di ordine 6

$\text{Ker}\,\Gamma \subseteq N(P_1)$ che ha 6 elementi dunque ha un unico 3-Sylow, che è Ker Γ ed è anche P_1.

normalizzatore del p-Sylow

$\text{Ker}\,\Gamma \subseteq N(P_2)$ che ha 6 elementi dunque ha un unico 3-Sylow di Ker Γ ed anche P_2. ASSURDO ($P_1 = \text{Ker}\,\Gamma = P_2$ ma $P_i \neq P_j$ per $i \neq j$)

- Se fosse $|\text{Ker}\,\Gamma| = 6$ avrei:

$$\text{Ker}\,\Gamma = \underbrace{N(P_1)}_{\text{ha un unico 3-Sylow: } P_1} = \underbrace{N(P_2)}_{\dots P_2} = \underbrace{N(P_3)}_{\dots P_3} = \underbrace{N(P_4)}_{\dots P_4} \Rightarrow ↯$$

- Se fosse $|\text{Ker}\,\Gamma| = 2$ allora $\text{Ker}\,\Gamma = \}e, x\{$ con x di ordine 2.

OSS $x \in Z(G)$ perché $\text{Ker}\,\Gamma \triangleleft G \Rightarrow gxg^{-1} \in \text{Ker}\,\Gamma \quad \forall g \in G$

$$gxg^{-1} \begin{array}{l} \nearrow e \to gxg^{-1} = e \to x = geg^{-1} \to x = e \quad \text{ASSURDO} \\ \searrow x \to \forall g \in G \quad gxg^{-1} = x \end{array}$$

Allora contiamo in G gli elementi di ordine 3, stanno in P_1, P_2, P_3, P_4.

Sono $2 \cdot 4 = 8$. Sia y uno di questi 8 elementi di ordine 3

ha ordine 2 perché $\# \operatorname{Ker} \Gamma = 2$

Considero $y\boxed{x}$: ha ordine 6. Posso quindi produrre 8 elementi di ordine 6.

In G restano dunque $24 - 8 - 8 = 8$ elementi di ordine $\neq 3, 6$, quindi per Sylow I questi 8 elementi devono costituire l'unico 2-Sylow possibile ma questo è assurdo perché avevamo posto $n_2 \neq 1$.

- In conclusione, $|\operatorname{Ker} \Gamma| = 1$, cioè $\operatorname{Ker} \Gamma = \{e\}$, cioè Γ è iniettiva.

$\Rightarrow G \cong \operatorname{Im} \Gamma < S_4 \Rightarrow G \cong S_4$

28 - 10 - 2021 lezione 14 Prof. Gaiffi

Capitolo 2: I prodotti del tipo $G \rtimes \mathbb{Z}_3$ con $|G| = 8$

Se $n_2 = 1$ oppure $n_3 = 1$ si vede subito che G (di ordine 24) è prodotto semidiretto dei suoi Sylow. Studiamo il caso $n_2 = 1$.

$$N_2 \cong \begin{cases} \mathbb{Z}_8 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \\ \mathbb{Z}_2^3 \\ D_4 \\ Q_8 \end{cases} \quad e \quad N_3 \cong \mathbb{Z}_3 \text{ sempre}$$

Cominciamo con $\mathbb{Z}_8 \rtimes_\tau \mathbb{Z}_3$:

$$\tau : \mathbb{Z}_3 \longrightarrow \operatorname{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$1 \longmapsto (0,0) \rightarrow \text{unico elem. di ord che divide } 3$$

↳ ha ordine 3

esiste solo il τ banale allora $G \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \cong \mathbb{Z}_{24}$

Studio adesso $\mathbb{Z}_{2^3} \rtimes_\tau \mathbb{Z}_3$:

$$\tau : \mathbb{Z}_3 \longrightarrow \operatorname{Aut}(\mathbb{Z}_{2^3}) \cong GL(3, \mathbb{Z}_2)$$

$$1 \longmapsto M$$

$|GL(3, \mathbb{Z}_2)| =$
$(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$
$3 | 168 \Rightarrow \exists$ elem. di ord 3

in questo caso avrei τ BAN

dove $M^3 = Id$ e $M \neq Id$, $M^3 - I = 0 \rightarrow (M - I)(M^2 + M + I) = 0$

Sia f un'applicazione lineare associata ad M.

$(f - I)(f^2 + f + I) = 0$, allora vale che $\operatorname{Ker}(f - I) \oplus \operatorname{Ker}(f^2 + f + I) \cong \mathbb{Z}_2^3$

perché $(t-1)$ e (t^2+t+1) sono primi tra loro in $\mathbb{Z}_2[t]$

↳ irriducibile in $\mathbb{Z}_2[t]$

Per Bezout:

$$\lambda(t)(t-1)+\mu(t)(t^2+t+1)=1 \Rightarrow \lambda(f)(f-I)+\mu(f)(f^2+f+I)=I_d \Rightarrow$$

$$\Rightarrow \underbrace{\lambda(f)(f-I)v}_{\in Ker(f^2+f+I)}+\underbrace{\mu(f)(f^2+f+I)v}_{\in Ker(f-I)}=v$$

Può succedere $Ker(f^2+f+I)=\{0\}$? NO perché altrimenti $Ker(f-I)=\mathbb{Z}_2^3$ e dunque $f=I$ mentre $M\neq I$. Quindi $\exists\, w\in Ker(f^2+f+I)$ tale che $w\neq 0$. Considero $f(w)$ e noto che $w, f(w)$ sono linearmente INDIPENDENTI ($f(w)$ dovrebbe altrimenti essere un multiplo di w ma $f(w)\neq 0$ perché f è invertibile, $f(w)\neq w$ altrimenti $w\in Ker(f-I)\}$)

Scelgo per completamento una base $u, w, f(w)$ di $\mathbb{Z}_2^3$.

↳ identifica i vari prodotti semidiretti

$$\begin{array}{ccc} f(u) & f(w) & f(f(w)) \\ \end{array}$$
$$\begin{pmatrix} a & 0 & 0 \\ b & 0 & 1 \\ c & 1 & 1 \end{pmatrix}$$

↳ perché: $f^2+f+I=0$, $f^2(w)+f(w)+I=0$

$$\Rightarrow f^2w=-f(w)-I(w)=-f(w)-w \overset{\text{in } \mathbb{Z}_2}{=} f(w)+w$$

↳ va nel 3° elemento della base

Ma f è invertibile, dunque deve essere $a=1$

perché ho:

$$\det\begin{pmatrix} a & 0 & 0 \\ b & 0 & 1 \\ c & 1 & 1 \end{pmatrix}=0(b-c)+0(a-0)+1(a-0\cdot b)=a\overset{\text{invertibile}}{\neq}0$$

ma siamo in $\mathbb{Z}$ quindi: $a=1$

Quindi ottengo: $\begin{pmatrix} 1 & 0 & 0 \\ b & 0 & 1 \\ c & 1 & 1 \end{pmatrix}$

$\det(M-t\,Id)=(1-t)(t^2-t+1)$

Guardando il polinomio caratteristico si vede che 1 è autovalore.

Scelgo allora al posto di u un autovettore u' di autovalore 1.

$\underbrace{u'}_{\in Ker(f-Id)}, \underbrace{w, f(w)}_{\in Ker(f^2+f+Id)}$ quindi, rispetto questa base, ottengo la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

Quindi, a meno di coniugio posso immaginare che $\tau(1)=$

Per la Proposizione ho che $\alpha\circ\tau_2(K)\circ\alpha^{-1}=\tau_1(\beta(K))$ esiste dunque, a meno di isomorfismo un solo prodotto semidiretto del tipo $\mathbb{Z}_2^3\rtimes_\tau\mathbb{Z}_3$.

Troviamo questo gruppo:

Considero $\mathbb{Z}_2 \times A_4$ $(\# = 24)$

$\mathbb{Z}_2 \times \text{Klein} < \mathbb{Z}_2 \times A_4$

Dunque $\mathbb{Z}_2 \times$ Klein è un 2-Sylow ed è isomorfo a $\mathbb{Z}_2^3$.

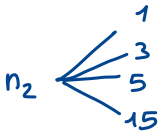
Contando gli ordini vedo che esistono in $\mathbb{Z}_2 \times A_4$ esattamente 8 elementi di ordine ≤ 2 e quindi l'unico 2-Sylow è $\mathbb{Z}_2 \times$ Klein.

Perciò $\mathbb{Z}_2 \times A_4$ è proprio il gruppo descritto.

Esercizio Ogni gruppo semplice di ordine 60 ha un sgrp di ordine 12.

Sol $n_5 > 1$ (per semplicità) $\Rightarrow n_5 = 6$

Ci sono dunque 24 elementi di ordine 5 $(= 6 \cdot (5 - \overset{\text{id}}{1}))$



No per semplicità

Se fosse $n_2 = 15$, $B_1, B_2, \dots, B_{15}$ i 2-Sylow.

Se fosse $B_i \cap B_j = \{e\}$ $\forall i \neq j$ avrei $\underset{\overset{\parallel}{15\,(4-1)}}{45}$ elementi di ordine 2 o 4 e $|G| = 24 + 45 + 1 \dots$ ↯

Esistono dunque i e j tc $|B_i \cap B_j| = 2$. Considero $N(B_i \cap B_j)$

$B_i \cap B_j \triangleleft B_i$ (ha indice 2)

$B_i \cap B_j \triangleleft B_j$ $(|B_i| = 2^2 \Rightarrow B_i$ è abeliano$)$

Allora $B_i < N(B_i \cap B_j)$

$B_j < N(B_i \cap B_j)$

Allora anche $\underbrace{B_i B_j}_{\text{prodotto di insiemi}} \subseteq N(B_i \cap B_j)$

Ma $|B_i B_j| = \dfrac{4 \cdot 4}{2} = 8$

Dunque so che $8 \leq |N(B_i \cap B_j)| \mid 60$ e $4 \mid |N(B_i \cap B_j)|$ perché $B_i < N(B_i \cap B_j)$: ~~8~~, 12, ~~16~~, 20, ~~24~~, ~~28~~, ~~32~~, ~~36~~, ~~40~~, ~~...~~, 60

Restano 12, 20, 60

NO perché sarebbe che $N(B_i \cap B_j) = G$ cioè $B_i \cap B_j \triangleleft \overset{\text{semplice}}{\boxed{G}}$ ↯

NO perché se così fosse avrei:

$G \curvearrowright G/N(B_i \cap B_j)$ e ho un omo

$\Gamma : G \to \text{Big}(^{G}/_{N(B_i \cap B_j)}) \cong S_3$ $\to \text{Ker}\,\Gamma \triangleleft G \Rightarrow \text{Ker}\,\Gamma = \{e\} \vee G$

$\overset{\parallel}{60/20} = 3$

$\mathrm{Ker}\,\Gamma \neq G$ perché devo "muovere" qualcosa, deve essere $\mathrm{Ker}\,\Gamma = \{e\}$

Ma quindi Γ è iniettiva $\Rightarrow |G| = 60 \nmid 6 = |S_3|$ ↯

⌜**Teorema dell'indice**

Se in un gruppo G c'è un sgruppo H di indice h tale che $|G| \nmid h!$ allora G non è semplice.

$G \curvearrowright G/H$ quindi $\exists$ l'omo $\Gamma : G \to \mathrm{Big}(G/H) \cong S_h$

se G è semplice $\Rightarrow \Gamma(G) \cong G$ perché $\mathrm{Ker}\,\Gamma = \{e\}$

Per il Teo di omo ho: $G \cong \Gamma(G) < S_h$ e quindi $|G| \mid |S_h| = h!$ ⌟

Quindi $|N(B_i \cap B_j)| = 12 \Rightarrow$ sgrp di ordine 12

Se invece $n_2 = 3$ o $n_2 = 5$. Prendo N_2 un 2-Sylow. Allora $|N(N_2)| = \frac{|G|}{n_2} = \frac{60}{n_2}$

$$\begin{tikzcd} & 20 \\ {} \arrow[ur] \arrow[dr] & & \neq \underset{|N_2|}{\overset{\|}{4}} \\ & 12 \end{tikzcd}$$

Dato che $N_2 < N(N_2)$ vale che $4 \mid |N(N_2)| \mid 60$

$|N(N_2)| = \cancel{8}, 12, \cancel{18}, \cancel{20}, \cancel{24}, \cancel{28}, \cancel{32}, \cancel{\dots}, \cancel{60}$ esattamente come prima si conclude $|N(N_2)| = 12$

ES Se G è semplice di ordine 60 allora $G \cong A_5$ ☐

Sol: Prendo $H < G$, $|H| = 12$ so che esiste per l'es precedente

$G \curvearrowright G/H$

$\Gamma : G \to \mathrm{Big}(G/H) \cong S_5$

$\mathrm{Ker}\,\Gamma = \{e\}$ perché G è semplice. Dunque $\Gamma(G)$ ha 60 elementi ed è $\Gamma(G) < S_5$. Dunque

- $\Gamma(G) \leqslant A_5$ nel qual caso $\Gamma(G) = \textcircled{A_5} \to$ semplice!
- $|\Gamma(G) \cap A_5| = 30$ ↯↯ perché sarebbe un sgrp normale sia di $\Gamma(G)$ che di A_5 (indice 2) ma sono entrambi gruppi semplici!

$\Rightarrow G \cong A_5$

Esercizio Quali sono i gruppi del tipo $\mathbb{Z}_4 \rtimes_\tau \mathbb{Z}_4$?

$\tau : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$

$$\begin{tikzcd} & {} \arrow[r, "\tau_{\mathrm{ban}}"] & 0 \\ 1 \arrow[ur] \arrow[dr] \\ & {} \arrow[r, "\tau_1"] & 1 \end{tikzcd}$$

$0 \to$ prodotto diretto $\mathbb{Z}_4 \times \mathbb{Z}_4$.

Considero dunque $\mathbb{Z}_4 \rtimes_{\tau_1} \mathbb{Z}_4$ ha ordine 16

generatori $\begin{cases} x = (1,0) \\ y = (0,1) \end{cases}$

$x^4 = (0,0) \qquad x^4 = e$

$y^4 = (0,0) \qquad y^4 = e$

Mi interessa sapere quanto vale yxy^{-1}

$x^a y^b \leftrightarrow (a,b)$ notazione

$yx = (0,1)(1,0) = (0 + \underset{\swarrow\ \in \mathrm{Aut}(\mathbb{Z}_4) \text{ è } -\mathrm{Id}}{\tau_1}(1)(1), 1+0) = (-1, 1) = x^{-1}y$

Dunque $yxy^{-1} = x^{-1}$.

La penso in un altro modo

$yx = \underbrace{yx^{-1}y^{-1}}_{\in (x) \text{ perché } (x) \text{ è normale}} y$

Dunque il nostro gruppo $G = \mathbb{Z}_4 \rtimes_{\tau_1} \mathbb{Z}_4$ è generato da x, y con le relazioni:

$x^4 = e$, $y^4 = e$, $yxy^{-1} = x^{-1}$

DOMANDE:

① Chi è il centro? Risposta: (x^2, y^2)

② Chi è $G/(x^2)$?

③ Chi è $G/(y^2)$?

④ Chi è $G/(x^2y^2)$?

29-10-2021 lezione 15 Prof. Callegaro

CLASSIFICAZIONE DEI GRUPPI DI ORDINE 8

$|G| = 8$, togliamo il caso in cui ho $g \in G$ tc $\mathrm{ord}(g) = 8$ (avrei $\mathbb{Z}_8$)

Consideriamo allora il caso in cui $\exists x \in G$ tc $\mathrm{ord}(x) = 4$ e inoltre,

→ tutti gli elem. di ordine 2 stanno in $<x>$

$\nexists y \notin <x>, \mathrm{ord}(y) = 2 \Rightarrow \exists z \notin <x>$ tc $\mathrm{ord}(z) = 4$ abbiamo già visto i casi in cui $y \notin <x>$

non può avere ordine 1 o 2

Dunque ho: $e, x, x^2, x^3,$

$z, \underset{\underset{x^2}{\shortparallel}}{z^2}, z^3$ → ne mancano 2

$xz \in <x>$? NO ($z \in <x>$ ↯)

$xz \in \langle z \rangle$? NO ($x \in \langle z \rangle$ $\lightning$)

Ho trovato un nuovo elemento $\Rightarrow$ $\text{ord}(xz) = 4$ (non può avere ordine 1 o 2)

$(xz), (xz)^2 = x^2, (xz)^3$ → li ho trovati tutti, sono un gruppo?

Chiamo questi elementi $\underset{\underset{x}{\shortparallel}}{i}, \underset{\underset{z}{\shortparallel}}{j}, \underset{\underset{xz}{\shortparallel}}{K}$ e guardo come si comportano:

- $i \cdot j = K$
- $i^2 = j^2 = K^2 = -1$
- $i^3 = -i, \; j^3 = -j, \; K^3 = -K$

(NB) $\langle i \rangle, \langle j \rangle, \langle K \rangle$ sono ciclici, quindi sono abeliani, quindi l'unico elemento di ordine 2 commuta con tutti gli elementi perché $\in \langle i \rangle \cap \langle j \rangle \cap \langle K \rangle$

$$\Downarrow$$

$$Z(G) = \}1, -1\{$$

$\}1, i, j, K, -1, -i, -j, -K\{$ → 8 elementi

- Chi è $(ij)^{-1}$?

$(ji)(ij) = j(-1)j = -j^2 = 1$

Quindi scopro che: $(ji) = (\overset{K}{\widetilde{ij}})^{-1} = -K$

- Studiamo jk: $\quad jK = jij = -Kj = -ijj = -ij^2 = -i(-1) = i$
- Analogamente scopriamo: $Kj = -i \;, \; Ki = j \;, \; iK = -j$

Quello che otteniamo viene detto gruppo dei quaternioni Q_8

Ha 6 elementi di ordine 4, 1 di ordine 2 e 1 di ordine 1.

Per visualizzarlo: unità immaginaria

$GL(2, \mathbb{C})$

$$\begin{tikzcd} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \arrow[d, "2"', "\text{al quadrato}"] & , & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \arrow[d, "2", "\text{al quadrato}"'] \\ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} & , & \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \end{tikzcd}$$

generano un gruppo iso a Q_8

Automorfismi di gruppi di ordine 8

- $\text{Aut}(\mathbb{Z}_2^{\,3}) \cong GL(3, \mathbb{F}_2)$

$\mathbb{Z}_2$ è un campo → $\mathbb{Z}_2^{\,3}$ è spazio vettoriale → sono gli aut. dello sp. vett.

$|GL(3, \mathbb{F}_2)| = 7 \cdot 6 \cdot 4 = 168$

devo "togliere":

$$\begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix} \quad \left.\begin{array}{l} 8-1 \text{ scelte} \\ 8-2 \text{ scelte} \\ 8-4 \text{ scelte} \end{array}\right\} \; (\underset{\underset{\text{dim } 0}{\downarrow}}{\overset{\overset{\text{un punto}}{\uparrow}}{2^3-1}})(\underset{\underset{\text{dim } 1}{\downarrow}}{\overset{\overset{\text{una retta}}{\uparrow}}{2^3-2}})(\underset{\underset{\text{dim } 2}{\downarrow}}{\overset{\overset{\text{un piano}}{\uparrow}}{2^3-2^2}})$$

- $\text{Aut}(\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_4})$

$$\#\text{ elem di ordine } \leq 2 = 2 \cdot 2 = 4 \begin{cases} (0,0) \to \text{ord } 1 \\ \left.\begin{array}{l} (0,2) \\ (1,2) \\ (1,0) \end{array}\right\} \text{ord } 2 \end{cases}$$

generatore : lo posso mandare dove voglio?

$\#$ elem di ordine $= 2 = 4 - 1 = 3$

$\#$ elem di ordine $4 = 8 - 4 = 4$

$(1,0)$ non va in $(0,2)$ perché preso $x \in \mathbb{Z}_2 \times \mathbb{Z}_4$, $o(x) = 4 \Rightarrow x^2 = (0,2)$,

ma anche perché:

$\mathbb{Z}_2 \times \mathbb{Z}_4 \xrightarrow{②} \mathbb{Z}_2 \times \mathbb{Z}_4$ → manda multipli di 2 in multipli di 2

② → moltiplicazione per 2

$\text{Im } 2 = \langle (0,2) \rangle$ $\underbrace{\text{sgrp caratteristico}}$ di $\mathbb{Z}_2 \times \mathbb{Z}_4$

$G > H$ caratt. $\overset{\text{def}}{\iff}$ $\phi(H) = H \quad \forall \phi \in \text{Aut}(G)$

Contiamo gli $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4)$:

$\mathbb{Z}_2 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_4$

$(0,1) \longmapsto$ qualsiasi di ordine 4 ④ scelte

$(1,0) \longmapsto$ lo mando in uno dei due elem di ordine 2 ② scelte

8 possibili automorfismi: chi sono?

$$\begin{tikzcd}
(\mathbb{Z} \times \mathbb{Z}) \arrow[r, "\tilde{f}"] \arrow[d, "S"', "/\langle \binom{1}{0}, \binom{0}{1} \rangle"] & (\mathbb{Z} \times \mathbb{Z}) \arrow[d, "S"', "/\langle \binom{1}{0}, \binom{0}{1} \rangle"] \\
\mathbb{Z}_2 \times \mathbb{Z}_4 \arrow[r, "f"] \arrow[d, "/\langle \binom{0}{2} \rangle"'] & \mathbb{Z}_2 \times \mathbb{Z}_4 \arrow[d, "/\langle \binom{0}{2} \rangle"] \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \arrow[r, "\bar{f}"] & \mathbb{Z}_2 \times \mathbb{Z}_2
\end{tikzcd}$$

$\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_4}$ è un quoziente di $\mathbb{Z} \times \mathbb{Z}$, quindi posso fare dei "sollevamenti"

$\tilde{f}: \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2 \xrightarrow{\text{le associo una matrice}} \begin{pmatrix} \boxed{\begin{matrix} a \\ 2c \end{matrix}} & \begin{matrix} b \\ d \end{matrix} \end{pmatrix}$

garantisce che $\tilde{f}\binom{1}{0}$ ha ordine 2

a, b li considero "mod 2", $2c, d$ li considero "mod 4"

ce ne sono solo due
↑

$\bar{f} \in \text{Aut}(\mathbb{Z}_2^2) \cong S_3$ posso solo ottenere aut. di $\mathbb{Z}_2^2$ della forma $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} a & b \\ 2c & d \end{pmatrix} = \begin{pmatrix} 1 & b \\ 2c & d \end{pmatrix}$ $\quad c = 0, 1 \quad b = 0, 1$ $\quad d \equiv 1 \ (2) \quad d = 1, 3$ $\Rightarrow$ 8 matrici possibili

$\alpha = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Si nota che α e β non commutano $\Rightarrow \operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4) \cong D_4$

Esercizio Quanti sono $\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4)$ e $\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8)$?

- $\operatorname{Aut}(D_4) \rightsquigarrow \operatorname{Aut}(D_n) = ?$

$$D_n = \langle \rho, \sigma \mid \rho^2 = \sigma^n = 1 ,\ \rho\sigma\rho = \sigma^{-1} \rangle$$

Gli elementi di ordine n generano un sgrp caratteristico (indice 2)

$$f: \begin{cases} \rho \to \rho\sigma^i & i = 0, \dots, n-1 \\ \sigma \mapsto \sigma^j & (j, n) = 1 \end{cases}$$

Posso "sperare" di trovare al più $n \cdot \overbrace{\Phi(n)}^{\text{n° coprimi con n}}$ automorfismi.

Basta verificare che per ogni scelta di i, j $f: D_n \to D_n$ determina un aut.

Descrivo f su tutti gli elem. $f(\rho^a\sigma^b) = (\rho\sigma^i)^a \sigma^{bj}$ $\quad a = 0, 1,\ b = 0, \_, n-1$

Verifico che f è omo: $f(\rho^a\sigma^b) f(\rho^{a'}\sigma^{b'}) = f(\rho^a\sigma^b\rho^{a'}\sigma^{b'})$

caso $a = 0,\ a' = 0$

$$f(\sigma^b) f(\sigma^{b'}) = f(\sigma^{b+b'})$$

$$\sigma^{bj}\sigma^{b'j} = \sigma^{(b+b')j} \longrightarrow \text{ok}$$

caso $a = 0,\ a' = 1$

$$f(\sigma^b) f(\rho\sigma^{b'}) = f(\sigma^b\rho\sigma^{b'})$$

$$\sigma^{bj}\rho\sigma^{b'j} \overset{?}{=} f(\rho\sigma^{-b}\sigma^{b'})$$

$$\rho\sigma^{-bj}\sigma^i\sigma^{b'j} \Rightarrow \rho\sigma^i\sigma^{(-b+b')j}$$

$$\rho\sigma^{1\overset{\parallel}{+}(-b+b')j} \longrightarrow \text{ok}$$

Verificare: $a = 1,\ a' = 0$, $a = 1,\ a' = 1$

Vediamo che è una bigezione: basta verificare o che è in. o surg.

$\operatorname{Im} f \ni \sigma^j \ni \langle \sigma^j \rangle = \langle \sigma \rangle \Rightarrow \operatorname{Im} f = D_n$

$\operatorname{Im} f \ni \rho\sigma^i \notin \langle \sigma \rangle \Rightarrow f$ IN e SU

$$f(\rho\sigma^a) \mapsto \rho\sigma^i\sigma^{aj} = \rho\sigma^{i+aj}$$

$$\begin{array}{ccc} \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ \rotatebox{90}{$\in$} & & \\ a & \longmapsto & aj + i \end{array} \qquad j \in (\mathbb{Z}_n)^* \quad i \in \mathbb{Z}_n$$

$$\begin{tikzcd} \mathbb{R} \arrow[r] & \mathbb{R} \\ x \arrow[u, phantom, "\rotatebox{90}{$\in$}"] \arrow[r] & ax+b \end{tikzcd}$$

$a \neq 0 \quad b \in \mathbb{R}$

$\mathrm{Aut}(D_n) \simeq \mathrm{Aff}(\mathbb{Z}_n)$

$\mathrm{Aff}(\mathbb{Z}_n) \xrightarrow[\pi]{\text{omo}} (\mathbb{Z}_n)^*$

$\varphi_{i,j} \longmapsto j$

$\varphi_{i,j} : a \longmapsto ja + i$

$\mathrm{Ker}(\pi) = \mathbb{Z}_n$ (traslazioni)

$$\begin{tikzcd} \mathbb{Z}_n \arrow[r] & \mathrm{Aff}(\mathbb{Z}_n) \arrow[r] & (\mathbb{Z}_n)^* \arrow[l, bend left] \end{tikzcd}$$

$\varphi_{i,j} \longmapsto j$

$\varphi_{0,j} \xleftarrow[\text{omo}]{} j \qquad \varphi_{0j}(a) = aj$

quindi $\mathrm{Aut}(D_n) \cong \mathrm{Aff}(\mathbb{Z}_n) \cong \mathbb{Z}_n \rtimes (\mathbb{Z}_n)^*$

come agisce $(\mathbb{Z}_n)^*$ su $\mathbb{Z}_n$?

$\varphi_{0,j}^{-1}\, \varphi_{i,1}\, \varphi_{0j}$

$a \xmapsto[\varphi_{0j}]{} aj \xmapsto[\varphi_{i,1}]{} aj + i \xmapsto[\varphi_{0j}^{-1}]{} a + ki$

sia $k \in (\mathbb{Z}_n)^*$ tc $kj = 1$

Quindi $(\mathbb{Z}_n)^*$ agisce su $\mathbb{Z}_n$ per moltiplicazione

[$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & G \arrow[r] & H \arrow[r] \arrow[l, bend left, "\text{omo}"] & 0 \end{tikzcd}$$ successione esatta corta di gruppi non abe

equivale a dire $G = N \rtimes H$. Posso far agire $H\ (\subset G)$ su $N\ (\subset G)$ per coniugio :

$$\begin{tikzcd} N \rtimes H \\ (n, h) \arrow[u, phantom, "\rotatebox{90}{$\in$}"] \arrow[d, mapsto] \\ i(n)s(h) \\ G \arrow[u, phantom, "\rotatebox{-90}{$\in$}"] \end{tikzcd}$$

Per esercizio: Verificare che se definisco questo prodotto semidiretto usando l'azione per coniugio di H su N, il prodotto coincide con quello in G.

