Università di Pisa - Dipartimento di Matematica

Esercitazioni di ALGEBRA I

Simmaco Di Lillo
dsimmaco@gmail.com

Rielaborazione delle lezioni di F. Callegaro

a.a. 2019-20

Indice

Parte I
Gruppi

1 Azioni per coniugio su S_n e A_n

1.1 S_n

Proposizione 1.1. *in S_n due permutazioni sono coniugate se e solo se hanno analoga decomposizioni in cicli disgiunti.*

Dimostrazione. Supponiamo che $\sigma' = \tau\sigma\tau^{-1}$ allora

$$\sigma'(\tau(i)) = \tau\sigma\tau^{-1}\tau(i) = \tau(\sigma(i))$$

Dunque la decomposizione in cicli disgiunti di σ' si ottiene da quella di σ sostituendo ogni numero i con $\tau(i)$.
Supponiamo adesso che σ e τ' abbiano analoga decomposizione in cicli disgiunti, ovvero

$$\sigma = \left(\sigma_1^{(1)}, \dots, \sigma_{l_1}^{(1)}\right) \dots \left(\sigma_1^{(k)}, \dots, \sigma_{l_k}^{(k)}\right)$$

$$\tau = \left(\tau_1^{(1)}, \dots, \tau_{l_1}^{(1)}\right) \dots \left(\tau_1^{(k)}, \dots, \tau_{l_k}^{(k)}\right)$$

allora possiamo considerare la permutazione

$$\rho = \begin{pmatrix} \sigma_1^{(1)} & \cdots & \sigma_{l_1}^{(1)} & \cdots & \sigma_1^k & \cdots & \sigma_{l_k}^{(k)} \\ \\ \tau_1^{(1)} & \cdots & \tau_{l_1}^{(1)} & \cdots & \tau_1^k & \cdots & \tau_{l_k}^{(k)} \end{pmatrix}$$

e otteniamo $\tau = \rho\sigma\rho^{-1}$ □

Esempio 1.2 (Calcolo del centralizzatore in S_n).
Studiare il centralizzatore $\sigma = (1, 2, 3)$ in S_8
Dalla proposizione precedente $orb(\sigma)$ è dato dai 3-cicli quindi

$$|orb(\sigma)| = \binom{8}{3} 2!$$

da cui

$$|C(\sigma)| = 3 \cdot 5!$$

Osserviamo che le potenze di σ appartengono al centralizzatore, così come quelle permutazioni di S_8 che lasciano fissi $1, 2, 3$.
Poichè le permutazioni che lasciano fissi $1, 2, 3$ sono isomorfe a S_5 e le potenze distinte di σ sono 3 otteniamo che

$$C(\sigma) = \{\sigma^i\beta \,| i = 0, 1, 2 \ \beta \in S_{\{4,5,6,7,8\}}\}$$

Generalizzando quanto detto sopra a tutte le permutazioni con un solo ciclo

Proposizione 1.3. *Sia $\sigma \in S_n$ con $o(\sigma) = o$ allora*

$$C(\sigma) = \{\sigma^i\beta \,|\, i = 0, \dots, o-1, \ \beta \in S_{n-o}\}$$

dove con S_{n-0} intendiamo quelle permutazione di S_n che lasciano fissi gli elementi mossi da σ

Possiamo considerare un meccanismo analogo anche se σ è scritto in cicli disgiunti ma con tutti i cicli di **lunghezza differenti**

Esempio 1.4. *Studiare il centralizzatore di* $\sigma = (1,2,3)(4,5,6)$ *in* S_6
Il numero dei 2 3-cicli in S_6 *è*

$$\frac{1}{2}\cdot\binom{6}{3}2!\cdot\binom{3}{3}2!$$

dunque il centralizzatore ha 18 *elementi.*
Se consideriamo il meccanismo di sopra riusciamo ad elencare solamente 9 *ovvero quelli della forma* $(1,2,3)^i(4,5,6)^j$ *con* $i,j=0,1,2$.
Gli altri elementi sono dati da quelle permutazioni che scambiano gli insiemi $\{1,2,3\}$ *e* $\{4,5,6\}$ *e ciò può essere fatto in* 2 *modi (azione di* S_2 *sugli insiemi).*
Dunque abbiamo trovato tutti gli elementi del centralizzatore

$$C(\sigma) =< (1,2,3),(4,5,6) > \rtimes S_2$$

1.2 A_n

In A_n le cose sono differenti infatti non tutte le permutazioni con la stessa struttura in cicli sono disgiunte.

Teorema 1.5. *Sia G un gruppo e H un suo sottogruppo di indice 2.*
Sia $Z < G$ allora si verifica una delle 2 ipotesi

- $Z < H$
- $|Z| = 2|Z \cap H|$

Dimostrazione. Poichè H ha indice 2 è normale in G.
Consideriamo la mappa

$$\epsilon : G \to G \backslash H$$

Ora se $\epsilon(z) = 0 \quad \forall z \in Z$ allora $Z < H$.
Altrimenti $\epsilon_{|Z}$ è surgettivo quindi dal primo teorema di isomorfismo

$$Z \backslash \ker(\beta_|) \cong G \backslash H \cong \mathbb{Z}_2$$

ma $\ker(\beta_|) = Z \cap H$ quindi

$$\frac{|Z|}{|Z \cap H|} = |\mathbb{Z}_2| = 2$$

dunque la seconda tesi □

Dunque in A_n si possono verificare 2 situazioni differenti

$$C_{A_n}(\sigma)| \subsetneqq C_{S_n}(\sigma) \quad \Rightarrow \quad orb_{A_n}(\sigma) = orb_{S_n}(\sigma)$$

oppure

$$C_{A_n}(\sigma) = C_{S_n}(\sigma) \quad \Rightarrow \quad |orb_{A_n}(\sigma)| = \frac{1}{2}|orb_{S_n}(\sigma)|$$

Teorema 1.6. *Sia $\sigma \in A_n$ una permutazione scritta come prodotto di r cicli disgiunti di lunghezza rispettivamente l_1 (considerando anche i cicli di lunghezza 1)*

- *se tutti i l_i sono dispari e a due a due diversi allora:*
  $C_{A_n}(\sigma)$ contiene metà elementi di $C_{S_n}(\sigma)$
- *altrimenti i 2 centralizzatori coincidono*

2 Gruppo diedrale

Consideriamo il gruppo D_n delle isometrie del piano che mandano un n-agono regolare in sé .

Facciamo agire il gruppo diedrale sui vertici del n-agono:

- Il vertice 1 può essere mandato in uno dei n vertici.
- Il vertice 2 essendo adiacente al vertice 1 deve essere mandato in uno dei 2 vertici adiacenti all'immagine del vertice 1 dunque ci sono 2 possibilità
- Il centro dell' n-agono deve andare nel centro

Dunque