]

04-11-2021 Lezione 16 Prof. Gaiffi

ESTENSIONE DI CAMPI: $F \subseteq K$ ⇝ $\underbrace{\mathrm{Aut}(K/F)}_{\text{Studieremo questo gruppo}}$ GRUPPO CHE LASCIA FISSO K

ESEMPIO: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$

aggiunge 2 elem: $-\sqrt{2}$ $\sqrt{2}$

Un automorfismo $f(x)$ manderà radici di un polinomio in radici

Si troverà un sottocampo in una certa estensione

~ o ~

(Vedi capitolo 14, Paragrafo 2 dispense di Aritmetica → Fine teoria dei campi finiti)

Siano F e F' due campi. Sia $\phi: F \to F'$ iso

Chiamo $\tilde{\phi}$ l'isomorfismo di anelli:

$$\tilde{\phi}: F[x] \longrightarrow F'[x]$$

$$a_n x^n + \dots \longmapsto \phi(a_n)x^n + \dots$$

$F(a) :=$ più piccolo sotto-campo che contiene a e F

$F[a] :=$ non è sempre un campo: è un anello che è un campo $\Leftrightarrow$ a è algebrico su F

Teorema Siano F, F', ϕ come prima

Siano $F \subseteq L$ e $F' \subseteq L'$ due estensioni

sia $a \in L$ algebrico su F, con polinomio minimo $p(x)$.

Sia $a' \in L'$ una radice di $\tilde{\phi}(p(x))$

$$\begin{tikzcd} L & \overset{\text{radice } p(x)}{a} & L' & a' \to \text{radice } \tilde{\phi}(p(x)) \\ F \arrow[u, phantom, "\rotatebox{90}{$\subseteq$}"] \arrow[rr, leftrightarrow, "\text{ISO}"'] & & F' \arrow[u, phantom, "\rotatebox{90}{$\subseteq$}"] \end{tikzcd}$$

Allora esiste $\phi': F[a] \to F'[a']$ tale che $\phi'(a) = a'$ e $\phi'|_F = \phi$

Poiché a è algebrico si ha $F[a] = F(a)$

Dim:

$$\vartheta: F[x] \xrightarrow[\text{ISO}]{\tilde{\phi}} F'[x] \xrightarrow{\pi} F'[x]/(\tilde{\phi}(p(x)))$$

proiezione

$x \mapsto x \mapsto x + (\tilde{\phi}(p(x)))$

$K \in F \mapsto \phi(K) \mapsto \phi(K) + (\tilde{\phi}(p(x)))$

è un OMOMORFISMO

$\mathrm{Ker}\,\vartheta = (p(x))$ ideale generato da $p(x)$

Per il I teorema di OMO: $\vartheta': F[x]/(p(x)) \xrightarrow[\text{ISO}]{\sim} F'[x]/(\tilde{\phi}(p(x)))$

Più in dettaglio:

$$\vartheta' : x + p(x) \longmapsto x + \tilde{\phi}(p(x))$$

Inoltre $\vartheta'|_F$ coincide con ϕ

$$\begin{tikzcd}
F[x]/(p(x)) \arrow[r, phantom, "\overset{\vartheta'}{\cong}"] \arrow[r, bend left, "{[x] \to [x']}"] & F'[x]/(\tilde{\phi}(p(x))) \arrow[d, "{[a']}"] \\
F[a] \arrow[u, "\gamma := \cong", "{[x]}"'] \arrow[r, bend left] & F'[a'] \arrow[u, phantom, "\gamma' := \cong"']
\end{tikzcd}$$

$\leftarrow$ visto l'anno scorso

$\gamma(a) = x + p(x)$
$\gamma|_F = Id$

$\gamma'(a') = x + \tilde{\phi}(p(x))$
$\gamma'|_{F'} = Id$

Ripasso:

$$F[x] \longrightarrow F[a]$$
$$q(x) \longmapsto q(a)$$

Per il I teo di OMO: $F[x]/(p(x)) \overset{\wedge}{\cong} F[a]$

$$x + p(x) \longleftrightarrow a$$

L'omo richiesto è: $(\gamma')^{-1} \circ \vartheta' \circ \gamma : F[a] \to F[a']$

<u>Teorema</u> Siano F, F', ϕ come sopra

Dato $f(x) \in F[x]$ NON NULLO. Sia E un campo di spezzamento di $f(x)$ su F. Sia E' un campo di spezzamento di $\tilde{\phi}(f(x)) \in F'[x]$ su F'. Allora $\exists\ \phi'$ iso:

$$\phi' : E \longrightarrow E' \quad \text{tale che}$$
$$\phi'|_F = \phi$$

<u>Dim</u>: Per induzione su $\deg f(x)$

- $\deg f(x) = 1$ BANALE
- $\deg f(x) > 1$. Sia $g(x)$ un fattore IRRIDUCIBILE di $f(x)$.

Sia $a \in E$ una radice di $g(x)$.

Sia $a' \in E'$ " " di $\tilde{\Phi}(g(x))$.

Il Teorema dice che $\exists\ \vartheta$ ISO.

$$\vartheta : F[a] \to F'[a']$$

tale che $\vartheta(a) = a'$ e $\vartheta|_F = \phi$

$$\begin{tikzcd}
E & E' \\
F[a] \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\vartheta"] & F'[a] \arrow[u, phantom, sloped, "\subseteq"] \\
F \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\phi"] & F' \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

$\tilde{\vartheta} : F(a)[x] \to F'(a')[x]$

In $F[a][x]$ il polinomio $f(x)$ si fattorizza come:

$f(x) = (x-a)\bar{f}(x)$ con $\deg \bar{f}(x) = \deg f(x) - 1$

Applico $\tilde{\vartheta}$: $\tilde{\vartheta}(f(x)) = (x-a)\tilde{\vartheta}(\bar{f}(x))$

Per hp induttiva (considerando il polinomio $\bar{f}(x)$ e i campi base $F[a]$ e $F'[a']$) so che esiste $\phi' : E \to E'$ tale che $\phi'|_{F[a]} = \vartheta$

Noto dunque $\phi'|_F = \phi$ e ϕ' è l'ISO cercato.

□

Corollario Sia F campo e siano E e E' due campi di spezzamento di un polinomio non nullo $f(x) \in F[x]$. Allora esiste un iso $\phi' : E \to E'$ tale che $\phi'|_F = Id$.

(Vedi Capitolo 10, Dispense di Algebra)

Lemma Sia $f(x) \in F[x]$ $\quad (F[x])^* = F^*$

Se $f(x)$ ha fattori (non invertibili) multipli in $F[x]$ allora il grado di $MCD(f(x), \overset{\text{DERIVATA}}{f'(x)}) \geq 1$

Dim Scrivo $f(x) = g_1^2(x)q(x)$

$$f'(x) = 2g(x)g'(x)q(x) + g^2(x)q'(x) = g(x)[2g'(x)q(x) + g(x)q'(x)]$$

E quindi $g(x) \mid MCD(f, f')$

Teorema Sia $f(x) \in F[x]$

Allora $f(x)$ non ha fattori multipli in $E[x]$ (dove E è un cds di $f(x)$ su F) sse $MCD(f, f') = 1$

NOTA: $MCD(f, f') = 1$ in $F[x]$ sse $MCD(f, f') = 1$ in $E[x]$

Dim

⇒) sia f senza fattori multipli in $E[x]$

$$f(x) = \prod_{i=1}^{n} (x - a_i) \qquad a_i \in E \quad a_i \neq a_j$$

saltato → lo derivo

Allora $f'(x) = (x \overset{\frown}{-} a_1)(x - a_2) \cdots (x - a_n) + (x - a_1)(x \overset{\frown}{-} a_2) \cdots (x - a_n) + \ldots$

e dunque $f'(a_i) \neq 0$ $\forall i$. Dunque f e f' non hanno radici in comune in E. Se avessero un $d(x)$ in comune tale $d(x)$ avrebbe in E una radice che è comune a f e f'. Dunque $MCD(f, f') = 1$.

⇐) Sia $MCD(f, f') = 1$

Se $f(x)$ ha fattori multipli in $F[x]$ sappiamo per il lemma che $MCD(f, f')$ ha grado ≥ 1. ASSURDO.

□

Domande: Se ho un polinomio irriducibile $p(x) \in F(x)$ posso dire che $p(x)$ non ha radici multiple (in un cds E)?

Se $\text{char} F = 0$ è vero che $p(x)$ non ha radici multiple.

Infatti $MCD(p(x), p'(x)) \in \{1, p(x)\}$ perché $p(x)$ è irriducibile, ma avrei $\deg p'(x) = \deg p(x) - 1$, dunque $p(x) \nmid p'(x)$, allora $MCD(p(x), p'(x)) = 1$ e per il Teorema precedente, $p(x)$ non ha radici multiple in E.

Se $\text{char} F = p$, con p primo, cosa succede? Sia $g(x)$ un polinomio irriducibile. Il discorso qui sopra funziona a meno che $g'(x) = 0$.

Sia F un CAMPO FINITO, $\text{char} F = p$

$$g'(x) = 0 \Leftrightarrow g(x) = a_n (x^p)^n + \ldots + a_1 x^p + a_0, \text{ con } a_0, \ldots, a_n \in F$$

Sia $\mathcal{F}: F \to F$, $a \mapsto a^p$ OMO DI FROBENIUS, iniettivo. Ma F finito ⇒ $\mathcal{F}$ surgettivo, dunque è isomorfismo, allora:

$$a_n = \mathcal{F}(b_n) = b_n^p, \; a_{n-1} = \mathcal{F}(b_{n-1}) = b_{n-1}^p, \ldots, a_1 = \mathcal{F}(b_1) = b_1^p, a_0 = \mathcal{F}(b_0) = b_0^p$$

In conclusione $g(x) = b_n^p (x^p)^n + \dots + b_1^p x^p + b_0^p$

$$= b_n^p (x^n)^p + \dots + b_1^p x^p + b_0^p$$

$$= (b_n (x^n) + \dots + b_1 x + b_0)^p$$ PERCHÉ SONO IN $\mathbb{F}_p$

ASSURDO perché $g(x)$ è IRRIDUCIBILE. Anche in un campo F di char p finito accade che $g(x)$ IRRIDUCIBILE $\Rightarrow$ $g(x)$ non ha radici multiple (nel cds)

Ultima possibilità: sia F campo di char p INFINITO.

Sia $F = \mathbb{Z}_p(t) = \{ q(t)/h(t) \mid q(h),\ h(t) \in \mathbb{Z}_p(t) \text{ e } h(t) \neq 0 \}$

$\llcorner$ variabile

Prendo il polinomio $g(x) \in F[x] = \mathbb{Z}_p(t)[x]$

$$g(x) = x^p - t$$ → IRRIDUCIBILE per LEMMA DI GAUSS* + EISENSTEIN*

*) $g(x)$ è IRRID in $\mathbb{Z}_p(t)[x] \Leftrightarrow$ è IRRID in $\mathbb{Z}_p[t][x]$

*) applicato con l'irriducibile t di $\mathbb{Z}_p[t]$

Dunque $g(x) = x^p - t$ è irrid. in $F[x]$. Vale che $g'(x) = 0$

sia E un cds di $g(x)$ su $F = \mathbb{Z}_p(t)$

Sia $\alpha \in E$ una radice: $g(\alpha) = 0 \to \alpha^p - t = 0 \to \alpha^p = t$ (anche E ha caratteristica p)

Allora in $E[x]$ $g(x)$ si fattorizza come $g(x) = x^p - t = x^p - \alpha^p \overset{\downarrow}{=} (x - \alpha)^p$.

Quindi ho radici multiple in $E[x]$. Quindi questo caso NON FUNZIONA.

05-11-2021 Lezione 17 Prof. Callegaro

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, equal] & G \arrow[r, "\beta"] & K \arrow[r] \arrow[l, bend left, "\beta'"'] \arrow[d, equal] & 1 \\
1 \arrow[r] & N \arrow[r] & N \rtimes_\varphi K \arrow[r] \arrow[u, "\gamma", "\wr"'] & K \arrow[r] & 1
\end{tikzcd}$$

successione esatta corta

$\beta(\beta'(K)) = K$ β' è OMO di GRUPPI

$\hookrightarrow$ sezione

chi è $\varphi : K \to \mathrm{Aut}(N)$?

$K \in K$

$n \in N$

↗ per costruzione

$$\varphi_K : n \longrightarrow \alpha^{-1}(\beta'(\gamma\alpha(n)\beta'(K)^{-1}) \in N$$

$K n K^{-1}$ → così agisce il grp sul sgrp n.

$\varphi_n \in \mathrm{Aut}(N)$ perché il coniugio è un automorfismo

$\varphi . K \longrightarrow \mathrm{Aut}(N)$ è omo

Voglio vedere che $\varphi_K(\varphi_{K'}(n)) = \varphi_{KK'}(n)$

$\varphi_K(\varphi_{K'}(n)) = \alpha^{-1}(\beta'(K)\alpha(\varphi_{K'}(n))\beta'(K)^{-1}) = \alpha^{-1}(\beta'(K)\beta'(K')\alpha(n)\beta'(K')^{-1}\beta'(K)^{-1}) =$

$= \alpha^{-1}(\beta'(KK')\alpha(n)\beta'(KK')^{-1}) = \varphi_{KK'}(n)$ $\square$

$\gamma : N \rtimes_\varphi K \longrightarrow G$

$(n, K) \longmapsto \alpha(n)\beta'(K) \in G$

Verifica che γ è omo: prodotto in $N \rtimes K$

$\gamma((n,K_1)\cdot(n,K_2)) = \gamma(n_1\varphi_{K_1}(n_2), K_1K_2) = \alpha(n_1\varphi_{K_1}(n_2))\beta'(K_1K_2) =$

$= \alpha(n_1)\alpha(\varphi_{K_1}(n_2))\beta'(K_1)\beta'(K_2) = \alpha(n_1)\beta'(K_1)\alpha(n_2)\cancel{\beta'(K_1)^{-1}}\cancel{\beta'(K_1)}\beta'(K_2)$

$= \alpha(n_1)\beta'(K_1)\cdot\alpha(n_2)\beta'(K_3) = \gamma(n_1,K_1)\gamma(n_2,K_2) \Rightarrow \gamma$ è omo

Automorfismi di gruppi di ordine 8 (continua)

- $\underset{\varphi}{\underset{\rotatebox{90}{$\in$}}{\mathrm{Aut}(Q_8)}} \cong$? vogliamo capire chi è

$i, j, K = ij$ generatori di Q_8

$i \overset{\varphi}{\longmapsto}$ el. di ordine 4 6 elem di ordine 4 $\Rightarrow$ 6 scelte

$j \overset{\varphi}{\longmapsto}$ " " " 4 6 elem di ordine 4 $- \varphi(i)$ e $\varphi(-i) \Rightarrow$ 4 scelte

$K \overset{\varphi}{\longmapsto}$ la scelta è determinata da ij

$|\mathrm{Aut}(Q_8)| \leq 24$

Considero $\{i, -i\}, \{j, -j\}, \{K, -K\}$ 3 sottoinsiemi di Q_8

Sia $\varphi \in \mathrm{Aut}(Q_8) \Rightarrow \varphi$ permuta i 3 insiemi <u>ES</u>: $\varphi(i) = j \Rightarrow \varphi(-i) = -j$

Cioè l'immagine dell'inverso è det., quindi φ manda insiemi in insiemi

Considero l'omomorfismo $\mathrm{Aut}(Q_8) \xrightarrow{\pi} S_3$

π è <u>su</u> $\begin{cases} i \to j \\ j \to i \\ K \to -K \end{cases}$ corrisponde alla permutazione $(1, 2)$

$\begin{cases} i \to j \\ j \to K \\ K \to i \end{cases}$ corrisponde alla permutazione $(1, 2, 3)$

Chi è $\mathrm{Ker}\,\pi$?

generatori di Ker π

$$\begin{cases} i \longmapsto -i \\ j \longmapsto -j \\ k \longmapsto -k \end{cases}$$ ha ordine 2

$$\begin{cases} i \longmapsto i \\ j \longmapsto -j \\ k \longmapsto -k \end{cases}$$ ha ordine 2

Ho scoperto che il nucleo contiene almeno 3 elementi (id e i generatori), ma ha due elementi di ordine 2 $\Rightarrow$ avrà almeno 4 elementi.
Ma π è surgettiva $\Rightarrow \mathrm{Im}\,\pi = S_3$ e $\mathrm{Aut}(Q_8)/_{\mathrm{Ker}\,\pi} \cong S_3$.

Poiché $|\mathrm{Aut}(Q_8)| \leq 24$ ho che $|\mathrm{Ker}\,\pi|$ è al massimo 4. Dunque ho $4 \leq |\mathrm{Ker}\,\pi| \leq 4 \Rightarrow |\mathrm{Ker}\,\pi| = 4$

$$\Downarrow$$

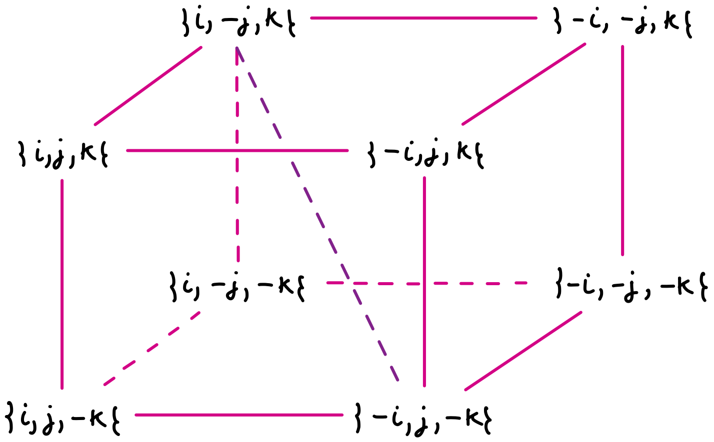
$$\mathrm{Ker}\,\pi \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}_2 \times \mathbb{Z}_2 \arrow[r] & \mathrm{Aut}(Q_8) \arrow[r] & S_3 \arrow[r] \arrow[l, bend left] & 1 \end{tikzcd}$$

↳ si riesce a trovare una sezione (laborioso)

Claim: $\mathrm{Aut}(Q_8) = S_4$

Soluzione "geometrica":



Voglio trovare un isomorfismo tra Aut(Q_8) e S_4, quindi voglio far agire Aut(Q_8) su un insieme di 4 elementi. Posso associare al cubo le sue diagonali. Considero quindi insiemi del tipo {}-i, j, -k{ , }i, -j, k{{ in cui fisso due vertici opposti del cubo e quindi determino univocamente una diagonale. Adesso considero:

- $\begin{cases} i \mapsto j \\ j \mapsto k \\ k \mapsto i \end{cases} \in \mathrm{Aut}(Q_8)$ fissa }}i, j, k{, }-i, -j, -k{{ e permuta le altre

3 diagonali ciclicamente $\Rightarrow$ ottengo un 3-ciclo in S_4;

- $\begin{cases} i \mapsto -i \\ j \mapsto j \\ k \mapsto -k \end{cases} \in \mathrm{Aut}(Q_8)$ manda:
  }}i, j, k{, }-i, -j, -k{{ ⟷ }}-i, j, -k{, }i, -j, k{{
  }}i, j, -k{, }-i, -j, k{{ ⟷ }}-i, j, k{, }i, -j, -k{{

$\Rightarrow$ ottengo un 2-2-ciclo in S_4;

- $\begin{cases} i \mapsto j \\ j \mapsto i \\ k \mapsto -k \end{cases} \in \operatorname{Aut}(Q_8)$ manda $\{\{i,j,k\},\{-i,-j,-k\}\} \longmapsto \{\{i,j,k\},\{-i,-j,k\}\}$

e lascia fisse le altre 2 diagonali, quindi mi dà un 2-ciclo in S_4;

- $\begin{cases} i \mapsto j \\ j \mapsto -i \\ k \mapsto k \end{cases} \in \operatorname{Aut}(Q_8)$ manda $\{\{i,j,k\},\{-i,-j,-k\}\} \longmapsto \{\{i,j,-k\},\{i,-j,-k\}\}$

  $\longmapsto \{\{-i,-j,k\},\{i,j,-k\}\} \mapsto \{\{i,-j,k\}\} \mapsto \{\{i,j,k\},\{-i,-j,-k\}\}$,

  quindi mi dà un 4-ciclo in S_4.

Facendo agire $\operatorname{Aut}(Q_8)$ sull'insieme delle 4 diagonali del cubo ho scoperto che ho un omomorfismo $g: \operatorname{Aut}(Q_8) \longrightarrow S_4$ la cui immagine contiene un 2-ciclo, un 2-2-ciclo, un 3-ciclo e un 4-ciclo.

Esercizio $\operatorname{Imm} g = S_4$

- $\operatorname{Aut}(\mathbb{Z}_8) \cong$?

Sappiamo già che $\operatorname{Aut}(\mathbb{Z}_{2^n}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ e anche che $\operatorname{Aut}(\mathbb{Z}_{p^n}) \cong (\mathbb{Z}_p)^* \times \mathbb{Z}_{p^{n-1}}$, con p primo dispari, dunque $\operatorname{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Esercizio: Per quali valori di n il gruppo $\operatorname{Aut}(\mathbb{Z}_n)$ è ciclico?

Se n è diviso da due primi dispari distinti, è della forma $n = 2^a p_1^{b_1} \cdot \ldots \cdot p_h^{b_h}$, con $p_1, \ldots, p_h$ primi dispari e $b_1, b_2 > 1$, allora

$$\underbrace{\mathbb{Z}_n \cong \mathbb{Z}_{2^a} \times \mathbb{Z}_{p_1^{b_1}} \times \ldots \times \mathbb{Z}_{p_h^{b_h}}}_{} \Rightarrow \operatorname{Aut}(\mathbb{Z}_n) \cong \operatorname{Aut}(\mathbb{Z}_{2^a}) \times \operatorname{Aut}(\mathbb{Z}_{p_1^{b_1}}) \times \ldots \times \operatorname{Aut}(\mathbb{Z}_{p_h^{b_h}})$$

↳ prodotto dei p-Sylow → sono unici ⇒ sono caratteristici

Noto che $\mathbb{Z}_2 \leq \operatorname{Aut}(\mathbb{Z}_{p_i^{b_i}})$ $\forall i = 1, \ldots, h$, quindi mi restringo al caso $n = 2^a p^b$, con p primo dispari. Dal momento che $\operatorname{Aut}(\mathbb{Z}_2) \cong \{0\}$ e $\operatorname{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, gli n possibili sono: $n = 1, 2, 4, p^m, 2p^m$ con p primo dispari.

Def Sia G un gruppo, il sottogruppo dei commutatori o sottogruppo derivato $G' = [G, G]$ è il sottogruppo generato dagli elementi della forma $ghg^{-1}h^{-1}$ che scriviamo come $[g, h]$, al variare di $g, h \in G$.

$gh = ghg^{-1}h^{-1}hg = [g,h]hg$ e anche $gh = hg[g^{-1}, h^{-1}]$.

Proposizione: G' è caratteristico in G.

Dim. Dato un qualsiasi $\varphi \in \mathrm{Aut}(G)$, si ha che $\varphi([g,h]) = [\varphi(g), \varphi(h)]$.

Prop. G/G' è abeliano.

Dim. $gG'hG' = ghG' = gh\overset{h^{-1}g^{-1}hg}{\overset{\shortparallel}{[h^{-1}, g^{-1}]}}G' = hG'gG'$

Prop: Sia $f: G \to H$ un omo surgettivo tale che H è abeliano, allora $G' < \mathrm{Ker} f$ e quindi $\exists\, \bar{f}$ tale che

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

Dim.

Visto che H è abeliano, se prendo un qualsiasi commutatore $[g,h] \in G'$ ho che $f([g,h]) = f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = e_H$

$\Rightarrow G' < \mathrm{Ker} f$, in quanto se tutti i commutatori sono dentro al nucleo c'è anche il gruppo da loro generato.

Rendere un gruppo abeliano vuol dire quozientarlo almeno per i commutatori.

Def Chiamo *serie derivata* di G la successione

$$G > G' > G^{(2)} > \dots \quad \text{dove} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

Può succedere che $G' = G$, in tal caso G è detto *perfetto*.

Def. Un gruppo G è *risolubile*, se esiste una *serie subnormale* $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{0\}$, cioè $G_{i+1} \triangleleft G_i$ $\forall i$, tale che G_i/G_{i+1} è abeliano $\forall i$.

Oss: Se la serie derivata termina con $\{0\}$ $\Rightarrow$ G è risolubile.

Prop. Un gruppo G è risolubile $\Leftrightarrow$ è risolubile per commutatori (cioè la serie derivata termina).

Dim. $(\Leftarrow)$ è l'*Osservazione* fatta prima.

$(\Rightarrow)$ G è risolubile, quindi $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{0\}$:

G_0/G_1 è abeliano $\Rightarrow G_1 > G' \Rightarrow G_1 \triangleright G'$;

G_1/G_2 è abeliano $\Rightarrow G_2 > G_1' > G^{(2)} \Rightarrow G_2 \triangleright G_1' \triangleright G^{(2)}$, e così via...

Quindi $G_n \triangleright \dots \triangleright G^{(n)} = \{0\}$.

Esercizio: S_n con $n \geqslant 5$ non è risolubile.

Dim. Infatti la serie derivata di S_n è $S_n \triangleright A_n \triangleright A_n \triangleright \dots$ in quanto A_n è perfetto (oltre che semplice).

Avere un gruppo risolubile corrisponde a dire che posso ottenere un certo campo aggiungendo delle radici.

Esercizio Sia $H > \mathbb{Z}^4$ tale che $H = \left\langle \begin{pmatrix} 1 \\ 2 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ 8 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 8 \\ 0 \end{pmatrix} \right\rangle$.

Chi è $\mathbb{Z}^4/H$?

Soluzione: Costruisco la matrice $\begin{pmatrix} 1 & 0 & 1 \\ 2 & 4 & -2 \\ 2 & 8 & 8 \\ 4 & 2 & 0 \end{pmatrix}$ e le applico le seguenti operazioni di riga/colonna:

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & 4 & -2 \\ 2 & 8 & 8 \\ 4 & 2 & 0 \end{pmatrix} \xrightarrow{C_3 \to C_3 - C_1} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 4 & -4 \\ 2 & 8 & 6 \\ 4 & 2 & -4 \end{pmatrix} \xrightarrow[R_4 \to R_4 - 4R_1]{R_{2,3} \to R_{2,3} - 2R_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & -4 \\ 0 & 8 & 6 \\ 0 & 2 & -4 \end{pmatrix}$$

$$\xrightarrow{R_2 \leftrightarrow R_4} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & -4 \\ 0 & 8 & 6 \\ 0 & 2 & -4 \end{pmatrix} \xrightarrow[R_4 \to R_4 - 2R_2]{R_3 \to R_3 - 4R_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -4 \\ 0 & 0 & 22 \\ 0 & 0 & 4 \end{pmatrix} \xrightarrow[R_3 \to R_3 - 5R_4]{C_3 \to C_3 + 2C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 4 \end{pmatrix}$$

$$\xrightarrow{R_4 \to R_4 - 2R_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

FORMA NORMALE DI SMITH

Quindi guardando le 4 righe della matrice in forma normale di Smith ottengo:

$$\mathbb{Z}^4/H \cong \{0\} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z} \cong \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}$$

10-11-2021 Lezione 18 Prof. Gaiffi

Esercizio (condizione necessaria perché due prodotti semidiretti di p-grp siano isomorfi)

Sia N un gruppo di ordine p^α e sia H un gruppo di ordine q^β con p e q primi distinti e $\alpha > 0$, $\beta > 0$. Sappiamo che $N \rtimes_{\tau_1} H \cong N \rtimes_{\tau_2} H$.

Allora $\mathrm{Ker}\,\tau_1 \cong \mathrm{Ker}\,\tau_2$.

Dim.

NOTAZIONE: $\overline{N} = \}(n,e) \mid n \in N\{$

$\forall K < H \quad \overline{K} = \}(e,k) \mid k \in K\{$

in particolare $\overline{H} = \}(e,h) \mid h \in H\{$

Sia $C(\overline{N}) = \}g \in G \mid gx = xg \ \forall x \in \overline{N}\{$

PRIMO PASSO

Si nota $\overline{\mathrm{Ker}\,\tau} = \overline{H} \cap C(\overline{N})$. Ricordo che $\mathrm{Ker}\,\tau < H$, infatti

$$(e,h) \in \overline{\mathrm{Ker}\,\tau} \iff h \in \mathrm{Ker}\,\tau \iff \forall n \in N \quad \tau(h)(n) = n \quad (\text{ovvero } \tau(h) = I)$$

$$\iff \forall n \in N \quad (n,h) = (\tau(h)(n), h) \iff \forall n \in N \quad \underbrace{(n,e)(e,h)}_{(n,h)} = \underbrace{(e,h)(n,e)}_{\substack{\text{per def è} \\ (e\cdot\tau(h)(n),h)}}$$

$$\iff (e,h) \in C(\overline{N}) \cap \overline{H}$$

SECONDO PASSO

$$G_1 = N \rtimes_{\tau_1} H \qquad G_2 = N \rtimes_{\tau_2} H$$

Chiamo $\overline{N}$ e $\overline{H}$ in entrambi, $C_1(\overline{N})$ in G_1, $C_2(\overline{N})$ in G_2.

Sia $f: G_1 \to G_2$ ISOMORFISMO.

Dato che $\overline{N} \lhd G_1$ e inoltre, essendo il p-Sylow, è l'unico sottogruppo di quell'ordine, e dato che lo stesso vale in G_2 deve valere $f(\overline{N}) = \overline{N}$.

Noto che $\overline{H}$ è un q-Sylow di G_1 e $f(\overline{H})$ è un q-Sylow di G_2.

Dunque $f(\overline{H})$ e $\overline{H}$ sono coniugati in G_2: $\exists g \in G_2$ tale che $f(\overline{H}) = g\overline{H}g^{-1}$

TERZO PASSO Studio $f(\overline{\mathrm{Ker}\,\tau_1}) \underset{\substack{\uparrow \\ \text{per il PRIMO PASSO}}}{=} f(\overline{H} \cap C_1(\overline{N})) = f(\overline{H}) \cap f(C_1(\overline{N})) =$

$= \underbrace{g\overline{H}g^{-1}} \cap C_2(\underset{\uparrow}{f}(\overline{N}))$

mi piacerebbe dire che $C_2(\overline{N}) = g\, C_2(\overline{N})\, g^{-1}$ perché in tal caso avrei:

$= g\overline{H}g^{-1} \cap g\, C_2(\overline{N})\, g^{-1} = g(\overline{H} \cap C_2(\overline{N}))g^{-1} \underset{\substack{\uparrow \\ \text{I PASSO}}}{=} g(\overline{\ker \tau_2})g^{-1}$

Quindi $f(\overline{\ker \tau_1}) = g(\overline{\ker \tau_2})g^{-1}$

$$\overline{\ker \tau_1} \cong g(\overline{\ker \tau_2})g^{-1} \cong \overline{\ker \tau_2}$$

Ma $\overline{\ker \tau_1} \cong \ker \tau_2$, quindi avrei finito: $\ker \tau_1$

Basta dimostrare $g\, C_2(\overline{N})\, g^{-1} = C_2(\overline{N})$

Basta dimostrare $g\, C_2(\overline{N})\, g^{-1} \subseteq C_2(\overline{N})$ per ragioni di cardinalità.

Ossia basta dimostrare che se $x \in C_2(\overline{N})$ e $\bar{n} \in N$ allora $(gxg^{-1})\bar{n} = \bar{n}(gxg^{-1})$.

Noto che $gxg^{-1}\bar{n} = gx(\overbrace{g^{-1}\bar{n}g}^{\in \overline{N} \text{ perché } \overline{N} \text{ è normale}})g^{-1} \underset{\substack{\uparrow \\ x \in C(\overline{N})}}{=} g(g^{-1}\bar{n}g)x g^{-1} = \bar{n}gxg^{-1}$ COME VOLEVAMO

□

Nota: L'esercizio funziona anche se N non è p-gruppo ma è comunque l'unico gruppo di ordine $|N|$ in $N \rtimes H$

POLINOMI SEPARABILI

Def Sia F campo. Un polinomio irrid. $g(x) \in F[x]$ si dice separabile se $g'(x) \neq 0$. Un polinomio $f(x) \in F[x]$ si dice separabile se è prodotto di IRRIDUCIBILI SEPARABILI.

OSS: Se f è SEPARABILE allora non ha radici multiple in un campo di spezzamento.

Prop: Sia $F \subseteq E$. Se $f(x) \in F[x]$ si spezza in $E[x]$ come $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ con $\alpha_1, \alpha_2, \dots, \alpha_n$ a due a due distinti, allora $f(x)$ è separabile.

Dim. Sia $g(x) \in F[x]$ un fattore irriducibile di $f(x)$. Devo mostrare che $g'(x) \neq 0$. Ora so che in $E[K]$ $g(x) = (x - a_{i_1})(x - a_{i_2}) \dots (x - a_{i_k})$ con $a_{i_1}, a_{i_2}, —, a_{i_k} \in \} a_1, —, a_n \{$ distinte.

$g'(a_{i_1}) \neq 0$ come visto la volta scorsa. Dunque $g'(x) \neq$ polinomio 0 allora $g(x)$ è irriducibile separabile. □

<u>Prop</u>: Sia $g(x) \in F[x]$ IRRIDUCIBILE E SEPARABILE e sia E campo di spezzamento di $g(x)$ su F.

Sia $a \in E$ una radice di $g(x)$. Allora $|\{\phi : F(a) \to E$ $\overset{\text{SONO INIEZIONI}}{\text{OMOMORFISMI}}$ tc

$$\phi_{|F} = Id_{|F}\}| = [F(a):F] \\ = \deg g(x)$$

<u>Dim</u>. Per un Teo di Aritmetica sappiamo che se $a,b \in E$ sono due radici distinte di $g(x)$ allora $\exists!$ Iso $\underset{\substack{\cap\\ E}}{F(a)} \to \underset{\substack{\cap\\ E}}{F(b)}$ che lascia fisso F e manda a in b.

Quindi ho almeno $\deg g(x)$ INIEZIONI $F(a) \to E$.

Viceversa noto che se $\phi : F(a) \to E$ e $\phi_{|F} = Id$ allora $\tilde{\phi}(g(x)) = g(x)$ dunque $\phi(a)$ è ancora una radice di $g(x)$.

Dunque tutti i ϕ cercati sono del tipo $F(a) \to F(b)$.

<u>Corollario</u>: Sia $g(x) \in F[x]$ irriducibile e separabile. Sia E campo di spezzamento di $g(x)$ su T. Sia $a \in E$ una radice di $g(x)$ e sia $K \in F(a) \setminus F$. Allora $\exists\, \tau : F(a) \to E$ con $\tau_{|F} = Id$ e $\tau(K) \neq K$.

<u>Dim</u>. $\underbrace{\overbrace{F \subseteq F(K)} \subseteq F(a)}$

Considero il polinomio minimo di a in $F(K)[x]$.

Sia $q(x) \in F(K)[x]$ e $q(x) \mid g(x)$. Ma $g(x)$ non ha radici multiple. Dunque anche $q(x)$ non ha radici multiple. Per la Proposizione allora $q(x)$ è separabile.

Per la proposizione precedente $|\{\phi : F(a) \to E$ e $\phi_{|F(K)} = Id\}| = [F(a):F(K)]$

inoltre $|\{\phi : F(a) \to E$ e $\phi_{|F} = Id\}| = [F(a): F]$

Noto che $[F(K):F] > 1$ per la scelta di K $(\in F(a) \setminus F)$

Per il teorema delle torri:

$[F(a):F] = [F(a):F(K)]\cdot\underbrace{[F(K):F]}_{>1}$

e quindi $[F(a):F] > [F(a):F(K)]$

Dunque esistono immersioni $F(a) \to E$ che non fissano $F(K)$ il che equivale a dire che non fissano K.

□

Corollario:

Sia E il cds su F di un polinomio separabile $g(x) \in F[x]$.

Sia $a \in E \setminus F$. Allora $\exists\ \tau : E \to E$ AUTOMORFISMO tale che $\tau(a) \neq a$ e $\tau_{|F} = Id$

Dim. $E = F(a_1, a_2, \dots, a_t)$ dove $a_1, a_2, \dots, a_t$ sono le radici di $g(x)$.

Sia i tc $a \notin F(a_1, \dots, a_{i-1})$ ma $a \in F(a_1, \dots, a_i)$.

Sia $g_i(x)$ il polinomio minimo di a_i in $F(a_1, \dots, a_{i-1})[x]$ e sia $L \subseteq E$ il campo di spezzamento di $g_i(x)$ su $F(a_1, \dots, a_{i-1})$

Noto che $g_i(x)$ è separabile perché $g_i(x) \mid g(x)$ ⊛

allora $\exists\ \tau' : F(a_1, \dots, a_{i-1})(a_i) \to L$ con $\tau'(a) \neq a$ per il Corollario precedente.

$$\begin{tikzcd}
 & E \arrow[r, dashed] & E \\
g(x) & F(a_1, \dots, a_{i-1})(a_i) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\tau'"] & L \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

□

11-11-2021 Lezione 19 Prof. Gaiffi

⊛ Perché $g_i(x)$ è separabile?

$g(x) = p_1^{d_1}(x)\, p_2^{d_2}(x) \dots p_k^{d_k}(x)$ con p_i $i = 1, \dots, k$ irriducibili e separabili

Guardo $g(x)$ in $F(a_1, \dots, a_{i-1})[x]$. So che $g_i(x)$ è IRRIDUCIBILE e $g_i(x) \mid g(x)$

↳ divide uno dei $p_r(x)$ iniziali

D'altra parte la fattorizzazione in irrid. di $g(x)$ in $F(a_1, \dots, a_{i-1})[x]$ si ottiene considerando tutte le fattorizzazioni dei $p_t(x)$.

Allora $g_i(x) \mid p_t(x)$ per un certo t.

Ma $p_t(x)$ è IRRIDUCIBILE e SEPARABILE $\Rightarrow g_i(x)$ ha radici distinte.

Allora per la proposizione già vista $g_i(x)$ è separabile.

Def se $F \subseteq E$ estensione, un elemento $a \in E$ è separabile su F se è algebrico e il suo polinomio minimo è separabile.

Teorema Sia $F \subseteq E$ estensione finita. Sia $E = F(\overbrace{\alpha, \underbrace{\beta_1, \dots, \beta_n}_{\text{separabili}}}^{\text{algebrici}})$ con i β_i separabili su F. Allora $\exists\, \delta \in E$ tc $E = F(\delta)$

↳ elemento primitivo

Dim. • Se F è campo finito, anche E, che è estensione finita, è finito

Dunque E^* è ciclico, $E^* = (\gamma)$. Dunque $F(\gamma) = E$.

• Sia F infinito. Basta dimostrare $F(\alpha, \beta_1) = F(\delta)$

Sia $f(x)$ il polinomio minimo di α su F.

Sia $g(x)$ " " " " β_1 su F.

Considero $f(x)g(x)$. Se E non è il cds di $f(x)g(x)$ lo estendo ad $\tilde{E}$.

In $\tilde{E}[x]$ vale $f(x) = \prod_{i=1}^{\deg f} (x - a_i)$ $\quad a_1 = \alpha$

$$g(x) = \prod_{k=1}^{\deg g} (x - b_k)$$

Sappiamo che $\underset{\overset{\shortparallel}{\beta_1}}{b_1}, \dots, b_k$ sono a due a due distinti.

Presi i e k considero $a_i + x b_k = \alpha + x \beta_1 \Rightarrow x = \dfrac{a_1 - \alpha}{\beta_1 - b_k}$

Ho un numero finito di tali soluzioni.

$x \in \tilde{E}$. Dato che F è infinito scelgo $r \in F$ diverso da queste soluzioni.

Dunque $a_1 + r b_k \neq \alpha + r \beta_1$ $\forall k \neq 1$ e $\forall i$

Dico che δ è proprio $\alpha + r \beta_1$

Devo dimostrare che $F(\alpha, \beta_1) = F(\delta) = F(\alpha + r\beta_1)$

$F(\alpha + r\beta_1) \subseteq F(\alpha, \beta_1)$ OVVIA

Noto che β_1 è radice di $g(x)$ ma è radice anche di $f(\delta - rx)$.

Infatti $f(\delta - r\beta_1) = f(\alpha) = 0$

Allora in $\tilde{E}(x)$ $x - \beta_1$ divide sia $f(\delta - rx)$

Dico che in $\tilde{E}(x)$ $MCD(f(\delta - rx), g(x)) = x - \beta_1$

Devo controllare se per b_i con $i > 1$ $x - b_i$ divide $f(\delta - rx)$ ossia se $f(\delta - rb_i) = 0$. $\delta - rb_i = \alpha + r\beta_1 - r b_i$

MAI VERO $a + r\beta_1 \neq a_\ell + r b_i$

$a + r\beta_1 - rb_i \neq a_\ell \quad \forall \ell$

Dunque il $MCD(f(\delta - rx), g(x))$ in $F(\delta)[x]$ non è 1

Allora è un polinomio non costante che divide $x - \beta_1$. Dunque ha grado 1, diciamo che è $c_1 x + c_0$

$$c_1 x + c_0 \mid x - \beta_1 \text{ in } \tilde{E}(x).$$

Allora β_1 è radice di $c_1 x + c_0$

$$c_1 \beta_1 + c_0 = 0$$

$$\beta_1 = -\frac{c_0}{c_1}$$

Allora $\beta_1 \in F(\delta)$. Ma $\delta = \alpha + r\beta_1$ dunque $\alpha = \delta - r\beta_1 \in F(\delta)$

Dunque $F(\alpha, \beta_1) \subseteq F(\delta)$. □

17-11-2021 Lezione 20 Prof. Gaiffi

TEORIA DI GALOIS

Data $F \subseteq E$ un'estensione di campi, chiamiamo $\text{Aut}(E/F)$ l'insieme degli automorfismi di E che lasciano fissi tutti gli elementi di F.

Chiamiamo anche $E' = \{h \in E \mid \phi(h) = h \quad \forall \phi \in \text{Aut}(E/F)\}$. (potrebbero esserci più punti fissi)

Oss: E' è un campo ed è detto il "campo fisso" di $\text{Aut}(E/F)$

Può essere F e basta o può essere più grande:

Esempi: 1) $E = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$, $\phi \in \text{Aut}(E/F)$ è determinato da $\phi(\sqrt{2})$. $\phi(\sqrt{2})$ dovrà essere una radice di $x^2 - 2$ perché $\tilde{\phi}(x^2 - 2) = x^2 - 2$, dunque $\phi(\sqrt{2}) = \pm\sqrt{2}$, da cui $\text{Aut}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) = \{Id, \theta\}$

$\theta(a + b\sqrt{2}) = a - b\sqrt{2}$ $\forall a, b \in \mathbb{Q}$. Perciò $\mathbb{Q}(\sqrt{2})' = \mathbb{Q}$. $E' = F$

↓

$\mathbb{Q}(\sqrt{2})$ è un $\mathbb{Q}$ spazio vettoriale con base $\{1, \sqrt{2}\}$

2) $\mathbb{Q}(\sqrt[3]{2}) = E$, $\mathbb{Q} = F$, $\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{2}) / \mathbb{Q}\right) = \{Id\}$ perchè se $\phi \in \mathrm{Aut}(E/F)$

$\hookrightarrow \mathbb{Q}(\sqrt[3]{2})' = \mathbb{Q}(\sqrt[3]{2})$

ϕ è determinato da $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$

deve $\in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, deve essere radice di $x^3 - 2$, le altre 2 radici $\in \mathbb{C}$

Def Un'estensione $F \subseteq E$ si dice di Galois se E è $\underbrace{\text{finita}}_{\text{vale solo in questo corso}}$ su F, e se il campo fisso di $\mathrm{Aut}(E/F)$ è F.

In tal caso $\mathrm{Aut}(E/F)$ si dice il GRUPPO DI GALOIS dell'estensione.

Oss: $\mathbb{Q}(\sqrt{2})$ è di Galois, $\mathbb{Q}(\sqrt[3]{2})$ no.

Prop (Esercizio): Sia $[E : F] < +\infty$ allora $\mathrm{Aut}(E/F)$ è gruppo finito.

Teorema: Sia $F \subseteq E$ di Galois. Allora ogni $a \in E$ è radice di un polinomio IRRIDUCIBILE e SEPARABILE $f(x)$ ($\Rightarrow a$ è separabile). Inoltre E contiene un cds di $f(x)$ ($\Rightarrow$ tutte le radici di $f(x)$ sono in E).

Dim. Costruisco $f(x) = \prod_{\gamma \in O} (x - \gamma)$ dove $O = \{\phi(a) \mid \phi \in \mathrm{Aut}(E/F)\}$

Per costruzione $f(x) \in E[x]$. Sia $\phi \in \mathrm{Aut}(E/F)$.

$$\tilde{\phi} : E[x] \longrightarrow E[x]$$

$$f(x) \longrightarrow \prod_{\gamma \in O} \tilde{\phi}(x - \gamma)$$

$$= \prod_{\gamma \in O} (x - \underbrace{\phi(\gamma)}_{\text{permuta i } \gamma \text{ perchè è Automorfismo } (\Rightarrow \text{bigettiva})})$$

$$= \prod_{\gamma \in O} (x - \gamma) = f(x)$$

perchè $\phi|_O \in Big(O)$

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ con $a_i \in E$

Ma dall'osservazione precedente so che $\forall \phi \in \mathrm{Aut}(E/F)$ ho

$$\tilde{\phi}(f(x)) = \phi(a_n) x^n + \dots + \phi(a_1) x + \phi(a_0) = f(x) =$$

mi manda $f(x)$ in $f(x)$

$$= a_n x^n + \dots + a_1 x + a_0$$

Dunque per esempio $\phi(a_n) = a_n$ $\forall \phi \in \mathrm{Aut}(E/F)$ quindi $a_n \in E' = F$

perchè l'estensione è di Galois

Dunque ho scoperto che $f(x) \in F[x]$.

Se dimostro che $f(x)$ è irriducibile in $F[x]$ ho finito.

Supponiamo che $f(x)$ sia riducibile:

$f(x) = f_1(x) f_2(x) \qquad f_1(x), f_2(x) \in F[x]$

Sia $f_1(a) = 0$. Allora $\forall \gamma \in O$ $f_1(\gamma) = 0$ dunque $f_1(x) = K f(x)$ (VEDI DISPENSE) $\square$

Teorema Sia $F \subseteq E$. L'estensione è di Galois $\Leftrightarrow$ E è il cds su F di un polinomio $f(x)$ separabile.

Dim. $\Rightarrow$) Sia $F \subseteq E$ di Galois, $E = F(a_1, \dots, a_n)$, perché E è finita. a_i è algebrico su F $\forall i = 1, \dots, n$, perché $F(a_i) \subseteq E$ e dunque $[F(a_i) : F]$ è finito $\forall i = 1, \dots, n$. Per il Teorema precedente gli a_i sono separabili.

Per il Teorema dell'elemento primitivo $E = F(\gamma)$ per qualche γ.

Costruisco $f(x)$ il polinomio minimo di γ: so che $f(x)$ è separabile per costruzione e che tutte le sue radici sono in E. Sia K il campo di spezzamento di $f(x)$ su F. So che $E = F(\gamma) \subseteq K \subseteq E \Rightarrow E = K$.

$\Leftarrow$) Sia E il cds su F di un polinomio separabile. $[E : F]$ è finito. Studio adesso E', il campo fisso di $Aut(E/F)$. Dunque se $a \in E \setminus F$, per un Corollario $a \notin E'$, dunque $E' \neq E \Rightarrow E' = F \Rightarrow F \subseteq E$ è di Galois.

Corollario (Normalità di E): Sia $F \subseteq E$ di Galois e $E \subseteq L$ estensione, allora ogni $\psi \in Aut(L/F)$ manda E in E.

Dim. E è il cds di un polinomio separabile $f(x) \in F[x]$ (VEDI DISPENSE)

Corollario: Sia $F \subseteq E$ di Galois, allora $|Aut(E/F)| = [E : F]$

Dim: $[E : F] \overset{E=F(\gamma)}{=} [F(\gamma) : F] = |\{\phi : F(\gamma) \to E \text{ omomorfismi tali che } \phi_{|F} = Id\}| =$

$= |\{\phi : E \to E \text{ omomorfismi tali che } \phi_{|F} = Id\}| = |Aut(E/F)|$

Esercizio (10.4.4): Determinare il polinomio minimo di ζ_5 su $\mathbb{Q}(i)$

Soluzione: ζ_5 è radice di $x^4 + x^3 + x^2 + x + 1$ che è irriducibile in $\mathbb{Q}[x]$

Costruiamo il "diamante" di estensioni:

$$\begin{tikzcd}
 & \mathbb{Q}(i,\zeta_5) & \\
\mathbb{Q}(\zeta_5) \arrow[ur, dash, "2 \geqslant ?"] & & \mathbb{Q}(i) \arrow[ul, dash, "? \leqslant 4"'] \\
 & \mathbb{Q} \arrow[ul, dash, "4"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

È decisivo sapere se $i \in \mathbb{Q}(\zeta_5)$ o no

Primo approccio: uso che $\cos(72°) = \frac{\sqrt{5}-1}{4}$ e $\sin(72°) = \frac{\sqrt{2(5+\sqrt{5})}}{4}$.

Secondo approccio: scrivo $i = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3$, con $a, b, c, d \in \mathbb{Q}$, perché $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ è base di $\mathbb{Q}(\zeta_5)$ su $\mathbb{Q}$.

Terzo approccio: noto che $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$ è di Galois perché è cds del polinomio separabile $x^4+x^3+x^2+x+1$. Il gruppo di Galois $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ ha $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ elementi.

Sia $\left.\begin{aligned} \phi : \mathbb{Q}(\zeta_5) &\longrightarrow \mathbb{Q}(\zeta_5) \\ \zeta_5 &\longmapsto \zeta_5^2 \end{aligned}\right\}$ lascia fisso $\mathbb{Q}$

Come visto ad Aritmetica, tale ϕ esiste.

$\phi \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ ha ordine 4: $\phi^2(\zeta_5) = \zeta_5^4 = \zeta_5^{-1} \Rightarrow \phi^4 = \mathrm{Id}$

$$\phi^2 : \zeta_5 \longrightarrow \zeta_5^2 \rightarrow \zeta_5^4 = \zeta_5^{-1}$$

$$\phi^3 : \zeta_5 \longrightarrow \zeta_5^2 \rightarrow \zeta_5^4 \rightarrow \zeta_5^8 = \zeta_5^3$$

$$\phi^4 : \zeta_5 \longrightarrow \zeta_5 \rightarrow \zeta_5^4 \rightarrow \zeta_5^8 \rightarrow \zeta_5^{16} = \zeta_5$$

Se ho un campo intermedio K, $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\zeta_5)$,

$$\mathrm{Aut}(\mathbb{Q}(\zeta_5)/K) < \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

$K \subset \mathbb{Q}(\zeta_5)$ è di Galois o no? Sì, perché è sempre campo di spezzamento di $x^4+x^3+x^2+x+1$. So allora che $|\mathrm{Aut}(\mathbb{Q}(\zeta_5)/K)| = [\mathbb{Q}(\zeta_5) : K] = 2$. Visto che $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, allora $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/K) = \{\mathrm{Id}, \phi^2\}$. Dato che $K \subset \mathbb{Q}(\zeta_5)$ è di Galois, $\mathbb{Q}(\zeta_5)' = K$ ossia K è il campo fisso di Id, ϕ^2

$\Rightarrow K$ è caratterizzato ed unico. So che $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$ perché

$\zeta_5 + \frac{1}{\zeta_5}$ è radice x^2+x-1 : $\zeta_5^4+\zeta_5^3+\zeta_5^2+\zeta_5+1=0 \Rightarrow \frac{1}{\zeta_5}+\frac{1}{\zeta_5^2}+\zeta_5^2+\zeta_5+1=0$

$\Rightarrow \left(\zeta_5+\frac{1}{\zeta_5}\right)^2+\zeta_5+\frac{1}{\zeta_5}-1=0$. Le radici di x^2+x-1 sono $x_{1,2}=\frac{-1\pm\sqrt{5}}{2} = \zeta_5+\frac{1}{\zeta_5}$

$\Rightarrow \sqrt{5}\in\mathbb{Q}(\zeta_5)$. $\mathbb{Q}(\sqrt{5})$ è l'unico sgrp dell'est. $\mathbb{Q}\subseteq\mathbb{Q}(\zeta_5)$.

$i\notin\mathbb{Q}(\zeta_5)$ altrimenti $\mathbb{Q}\subseteq \underbrace{\mathbb{Q}(i)}_{\substack{\not\subseteq\\ \mathbb{R}}} \subsetneq \underbrace{\mathbb{Q}(\zeta_5)}_{\substack{\not\subseteq\\ \mathbb{R}}}$

18-11-2021 lezione 21 Prof. Gaiffi

Esercizio: $\mathbb{Q}(\sqrt{2},\sqrt{3})$ è di Galois? In tal caso calcolare il gruppo di Galois $\mathrm{Aut}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$.

Risposta: Sì perché $\mathbb{Q}(\sqrt{2},\sqrt{3})$ è cds del polinomio:

$p(x)=(x^2-2)(x^2-3)$.

Sappiamo da ieri che $\left|\mathrm{Aut}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)\right| = \left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right] \overset{\circledast}{=} 4$

$\circledast$ perché

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

perché $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$

$\sqrt{3}=a+b\sqrt{2}$ con $a,b\in\mathbb{Q}$ ↯

$\mathbb{Q}(\sqrt{3})\subseteq\mathbb{Q}(\sqrt{3},\sqrt{2})$

Dato che x^2-2 è irriducibile in $\mathbb{Q}(\sqrt{3})[x]$ so che $\exists\ \vartheta$ ISO

$$\begin{array}{ccc}
\vartheta: \mathbb{Q}(\sqrt{3})(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{3})(-\sqrt{2}) \\
\shortparallel & & \shortparallel \\
\mathbb{Q}(\sqrt{3},\sqrt{2}) & & \mathbb{Q}(\sqrt{3},\sqrt{2}) \\
\sqrt{2} & \longmapsto & -\sqrt{2}
\end{array} \quad \text{e} \quad \vartheta|_{\mathbb{Q}(\sqrt{3})}=\mathrm{Id}$$

ϑ esiste, $\vartheta\neq\mathrm{Id}$, $\vartheta\in\mathrm{Aut}\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}(\sqrt{3})\right)$ sgruppo di $\mathrm{Aut}\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right)$.

Noto che $\vartheta^2=\mathrm{Id}$.

Analogamente costruisco:

$\varphi \in Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}(\sqrt{2})\right)$, $\varphi|_{\mathbb{Q}(\sqrt{2})} = Id$

$\varphi(\sqrt{3}) = -\sqrt{3}$

φ esiste e appartiene a $Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}(\sqrt{2})\right) \subseteq G$

Noto che $\varphi \neq Id$ e $\varphi^2 = Id$.

Noto che $\vartheta \neq \varphi$. Allora ho trovato in $Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right)$ almeno due elementi distinti di ordine 2, dunque è $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Per ora sappiamo solamente questo

Esistono altri campi K tali che $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\sqrt{2},\sqrt{3})$?

Si osserva che per tale K deve valere $[K:\mathbb{Q}] = 2$

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ \cup\!| \\ \boxed{K} \\ \cup\!| \\ \mathbb{Q} \end{array}$$

è di Galois perché $\mathbb{Q}(\sqrt{2},\sqrt{3})$ è il cds di $(x^2-2)(x^2-3)$ anche su K.

Sia G_1 il suo gruppo di Galois : $|G_1| = [\mathbb{Q}(\sqrt{2},\sqrt{3}):K] = 2$

Inoltre per definizione $G_1 < Aut\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$ e il campo fisso di G_1 è K perché l'estensione è di Galois.

Dunque K è determinato dal sottogruppo G_1.

Dato che in $\mathbb{Z}_2 \times \mathbb{Z}_2$ esistono 3 sgruppi di ordine 2, ci sono al massimo 3 distinti campi K.

$\mathbb{Q}(\sqrt{2})$ è il campo fissato da $\{Id, \varphi\}$

$\mathbb{Q}(\sqrt{3})$ è " " " da $\{Id, \vartheta\}$

Il terzo sgruppo è $\{Id, \vartheta\varphi\}$.

Noto che se considero $\sqrt{2}\sqrt{3} = \sqrt{6}$.

Vale $\vartheta\varphi(\sqrt{2}\sqrt{3}) = \vartheta(\sqrt{2}(-\sqrt{3})) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{2}\sqrt{3}$

Il campo fissato da $\{Id, \vartheta\varphi\}$ è $\mathbb{Q}(\sqrt{6})$.

NON CI SONO ALTRI CAMPI INTERMEDI !

Nota (superflua): $\mathbb{Q}(\sqrt{6}) \neq \mathbb{Q}(\sqrt{2})$.

Se fosse $\mathbb{Q}(\sqrt{6}) = \mathbb{Q}(\sqrt{2})$ avrei $\frac{\sqrt{6}}{\sqrt{2}} = \sqrt{3} \in \mathbb{Q}(\sqrt{2})$ ASSURDO! (per ragioni di grado)

Ma anche perché: ognuno di questi campi è il campo fisso di un sgrp di ord. 2. Dato che $\{Id, \varphi\}$ fissa $\mathbb{Q}(\sqrt{2})$ ma $\varphi(\sqrt{6}) = -\sqrt{6} \Rightarrow \mathbb{Q}(\sqrt{6}) \neq \mathbb{Q}(\sqrt{2})$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

L'estensione e tutti i suoi sottocampi

Se mi chiedo qual è il grado $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}]$ posso subito dire $= 4$.

Perché $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

Ma è diverso da $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})^*$.

Allora deve essere $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

* potete ragionare in due modi:

- $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}) \Rightarrow \sqrt{2}+\sqrt{3} - \sqrt{2} = \sqrt{3} \in \mathbb{Q}(\sqrt{2})$ ↯
- $\mathbb{Q}(\sqrt{2}) = Fix(\{Id, \varphi\})$ ma $\varphi(\sqrt{2}+\sqrt{3}) = \sqrt{2} - \sqrt{3} \Rightarrow \sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

Prop: Sia $F \subseteq E$ di Galois. Sia $H < Aut(E/F)$ tale che il suo campo fisso $\{a \in E \mid h(a) = a \quad \forall h \in H\}$ coincide con F allora $H = Aut(E/F)$

Dim: $E = F(\delta)$, $f(x) = \prod_{\gamma \in O_H} (x - \gamma)$

$O_H = \{h(\delta) \mid h \in H\}$ (orbita) scopro che $f(x) \in F[x]$ e che è irriducibile.

Dunque $f(x)$ è il polinomio minimo di δ.

$|H| \geq |O_H| = \deg f(x) = [E : F] = |Aut(E/F)|$. Allora deve essere $H = Aut(E/F)$.

□

Sia $F \subseteq E$ di Galois.

$C = \{K \text{ campo} \mid F \subseteq K \subseteq E\}$ campi

$S = \{G \mid G < Aut(E/F)\}$ sottogruppi

$$i: C \longrightarrow S$$

$$K \longmapsto \mathrm{Aut}(E/K)$$

$$j: S \longrightarrow C$$

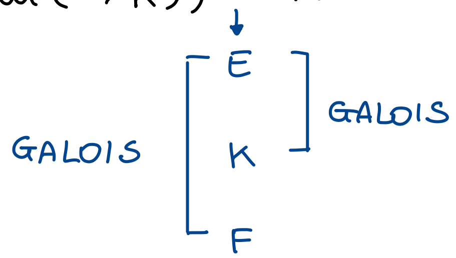
$$G \longmapsto \{a \in E \mid g(a) = a \ \forall g \in G\}$$

I Teorema di Galois:

Le mappe i e j sono l'una l'inversa dell'altra.

Dim: Sia $K \in C$,

$$ji(K) = j(\mathrm{Aut}(E/K)) = K$$



Inoltre $ij(G) = i(\underbrace{j(G)}_{\text{campo}}) = \mathrm{Aut}(E/j(G))$.

Considero G: noto che $G < \mathrm{Aut}\left(E/j(G)\right)$

Per la Prop. $G = \mathrm{Aut}(E/j(G))$. □

II Teorema di Galois

Sia $F \subseteq E$ di Galois, e sia $F \subseteq K \subseteq E$.

Allora $F \subseteq K$ è di Galois se e solo se $\mathrm{Aut}(E/K) \triangleleft \mathrm{Aut}(E/F)$.

In tal caso $\mathrm{Aut}(K/F) \cong \mathrm{Aut}(E/F) \big/ \mathrm{Aut}(E/K)$.

Dim: $F \subseteq K \subseteq E$

$\Rightarrow$) Sia $F \subseteq K$ di Galois

$$\phi: \mathrm{Aut}(E/F) \longrightarrow \mathrm{Aut}(K/F)$$

$$\psi \longmapsto \psi|_F$$

RICORDA: Se $F \subseteq E$ è di Galois e L è estensione di E allora ogni $\sigma \in \mathrm{Aut}(L/F)$ manda E in E (normalità di E)

Per il corollario la ϕ è ben definita.

Noto che ϕ è omo e $\ker \phi = \mathrm{Aut}(E/K)$. ← dunque è sgruppo NORMALE!

Resta solo da dimostrare che ϕ è surgettiva.

Sia $\tau : K \to K$ tc $\tau|_F = id$, ovvero $\tau \in \mathrm{Aut}(K/F)$.

Ricordo che $F \subseteq E$ è di Galois, allora E è cds su F di un polinomio $g(x)$ separabile. $g(x) \in F[x]$.

$$\begin{tikzcd}
E \arrow[r, dashed, "\text{esiste } T"] & E \\
K \arrow[u, dash, dashed, "\substack{\text{campo di}\\ \text{spezzamento}\\ \text{di } g(x)}"] \arrow[r, "\tau"] & K \arrow[u, dash, dashed]
\end{tikzcd}$$

$\tilde{\tau}(g(x)) = g(x)$

esiste T che estende τ per il Teorema (14.10 disp. di Arit.).

Dunque $\phi(T) = T|_K = \tau$ e ϕ è surgettiva.

(per $\Leftarrow$ vedi dispense)

19-11-2021 Lezione 22 Prof. Callegaro

Esercizio: $\alpha = \sqrt{2 + i\sqrt{2}}$ calcoliamo il polinomio minimo

$\alpha^2 = 2 + i\sqrt{2} \Rightarrow (\alpha^2 - 2)^2 = (i\sqrt{2})^2 = \alpha^4 - 4\alpha^2 + 4 = -2$

$\Rightarrow \alpha^4 - 4\alpha^2 + 6 = 0 \Rightarrow p(x) = x^4 - 4x^2 + 6$ è irriducibile?

(Sì per Eisenstein con $p=2$, ma vediamolo in un altro modo)

$\mathbb{Q}(\alpha) \ni i\sqrt{2}$

Sia K il cds di $p(x) = x^4 - 4x^2 + 6$

$i\sqrt{2} \in K$ $\quad K/\mathbb{Q}$ è di Galois

$\exists\ \tau \in \mathrm{Aut}(K/\mathbb{Q})$ tc $\tau(i\sqrt{2}) \neq i\sqrt{2}$

$i\sqrt{2}$ è radice del polinomio $x^2 + 2$

$\tau : i\sqrt{2} \longmapsto -i\sqrt{2}$

$\tau(\alpha^2) = 2 - i\sqrt{2}$

$\tau(\alpha) = \pm\sqrt{2 - i\sqrt{2}} = \pm\beta$

Chi possono essere le radici del polinomio minimo di α?

$(\alpha, -\alpha)$, (α, β) , $(\alpha, -\beta)$, $(\alpha, -\alpha, \beta, -\beta)$

Se le radici sono $(\alpha, -\alpha)$ come termine noto avremmo $2 + i\sqrt{2} \notin \mathbb{Q}$

(α, β) $\quad \sqrt{4+2} = \sqrt{6} \notin \mathbb{Q}$

$(\alpha, -\beta)$ $\quad -\sqrt{6} \notin \mathbb{Q}$

Dunque possiamo concludere che il polinomio minimo è di grado 4

- $\alpha^2 + 1$ è radice di $(x-3)^2 + 2$ e questo necess. è il suo pol. min.

Esercizio: $\alpha = \sqrt{2+\sqrt{3}}$, trovare pol. minimo e cds

$\alpha^2 = 2 + \sqrt{3} \Rightarrow \alpha$ è radice di $(x^2-2)^2 - 3 \Rightarrow p(x) = x^4 - 4x^2 + 1$

K è il cds di p(x) su $\mathbb{Q}$.

Sia $\tau \in \mathrm{Aut}(K/\mathbb{Q})$, $\tau(\sqrt{3}) = -\sqrt{3}$

$\tau(\alpha) = \pm\sqrt{2-\sqrt{3}}$

$\underset{\alpha}{\underset{\shortparallel}{\sqrt{2+\sqrt{3}}}} \cdot \underset{\alpha^{-1}}{\underset{\shortparallel}{\sqrt{2-\sqrt{3}}}} = 1 \longrightarrow \mathbb{Q}(\alpha)$ contiene tutte le radici di p(x)

Chi sta in $\mathbb{Q}(\alpha)$? $\mathbb{Q}(\alpha) \ni \overset{\alpha^2-2}{\overset{\shortparallel}{\sqrt{3}}}, \sqrt{6}$

$$\left(\alpha + \frac{1}{\alpha}\right)^2 = \alpha^2 + \frac{1}{\alpha^2} + 2 = 2 + \sqrt{3} + 2 - \sqrt{3} + 2 = 6$$

$$\Rightarrow \alpha + \frac{1}{\alpha} = \pm\sqrt{6}$$

$$\begin{tikzcd} \mathbb{Q}(\alpha) \arrow[dd, dash, "\leq 4"'] \arrow[dr, dash, "1"] & \\ & \mathbb{Q}(\sqrt{3},\sqrt{6}) = K \\ \mathbb{Q} \arrow[ur, dash, "4"'] & \end{tikzcd}$$

$1 \to \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\alpha)$

$4 \to$ lo sappiamo

$\Rightarrow \alpha$ ha grado 4 su $\mathbb{Q}$ e p(x) è il polinomio minimo di α

$\mathbb{Q}(\sqrt{3},\sqrt{6})$ è proprio il cds di p(x) su $\mathbb{Q}$

Vorrei scrivere $\alpha = a \cdot \underline{1} + b \cdot \underline{\sqrt{3}} + c \cdot \underline{\sqrt{6}} + d \cdot \underline{\sqrt{2}}$

base dello sp. vettoriale K di dim 4

ho più di un el. di ordine 2

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\sqrt{3} \longmapsto \pm\sqrt{3}$$

$$\sqrt{6} \longmapsto \pm\sqrt{6}$$

$$\begin{array}{lll} \tau: \sqrt{2} \longmapsto \sqrt{2} & \sigma: \sqrt{2} \longmapsto -\sqrt{2} & \tau\sigma: \sqrt{2} \longmapsto -\sqrt{2} \\ \quad \sqrt{3} \longmapsto -\sqrt{3} & \quad \sqrt{3} \longmapsto \sqrt{3} & \quad \sqrt{3} \longmapsto -\sqrt{3} \\ \quad \sqrt{6} \longmapsto -\sqrt{6} & \quad \sqrt{6} \longmapsto -\sqrt{6} & \quad \sqrt{6} \longmapsto \sqrt{6} \end{array}$$

$$\begin{array}{lll} \alpha \longmapsto \alpha & \alpha \longmapsto 1/\alpha & \alpha \longmapsto -1/\alpha \\ \sqrt{3} \longmapsto \sqrt{3} & \sqrt{3} \longmapsto -\sqrt{3} & \sqrt{3} \longmapsto -\sqrt{3} \\ \sqrt{6} \longmapsto -\sqrt{6} & \sqrt{6} \longmapsto \sqrt{6} & \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{2} \longmapsto -\sqrt{2} & \sqrt{2} \longmapsto -\sqrt{2} & \sqrt{6} \longmapsto \sqrt{6} \\ \downarrow & \downarrow & \downarrow \\ \text{è } \sigma & \text{è } \tau\sigma & \text{è } \tau \end{array}$$

$$\sigma(\underbrace{\alpha - \alpha}_{\overset{\shortparallel}{0}}) = 2a + 2b\sqrt{3} = 0 \Rightarrow a = b = 0$$

$$\tau\sigma\left(\underbrace{\alpha + \frac{1}{\alpha}}_{\overset{\shortparallel}{\pm\sqrt{6}}}\right) = 2a + 2c\sqrt{6} = \pm\sqrt{6} \Rightarrow c = \pm\frac{1}{2}$$

$$\underbrace{\alpha + \sigma(\alpha)}_{\overset{\shortparallel}{\alpha - \alpha = 0}} = 2a + 2b\sqrt{3} \qquad \alpha + \tau\sigma(\alpha) = \alpha + \frac{1}{\alpha} = 2a + 2c\sqrt{6} \qquad \alpha + \tau(\alpha) = 2a + 2d\sqrt{2}$$

$$2\alpha + 2d\sqrt{2} = \pm\sqrt{2} \Rightarrow d = \pm\frac{1}{2} \qquad \Rightarrow \alpha = \pm\frac{1}{2}\sqrt{2} \pm \frac{1}{2}\sqrt{6}$$

$$\left(\frac{1}{2}(\sqrt{2} + \sqrt{6})\right)^2 = \frac{1}{4}(2+6+2\cdot 2\sqrt{3}) = 2 + \sqrt{3}$$

Esercizio: Trovare il cds e il gruppo di Galois di $p(x) = x^4 - 6x^2 + 25$ su $\mathbb{Q}$

polinomio biquadratico: $x^2 = 3 \pm \sqrt{3^2 - 25} = 3 \pm i4$

$$\Rightarrow x = \pm\sqrt{3 \pm 4i}$$

$$\alpha = \sqrt{3+4i} \qquad \beta = \sqrt{3-4i} \qquad \alpha\beta = \sqrt{25} = \pm 5 \qquad \frac{1}{\alpha} = \frac{\sqrt{3-4i}}{5}$$

$$\left(\alpha + \frac{5}{\alpha}\right)^2 = \left(\sqrt{3+4i} \pm \sqrt{3-4i}\right)^2 = 3 + 4i + 3 - 4i \pm 10 \begin{cases} 16 \\ -4 \end{cases}$$

16 → mi dice che $\alpha + \frac{5}{\alpha} = \pm\sqrt{16}$

$$\alpha + \frac{5}{\alpha} = \pm 4 \Rightarrow \alpha \text{ soddisfa } \quad x^2 + 4x + 5 = 0$$

$$x^2 - 4x + 5 = 0$$

non era irriducibile

$$(x^2+4x+5)(x^2-4x+5) = (x^2+5)^2 - 16x^2 = x^4 - 6x^2 + 25 = \overset{\downarrow}{p(x)}$$

⇒ cds di $p(x)$ è $\mathbb{Q}(i)$

$x = -2 \pm i$

$x = 2 \pm i$

Esercizio: $\mathbb{Q}[x]$ $\quad x^3 - x + 1$ $\quad$ cds e grp di Galois?

$x^3 - 3x + 1$

non hanno radici in $\mathbb{Q}$ e sono di grado 3 ⇒ irrid. in $\mathbb{Q}$

Allora il grado del cds è 3 o 6 su $\mathbb{Q}$. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

$$\mathrm{Gal}\left(K/\mathbb{Q}\right) = \begin{cases} S_3 \\ A_3 \end{cases}$$

Siano $\alpha_1, \alpha_2, \alpha_3$ le radici del polinomio irr. di grado 3

$\delta := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$

$\sigma \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$

$\sigma(i) = \delta$ se σ è pari

$\qquad = -\delta$ se σ è dispari

Considero $\Delta = \delta^2$: sicuramente è fissato da $\mathrm{Gal}\left(K/\mathbb{Q}\right)$

$x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \rightsquigarrow \Delta = -4a^3 - 27b^2$

Se Δ è un quadrato in $\mathbb{Q}$ ⇒ δ fissato da Galois $\rightsquigarrow A_3$

Se Δ non è un quadrato in $\mathbb{Q}$ ⇒ δ non è fissato da Galois $\rightsquigarrow S_3$

Se prendo $p(x) = x^3 - x + 1$

$\Delta = 4(-1)^3 - 27(4) = 4 \cdot 27 = -23 \rightsquigarrow \mathrm{Gal} = S_3$

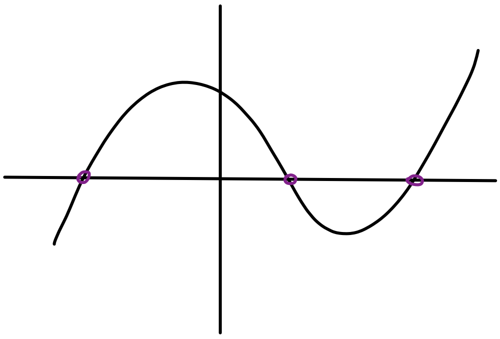
Se prendo $p(x) = x^3 - 3x + 1$

$\Delta = -4(-3)^3 - 27 = 3 \cdot 27 = 81 = 9^2 \rightsquigarrow \mathrm{Gal} = A_3$

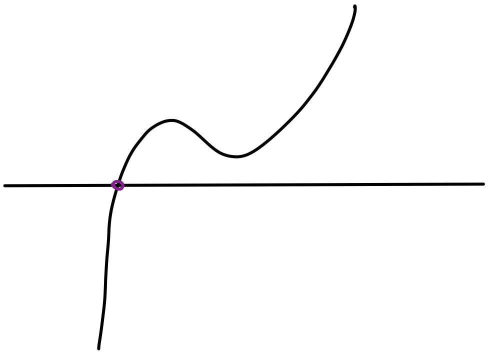
Oss: Il fatto che $\exists x$ tc $x^2 = 0$ ⇒ $\alpha_1 + \alpha_2 + \alpha_3 = 0$

Se $\alpha_1 + \alpha_2 + \alpha_3 = \lambda \rightsquigarrow p(x) \rightsquigarrow p(x + \lambda/3)$ somma delle radici

Sia $p(x) = x^3 + ax + b$ (irriducibile), allora questo può avere due possibili grafici:

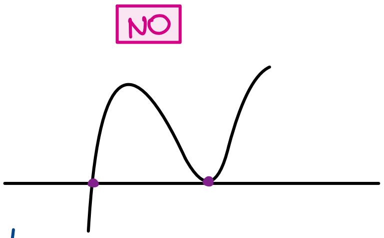


3 radici reali



1 radice reale + 2 complesse coniugate

α_2, α_3 } si scambiano tramite coniugio
↓
∃ una trasp. dispari
↓
S_3



↳ avrebbe fattori in comune con la sua derivata : $(x-\alpha_1)(x-\alpha_2)^2$

$p(x) = x^3 + ax + b$
↓
$p'(x) = 3x^2 + a \longrightarrow x = \pm\sqrt{-\frac{a}{3}}$

$$\left.\begin{aligned} f(x_1) &= \sqrt{\frac{a}{3}}^3 + a\sqrt{-\frac{a}{3}} + b \\ f(x_2) &= -\sqrt{-\frac{a}{3}} - a\sqrt{-\frac{a}{3}} + b \end{aligned}\right\} f(x_1)f(x_2) = \left(b + a\frac{2}{3}\sqrt{-\frac{a}{3}}\right)\cdot\left(b - a\frac{2}{3}\sqrt{-\frac{a}{3}}\right) =$$

$= b^2 + \frac{4}{27}a^3 < 0 \iff 3$ radici $\in \mathbb{R}$

$-27b^2 - 4a^3 > 0$

$f(x)$ irrid. di grado p primo $\Rightarrow$ $p-2$ radici reali ⊛
2 radici complesse coniugate

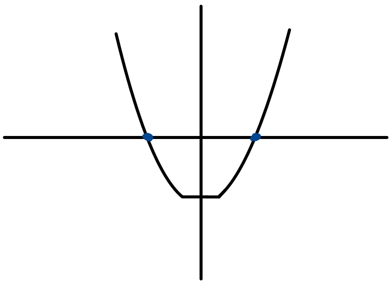
Sia α radice $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$. Sia K campo di spezzamento.

$G = \mathrm{Gal}\left(K/G\right) < S_p$, $p \mid |G| \Rightarrow$ contiene un p-ciclo

⊛ $\Rightarrow$ G contiene una trasp. $\Rightarrow G = \overset{\text{primo}}{S_p} = \langle \sigma\tau, \sigma^2 = id, \sigma^p = id \rangle$

Es: $f(x) = x^5 - 4x + 2$

$f'(x) = x^4 - 4 \xrightarrow[\text{a prima}]{\text{analogo}}$



→ Si scopre che ci sono tre radici reali e due complesse coniugate
⇓
Esistono polinomi di grado 5 il cui grp di Gal è S_5

24-11-2021 Lezione 23 Prof. Gaiffi

III Teorema di Galois (corrispondenza di Galois)

Sia $F \subseteq E$ estensione di Galois. Se $F \subseteq K \subseteq E$ allora $|\mathrm{Aut}(E/K)| = [E:K]$

e inoltre $[K:F]$ = indice di $\mathrm{Aut}(E/K)$ in $\mathrm{Aut}(E/F)$

Dim: $|\mathrm{Aut}(E/F)| \underset{F\subseteq E \text{ di Galois}}{=} [E:F] \overset{\text{Teo Torri}}{=} [E:K][K:F] \underset{K\subseteq E \text{ di Galois}}{=} |\mathrm{Aut}(E/K)|\cdot[K:F]$ □

TEOREMA FONDAMENTALE DELL'ALGEBRA

Ogni polinomio non costante in $\mathbb{C}[x]$ ammette una radice in $\mathbb{C}$.

Dim: Equivale a dire che $\mathbb{C} = \mathbb{R}(i)$ ammette estensioni finite solo di grado 1. Sia L estensione finita di $\mathbb{C}$, voglio dimostrare che $L = \mathbb{C}$.

Osservo che $L \subseteq E$ tale che $[E:\mathbb{R}]$ di Galois.

Infatti $L = \mathbb{R}(i)(\alpha_1, \dots, \alpha_n)$ (l'estensione è finita)

Per il Teo dell' elemento primitivo: $L = \mathbb{R}(\delta)$

(notate: $\alpha_1, \dots, \alpha_n$ separabili perché siamo in caratteristica 0)

Sia $f(x) \in \mathbb{R}[x]$ il polinomio minimo di δ (in part. $f(\delta) = 0$)

Sia E cds di $f(x)$ che contiene δ. Dunque $E \supseteq L = \mathbb{R}(\delta) \supseteq \mathbb{R}(i) \supseteq \mathbb{R}$

STRATEGIA: Dimostrare che $E = \mathbb{R}(i)$ allora anche $L = \mathbb{R}(i)$

Sia $G = \mathrm{Aut}(E/\mathbb{R})$ gruppo di Galois.

$$|G| = [E:\mathbb{R}] = [E:\mathbb{R}(i)]\underbrace{[\mathbb{R}(i):\mathbb{R}]}_{2} = 2\,[E:\mathbb{R}(i)]$$

Sia N_2 il 2-Sylow di G ($N_2 < G$)

Per la corrispondenza di Galois, a N_2 corrisponde un sottocampo $J(N_2)$. $\quad \underbrace{\mathbb{R} \subseteq J}(N_2) \subseteq E$

$J(N_2) = \{ a \in E \mid \varphi(a) = a$

Per il terzo teorema di Galois

$$[J(N_2):\mathbb{R}] = \underbrace{\text{indice di } N_2 \text{ in } G}_{\text{è dispari!}}$$

Per il Teo dell'el. primitivo $J(N_2) = \mathbb{R}(\alpha)$.

Sia $g(x)$ il pol minimo su $\mathbb{R}$ di α. Dunque $\deg g(x) = [J(N_2):\mathbb{R}]$ è dispari!

Per un noto Teorema di analisi deve essere $\deg g(x) = 1$.

Ma allora $\mathbb{R}(\alpha) = \mathbb{R}$ ossia $J(N_2) = \mathbb{R}$.

Allora per la corrispondenza di Galois $N_2 = G$

$$\left.\begin{array}{c} E \\ \cup\!\mid \\ \mathbb{R}(i) \\ \cup\!\mid \\ \mathbb{R} \end{array}\right] \mathrm{Aut}(E/\mathbb{R}) = N_2 = G$$

Considero $G_1 < G \quad G_1 = \mathrm{Aut}(E/\mathbb{R}(i))$

$|G_1| \mid |G|$ dunque $|G_1| = 2^s$

Se $G_1 = \{e\}$ allora $[E:\mathbb{R}(i)] = |G_1| = 1$ e ho finito.

Se fosse $G_1 \neq \{e\}$ per il I Teo di Sylow esiste $G_2 < G_1$ tale che $|G_2| = 2^{s-1}$. Considero $\mathcal{J}(G_2)$ e osservo che:

$$\left.\begin{array}{c} E \\ \cup\!| \\ \mathcal{J}(G_2) \\ \cup\!| \\ \mathbb{R}(i) \end{array}\right]$$

Per il terzo teorema di Galois $[\mathcal{J}(G_2):\mathbb{R}(i)] =$ indice di G_2 in G_1 cioè $= 2$. Questo è assurdo perché sappiamo che estensioni di $\mathbb{C}$ di grado 2 non esistono, visto che di un polinomio in $\mathbb{C}[x]$ di grado 2 sappiamo trovare le radici con la formula risolutiva. □

Esercizio: Sia $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$. Dimostrare che $[K:\mathbb{Q}]$ è di Galois e determinare $\mathrm{Aut}(K/\mathbb{Q})$. Determinare tutti i campi F tali che $\mathbb{Q} \subseteq F \subseteq K$ tali che $[F:\mathbb{Q}] = 6$.

Dim.

Osservo che il campo di spezzamento di $(x^3-3)(x^2-3)$ è $\mathbb{Q}(\sqrt[3]{3}, \xi_3, \sqrt{3})$ e che tale campo è uguale a $\mathbb{Q}(\sqrt[3]{3}, i, \sqrt{3}) = K$ visto che $\xi_3 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$

Dunque K è cds di un pol. separabile, dunque $\mathbb{Q} \subseteq K$ è di Galois

Calcolo $[K:\mathbb{Q}]$:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) \arrow[dl, dash, "3"'] \arrow[dd, dash, "6"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[3]{3}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Dato che $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{2}):\mathbb{Q}] \leq 6$ ed è diviso da 2 e da 3, si ha $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}):\mathbb{Q}] = 6$. Considero $K = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})(i)$, dunque si ha $[K:\mathbb{Q}] = 12$ per il Teo delle Torri ($i \notin \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})$ perché $\subseteq \mathbb{R}$)

$$\begin{tikzcd}[column sep=small]
 & & K \arrow[dl, dash] \arrow[dr, dash] & & \\
\text{di Galois} & \mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"] & & \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \arrow[dl, dash, "6 \text{ per motivi standard}"] & \text{di Galois} \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Noto che $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt[3]{3}, \zeta_3) = \mathbb{Q}$ perché può essere $\left\langle \begin{array}{l} \mathbb{Q} \\ \mathbb{Q}(\sqrt{3}) \end{array} \right.$

per ragioni di grado e se fosse $= \mathbb{Q}(\sqrt{3})$ avrei che $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$, ossia $K = \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$.

Ma ho già dimostrato che $[K : \mathbb{Q}] = 12$ e dunque ASSURDO.

Costruisco $\phi : \mathrm{Aut}(K/F) \to \mathrm{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \times \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q})$

$$\sigma \longmapsto \left(\sigma|_{\mathbb{Q}(\sqrt{3})}, \sigma|_{\mathbb{Q}(\sqrt[3]{3}, \zeta_3)} \right)$$

ϕ è ben definita perché $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$ e $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$ sono di Gal.

ϕ è omomorfismo (verifica immediata)

ϕ è iniettiva, perché se $\sigma|_{\mathbb{Q}(\sqrt{3})} = Id$ e $\sigma|_{\mathbb{Q}(\sqrt[3]{3}, \zeta_3)} = Id$, allora ho $\sigma(\sqrt{3}) = \sqrt{3}$, $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$ e $\sigma(\zeta_3) = \zeta_3$, allora $\sigma = Id \Rightarrow \sigma(K) = K$ cioè σ fissa tutto K.

Per ragioni di cardinalità $(12 = 2 \cdot 6)$ ϕ è anche bigettiva, dunque ϕ è isomorfismo.

$$\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \underbrace{\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}\right)}_{D_3 = S_3}$$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \arrow[dl, dash, "\tau"'] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{3}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\tau \in \mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}(\sqrt[3]{3})\right) \left\langle \begin{array}{l} \tau(\sqrt[3]{3}) = \sqrt[3]{3} \\ \tau(\zeta_3) = \zeta_3^2 \end{array} \right.$$

τ esiste perché considero il polinomio $x^2 + x + 1$ che è irriducibile su $\mathbb{Q}(\sqrt[3]{3})$ e ζ_3 e ζ_3^2 sono le sue radici.

Uso un teorema visto ad Aritmetica,

$$\tau : \mathbb{Q}(\sqrt[3]{3})(\zeta_3) \longrightarrow \mathbb{Q}(\sqrt[3]{3})(\zeta_3^2)$$

$$\zeta_3 \longmapsto \zeta_3^2$$

Analogamente considero $\sigma \in \mathrm{Aut}\left(\mathbb{Q}(\zeta_3, \sqrt[3]{3}) / \mathbb{Q}(\zeta_3)\right)$ tale che

$\sigma(\zeta_3) = \boxed{\zeta_3}$

$\sigma(\sqrt[3]{3}) = \boxed{\sqrt[3]{3}\,\zeta_3}$ → sono entrambe radici di x^3-3, irriducibile su $\mathbb{Q}(\zeta_3)$

τ e σ appartengono anche a $\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}\right)$

Verifico che: $\tau^2 = Id$

$\sigma^3 = Id$

e che: $\tau\sigma\tau = \sigma^{-1}$

Infatti: $\tau\sigma\tau(\zeta_3) = \tau\sigma(\zeta_3^2) = \tau(\zeta_3^2) = \zeta_3^4$

$\tau\sigma\tau(\sqrt[3]{3}) = \tau\sigma(\sqrt[3]{3}) = \tau(\sqrt[3]{3}\cdot\zeta_3) = \sqrt[3]{3}\,\zeta_3^2$

Verificare che: $\sigma^{-1}(\zeta_3) = \zeta_3$

$\sigma^{-1}(\sqrt[3]{3}) = \sqrt[3]{3}\,\zeta_3^2$

con questo abbiamo dimostrato che $\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}\right) \cong D_3 \cong S_3$

25-11-2021 Lezione 24 Prof. Gaiffi

(Soluzione alternativa all'esercizio di ieri)

Si osserva che $\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}\right)$ posso vederlo come sgruppo di S_3 ("si immerge")

Infatti prendo $X = \{\sqrt[3]{3}, \sqrt[3]{3}\,\zeta_3, \sqrt[3]{3}\,\zeta_3^2\}$ e dato $\sigma \in \mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}\right)$

$\sigma|_X$ è una bigezione di X ↘ 3 radici di x^3-3

chiaramente $\sigma(X) \subseteq X$, ma per motivi di # è proprio una big.

Possiamo sempre immergere $X = \{$radici del pol.$\}$ in $Big(X)$.

In generale non vale l'isomorfismo, in questo caso (per motivi di cardinalità), sono isomorfi però.

Dunque ho un omo iniettivo da $\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{3}, \zeta_3)/\mathbb{Q}\right) \longrightarrow S_3$ e per ragioni di cardinalità, IN QUESTO CASO è un ISOMORFISMO.

2) Trovare tutti i campi intermedi (= sottocampi) F tali che $[F : \mathbb{Q}] = 6$

Per il III Teo di Galois tali campi corrispondono ai sgrp di indice 6 di $\mathbb{Z}_2 \times S_3 = \mathrm{Aut}\left(K/\mathbb{Q}\right)$, ossia ai sgruppi di ordine 2.

$\mathbb{Z}_2$ ↓ 1 elem di ord 2

S_3 ↳ 3 elem di ordine 2

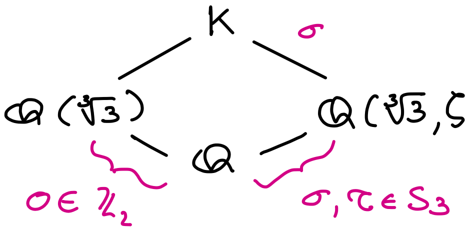
$(0, (i,j))$ 3 elem

$(1, (i,j))$ 3 elem

$(1, id)$ 1 elem

$\Big\}$ 7 elem di ordine 2

Ci sono dunque 7 s.gruppi di ordine 2, avrò allora 7 sottocampi



$\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times S_3$

$(0, \sigma)$

esiste dunque $\tilde{\sigma} \in \mathrm{Aut}(K/\mathbb{Q})$

$\tilde{\sigma}(\sqrt{3}) = \sqrt{3}$

$\tilde{\sigma}(\zeta_3) = \zeta_3$

$\tilde{\sigma}(\sqrt[3]{3}) = \sqrt[3]{3}\,\zeta_3$

Ugualmente noto che $\tilde{\tau}$

$\tilde{\tau}(\sqrt{3}) = \sqrt{3}$

$\tilde{\tau}(\zeta_3) = \zeta_3^2$

$\tilde{\tau}(\sqrt[3]{3}) = \sqrt[3]{3}$

Esiste anche $\gamma \mapsto (1, e)$

$\gamma(\sqrt{3}) = -\sqrt{3}$

$\gamma(\zeta_3) = \zeta_3$

$\gamma(\sqrt[3]{3}) = \sqrt[3]{3}$

$$\left.\begin{array}{l} o(\gamma)=2 \\ o(\tilde\tau)=2 \\ o(\tilde\sigma)=3 \end{array}\right\} \text{generano } \mathrm{Aut}(K/\mathbb{Q}) \text{ visto che le loro imm. generano } \mathbb{Z}_2\times S_3$$

Noto che $\tilde\tau, \tilde\tau\tilde\sigma, \tilde\tau\tilde\sigma^2$ hanno ordine 2 :

$(0, \overbrace{(i,j)}^{\tilde\tau})$

$(0, \underbrace{\overbrace{(i,j)(x,y,z)}^{\tilde\tau\tilde\sigma}}_{\text{dispari} \Rightarrow \text{trasposizione}})$

$(0, \underbrace{\overbrace{(i,j)(x,y,z)^2}}_{\tilde\tau\tilde\sigma^2})$

Anche γ ha ordine 2.

Devo studiare i loro campi fissi.

Basta dunque trovare per ognuno di questi elementi il s.campo di K da lui fissato. Notazione: $\mathrm{Fix}(\overset{\curvearrowright \text{elemento}}{j})$

$\mathrm{Fix}(\tilde\tau) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ che ha grado 6

$\mathrm{Fix}(\tilde\tau\tilde\sigma) = ?$

$\Downarrow$

$\sqrt{3}$ perché è fissato sia da $\tilde\tau$ che da $\tilde\sigma$

$\tilde\tau\tilde\sigma(\sqrt[3]{3}\,\zeta_3) = \tilde\tau(\sqrt[3]{3}\,\zeta_3^2) = \sqrt[3]{3}\,\zeta_3^4 = \sqrt[3]{3}\,\zeta_3$ FISSATO!

dunque $\mathrm{Fix}(\tilde\tau\tilde\sigma) = \mathbb{Q}(\underbrace{\sqrt[3]{3}\,\zeta_3}_{\text{est. di grado } 3}, \underbrace{\sqrt{3}}_{\text{est di grado } 2})$ (per ragioni di grado)

$\mathrm{Fix}(\gamma\tilde\tau) = ?$

$\gamma\tilde\tau \in \mathrm{Aut}(K/\mathbb{Q}(\sqrt[3]{3}))$, l'estensione $\mathbb{Q}(\sqrt[3]{3}) \subseteq K$ di grado 4.

$K = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, \zeta_3)$] "salto" di 2 → ζ_3 è radice di x^2+x+1

$\cup\!\!\mid$ ↳ base $1, \zeta_3$

$\mathbb{Q}(\sqrt[3]{3}, \sqrt{3})$] "salto" di 2 → base $1, \sqrt{3}$

$\cup\!\!\mid$

$\mathbb{Q}(\sqrt[3]{3})$] "salto" di 3

$\cup\!\!\mid$

$\mathbb{Q}$

BASE di K su $\mathbb{Q}(\sqrt[3]{3})$ è $\}1, \zeta_3, \sqrt{3}, \sqrt{3}\,\zeta_3\{$

$\gamma\tilde\tau : K \to K$ è applicazione $\mathbb{Q}(\sqrt[3]{3})$-lineare

$\gamma\tilde\tau$ rispetto alla base fissata in partenza e in arrivo ha matrice:

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Colonna 1: $\gamma\tilde{\tau}(1) = 1 = 1 \cdot 1 + 0 \cdot \zeta_3 + 0 \cdot \sqrt{3} + 0 \cdot \sqrt{3}\zeta_3$

Colonna 2: $\gamma\tilde{\tau}(\zeta_3) = \zeta_3^2 = -1 - \zeta_3$

Colonna 3: $\gamma\tilde{\tau}(\sqrt{3}) = -\sqrt{3}$

Colonna 4: $\gamma\tilde{\tau}(\sqrt{3}\zeta_3) = -\sqrt{3}\zeta_3^2 = -\sqrt{3}(-1-\zeta_3) = \sqrt{3} + \sqrt{3}\zeta_3$

$$\mathrm{Fix}(\gamma\tilde{\tau}) = \mathrm{Ker}(\gamma\tilde{\tau} - \mathrm{Id}) = \mathrm{Ker}\begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \underbrace{\mathrm{Span}\left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix}\right)}$$

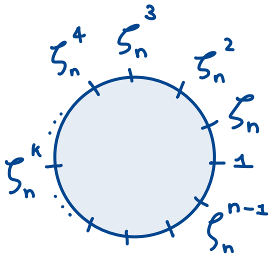
gli elem sono dati da $a \cdot 1 + b(\sqrt{3} + 2\sqrt{3}\zeta_3)$ ⟶ per questo

$$\mathrm{Fix}(\gamma\tilde{\tau}) = \mathbb{Q}(\sqrt[3]{3}, \underbrace{\sqrt{3} + 2\sqrt{3}\,\zeta_3}_{3i}) = \mathbb{Q}(\sqrt[3]{3}, i)$$

(TROVARE TUTTI E 7 I CAMPI)

POLINOMI CICLOTOMICI

Def: $\phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i)$ dove α_i sono le radici primitive e n-esime di 1



GRUPPO MOLTIPLICATIVO $(\zeta_n) \cong \mathbb{Z}_n$

A priori $\phi_n(x) \in \mathbb{C}[x]$, ma ...

$\phi_1 = x - 1$

$\phi_2 = x + 1$

$\phi_3 = x^2 + x + 1$

$\phi_4 = x^2 + 1$

$\phi_5 = x^4 + x^3 + x^2 + x + 1$

$\phi_6 = x^2 - x + 1$

$\phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\phi_8 = x^4 + 1$

$\phi_9 = x^6 + x^3 + 1$

In realtà hanno coef. in $\mathbb{Z}$ e sono irriducibili

Oss: $\prod_{d \mid n} \phi_d(x) = x^n - 1$

Teorema: Per ogni $n \geq 1$ $\phi_n(x) \in \mathbb{Z}[x]$ ed è IRRIDUCIBILE in $\mathbb{Z}[x]$ (e quindi in $\mathbb{Q}[x]$). Inoltre il campo di spezzamento di $\phi_n(x)$

su $\mathbb{Q}$ è $\mathbb{Q}(\zeta_n)$ e ha grado $\varphi(n)$ e $\mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)=\mathbb{Z}_n^*$

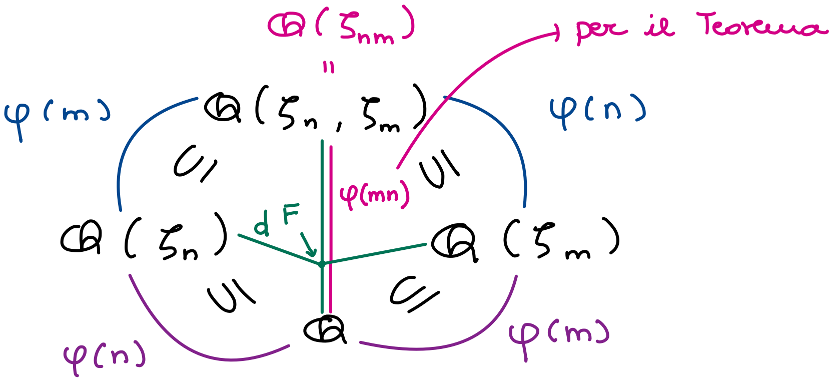
Corollario: Siano m, n primi tra loro.

Allora $\mathbb{Q}(\zeta_m,\zeta_n)=\mathbb{Q}(\zeta_{mn})$, $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m)=\mathbb{Q}$

Esempio: $\zeta_4=i$ allora $\underbrace{\mathbb{Q}(\zeta_4)}_{\mathbb{Q}(i)}\cap\mathbb{Q}(\zeta_5)=\mathbb{Q}$

$\mathbb{Q}(\zeta_4,\zeta_5)\overset{\subseteq}{\underset{\supseteq}{=}}\mathbb{Q}(\zeta_{20})$

Dim (Corollario):



visto ad Aritmetica
↓

$\varphi(mn)=\varphi(m)\varphi(n)$

$F=\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m)$, se fosse $F\neq\mathbb{Q}$ avrei $[\mathbb{Q}(\zeta_n):F]=d\mid\varphi(n)$ ma allora $[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}(\zeta_m)]\leq d$ per il Teorema delle Torri. ASSURDO.

Dunque $[\mathbb{Q}(\zeta_n):F]=\varphi(n)\Rightarrow[F:\mathbb{Q}]=1\Rightarrow F=\mathbb{Q}$.

□

CAMPI FINITI

$\mathbb{Z}_p\subseteq K$ allora K ha grado p^n.

Gli elementi di K sono tutte e sole le radici di $x^{p^n}-x$.

(Studiare il Teo 14.17 delle dispense di Aritmetica)

Oss: $\mathbb{F}_{p^n}$ è estensione di Galois di $\mathbb{Z}_p$ perché è campo di spezzamento di $x^{p^n}-x$ che ha radici tutte distinte ed è dunque separabile.

Chi è $\mathrm{Aut}\left(\mathbb{F}_{p^n}/\mathbb{Z}_p=\mathbb{F}_p\right)=?$

Ha n elementi. Consideriamo l'omomorfismo di Frobenius.

$$\mathcal{F}\in\mathrm{Aut}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$$

Sappiamo $\mathcal{F}^n=\mathrm{Id}$

Se $o(F)=n$ allora il gruppo di Galois è generato da F ed è $\cong \mathbb{Z}_n$

Ricordiamo che $(\mathbb{F}_{p^n})^*$ è ciclico, generato da γ. Dunque $o(\gamma)=p^n-1$.

Allora se $r<n$, $F^r(\gamma)=\gamma^{p^r}\neq\gamma$.

Questo mostra che $F^r\neq Id$ dunque $o(F)=n$. □

26 - 11 - 2021 lezione 25 Prof. Callegaro

Esercizio 1: Sia $p(x)=x^4+ax^2+b\in\mathbb{Q}[x]$ polinomio biquadratico irriducibile. Qual è il suo campo di spezzamento K e il suo gruppo di Galois: $Gal\left(cds/\mathbb{Q}\right)$?

Oss: Se avessi un polinomio di grado 2 t^2+at+b irriducibile in $\mathbb{Q}$, allora avrei che dato $\Delta=a^2-4b$, $\sqrt{\Delta}\notin\mathbb{Q}$, ovvero Δ non è un quadrato in $\mathbb{Q}$. Se fosse un quadrato allora il polinomio si fattorizza su $\mathbb{Q}[t]$. Ma allora $p(x)$ si fattorizza su $\mathbb{Q}[x]$.

Cosa so riguardo al termine b?

Esempio: $x^4-6x+\textcircled{25}=(x^2+5+4x)(x^2+5-4x)$

↳ è fondamentale sia un quadrato

Chiamiamo ω_1,ω_2 le radici di t^2+at+b. Chiaramente $\omega_1\omega_2=b$.

Se $\sqrt{\Delta}\in\mathbb{Q}$ o se mi metto in $\mathbb{Q}[\sqrt{\Delta}]$ ho che $t^2+at+b=(t-\omega_1)(t-\omega_2)$

$\Rightarrow x^4+ax^2+b=(x^2-\omega_1)(x^2-\omega_2)\Rightarrow$ le radici di $p(x)$ sono $\pm\sqrt{\omega_1},\pm\sqrt{\omega_2}$

Se $p(x)$ fosse riducibile (prodotto di 2 fattori di grado 2) avrei

$$p(x)=\underbrace{(x^2-\omega_1)}_{P_1}\underbrace{(x^2-\omega_2)}_{P_2} \qquad \text{caso ①}$$

$$=\underbrace{\left[(x-\sqrt{\omega_1})(x-\sqrt{\omega_2})\right]}_{P_1}\underbrace{\left[(x+\sqrt{\omega_1})(x+\sqrt{\omega_2})\right]}_{P_2} \qquad \text{caso ②}$$

$$=\underbrace{\left[(x-\sqrt{\omega_1})(x+\sqrt{\omega_2})\right]}_{P_1}\underbrace{\left[(x+\sqrt{\omega_1})(x-\sqrt{\omega_2})\right]}_{P_2} \qquad \text{caso ③}$$

Chi sono i termini noti?

① $\underbrace{\omega_1,\ \omega_2}_{\in\mathbb{Q}\ \Rightarrow\ \sqrt{\Delta}\in\mathbb{Q}}$, ② $\sqrt{\omega_1}\sqrt{\omega_2}$, $\sqrt{\omega_1}\sqrt{\omega_2}$, ③ $-\sqrt{\omega_1}\sqrt{\omega_2}$, $-\sqrt{\omega_1}\sqrt{\omega_2}$

Mi chiedo: b è un quadrato in $\mathbb{Q}$?

- NO $\Rightarrow$ sono sicuro che è irriducibile su $\mathbb{Q}[x]$ (se $\sqrt{\Delta} \notin \mathbb{Q}$)
- SI. Il fatto che Δ non è un quadrato in $\mathbb{Q}$ non basta come garanzia di irriducibilità.

Potrei avere $p(x)=(x^2+\sqrt{b}+cx)(x^2+\sqrt{b}-cx)$

oppure

$$p(x)=(x^2+cx-\sqrt{b})(x^2-cx-\sqrt{b})$$

$\Rightarrow$ $2\sqrt{b}\,x^2-c^2x^2=ax^2 \Rightarrow \underbrace{2\sqrt{b}-a}_{\text{quadrato in } \mathbb{Q}}=c^2$

La richiesta è: $p(x)$ irriducibile $\Leftrightarrow$ Δ non è un quadrato in $\mathbb{Q}$
+
(b non è un quadrato in $\mathbb{Q}$)
oppure
(b è un quadrato in $\mathbb{Q}$ e $-a\pm2\sqrt{b}$ non è un quadrato in $\mathbb{Q}$)

$\Rightarrow$ Questo mi dice che nel cds di $p(x)$ ho almeno $\sqrt{\Delta}$

Considero il campo $\mathbb{Q}(\sqrt{\Delta})$: noto che $[\mathbb{Q}(\sqrt{\Delta}):\mathbb{Q}]=2$ visto che Δ non è un quadrato. Mi chiedo ora: b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$?

2 casi:

SÌ
- ⓐ b è un quadrato in $\mathbb{Q}$
- ⓑ b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$ ma non in $\mathbb{Q}$

NO

SÌ) Si ha $\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{\Delta}) \xrightarrow[\downarrow]{2} \mathbb{Q}(\sqrt{\Delta},\sqrt{\omega_1})$

Perché $\omega_1 \in \mathbb{Q}(\sqrt{\Delta})$ e $\sqrt{\omega_1}$ è radice di $p(x)$ che è irriducibile di grado 4 perché $[\mathbb{Q}(\sqrt{\omega_1}):\mathbb{Q}]=4$. Dunque il grado è sia ≥ 2 che ≤ 2.

Noto che $\sqrt{b}\in\mathbb{Q}(\sqrt{\Delta},\sqrt{\omega_1})$ e $\sqrt{b}=\sqrt{\omega_1}\sqrt{\omega_2} \Rightarrow \sqrt{\omega_2}\in\mathbb{Q}(\sqrt{\Delta},\sqrt{\omega_1})$

$\Rightarrow K=\mathbb{Q}(\sqrt{\Delta},\sqrt{\omega_1})$ è il cds di $p(x)$ e ha grado 4 su $\mathbb{Q}$.

- caso ⓐ: chi è $G=\mathrm{Gal}\left(K/\mathbb{Q}\right)$?

$\exists\,\sigma\in G$ tale che $\sigma(\sqrt{\omega_1})=-\sqrt{\omega_1} \Rightarrow \sigma(\sqrt{\omega_2})=-\sqrt{\omega_2}$, visto che

$\sigma(\sqrt{b}) = \sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2}$ che deve essere fissato perché $\sqrt{b} \in \mathbb{Q}$.

$\exists \tau \in G$ tale che $\tau(\sqrt{\omega_1}) = \sqrt{\omega_2} \Rightarrow \tau(\sqrt{\omega_2}) = \sqrt{\omega_1}$ visto che $\tau(\sqrt{b}) = \sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2}$

che deve essere fissato perché $\sqrt{b} \in \mathbb{Q}$.

Ho questa situazione:

$$\begin{tikzcd}
\sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"] \arrow[d, leftrightarrow, "\sigma"'] & \sqrt{\omega_2} \arrow[d, leftrightarrow, "\sigma"] \\
-\sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"'] & -\sqrt{\omega_2}
\end{tikzcd}
\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$\uparrow$ ho due trasformazioni che commutano

– caso ⓑ: Cosa implica questa condizione?

Esempio: 3 è un quadrato in $\mathbb{Q}(\sqrt{2})$? Gli elementi di $\mathbb{Q}(\sqrt{2})$ sono del tipo $\alpha + \beta\sqrt{2}$ con $\alpha, \beta \in \mathbb{Q} \Rightarrow (\alpha + \beta\sqrt{2})^2 = \alpha^2 + 2\beta^2 + 2\alpha\beta\sqrt{2}$, voglio che $\alpha\beta = 0$ allora o $\alpha^2 = 3$ (NO) o $(\beta\sqrt{2})^2 = 2\beta^2 = 3$ (NO) $\Rightarrow 3$ non è un quadrato in $\mathbb{Q}(\sqrt{2})$.

Da questo deduco che se b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$ ma non in $\mathbb{Q}$

$\Rightarrow b \cdot \Delta$ è un quadrato in $\mathbb{Q}$

Infatti ho $b = (\alpha + \beta\sqrt{\Delta})^2 = \underset{\downarrow}{\alpha^2} + \underbrace{2\sqrt{\Delta}\,\alpha\beta}_{=0} + \boxed{\Delta\beta^2} \Rightarrow b = \Delta\beta^2 \Rightarrow b \cdot \Delta = \overbrace{\Delta^2\beta^2}^{\mathbb{Q} \ni (\Delta\beta)^2}$

$= 0$ altrimenti b sarebbe un quadrato in $\mathbb{Q}$

Chi è $G = \mathrm{Gal}\left(K/\mathbb{Q}\right)$?

$\exists \sigma$ tale che $\sigma(\sqrt{\omega_1}) = \sqrt{\omega_2} \Rightarrow \sigma(\omega_1) = \omega_2$

$\Downarrow$

$\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$

$b\Delta = \beta^2\Delta^2 \Rightarrow \sqrt{b} = \beta\sqrt{\Delta} \longleftarrow ⓤ \Downarrow$

$\sigma(\sqrt{b}) = -\sqrt{b}$

$\hookrightarrow \sigma(\sqrt{\omega_1}\sqrt{\omega_2}) = -\sqrt{\omega_1}\sqrt{\omega_2}$

$\Downarrow$

$\sigma(\sqrt{\omega_2}) = -\ \omega_1$

$$\begin{tikzcd}
\sqrt{\omega_1} \arrow[r, mapsto, "\sigma"] & \sqrt{\omega_2} \arrow[d, mapsto, "\sigma"] \\
-\sqrt{\omega_2} \arrow[u, mapsto, "\sigma"] & -\sqrt{\omega_1} \arrow[l, mapsto, "\sigma"]
\end{tikzcd}
\Rightarrow G \cong \mathbb{Z}_4$$

$\hookrightarrow \sigma, \sigma^3$ ha ordine 4

σ^2 ha ordine 2

σ^4 ha ordine 1

NO) Analizziamo il grado del cds su $\mathbb{Q}$.

$$[K:\mathbb{Q}] = \overbrace{[\mathbb{Q}(\sqrt{\omega_1},\sqrt{b},\sqrt{\Delta}):\mathbb{Q}(\sqrt{b},\sqrt{\Delta})]}^{d}\overbrace{[\mathbb{Q}(\sqrt{b},\sqrt{\Delta}):\mathbb{Q}(\sqrt{\Delta})]}^{2}\overbrace{[\mathbb{Q}(\sqrt{\Delta}):\mathbb{Q}]}^{2}$$

$= d \cdot 2 \cdot 2$ con $d \leq 2$

Poiché $\sqrt{b} \notin \mathbb{Q}(\sqrt{\Delta})$, esiste $\sigma \in Gal\left(K/\mathbb{Q}(\sqrt{\Delta})\right)$ tale che $\sigma(\sqrt{b}) \neq \sqrt{b}$ e quindi $\sigma(\sqrt{b}) = -\sqrt{b}$.

Poiché $\sqrt{\Delta}$ è fissato da σ, abbiamo $\left.\begin{array}{l}\sigma(\omega_1) = \omega_1 \\ \sigma(\omega_2) = \omega_2\end{array}\right\} \Rightarrow \begin{array}{l}\sigma(\sqrt{\omega_1}) = \pm\sqrt{\omega_1} \\ \sigma(\sqrt{\omega_2}) = \pm\sqrt{\omega_2}\end{array}$

Affermo che $\sigma(\sqrt{\omega_1}) = -\sqrt{\omega_1}$ oppure $\sigma(\sqrt{\omega_2}) = -\sqrt{\omega_2}$.

Infatti altrimenti σ sarebbe banale, in contraddizione con $\sigma(\sqrt{b}) = -\sqrt{b}$.

Supponiamo, a meno di scambiare ω_1 e ω_2, che $\sigma(\sqrt{\omega_1}) = -\sqrt{\omega_1}$.

Ne segue che $\sigma(\sqrt{\omega_2}) = \sigma\left(\sqrt{b}/\sqrt{\omega_1}\right) = (-\sqrt{b})/(-\sqrt{\omega_1}) = \sqrt{\omega_2}$

Quindi si ha:

$$\begin{tikzcd}
\sqrt{\omega_1} \arrow[dr, leftrightarrow, "\sigma"'] & \sqrt{\omega_2} \arrow[dl, leftrightarrow, "\sigma"] \\
-\sqrt{\omega_2} & -\sqrt{\omega_1}
\end{tikzcd}$$

Notiamo ora che $\sqrt{\Delta} \notin \mathbb{Q}(\sqrt{b})$ (altrimenti per questioni di grado avrei $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{b})$, che è falso).

Sia dunque $\tau \in Gal\left(K/\mathbb{Q}(\sqrt{b})\right)$ tale che $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$.

Quindi $\tau(\omega_1) = \omega_2$ e si deve avere che $\tau(\sqrt{\omega_1}) = \pm\sqrt{\omega_2}$.

Supponiamo $\tau(\sqrt{\omega_1}) = \sqrt{\omega_2}$. Allora $\tau(\sqrt{\omega_2}) = \tau\left(\sqrt{b}/\sqrt{\omega_1}\right) = \sqrt{b}/\sqrt{\omega_2} = \sqrt{\omega_1}$.

Allora:

$$\begin{tikzcd}
\sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"] & \sqrt{\omega_2} \\
-\sqrt{\omega_2} \arrow[r, leftrightarrow, "\tau"] & -\sqrt{\omega_1}
\end{tikzcd}$$

Si vede che $\tau\sigma$ ha ordine 4, mentre τ e σ hanno ordine 2.

Si ha il seguente diagramma:

$$\begin{tikzcd}
\sqrt{\omega_1} \arrow[d, mapsto, "\tau\sigma"'] & \sqrt{\omega_2} \arrow[l, mapsto, "\tau\sigma"'] \\
-\sqrt{\omega_2} \arrow[r, mapsto, "\tau\sigma"] & -\sqrt{\omega_1} \arrow[u, mapsto, "\tau\sigma"']
\end{tikzcd}$$

(Analogo se fosse stato $\tau(\sqrt{\omega_1}) = -\sqrt{\omega_2}$).

Dunque, poiché $G < S_4$, deve essere $G = \overset{\text{2-Sylow di } S_4}{D_4}$ e $[K : \mathbb{Q}] = 8$.

A questo punto posso guardare il quadro più ampio.

In $\mathrm{Gal}\left(K/\mathbb{Q}(\sqrt{\Delta})\right)$ ho:

$$\left.\begin{array}{ll} \sigma: & \sqrt{\omega_1} \longmapsto -\sqrt{\omega_1} \\ & \sqrt{\omega_2} \longmapsto \sqrt{\omega_2} \\ \text{e} \quad \sigma': & \sqrt{\omega_1} \longmapsto \sqrt{\omega_1} \\ & \sqrt{\omega_2} \longmapsto -\sqrt{\omega_2} \end{array}\right\} \text{generano uno } \mathbb{Z}_2 \times \mathbb{Z}_2$$

Ma in G devo avere anche un elementi di ordine 4, cerchiamoli:

$$\left.\begin{tikzcd}
\sqrt{\omega_1} \arrow[r, mapsto, "\lambda"] & \sqrt{\omega_2} \arrow[d, mapsto, "\lambda"] \\
-\sqrt{\omega_2} \arrow[u, mapsto, "\lambda"] & -\sqrt{\omega_1} \arrow[l, mapsto, "\lambda"']
\end{tikzcd}\right\} \lambda \text{ genera uno } \mathbb{Z}_4$$

$D_4 \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \Rightarrow$ ho trovato due generatori di G! $\Rightarrow G = \langle \lambda, \sigma \rangle$

Dentro il gruppo di Galois posso vedere i sottogruppi: cerco quindi i sottocampi di K pensandoli in corrispondenza con i sottogruppi di $G \cong D_4 = \langle \lambda, \sigma \rangle$:

$\langle \lambda \rangle$	$\langle \lambda^2 \rangle$	$\langle \lambda^2, \sigma \rangle$	$\langle \lambda^2, \lambda\sigma \rangle$
$\mathbb{Q}(\sqrt{b \cdot \Delta})$	$\mathbb{Q}(\sqrt{\Delta}, \sqrt{b})$	$\mathbb{Q}(\sqrt{\Delta})$	$\mathbb{Q}(\sqrt{b})$
$\langle \sigma \rangle$	$\langle \lambda\sigma \rangle$	$\langle \lambda^2\sigma \rangle$	$\langle \lambda^3\sigma \rangle$
$\mathbb{Q}(\sqrt{\omega_2}, \sqrt{\Delta})$	$\mathbb{Q}(\sqrt{\omega_1} - \sqrt{\omega_2}, \sqrt{b})$	$\mathbb{Q}(\sqrt{\omega_1}, \sqrt{\Delta})$	$\mathbb{Q}(\sqrt{\omega_1} + \sqrt{\omega_2}, \sqrt{b})$

$K = \mathbb{Q}(\zeta_5) \overset{4}{\text{———}} \mathbb{Q}$, $\mathrm{Aut}\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right) \cong (\mathbb{Z}_5)^* \cong \mathbb{Z}_4$

Esercizio 2. Per quali $n \in \mathbb{Z}$ $\sqrt{n} \in K = \mathbb{Q}(\zeta_5)$?

Sol: Sicuramente se n è un quadrato in $\mathbb{Z}$, $\sqrt{n} \in K$.

$\mathrm{Gal}\left(K/\mathbb{Q}\right)$ è generato da $\sigma : \zeta_5 \to \zeta_5^2$.

Chi è $K^{\langle \sigma^2 \rangle}$ (= il campo fissato dal sgrp generato da σ^2)?

Sicuramente $\alpha = \zeta_5 + \zeta_5^{-1} = \zeta_5 + \zeta_5^{4} \in K^{\langle \sigma^2 \rangle}$. Chi è il polinomio minimo di $\alpha \in K^{\langle \sigma^2 \rangle}$? $\alpha^2 = \zeta_5^2 + \zeta_5^3 + 2 \Rightarrow \alpha$ è radice di $x^2 + x - 1$ con $\Delta = 5$, quindi ha radici in $\mathbb{Q}(\sqrt{5}) \Rightarrow K^{\langle \sigma^2 \rangle} = \mathbb{Q}(\sqrt{5})$

$\rightarrow$ se $n = 5m^2$, con $m \in \mathbb{Z} \Rightarrow \sqrt{n} \in K$.

Esercizio 3: Per quali $n \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_7)$?

In generale, per quali $u \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_p)$ con p primo?

01-12-2021 lezione 26 Prof. Gaiffi

Teorema:

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i) \quad \text{di radici primitive } n\text{-esime di } 1$$

Dobbiamo dimostrare che:

1) $\Phi_n(x) \in \mathbb{Z}[x]$

2) Il campo di spezzamento di $\Phi_n(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\zeta_n)$ e il gruppo di Galois è $\cong \mathbb{Z}_n^*$

Notazione: $f(x) = x^n - 1$

Dim.

Considero il cds su $\mathbb{Q}$ di $f(x)$. Tale campo è $\mathbb{Q}(\zeta_n)$.

L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ è di Galois perché $x^n - 1$ è separabile.

$$\vartheta : \mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \longrightarrow \mathrm{Aut}(\mathbb{Z}_n)$$

$$\sigma \longmapsto \sigma|_{(\zeta_n)}$$

gruppo ciclico moltiplicativo generato da ζ_n

È ben definita.

(ζ_n) è il gruppo ciclico moltiplicativo generato da ζ_n.

Sia $\sigma_1 : (\zeta_n) \longrightarrow (\zeta_n)$

Dato che σ iniettivo $\Rightarrow$ σ bigettivo

σ è in particolare OMO MOLTIPLICATIVO allora $\sigma_1 \in Aut\left((\zeta_n)\right)$

Inoltre ϑ è iniettivo perché se $\sigma_1 =$ identità allora $\sigma(\zeta_n) = \zeta_n$ dunque

$\sigma = Id$ in $Aut\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$.

Oss: Per ora possiamo dunque dire che $\left|Aut\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)\right| \leqslant \varphi(n)$ $\circledast$

Lemma: Sia n intero positivo, sia ω una radice primitiva n-esima di 1. Sia $q(x) \in \mathbb{Z}[x]$ il suo polinomio minimo PRIMITIVO.

↳ polinomio minimo in $\mathbb{Q}$ con i coef. "aggiustati"

Allora $\forall p$ primo tale che $p \nmid n$, vale che ω^p è radice di $q(x)$.

Dim (Lemma)

Per il Lemma di Gauss: $f(x) = x^n - 1 = q(x)g(x)$ con $\underbrace{q(x), g(x)}_{\text{PRIMITIVI}} \in \mathbb{Z}[x]$

Dato che il coef. direttore di $f(x)$ è 1 posso supporre che i coef. dir. di $q(x)$ e $g(x)$ siano entrambi 1 (l'alternativa era entrambi $= -1$).

So che ω è radice di $q(x)$ ω^p è radice di $x^n - 1$ dunque se non fosse radice di $q(x)$ dovrebbe essere radice di $g(x)$.

Dunque ω è radice di $g(x^p)$. Allora $q(x) \mid g(x^p)$

↳ perché era pol minimo di ω

Per il Lemma di Gauss $\overbrace{g(x^p) = q(x)h(x)}^{\circledast}$ con $h(x) \in \mathbb{Z}[x]$ PRIMITIVO e si osserva che il coef. direttore di $h(x)$ è 1.

Proietto la relazione $\circledast$ in $\mathbb{Z}_p[x]$.

Osservo che $\overline{g(x^p)} = (\bar{g}(x))^p$ (non si annullano perché i pol. erano monici)

perché in $\mathbb{Z}_p[x]$ per ogni polinomio $\gamma(x)$ vale $\gamma(x^p) = (\gamma(x))^p$

Dunque in $\mathbb{Z}_p[x]$, riassumendo, ho:

$*$ $\bar{f}(x) = \bar{q}(x)\,\bar{g}(x)$ e $**$ $(\bar{g}(x))^p = \bar{q}(x)\,\bar{h}(x)$

$**$ implica che una radice di $\bar{q}(x)$ (in una estensione) è anche radice di $\bar{g}(x)$.

Da $*$ deduco dunque che $\bar{f}(x)$ ha almeno una radice multipla.

Ma $\bar{f}'(x) = n\,x^{n-1}$ e ricordiamo che $p \nmid n$ dunque non è 0.

Sia b l'inverso di n in $\mathbb{Z}_p$. Consideriamo:

$$\bar{f}(x) - b\,\bar{f}'(x)\,x = x^n - 1 - x^n = -1$$

dunque $\mathrm{MCD}(\bar{f}, \bar{f}) = 1$ e questo contraddice il criterio della derivata. □

Dim. Teo. (continua)

Sia $q(x)$ come sopra, il polinomio minimo primitivo in $\mathbb{Z}[x]$ di ζ_n.

Le radici primitive n-esime di uno sono della forma ζ_n^k con $(n,k)=1$.

Sia $k = p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ con $(p_i, n) = 1$.

ζ_n è radice di $q(x)$ (per costruzione)

Domanda: $\zeta_n^{p_1}$ è radice di $q(x)$? Sì, per il Lemma

$(\zeta_n^{p_1})^{p_1} = \zeta_n^{p_1^2}$ " " " $q(x)$? Sì, per il lemma applicato a $\zeta_n^{p_1}$

$\downarrow$ e così via

$\zeta_n^{p_1^{\alpha_1} \dots p_r^{\alpha_r}} = \zeta_n^k$ è radice di $q(x)$

Quindi $q(x)$ è diviso da tutte le radici n-esime primitive.

Dunque $\Phi_n(x) \mid q(x)$. Ma $\deg q(x) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$

↳ perché $q(x)$ è pol min di ζ_n

$$\text{Ma } [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \left| \mathrm{Aut}\left(\underbrace{\mathbb{Q}(\zeta_n) / \mathbb{Q}}_{\text{è di Galois perché } \mathbb{Q}(\zeta_n) \text{ è campo di spezzamento di } x^n - 1 \text{ su } \mathbb{Q}} \right) \right|$$

allora $\deg q(x) = \left| \mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \right| \leq \varphi(n)$ per la disuguaglianza ⊛

Dato che $\Phi_n(x) \mid q(x)$ deduco che $\deg q(x) = \varphi(n)$.

Poiché $\phi_n(x)$ e $q(x)$ sono entrambi monici segue che $\phi_n(x) = q(x)$.

FINALE: Tornando all'omomorfismo iniettivo ϑ

$$\vartheta : \mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \longrightarrow \mathrm{Aut}(\mathbb{Z}_n)$$

Ora, per ragioni di cardinalità sappiamo che è un ISO.

Infatti sappiamo che $\left|\mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)\right| = \varphi(n)$.

$\square$

—— o ——

Problema inverso di Galois:

1) Dato G gruppo finito, esiste un estensione di campi $F \subseteq K$ di Galois tale che $\mathrm{Aut}(K/F) \cong G$?

2) Dato G gruppo finito, esiste una estensione di campi $\mathbb{Q} \subseteq K$ tale che $\mathrm{Aut}(K/\mathbb{Q}) \cong G$? È un problema aperto (in generale).

Studiamo il caso G gruppo abeliano finito

Come sappiamo $\mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \mathbb{Z}_n^*$.

Dunque per esempio se io volessi costruire una estensione $\mathbb{Q} \subseteq K$ tale che $\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}_{14}$.

Potrei considerare $n = 29$, $\mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \mathbb{Z}_{29}^* \cong \mathbb{Z}_{28}$

In $\mathbb{Z}_{28}$ considero $H = (14) = \}0, 14\{$, ha indice 14.

$H \triangleleft \mathbb{Z}_{28}$ e per il teorema di corrispondenza di Galois il campo fisso di H, ossia $J(H)$ (Fix H) è tale che $[J(H) : \mathbb{Q}] = 14$, l'estensione $\mathbb{Q} \subseteq J(H)$ è di Galois, e $\mathrm{Aut}\left(J(H)/\mathbb{Q}\right) \cong \mathbb{Z}_{28}/H = (14)$

Cosa mi è servito? $\cong \mathbb{Z}_{14}$

Mi è servito prendere il 29, ossia un primo $\equiv 1 \mod 14$.

SUPPONIAMO di sapere (forma DEBOLE del teorema di Dirichlet) che $\forall n$ intero positivo ci sono infiniti primi della forma $kn + 1$

Sia A gruppo abeliano finito.

Allora $A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_s}$ con $d_1 \mid d_2 \mid \dots \mid d_s$.

Per la forma debole di Dirichlet posso prendere $p_1, \dots, p_s$ PRIMI DISTINTI.

$p_1 \equiv 1 \ (d_1)$

$p_2 \equiv 1 \ (d_2)$

$\vdots$

$p_s \equiv 1 \ (d_s)$

Considero $n = p_1 \cdots p_s$. Guardo l'estensione $\mathbb{Q}(\zeta_n) / \mathbb{Q}$: è di Galois.

$$\mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{p_1}) \times \mathrm{Aut}(\mathbb{Z}_{p_2}) \times \dots \times \mathrm{Aut}(\mathbb{Z}_{p_s})$$
$$\cong \mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \times \dots \times \mathbb{Z}_{p_s-1}$$

Prendo il sgrp. $H = (d_1) \times (d_2) \times \dots \times (d_s)$ di $\mathbb{Z}_{p_1-1} \times \dots \times \mathbb{Z}_{p_s-1}$

Considero $\mathcal{J}(H)$. Dato che H è normale (il gruppo è abeliano)

$\mathbb{Q} \leq \mathcal{J}(H)$ è di Galois e $\mathrm{Aut}\left(\mathcal{J}(H)/\mathbb{Q}\right) \cong \dfrac{\mathbb{Z}_{p_1-1} \times \dots \times \mathbb{Z}_{p_s-1}}{(d_1) \times \dots \times (d_s)}$

$$\cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_s} \cong A$$

——— o ———

Ripasso sui campi finiti:

Sappiamo che $\mathbb{F}_{p^n}$ è di Galois su $\mathbb{F}_p$ perché è campo di spezzamento di $x^{p^n} - x$ e sappiamo che $\mathrm{Aut}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \cong \mathbb{Z}_n$ (generatore $\mathcal{F}$)

Per ogni $d \mid n$ ho in $\mathbb{Z}_n$ un sgruppo isomorfo a $\mathbb{Z}_d$ (ossia $\left(\frac{n}{d}\right)$).

Allora $\mathcal{J}\left(\left(\frac{n}{d}\right)\right)$ è un sottocampo di $\mathbb{F}_{p^n}$ il cui grado su $\mathbb{F}_p$ è d.

Allora tale sottocampo è isomorfo a $\mathbb{F}_{p^d}$.

D'altra parte sapevamo già che se $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$ allora $[K : \mathbb{F}_p] \mid n$.

Conclusione: I sottocampi di $\mathbb{F}_{p^n}$ sono tutti e soli gli $\mathbb{F}_{p^d}$ con $d \mid n$

Conseguenza sui polinomi:

Sia $f(x)$ un polinomio di grado d irriducibile su $\mathbb{F}_p$.

$$\mathbb{F}_p / (f(x)) = K \cong \mathbb{F}_{p^d}$$

Sappiamo inoltre che $f(x)$ ha tutte le radici in $\mathbb{F}_{p^d}$.

Infatti sicuramente in K $f(x)$ ha una radice α.

Inoltre so che gli el di $K \cong \mathbb{F}_{p^d}$ sono tutte e sole le sol di $x^{p^d} - x$.

Allora $f(x) \mid x^{p^d} - x$ perché entrambi hanno α una radice e $f(x)$ è il polinomio minimo.

Allora tutte le radici di $f(x)$ sono anche radici di $x^{p^d} - x$ e dunque sono in K.

Per ragioni di grado K è il campo di spezzamento di $f(x)$

Dato che $f(x)$ era un qualunque irriducibile di grado d, posso concludere che $\mathbb{F}_{p^d}$ è il campo di spezzamento di qualunque polinomio irriducibile de grado d su $\mathbb{F}_p$.

Corollario: Sia $f(x) \in \mathbb{F}_p(x)$, $f(x) = q_1(x) \dots q_k(x)$ con i $q_i(x)$ irriducibili di grado rispettivamente $\beta_1, \beta_2, \dots, \beta_k$.

Allora il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^{mcm(\beta_1, .., \beta_k)}}$.

Dim. Sia K il campo di spezzamento. Dato che contiene un cds di $q_1(x)$ allora contiene $\mathbb{F}_{p^{\beta_1}}$, dunque $\beta_1 \mid [K : \mathbb{F}_p]$,

e così via...

$$\beta_j \mid [K : \mathbb{F}_p],$$

dunque $mcm(\beta_1, \dots, \beta_k) \mid [K : \mathbb{F}_p]$ e viceversa $\mathbb{F}_{p^{mcm(\beta_1, \dots, \beta_k)}}$ ha questo grado.

02-12-2021 Lezione 27 Prof. Gaiffi

Esercizio (11.3.9): Sia $\mathbb{K}$ sottoestensione di Galois K.

Sia F sottoestensione di K. Siano $\mathbb{K}, F \subseteq L$. Allora $\mathbb{K}F$ è di Galois su F e $\mathbb{K}$ è di Galois su $\mathbb{K} \cap F$.

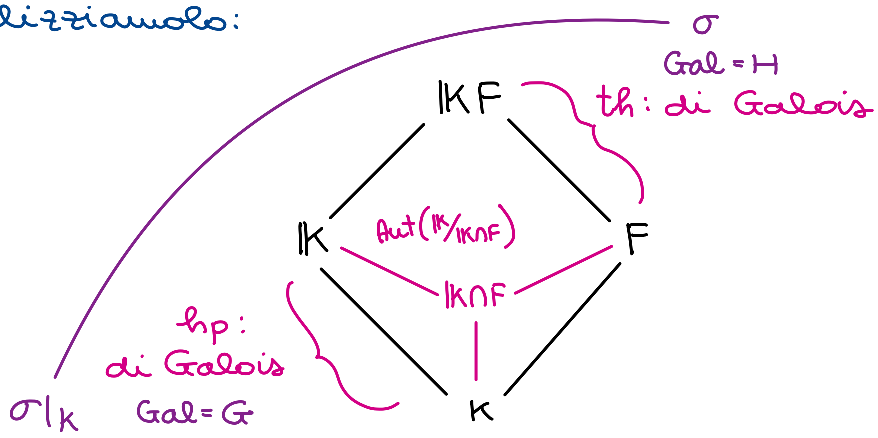
Siano $H = \text{Aut}\left(\mathbb{K}F/_F\right)$ e $G = \text{Aut}\left(\mathbb{K}/_K\right)$.

Sia $\Phi : H \to G$

$$\sigma \mapsto \sigma|_K$$

allora Φ è isomorfismo fra H e $\text{Aut}\left(\mathbb{K}/_{\mathbb{K}\cap F}\right)$.

Visualizziamolo:



$\mathbb{K}F = \left\{ \dfrac{\text{somme finite di prodotti di el. di } K \text{ ed el di } F}{\text{somme finite di } \ldots \neq 0} \right\}$

Esempio: $\dfrac{k_1 f_1 + k_2 f_2 + \ldots + k_s f_s}{\underbrace{k_1' f_1' + k_2' f_2' + \ldots + k_s' f_s'}_{\neq 0}}$

Dim: Sia $\sigma \in \text{Aut}\left(\mathbb{K}F/_F\right)$.

$\sigma|_K \in \text{Aut}\left(\mathbb{K}/_K\right)$ perché $\mathbb{K} \supseteq K$ è di Galois.

Quindi Φ è OMO ben definito.

Poiché σ fissa F allora $\sigma|_K$ fissa $\mathbb{K}\cap F$ quindi $\text{Im}\,\Phi \subseteq \text{Aut}\left(\mathbb{K}/_{\mathbb{K}\cap F}\right)$.

Chi è $\text{Ker}\,\Phi$? Sia $\sigma \in \text{Ker}\,\Phi$ allora $\Phi|_K = $ identità.

σ fissa F e fissa $\mathbb{K}$, quindi σ fissa tutti gli elementi $\dfrac{k_1 f_1 + \cdots}{k_1' f_1' + \cdots}$ di $\mathbb{K}F$.

Dunque Φ è iniettiva.

Sia $\alpha \in \mathbb{K}$ un elemento lasciato fisso da tutti gli automorfismi di

$\text{Im}\,\Phi = \Phi(H)$ è $\sigma|_K$.

Dunque $\forall \sigma \in Aut\left(\mathbb{K}F/F\right)$ vale che $\sigma|_{\mathbb{K}}(\alpha)=\alpha$, ossia $\sigma(\alpha)=\alpha$.

Poiché $\mathbb{K}F \supseteq F$ è di Galois ⊛ $\alpha \in$ al campo base F.

Dunque scopro che $\alpha \in \mathbb{K}\cap F$. Ho dunque dimostrato che il campo fisso di $\Phi(H)$ è $\mathbb{K}\cap F$. Poiché $\mathbb{K} \supseteq \mathbb{K}\cap F$ è di Galois, per la Prop. 11.1.1 vale che $\Phi(H)=Aut\left(\mathbb{K}/\mathbb{K}\cap F\right)$.

↳ perché l'estensione alta è di Galois

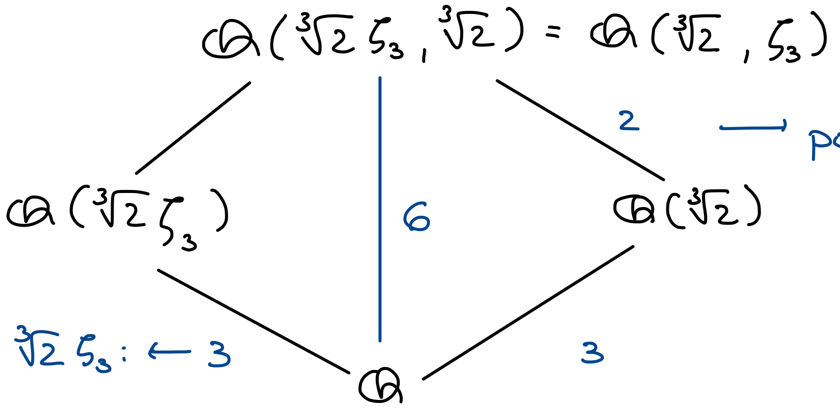
⊛ perché $\mathbb{K}$ è un campo di spezzamento di un polinomio separabile $f(x) \in k[x]$. $\mathbb{K}F$ è campo di spezzamento di $f(x)$ su F

OSSIA se $\mathbb{K}=k(\gamma_1,\dots,\gamma_r)$, $\mathbb{K}F=F(\gamma_1,\dots,\gamma_r)$

Corollario: Siano $\mathbb{K}$ ed F come nelle ipotesi sopra.

Allora $[\mathbb{K}F : F] \mid [\mathbb{K}:k]$. È falso se $\mathbb{K}$ non è di Galois.

Controesempio se $\mathbb{K} \supseteq k$ non è di Galois:



⟶ pol min di ζ_3: x^2+x+1

pol. min di $\sqrt[3]{2}\zeta_3$: ← 3
x^3-2

Esercizio (11.3.10):

Siano K_1 e K_2 estensioni di Galois di k e sia $K_1, K_2 \subseteq L$ campo. Allora K_1K_2 è di Galois su k. Inoltre la mappa

$$\vartheta : Aut\left(K_1K_2/k\right) \longrightarrow Aut\left(K_1/k\right) \times Aut\left(K_2/k\right)$$

è un omomorfismo iniettivo.

Inoltre se $K_1 \cap K_2 = k$ allora ϑ è isomorfismo.

Dim. K_1 sia campo di spezzamento di un certo polinomio $f_1(x)$ su k.
K_2 " " " " " " " $f_2(x)$ su k.

separabili

Allora $K_1K_2 = K(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$ dove $\alpha_1, \dots, \alpha_r$ sono le radici di $f_1(x)$

e $\beta_1, \dots, \beta_s$ " " " di $f_2(x)$

Dunque K_1K_2 è il cds di $f_1(x)f_2(x)$ che è separabile in quanto prodotto di separabili.

ϑ omo iniettivo è immediato perché se per un $\sigma \in \mathrm{Aut}\left(K_1K_2/K\right)$.

Vale $\sigma|_{K_1} = id$ e $\sigma|_{K_2} = id$, allora $\sigma = Id$ su K_1K_2.

Sia infine $K_1 \cap K_2 = K$.

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash, "\text{di Galois}"'] \arrow[dr, dash, "\substack{H\ \sigma \\ \text{di Galois}}"] & \\
K_1 \arrow[dr, dash, "\substack{\text{di Galois} \\ \sigma_1\ G}"'] & & K_2 \arrow[dl, dash, "\text{di Galois}"] \\
 & K = K_1 \cap K_2 &
\end{tikzcd}$$

Per quanto visto nell'esercizio precedente, se $\sigma_1 \in G = \mathrm{Aut}\left(K_1/K\right)$

$\exists\, \sigma \in \mathrm{Aut}\left(K_1K_2/K_2\right)$ tale che $\sigma|_{K_1} = \sigma_1$.

Ora noto che $\vartheta(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2}) = (\sigma_1, Id)$.

Allora in $\mathrm{Im}\,\vartheta$ ho $\mathrm{Aut}\left(K_1/K\right) \times \}Id\{$.

Analogamente dimostro che in $\mathrm{Im}\,\vartheta$ c'è $\}Id\{ \times \mathrm{Aut}\left(K_2/K\right)$.

Dunque $\mathrm{Im}\,\vartheta = \mathrm{Aut}\left(K_1/K\right) \times \mathrm{Aut}\left(K_2/K\right)$.

Esercizio Si consideri K campo di spezzamento su $\mathbb{Q}$ di $x^5 - 2$.

Determinare $[K : \mathbb{Q}]$ e $\mathrm{Aut}\left(K/\mathbb{Q}\right)$ e infine descrivere, se esistono, i sottocampi di K di grado 5 su $\mathbb{Q}$.

Sol.

$$\begin{tikzcd}
 & K = \mathbb{Q}(\zeta_5, \sqrt[5]{2}) \arrow[dl, dash, "\substack{\text{di Galois} \\ \text{il Gal fissa}}"'] \arrow[dr, dash, "\leq 4"] \arrow[dd, dash, dashed, "\substack{\text{di Galois} \\ 20}"] & \\
\mathbb{Q}(\zeta_5) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\sqrt[5]{2}) \arrow[dl, dash, "5"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

chiamo H il suo Gal
↑
di Galois

chiamo G il Gal
↑
di Galois
(cds di Φ_4)

4 ↓ perché radice di Φ_4

5 ↓ radice di $x^5 - 2$ irrid. per Eis. + L.G.

$\mathrm{Aut}\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right) \underset{\substack{\downarrow \\ \text{per il} \\ \text{Teorema}}}{\cong} \mathbb{Z}_5^* \cong \mathbb{Z}_4$ → è ciclico

↓

è ciclico generato da τ dove $\tau(\zeta_5) = \zeta_5^2$

Per il primo esercizio so che $H \cong G$ e più precisamente che esiste $\tilde{\tau} \in \mathrm{Aut}\left(K/\mathbb{Q}(\sqrt[5]{2})\right) = H$ tale che $\tilde{\tau}|_{\mathbb{Q}(\zeta_5)} = \tau$

IN CONCRETO:
$$\left.\begin{aligned} \tilde{\tau}(\sqrt[5]{2}) &= \sqrt[5]{2} \\ \tilde{\tau}(\zeta_5) &= \zeta_5^2 \end{aligned}\right\} o(\tilde{\tau}) = 4 \rightarrow \text{stesso ordine di } \tau$$

Ora noto che $\mathrm{Aut}\left(K/\mathbb{Q}(\zeta_5)\right)$ è ciclico di ordine 5 ed è generato da σ

$\sigma(\zeta_5) = \zeta_5$ → lascio fisso il campo base

$\sigma(\sqrt[5]{2}) = \sqrt[5]{2}\,\zeta_5$

Dunque in $\mathrm{Aut}(K/\mathbb{Q})$ ho $(\tilde{\tau})$ e (σ).

Dato che $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$ è di Galois, $(\sigma) \triangleleft \mathrm{Aut}(K/\mathbb{Q})$.

Poiché $(\sigma) \cap (\tilde{\tau}) = \{0\}$ segue che $\mathrm{Aut}(K/\mathbb{Q}) = (\sigma)(\tilde{\tau})$ ossia è $\cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$

Es: Fare il coniugio $\tau \sigma^j \tau^{-1} = \sigma^{2j}$

Per descrivere i sottocampi di grado 5 come i sgrp di $\mathrm{Aut}(K/\mathbb{Q})$ di ordine 4. Uno lo conosco: è $H = (\tilde{\tau})$ (ha ordine 4)

Non è normale perché il suo $\underbrace{\text{campo fisso}}_{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{2})}$ non è di Galois, ma è un 2-Sylow.

$n_2 \equiv 1 \ (2)$ e $n_2 \mid 5$. Visto che $\boxed{n_2 \neq 1}$ allora $n_2 = 5$.

Quindi per il teorema di corrispondenza so che avrò 5 sottogruppi.

Uno di essi è $\mathbb{Q}(\sqrt[5]{2})$. Gli altri 2-Sylow sono i coniugati di H:

$$H, \ \sigma H \sigma^{-1}, \ \sigma^2 H \sigma^{-2}, \ \sigma^3 H \sigma^{-3}, \ \sigma^4 H \sigma^{-4}$$

So che $\mathrm{Fix}(H) = \mathbb{Q}(\sqrt[5]{2}) = K_0$, chi è $\mathrm{Fix}(\sigma H \sigma^{-1})$?

Considero $\sigma(\mathbb{Q}(\sqrt[5]{2}))$, è un sottocampo.

Considero ora $\sigma H \overbrace{\sigma^{-1}\sigma}^{id}(\mathbb{Q}(\sqrt[5]{2}))$

$\sigma h \sigma^{-1}\sigma (\overset{\Downarrow}{p}) \to$ viene mandato in sé stesso

Dunque $\mathrm{Fix}(\sigma H \sigma^{-1}) = \sigma(\mathbb{Q}(\sqrt[5]{2})) = \mathbb{Q}(\sqrt[5]{2}\,\zeta_5) = K_1$

Analogamente $\mathrm{Fix}(\sigma^i H \sigma^{-i}) = \sigma^i(\mathbb{Q}(\sqrt[5]{2})) = K_i$ sono tutti distinti tra loro

Oss: Noto che $\forall i \neq j \quad K_i \cap K_j = \mathbb{Q}$ (Per ragioni di grado)

* * *

Problema inverso di Galois (FORMULAZIONE I)

1) Dato G gruppo finito, esiste un estensione di campi $F \subseteq K$ di Galois tale che $\mathrm{Aut}(K/F) \cong G$?

Sia $G = S_n$. Considero $F(x_1, \dots, x_n) = \left\{ \dfrac{g(x_1,\dots,x_n)}{h(x_1,\dots,x_n)} \;\middle|\; \begin{array}{l} g(\dots) \in F[x_1,\dots,x_n] \\ h(\dots) \in F[x_1,\dots,x_n] \setminus \{0\} \end{array} \right\}$

S_n agisce su S_n permutando le variabili.

Agisce come un atomorfismo: $\sigma \in S_n$ $\quad \sigma(f+g) = \sigma(f) + \sigma(g)$

$$\sigma(fg) = \sigma(f)\,\sigma(g)$$

Dunque $\sigma \in \mathrm{Aut}\left(\mathrm{Fix}(x_1,\dots,x_n)/F\right)$.

Allora $S_n < \mathrm{Aut}\left(F(x_1,\dots,x_n)/F\right)$.

è di Galois e il Gal è S_n $\left[\begin{array}{c} F(x_1,\dots,x_n) \\ \cup| \\ \mathrm{Fix}(S_n) \\ \cup| \\ F \end{array}\right.$

Def. $\mathrm{Fix}(S_n)$ è il campo delle funzioni razionali simmetriche

03-12-2021 Lezione 28 Prof. Callegaro

Avevamo visto che $\sqrt{5} \in \mathbb{Q}(\varepsilon_5)$. Vediamo un altro caso.

Esercizio 1: ⓐ Quali sono gli $n \in \mathbb{Z}$ tali che $\sqrt{n} \in \mathbb{Q}(\zeta_7)$?

$\mathbb{Q}(\zeta_7)$ ha grado 6 su $\mathbb{Q}$, dunque devo considerare le sottoestensioni di grado 2 su $\mathbb{Q}$. Per il Teorema di Corrispondenza ciò equivale a trovare i sottogruppi del Galois di indice 2, ovvero di cardinalità 3. $G := \mathrm{Aut}\left(\mathbb{Q}(\xi_7)/\mathbb{Q}\right) \cong (\mathbb{Z}_7)^* \cong \mathbb{Z}_6$ che ha un unico sottogruppo di indice 2, e quindi di ordine 3, vediamo chi è:

G è generato da $\sigma: \zeta_7 \longrightarrow \zeta_7^3$ che ha ordine 6.

I sottogruppi di G da chi sono generati? C'è un sottogruppo di ordine 2 generato da σ^3 e uno di ordine 3 generato da σ^2.

Quindi voglio concentrarmi sul campo fisso dell'unico sottogruppo di ordine 3: quali elementi lascia fisso σ^2? $\sigma^2: \zeta_7 \longrightarrow \zeta_7^2$

Per capire chi sta nel campo fisso di $<\sigma^2>$ posso studiarne l'orbita: $\varepsilon_7 + \varepsilon_7^2 + \varepsilon_7^4 = \alpha$, è chiaro che α viene lasciato fisso

$\hookrightarrow \in \text{orb} \hookleftarrow$

da σ^2. Infatti ho:

$$\sigma^2(\varepsilon_7 + \varepsilon_7^2 + \varepsilon_7^4) = \sigma^2(\varepsilon_7) + \sigma^2(\varepsilon_7^2) + \sigma^2(\varepsilon_7^4) = \varepsilon_7^2 + \varepsilon_4^4 + \underset{\overset{\shortparallel}{\varepsilon_7}}{\varepsilon_7^8} = \alpha$$

Dunque ho la seguente torre di estensione:

$$\begin{tikzcd}
\mathbb{Q}(\varepsilon_7) \arrow[d, dash] \arrow[dd, dash, bend right=60, "6"'] & & \\
\mathbb{Q}(\alpha) \arrow[d, dash, "\leq 2"] & \subseteq & \mathbb{Q}(\varepsilon_7)^{<\sigma^2>} \arrow[dll, dash, "2"] \\
\mathbb{Q} & &
\end{tikzcd}$$

cioè il campo fisso rispetto a σ^2

Come faccio a concludere che sono $=$?

Considero $\alpha^2 = \underbrace{\varepsilon_7^2 + \varepsilon_7^4 + \varepsilon_7}_{\alpha} + 2\varepsilon_7^3 + 2\varepsilon_7^5 + 2\varepsilon_7^6$

So che $1 + \varepsilon_7 + \varepsilon_7^2 + \dots + \varepsilon_7^6 = 0$. Ma allora ho che:

$\alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha$ è radice di $p(x) = x^2 + x + 2$.

$\Delta = 1 - 8 = -7$ non è $\square$ in $\mathbb{Q} \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7}) = \mathbb{Q}(i\sqrt{7})$

Questo mi dimostra che il grado di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$ è 2 e quindi che $\mathbb{Q}(\alpha)$ è il campo fisso di $<\sigma^2>$.

Tutti i quadrati che posso trovare in $\mathbb{Q}(\varepsilon_7)$ si trovano in $\mathbb{Q}(i\sqrt{7})$.

ⓑ Cerco adesso $\mathbb{F}$ tc $\mathbb{Q}(\varepsilon_7) \subseteq \mathbb{F} \subseteq \mathbb{Q}$ di grado 3 su $\mathbb{Q}$.

Sarà $\text{Fix}(<\sigma^3>)$. Analogamente studio σ^3:

$$\left.\begin{aligned} \sigma^3: \quad & \varepsilon_7 \longrightarrow \varepsilon_7^{-1} \\ & \varepsilon_7 + \varepsilon_7^{-1} \longrightarrow \varepsilon_7^{-1} + \varepsilon_7 \end{aligned}\right\} \sigma^3 \text{ fissa } \beta = \varepsilon_7 + \varepsilon_7^{-1} \Rightarrow \mathbb{Q}(\beta) \subseteq \text{Fix}(<\sigma^3>) = \mathbb{F}$$

Voglio dimostrare che sono uguali, ho due strade:

① Dimostrare che il polinomio minimo di β ha grado 3

② So che ho questa estensione:

$$\begin{tikzcd}
\mathbb{Q}(\xi_7) \arrow[d, dash, "\leq 2"] \\
\mathbb{Q}(\beta) \arrow[d, dash, "\leq 3"] \\
\mathbb{Q} \arrow[uu, dash, bend left, "6"]
\end{tikzcd}$$

Mi basta dire che questa estensione ha grado ≤ 2

↓

Trovo il polinomio minimo di ξ_7 su $\mathbb{Q}(\beta)$

↓

$x^2 - \beta x + 1 \in \mathbb{Q}(\beta)[x]$ e si annulla in ξ_7

↓

L'estensione ha grado ≤ 2

<u>Esercizio</u>: Sia p un primo, per quali n ho $\sqrt{n} \in \mathbb{Q}(\xi_p)$?

<u>Esercizio 2</u>: ⓐ Trovare K un'estensione di Galois su $\mathbb{Q}$ tale che

$$\mathrm{Gal}\left(K/\mathbb{Q}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 .$$

$$K = \mathbb{Q}(\xi_{15}) \Rightarrow \mathrm{Gal}\left(\mathbb{Q}(\xi_{15})/\mathbb{Q}\right) \cong (\mathbb{Z}_{15})^* \cong (\mathbb{Z}_3)^* \times (\mathbb{Z}_5)^*$$
$$\cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

ⓑ Trovare K un'est. di Galois su $\mathbb{Q}$ tale che $\mathrm{Gal}\left(K/\mathbb{Q}\right) \cong \mathbb{Z}_8$

Cerco un primo p tale che $p \equiv 1 \ (8)$, ad esempio $p = 17$.

$G := \mathrm{Gal}\left(\mathbb{Q}(\xi_{17})/\mathbb{Q}\right) \cong (\mathbb{Z}_{17})^* \cong \mathbb{Z}_{16}$, prendo $\tau \in G$ tale che

$$\left.\begin{aligned} \tau : \ & \xi_{17} \longrightarrow \xi_{17}^{-1} \\ & \xi_{17} + \xi_{17}^{-1} \longrightarrow \xi_{17}^{-1} + \xi_{17} \end{aligned}\right\} \text{come prima: } \mathrm{Fix}(\langle \tau \rangle) = \mathbb{Q}(\underbrace{\xi_{17} + \xi_{17}^{-1}}_{\beta})$$

Ho la seguente torre di estensione:

$$\begin{tikzcd}
\mathbb{Q}(\xi_{17}) \arrow[d, dash, "\leq 2 \rightsquigarrow x^2 - \beta x + 1 \text{ pol. minimo}"] \\
\mathbb{Q}(\xi_{17} + \xi_{17}^{-1}) = K \Rightarrow \mathrm{Gal}\left(K/\mathbb{Q}\right) \cong \mathbb{Z}_8 \arrow[d, dash, "\leq 8"] \\
\mathbb{Q}
\end{tikzcd}$$

ⓒ Trovare K un'est. di Galois su $\mathbb{Q}$ tale che $\mathrm{Gal}\left(K/\mathbb{Q}\right) \cong \mathbb{Z}_2^3$

Considero $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, devo mostrare che ha grado 8 su $\mathbb{Q}$:

$$\begin{tikzcd}[arrows=-]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl] \arrow[dr] \arrow[dd, "4"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\sqrt{2}$ radice di x^2-2 ↙ ↝ x^2-3 si annulla in $\sqrt{3}$

$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$ perché altrimenti dovrei avere, presi $a,b\in\mathbb{Q}$

$(a+b\sqrt{3})^2=a^2+3b^2+2ab\sqrt{3}=2 \Rightarrow ab=0 \wedge (a^2=2 \vee 3b^2=2)$ ↯

In generale: $\mathbb{Q}(\sqrt{n})=\mathbb{Q}(\sqrt{m}) \Leftrightarrow mn$ è un □ in $\mathbb{Q}$

Ho dimostrato che $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$, per dimostrare $[\mathbb{K}:\mathbb{Q}(\sqrt{5})]=2$ non basta confrontare $\sqrt{5}$ con $\sqrt{2}$ e $\sqrt{3}$ perché in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ c'è una terza estensione quadratica: $\mathbb{Q}(\sqrt{6})$. Dunque ho:

$$\begin{tikzcd}[arrows=-]
 & & \mathbb{K} \arrow[dll] \arrow[dr] & \\
\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d] \arrow[dr] \arrow[drr] & & & \mathbb{Q}(\sqrt{5}) \arrow[ddl] \\
\mathbb{Q}(\sqrt{6}) \arrow[drr] & \mathbb{Q}(\sqrt{2}) \arrow[dr] & \mathbb{Q}(\sqrt{3}) \arrow[d] & \\
 & & \mathbb{Q} &
\end{tikzcd}$$

Per dimostrare che $[\mathbb{K}:\mathbb{Q}]=8$ mi basta vedere che queste quattro estensioni quadratiche sono tutte distinte.

Vediamo ora il Galois: $G:=\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ è generato da:

$$\sigma_1:\begin{cases}\sqrt{2}\longmapsto-\sqrt{2}\\ \sqrt{3}\longmapsto\sqrt{3}\\ \sqrt{5}\longmapsto\sqrt{5}\end{cases} \qquad \sigma_1:\begin{cases}\sqrt{2}\longmapsto\sqrt{2}\\ \sqrt{3}\longmapsto-\sqrt{3}\\ \sqrt{5}\longmapsto\sqrt{5}\end{cases} \qquad \sigma_1:\begin{cases}\sqrt{2}\longmapsto\sqrt{2}\\ \sqrt{3}\longmapsto\sqrt{3}\\ \sqrt{5}\longmapsto-\sqrt{5}\end{cases}$$

Siamo sicuri che un tale elemento esista perché se G ha 8 elementi questi saranno della forma $\sigma:\begin{cases}\sqrt{2}\longmapsto\pm\sqrt{2}\\ \sqrt{3}\longmapsto\pm\sqrt{3}\\ \sqrt{5}\longmapsto\pm\sqrt{5}\end{cases}$ perché siamo obbligati a mandare ogni elemento in una radice del suo polinomio minimo, ma in questo caso ho al massimo 8 elementi, quindi questo mi garantisce l'esistenza di $\sigma_1,\sigma_2,\sigma_3$: questi chiaramente commutano fra loro e hanno ordine 2.

Dunque possiamo concludere $G \cong \mathbb{Z}_2^3$.

<u>Esercizio 3</u>: Sia $p(x) = (x^4 - x^2 + 1)(x^2 - 3)$, calcolare il campo di spezzamento e gruppo di Galois su $\mathbb{Q}$ e su $\mathbb{F}_{13}$.

Noto che $(x^4 - x^2 + 1)(x^4 + x^2 + 1)(x^4 - 1) = x^{12} - 1$

Come sappiamo dalla teoria: $(x^4 - 1) = \phi_1(x)\phi_2(x)\phi_4(x)$ e $(x^4 + x^2 + 1) = \phi_3(x)\phi_6(x)$ e poiché $x^{12} - 1 = \prod_{d \mid 12} \phi_d(x)$ otteniamo $x^4 - x^2 + 1 = \phi_{12}(x)$, dunque il suo cds è $\mathbb{Q}(\varepsilon_{12})$, mentre $x^2 - 3$ si annulla in $\sqrt{3}$, dunque il suo cds è $\mathbb{Q}(\sqrt{3})$.

Per studiare il cds su $\mathbb{Q}$ di $p(x)$ studio quindi $\mathbb{Q}(\varepsilon_{12}, \sqrt{3})$

$$\begin{tikzcd}
& \mathbb{Q}(\varepsilon_{12}, \sqrt{3}) = \mathbb{K} \arrow[dl, dash] \arrow[dd, dash, "\leq 8"] \arrow[dr, dash] & \\
\mathbb{Q}(\varepsilon_{12}) \arrow[dr, dash, "\varphi(12) = 4"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Il gruppo è $\cong (\mathbb{Z}_{12})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ ← Galois

↓

3 sottoest. di grado 2

Per capire $[\mathbb{K} : \mathbb{Q}]$ devo studiare $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\varepsilon_{12})$.

Cerco le sottoestensioni non banali di $\mathbb{Q}(\varepsilon_{12})$:

ε_{12} è radice 12^a primitiva di 1

ε_{12}^3 è radice 4^a primitiva di 1

ε_{12}^4 è radice 3^a primitiva di 1

Dunque $\varepsilon_3 \cdot \varepsilon_4$ è radice 12^a primitiva di 1 $\Rightarrow \mathbb{Q}(\varepsilon_{12}) = \mathbb{Q}(\varepsilon_3, \varepsilon_4)$.

lo sapevamo anche dalla teoria

Allora ho il seguente "diamante":

$$\begin{tikzcd}
& \mathbb{Q}(\varepsilon_{12}) = \mathbb{K} \supseteq \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \arrow[dd, dash, "4"] \arrow[dr, dash] & \\
\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\varepsilon_3) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\varepsilon_4) = \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

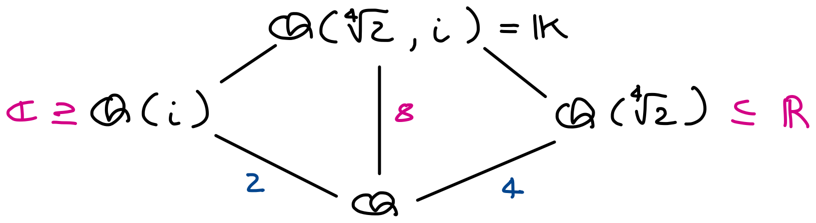
Dunque $\mathbb{Q}(\varepsilon_{12}, \sqrt{3}) = \mathbb{Q}(\varepsilon_{12}) = \mathbb{K}$ e $[\mathbb{K} : \mathbb{Q}] = 4$, quindi ho $Gal\left(\mathbb{K}/\mathbb{Q}\right) \cong (\mathbb{Z}_{12})^* \cong (\mathbb{Z}_3)^* \times (\mathbb{Z}_4)^* \cong \mathbb{Z}_2^2$ (come sappiamo dalla teoria).

In $\mathbb{F}_{13}$ ho invece che $x^{13}-x \equiv 0 \ (13) \ \forall x$, dunque si ha che il c. di sp. di x^4-x^2+1 è $\mathbb{F}_{13}$ perché $x^{13}-x \equiv x(x^{12}-1) \equiv 0 \ (13)$; d'altra parte $-3 \equiv 36 \ (13) \Rightarrow x^2-3=(x+6)(x-6)$, dunque il suo cds è $\mathbb{F}_{13} \Rightarrow$ Il cds di $p(x)$ su $\mathbb{F}_{13}$ è proprio $\mathbb{F}_{13}$.

Esercizio 4 (11.3.5 delle dispense): Calcolare il cds e gruppo di Galois di $p(x)=x^6-2x^4-8x^2+16$ su $\mathbb{Q}$, $\mathbb{F}_3$ e $\mathbb{F}_9$.

Noto che $p(x)=x^4(x^2-2)-8(x^2-2)=(x^2-2)(x^4-8)$, perciò considero $\mathbb{Q}(\sqrt{2},\sqrt[4]{8},i)$, ma $(\sqrt[4]{2})^2=\sqrt{2}$ e $(\sqrt[4]{2})^3=\sqrt[4]{8} \Rightarrow$ il cds è $\mathbb{Q}(\sqrt[4]{2},i)$.

Allora guardo le torri di estensioni:



Gli elementi di $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ sono del tipo $\begin{cases} \sqrt[4]{2} \longmapsto (i)^a \sqrt[4]{2} \\ i \longmapsto \pm i \end{cases}$, con $a=0,\dots,3$.
Poiché $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})|=8$, tutte queste "ipotesi di automorfismi" sono possibili.
Infine, visto che $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ ha un sottogruppo di ordine 4 e un sottogruppo di ordine 2 non normale e inoltre $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ non è di Galois, $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \cong D_4$.

Su $\mathbb{F}_3$, $p(x)=(x^2-2)(x^4-2)$. 2 non è un quadrato in $\mathbb{F}_3$, dunque $\mathbb{F}_3(\sqrt{2})$ è un'estensione di grado 2 in cui x^2-2 si spezza, ma esiste un'unica estensione di grado 2 ed è $\mathbb{F}_{3^2}=\mathbb{F}_9$.
Poiché $2^2 \equiv 1 \ (3)$, una radice 4^a di 2 è 8^a di 1. $\mathbb{F}_9^* \cong \mathbb{Z}_8$, quindi x^8-1 ha come radici gli elementi di $\mathbb{F}_9^*$. Quindi il gruppo di Galois è $\mathrm{Gal}\left(\mathbb{F}_{3^2}/\mathbb{F}_3\right) \cong \mathbb{Z}_2$

Esercizio 5: Calcolare il campo di spezzamento e gruppo di Galois del polinomio $f(x)=x^6-2$ su $\mathbb{Q}$.

Chiamo E il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ e chiamo $G = Gal(E/\mathbb{Q})$. Considero $E = \mathbb{Q}(\xi_6, \sqrt[6]{2})$. Sappiamo che $\xi_6^2 - \xi_6 + 1 = 0$, cioè ξ_6 è radice di x^2-x+1 che ha $\Delta = -3 \Rightarrow \mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{-3})$.

$$\begin{tikzcd}
 & E \arrow[dd, dash, "12"] \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{R} \not\supseteq \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\xi_6) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{R} \arrow[dl, dash, "6"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\rightsquigarrow$ $x^6 - 2$ è irriducibile per Eisenstein + Lemma di Gauss

Quindi $[E : \mathbb{Q}] = 12$. G non è abeliano perché $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{2})$ non è di Galois e quindi non tutti i sottogruppi di G sono normali in G.

G contiene un sottogruppo di ordine 6, in quanto se considero il campo $F = \mathbb{Q}(\sqrt{-3})$ e di conseguenza $E = F(\sqrt[6]{2})$, il gruppo $Gal(E/F)$ ha 6 elementi determinati univocamente in base a dove mando $\sqrt[6]{2}$, cioè $\sqrt[6]{2} \mapsto \xi_6^a \sqrt[6]{2}$, con $a = 0, \_, 5$ (cioè 6 scelte).

E contiene un campo K tale che $\mathbb{Q} \leq K$ è di Galois e $Gal(K/\mathbb{Q}) \cong \mathbb{Z}_2^2$?

⌜Soluzione:

$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$ e ha grado 2 su $\mathbb{Q}$
$\mathbb{Q}(\xi_6) = \mathbb{Q}(i\sqrt{3}) \subseteq E$ e ha grado 2 su $\mathbb{Q}$
$\Big\}$ $K = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$

$K \leq \mathbb{Q}$ è di Galois perché cds di $(x^2-x+1)(x^2-2)$, e $[K:\mathbb{Q}] = 4$, infatti:

$$i\sqrt{3} \in \mathbb{Q}(\sqrt{2}) \Leftrightarrow (a+b\sqrt{2})^2 = (i\sqrt{3})^2 \Leftrightarrow a^2 + 2ab\sqrt{2} + 2b^2 = -3 \Leftrightarrow 2ab\sqrt{2} = 0 \begin{cases} \overset{a=0}{\Rightarrow} 2b^2 = -3 \ \lightning \\ \overset{b=0}{\Rightarrow} a^2 = -3 \ \lightning \end{cases}$$

$|Gal(K/\mathbb{Q})| = 4$ e i suoi elementi devono mandare radici in radici.

Dunque ho $\sigma : \begin{cases} \sqrt{2} \to \pm\sqrt{2} \\ i\sqrt{3} \to \pm i\sqrt{3} \end{cases}$ 4 possibili automorfismi, tanti quanti gli elem. del Galois. I generatori sono: $\sigma_1 : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ i\sqrt{3} \to i\sqrt{3} \end{cases}$ e $\sigma_2 : \begin{cases} \sqrt{2} \to \sqrt{2} \\ i\sqrt{3} \to -i\sqrt{3} \end{cases}$.

$\sigma_1^2(\sqrt{2}) = \sqrt{2}$ e $\sigma_2^2(i\sqrt{3}) = i\sqrt{3}$, dunque sono due elementi di ordine 2.

Dunque $Gal\left(K/\mathbb{Q}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ ($\exists!\, x \in \mathbb{Z}_4$ tc $x^2 = e$)

⌟

09-12-2021 Lezione 29 Prof. Gaiffi

Esercizio: Sia K campo finito e siano α, β algebrici su K con $[K(\alpha):K]=5$ e $[K(\beta):K]=4$. Dimostrare che $[K(\alpha\beta):K]=20$

Sol: $K=\mathbb{F}_q$ con q potenza di un primo (conosciamo tutti i campi finiti)

$$\begin{tikzcd}
 & K(\alpha,\beta) \arrow[dl, dash] \arrow[dr, dash, "\leq 5"] \arrow[dd, dash, dashed, "20"'] & \\
K(\alpha) \arrow[dr, dash, "5"'] & & K(\beta) = \mathbb{F}_{q^4} \arrow[dl, dash, "4"] \\
 & K &
\end{tikzcd}$$

poiché $[K(\alpha,\beta):K] \leq 20$ ed è diviso da 4 e 5 allora $[K(\alpha,\beta):K]=20.$

$K \subseteq K(\alpha\beta) \subseteq K(\alpha,\beta)$

Dunque $$[K(\alpha\beta):K] = \begin{array}{l} \left.\begin{array}{l} 1 \\ 2 \\ 4 \end{array}\right\} \text{caso ①} \\ \left.\begin{array}{l} 5 \\ 10 \\ 20 \end{array}\right\} \text{caso ②} \end{array}$$

Caso ①: Avrei allora $\alpha\beta \in \mathbb{F}_{q^4}$ $\left(\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n} \Leftrightarrow d \mid n\right)$

Poiché $K(\beta)=\mathbb{F}_{q^4}$ in questo campo troverei $\frac{\alpha\beta}{\beta}=\alpha$, ma $[K(\alpha):K]=5$ ↯

Caso ②: allora $K(\alpha\beta)$ contiene $\mathbb{F}_{p^5} \cong K(\alpha)$ e quindi $K(\alpha\beta)$ contiene $\frac{\alpha\beta}{\alpha}=\beta$. Allora $[K(\alpha\beta):K]=20$ e per questioni di grado $K(\alpha\beta)=K(\alpha,\beta)$.

Esercizio: Sia $f(x) \in \mathbb{Q}[x]$ irriducibile di grado 6.

Determinare le possibili fattorizzazioni in $\mathbb{Q}(\sqrt{2})(x)$.

Sol: Sia $\alpha \in \mathbb{C}$ una radice di $f(x)$.

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha,\sqrt{2}) \arrow[dl, dash, "\leq 2"'] \arrow[dr, dash] \arrow[dd, dash, "6 \text{ o } 12"'] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "6"'] & & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

grado del fattore irrid. di $f(x)$ in $\mathbb{Q}(\sqrt{2})(x)$ che si annulla in α

$[\mathbb{Q}(\alpha,\sqrt{2}):\mathbb{Q}] = \begin{cases} 12 \\ 6 \end{cases}$

Di conseguenza $[\mathbb{Q}(\alpha,\sqrt{2}):\mathbb{Q}(\sqrt{2})] = \begin{cases} 3 \\ 6 \end{cases}$

Tutto dipende da se $\sqrt{2} \in \mathbb{Q}(\alpha)$ oppure no. Ci sono dunque 2 casi:

1) $f(x)$ si spezza in due fattori irrid. di grado 3 in $\mathbb{Q}(\sqrt{2})(x)$.

Es. $x^6 - 2 = (x^3 - \sqrt{2})(x^3 + \sqrt{2})$

2) $f(x)$ rimane irriducibile in $\mathbb{Q}(\sqrt{2})(x)$.

Es. $x^6 + x^5 + x^4 + x^3 + x + 1$

In $\mathbb{Q}(\zeta_7)$ dato che $\mathrm{Aut}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right) \cong \mathbb{Z}_6$ esiste una sola sottoestensione di grado 2 ed è $\mathbb{Q}(i\sqrt{7})$.

Quindi $\mathbb{Q}(\sqrt{2}) \not\subseteq \mathbb{Q}(\zeta_7)$ e $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ è irrid. in $\mathbb{Q}(\sqrt{2})(x)$

Esercizio: Sia $p(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$

① Trovare il campo di spezzamento K su $\mathbb{Q}$

② Calcolare $[K:\mathbb{Q}]$

③ Determinare $\mathrm{Aut}(K/\mathbb{Q})$

Sol: ① Si trovano le radici: $\pm\sqrt{1 \pm \sqrt{3}}$

Sia $\alpha = \sqrt{1+\sqrt{3}}$, $\beta = \sqrt{1-\sqrt{3}} \in \mathbb{C} \setminus \mathbb{R}$

$[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ perché $x^4 - 2x^2 - 2$ è irriducibile (per Eisenstein)

$$\begin{tikzcd}
\mathbb{Q}(\alpha,\beta) \arrow[d, dash, "\geq 2"] \\
\mathbb{Q}(\alpha) \arrow[d, dash, "4"] \\
\mathbb{Q}
\end{tikzcd}$$

Noto che $\alpha^2 = 1 + \sqrt{3}$. Dunque $\sqrt{3} \in \mathbb{Q}(\alpha)$. Ora $\beta^2 = 1 - \sqrt{3}$ quindi β è radice di $x^2 - 1 + \sqrt{3}$ in $\mathbb{Q}(\alpha)[x]$.

Allora $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] = 2$.

Infine $K = \mathbb{Q}(\alpha,\beta)$ dunque $[K:\mathbb{Q}] = 8$.

Noto che $\mathbb{Q} \leq \mathbb{Q}(\alpha)$ non è di Galois perché non è preservata dagli automorfismi in $\mathrm{Aut}(K/\mathbb{Q})$.

Quindi $\mathrm{Aut}(K/\mathbb{Q})$ non è abeliano perché contiene un sgrp non normale.

Dato che in Q_8 tutti i sottogruppi sono normali $\Rightarrow \mathrm{Aut}\left(K/\mathbb{Q}\right) \cong D_4$

vista la classificazione dei gruppi di ordine 8.

Guardiamo più in dettaglio.

Sia c un coniugio in $\mathbb{C}$:

$c(\alpha)=\alpha$

$c(-\alpha)=-\alpha$

$c(\beta)=-\beta$

$c(-\beta)=\beta$

$\mathbb{Q} \subseteq K$ è di Galois quindi è invariante per c che è automorfismo di $\mathbb{C}$

Quindi $c \in \mathrm{Aut}\left(K/\mathbb{Q}\right)$ e ha ordine 2.

Allora $\mathrm{Fix}(\langle c\rangle) = \mathbb{Q}(\alpha)$ (per ragioni di grado)

Se calcolo $\alpha\beta = \sqrt{1+\sqrt{3}}\,\sqrt{1-\sqrt{3}} = \sqrt{1-3} = i\sqrt{2} \in K$. Dunque $\mathbb{Q}(i\sqrt{2}) \subseteq K$.

↓ di Galois

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha\beta,\alpha)=\mathbb{Q}(\alpha,\beta)=K \arrow[dl, dash, "4"'] \arrow[dr, dash] & \\
\mathbb{Q}(i\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\alpha\beta$

$x^2+2 \leftarrow 2$

un Aut φ in $\mathrm{Aut}\left(K/\mathbb{Q}(i\sqrt{2})\right)$ è determinato da $\varphi(\alpha)$

β è determinato da α perché $\mathrm{Aut}\left(K/\mathbb{Q}(i\sqrt{2})\right)$ lascia fisso $i\sqrt{2} = \alpha\beta$.

Il polinomio x^4-2x^2-2 è irriducibile su $\mathbb{Q}(i\sqrt{2})$ perché il grado $[K : \mathbb{Q}(i\sqrt{2})] = 4$. In $\mathrm{Aut}\left(K/\mathbb{Q}(i\sqrt{2})\right)$

$\varphi_1 : \alpha \to \alpha$

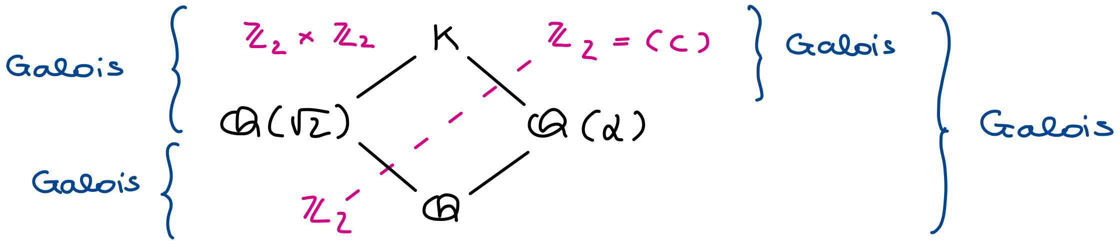
$\varphi_2 : \alpha \to -\alpha$

$\varphi_3 : \alpha \to \beta$

$\varphi_4 : \alpha \to -\beta$

ricorda: $\alpha\beta = i\sqrt{2}$ è fisso allora se $\alpha \to \alpha$, $\beta \to \beta$ mentre se $\alpha \to -\alpha$, $\beta \to -\beta$

Dunque $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ hanno ordine 2 (Sono il Klein)



$\mathrm{Aut}(K/\mathbb{Q}) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ ← uno dei due è normale, l'altro no e il loro prodotto dà tutto.

$c\varphi_3 c = \ ?$

$c\varphi_3 c(\alpha) = c\varphi_3(\alpha) = c(\beta) = -\beta$

Dunque $c\varphi_3 c = \varphi_4$ → Non commutano!

Es: Esibire un elemento di ordine 4 Hint: iniziare dall'oss. precedente

Esercizio: $x^7 - 2$, K campo di spezzamento su $\mathbb{Q}$. Sia $L = K \cap \mathbb{R}$.

① Calcolare $[L : \mathbb{Q}]$

② Dire se L è di Galois su $\mathbb{Q}$. Se non lo è, determinare la massima estensione di Galois contenuta in L.

Sol: radici $\zeta_7^i \alpha$ con $\alpha = \sqrt[7]{2}$

$$\begin{tikzcd} & K \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "42"] & \\ \mathbb{Q}(\zeta_7) \arrow[dr, dash, "6"'] & & \mathbb{Q}(\sqrt[7]{2}) \arrow[dl, dash, "7"] \\ & \mathbb{Q} & \end{tikzcd}$$

$\mathrm{Gal} \cong \mathbb{Z}_6$

↗ il coniugio $c \in \mathrm{Aut}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)$

$\mathrm{Fix}((c))$ ha dunque grado 3 su $\mathbb{Q}$.

$\overset{\shortparallel}{\mathbb{Q}(\zeta_7) \cap \mathbb{R}}$ è di Galois?

Dato che (c) è normale in $\mathbb{Z}_6$ allora $\mathbb{Q}(\zeta_7) \cap \mathbb{R} = \mathrm{Fix}((c))$ è di Galois* in $\mathbb{Q}$ e $\mathrm{Aut}\left(\mathrm{Fix}((c))/\mathbb{Q}\right) \cong \mathbb{Z}_3$. ⊛ Per il Teorema di corrispondenza!

Tentativo: Costruisco $\mathrm{Fix}((c))\mathbb{Q}(\alpha)$.

Per ragioni di grado $\mathrm{Fix}((c))\mathbb{Q}(\alpha)$ ha grado 21 su $\mathbb{Q}$

$$\begin{tikzcd}
& \mathrm{Fix}(\langle c\rangle)\mathbb{Q}(\alpha) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "21"] & \\
\mathrm{Fix}(\langle c\rangle) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "7"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Analogamente per ragioni di grado ho che $[K:\mathbb{Q}]=42$.

Noto che c è anche in $\mathrm{Aut}(K/\mathbb{Q})$.

$L=\mathrm{Fix}\, c$ visto come sottocampo di K allora $[L:\mathbb{Q}]=21$.

Dunque per ragioni di grado $L=(\mathbb{Q}(\zeta_7)\cap\mathbb{R})\mathbb{Q}(\alpha)$.

Infine, $\mathbb{Q}\leq L$ non è di Galois perchè contiene α ma non $\zeta_7\alpha$.

$$\begin{array}{l} \mathbb{Q}(\zeta_7)\cap\mathbb{R}\subset L \\ \quad \cup\!| \text{ è di Galois} \\ \mathbb{Q} \end{array}$$

Se M è la massima (per inclusione) sottoestensione di Galois di L allora $M\geq\mathbb{Q}(\zeta_7)\cap\mathbb{R}$ e dunque $3\mid[M:\mathbb{Q}]\mid 21$ dunque $[M:\mathbb{Q}]=3$ e $M=\mathbb{Q}(\varepsilon_7)\cap\mathbb{R}$.

10-12-2021 Lezione 30 Prof. Callegaro

Esercizio 1. Sia $p(x)=(x^2-2)(x^2-3)(x^2-6)$, chi è il cds su $\mathbb{Q}$?

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{6}) = \arrow[d] & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash, "4"] \\
\sqrt{6}=\sqrt{2}\cdot\sqrt{3} & \mathbb{Q}
\end{tikzcd}$$

$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)=\mathbb{Z}_2\times\mathbb{Z}_2$

$p(x)$ ha sempre almeno una radice in $\mathbb{F}_p$ $\forall p$ primo (Claim)

$$\left.\begin{array}{l} \text{Se } 2 \text{ non è un quadrato in } \mathbb{F}_p \\ \quad 3 \text{ " \ " \ " \qquad " \qquad " } \mathbb{F}_p \end{array}\right\} \Rightarrow 6 \text{ è un quadrato in } \mathbb{F}_p\ ?$$

$2,3\in\mathbb{F}_p^*$ ciclico di ordine $p-1$

$\square=\}x\in\mathbb{F}_p^*,\ \exists y\in\mathbb{F}_p^*$ tc $x=y^2\{$

in notazione additiva: $\square = \} x \in \underset{\substack{\downarrow \\ \text{ciclico} \\ \text{di ordine } m}}{G} \mid \exists y \in G \, , \, x = y + y = 2y \{$

Se prendo 2 elem. che non stanno nel gruppo allora questi staranno nell'unica altra classe laterale del gruppo

$G = C_m \longrightarrow \square = 2C_m$ e se m è pari $C_m / 2C_m \cong \mathbb{Z}_2$

In conclusione è sempre vero che il prodotto di due non quadrati è un quadrato in $\mathbb{F}_p$.

Esercizio 2: $p(x) = x^7 - 2$ su $\mathbb{F}_5$, chi è il cds? Gal?

Noto che $2 = (-2)^7$ in $\mathbb{F}_5$ perché $(-2)^4 = 4 = -1 \rightarrow (-2)^7 = (-2)^4(-2)^3 = 2$

$\Rightarrow p(x) = x^7 - (-2)^7$

Per avere il cds di $p(x)$ devo avere le radici 7-me di 1.

Per avere le radici 7e devo andare in un'estensione $\mathbb{F}_{5^k}$ in cui $\mathbb{F}_{5^k}^*$ contiene elementi di ordine $7 \Leftrightarrow \exists x \in \mathbb{F}_{5^k}^*$ tc $x^7 = 1$.

- $7 \mid 5^k - 1$ chi è l'ordine moltiplicativo di 5 modulo 7?

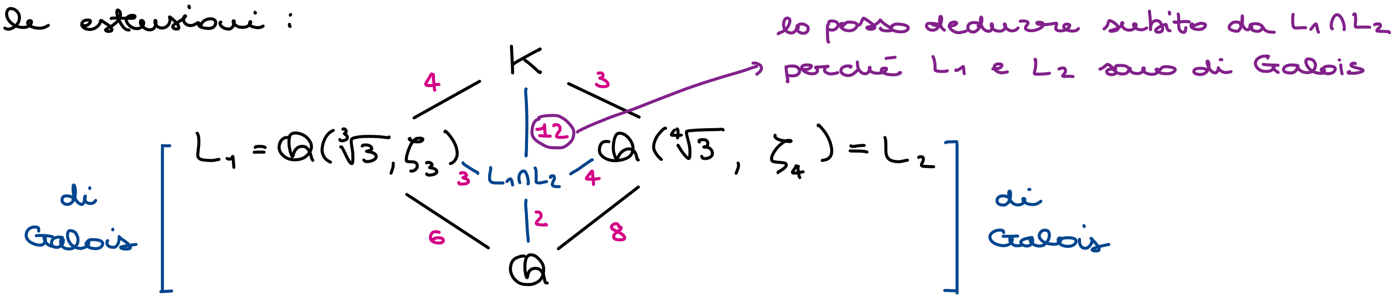
$5^2 \equiv 4 \ (7)$

$5^3 \equiv -1 \ (7)$

$5^6 \equiv 1 \ (7) \longrightarrow 7 \mid 5^6 - 1 \longrightarrow K = \mathbb{F}_{5^6} \overset{6}{\text{———}} \mathbb{F}_5 \, , \, \mathrm{Gal}\left(K / \mathbb{F}_5\right) \cong \mathbb{Z}_6$

Esercizio 3: $p(x) = (x^3 - 3)(x^4 - 3)$, cds su $\mathbb{Q}$.

Il cds è $K = \mathbb{Q}(\sqrt[3]{3}, \zeta_3, \sqrt[4]{3}, \zeta_4)$ ma per calcolare il grado devo ragionare con le estensioni:



$\sqrt[2]{3} \cdot i \in L_2 : \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3) \Rightarrow |L_1 \cap L_2| = 2$ è ≥ 2 e divide 6 e 8 $\Rightarrow$ è proprio 2

$\Rightarrow [K : \mathbb{Q}] = 24$.

- Mostrare che $\mathrm{Gal}\left(K / \mathbb{Q}\right)$ contiene un elemento σ tc σ fissa $i, \sqrt[3]{3}$

$\sigma : i\sqrt[3]{3} \longmapsto i\sqrt[3]{3}$

Considero il cds in questo modo:

Il gruppo di Galois ha 24 elementi $\Leftarrow 24$

$$\begin{tikzcd}
K = \mathbb{Q}(\sqrt[12]{3}, i) \arrow[d, dash, "2"] \\
\mathbb{Q}(\sqrt[12]{3}) = \mathbb{Q}(\sqrt[3]{3}, \sqrt[4]{3}) \arrow[d, dash, "12"] \\
\mathbb{Q}
\end{tikzcd}$$

Un elemento del gruppo è del tipo $\tau : \begin{cases} \sqrt[12]{3} \longmapsto \zeta_{12}^{a} \sqrt[12]{3} & a \in \mathbb{Z}_{12} \quad \text{12 scelte} \\ i \longmapsto \pm i & \text{2 scelte} \end{cases}$

Dunque ho 24 elem. in totale (come #Gal)

al massimo!

$$\sigma : \begin{cases} \sqrt[12]{3} \longmapsto -i \sqrt[12]{3} \\ i \longmapsto i \end{cases} \qquad \begin{aligned} \sqrt[4]{3} &\longmapsto i \sqrt[4]{3} \\ \sqrt[3]{3} &\longmapsto \sqrt[3]{3} \\ \frac{\sqrt[3]{3}}{\sqrt[4]{3}} &\longmapsto \frac{\boxed{-i}\sqrt[3]{3}}{\sqrt[4]{3}} \end{aligned}$$

$\frac{1}{i} = -i$

$\downarrow$ soddisfa le richieste

ottengo questo

scelta obbligata

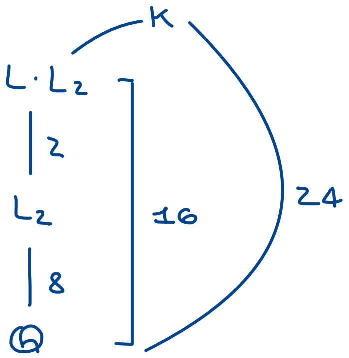
- Descrivere le sottoestensioni di K di grado 4 su $\mathbb{Q}$.

Sia $L \subset K$, $[L : \mathbb{Q}] = 4$. Allora per $L \cap \boxed{L_2}$ ho 3 possibili casi:

L_2 ha grado 8 su $\mathbb{Q}$

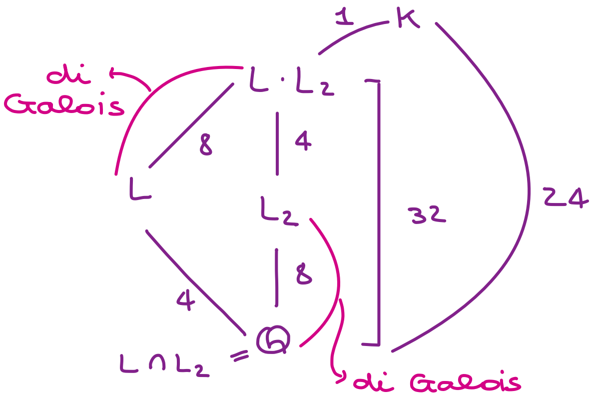
$$[L \cap L_2 : \mathbb{Q}] = \begin{cases} ① \text{ NO!} \\ ② \text{ NO!} \\ 4 \end{cases}$$

$[L \cap L_2 : \mathbb{Q}] = 2$



impossibile!

$[L \cap L_2 : \mathbb{Q}] = 1$



impossibile!

Quindi sto cercando le sottoestensioni di $L_2 = \mathbb{Q}(\sqrt[4]{3}, i)$ di grado 4 su $\mathbb{Q}$.

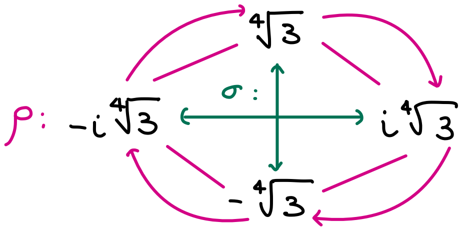
$\mathrm{Gal}(L_2/\mathbb{Q}) = D_4$
↳ è un sgrp di S_4 di 8 elementi ⇒ È D_4

In D_4 ho 5 el di ordine 2 (generano sgrp di indice 4)

$$D_4 = \left\langle \rho : \begin{cases} \sqrt[4]{3} \longmapsto \sqrt[4]{3}\, i \\ i \longmapsto i \end{cases} , \quad \sigma : \begin{cases} \sqrt[4]{3} \longmapsto \sqrt[4]{3} \\ i \longmapsto -i \end{cases} \right\rangle$$

↳ generatore di ordine 4 ↳ generatore di ordine 2 } generano tutto D_4

$\mathrm{Fix}\,\rho^2 = \mathbb{Q}(i, \sqrt[4]{3})$
$\mathrm{Fix}\,\sigma = \mathbb{Q}(\sqrt[4]{3})$
} c'è un contenimento e hanno lo stesso grado



$$\rho\sigma : \begin{cases} \sqrt[4]{3} \longmapsto i\sqrt[4]{3} \\ i \longmapsto -i \end{cases}$$

$\mathrm{Fix}(\rho^2\sigma) = \mathbb{Q}(i\sqrt[4]{3})$

$\mathrm{Fix}(\rho\sigma) \supset \mathbb{Q}(\underbrace{(i+1)\sqrt[4]{3}}_{v})$

$v \rightsquigarrow \underbrace{v^4}+12 = 0$
↳ irrid. per Eisenstein

$\mathrm{Fix}(\rho^3\sigma) = \mathbb{Q}((1-i)\sqrt[4]{3})$

$$\rho^2\sigma : \begin{cases} \sqrt[4]{3} \longmapsto -i\sqrt[4]{3} \\ i \longmapsto -i \end{cases}$$

Esercizio 4: Sia $t = x^3 + x^{-3}$ e $\mathbb{C}(x) \supset \mathbb{C}(t)$ un'estensione.

Che posso dire di questa estensione?

$$\begin{tikzcd}
\mathbb{C}(x) \arrow[d, dash, "\leq 3"] \\
\mathbb{C}(x^3) \arrow[d, dash, "\leq 2"] \\
\mathbb{C}(t) = \mathbb{C}(x^3 + x^{-3})
\end{tikzcd}$$

$\mathbb{C}(x^3)$ → chi è il polinomio minimo?

irriducibile in $\mathbb{C}[x^3][z]$
↓
$z^3 - x^3 \in \mathbb{C}(x^3)[z]$

$z^2 - tz + 1$ ha radici x^3, x^{-3}

$\Cap$

$\mathbb{C}(t)[z]$ ma lo posso pensare anche come pol. in $\mathbb{C}[t][z]$ ma

$x^3 \notin \mathbb{C}[t] = \mathbb{C}[x^3 + x^{-3}]$.

$\mathbb{C}(x)$ è di Galois su $\mathbb{C}(x^3)$.

$z^6 - tz^3 + 1$ è polinomio minimo di x in $\mathbb{C}(t)[z]$ e le radici sono $x\zeta_3^a$, $x^{-1}\zeta_3^a$ con $a \in \mathbb{Z}_3$.

$\mathbb{C}(x)/_{\mathbb{C}(t)}$ è di Galois di grado 6.

Un elemento $\sigma \in \mathrm{Gal}\left(\mathbb{C}(x)/_{\mathbb{C}(t)}\right)$ è determinato da $\sigma : x \longmapsto \zeta_3^a x^{\pm 1}$

Dunque ho 6 possibili elementi, tanti quanti #Gal

$\sigma_1 : x \longmapsto x^{-1} \qquad \sigma_1\sigma_2 : x \longmapsto \zeta_3 x^{-1}$

$\sigma_2 : x \longmapsto \zeta_3 x \qquad \sigma_2\sigma_1 : x \longmapsto \zeta_3^2 x^{-1}$

$\Rightarrow$ Gal non abeliano $\Rightarrow S_3$

- Quali sono le sottoestensioni proprie?

①
$$\begin{tikzcd}
\mathbb{C}(x^3) = \mathrm{Fix}(\sigma_2) \arrow[d, dash, "2"] \\
\mathbb{C}(t)
\end{tikzcd}$$

②
$$\begin{tikzcd}
\mathbb{C}(x) \arrow[d, dash, "\leq 2 \quad \text{perché radice di } z^2-(x+x^{-1})z+1"] & & \\
\mathbb{C}(x+x^{-1}) \arrow[rrd, dash, "\leq 3"'] & \subset & \mathrm{Fix}(\sigma_1) \arrow[d, dash, "3"] \\
& & \mathbb{C}(t)
\end{tikzcd}$$

③
$$\begin{tikzcd}
\mathbb{C}(x) \arrow[d, dash, "2"] & & \\
\mathrm{Fix}(\sigma_1\sigma_2) \arrow[rrd, dash, "\leq 3"'] & \subset & \mathbb{C}(x+\zeta_3 x^{-1}) \arrow[d, dash, "3"] \\
& & \mathbb{C}(t)
\end{tikzcd}$$

④

$$\begin{tikzcd}
\mathbb{C}(x) \arrow[d, dash, "\leq 2"] \arrow[r, phantom, "\to \; z^2-(x+\zeta_3^2 x^{-1})z+\zeta_3^2"] & {} \\
\mathrm{Fix}(\sigma_1\sigma_2^2) \supset \mathbb{C}(x+\zeta_3^2 x^{-1}) \arrow[d, dash, "\leq 3"] & \\
\mathbb{C}(t) &
\end{tikzcd}$$

Esercizio 5: Per quali $n \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_p)$ con p primo?

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[d, dash, "\varphi(p)=p-1"] \\
\mathbb{Q}
\end{tikzcd}
\longrightarrow \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}_p)^* \cong \mathbb{Z}_{p-1}$$

Contiene un'unica sottoestensione di grado 2 in $\mathbb{Q}$

$\updownarrow$ corrisponde

campo fisso dell'unico sgrp H di indice 2 in $\mathbb{F}_p^*$

Sia $\alpha = \sum_{\square \text{ in } \mathbb{Z}_p^*} \zeta_p^i = \sum_{\zeta_p^i \square \text{ in } \mathbb{F}_p^*} \zeta_p^i$

So anche però che $\sum_{i=0}^{p-1} \zeta_p^i = 0 = 1 + \sum_{\square \text{ in } \mathbb{Z}_p^*} \zeta_p^i + \sum_{\not\square \text{ in } \mathbb{Z}_p^*} \zeta_p^i$

Prendo $s = \sum_{\square \text{ in } \mathbb{Z}_p^*} \zeta_p^i - \sum_{\not\square \text{ in } \mathbb{Z}_p^*} \zeta_p^i$ che è invariante per H.

$S = \sum_{i \in \mathbb{Z}_p^*} \varepsilon_p(i) \zeta_p^i$ dove $\varepsilon_p(i) = \begin{cases} 1 & \square \text{ in } \mathbb{Z}_p^* \\ -1 & \not\square \text{ in } \mathbb{Z}_p^* \end{cases} \Rightarrow S^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \varepsilon_p(i)\varepsilon_p(j) \zeta_p^{i+j}$

Oss: In $\mathbb{Z}_p^*$ ho:

$\square \cdot \square = \square$

$\not\square \cdot \not\square = \square$

$\square \; \not\square = \not\square$

Guardo tutto in $\mathbb{Z}_p^*/_{\text{quadrati}} \cong \mathbb{Z}_2$, e ho che:

$$S^2 = \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} \varepsilon_p(ij)\zeta_p^{i+j} \overset{j=ik}{=} \sum_{i=1}^{p-1}\sum_{k=1}^{p-1} \varepsilon_p(i^2k)\zeta_p^{i+ik} = \sum_{i=1}^{p-1}\sum_{k=1}^{p-1} \varepsilon_p(k)\zeta_p^{i(k+1)} =$$

$$= \underbrace{\sum_{k=1}^{p-2}\sum_{i=1}^{p-1} \varepsilon_p(k)\zeta_p^{i(k+1)}}_{= -\varepsilon_p(k) \text{ perché } \sum_{i=1}^{p-1}\zeta_p^i = -1} + (p-1)\varepsilon_p(-1) = -\sum_{k=1}^{p-2} \varepsilon_p(k) + (p-1)\varepsilon_p(-1) =$$

$$= \underbrace{-\sum_{k=1}^{p-1} \varepsilon_p(k)}_{=0 \text{ perché } |\square| = |\not\square|} + p\varepsilon_p(-1) \Rightarrow S^2 = p\,\varepsilon_p(-1) = \begin{cases} p & \text{se } -1 \text{ è } \square \text{ in } \mathbb{Z}_p^* \\ -p & \text{se } -1 \text{ è } \not\square \text{ in } \mathbb{Z}_p^* \end{cases}$$

ma -1 è $\square$ in $\mathbb{Z}_p^* \iff 4 \mid p-1$, dunque $n = m^2$ o $n = m^2\sqrt{p}$ con $m \in \mathbb{Z}$,

e -1 è $\not\square$ in $\mathbb{Z}_p^* \iff 4 \mid p+1$, dunque $n = m^2$ o $n = m^2\sqrt{-p}$, con $m \in \mathbb{Z}$.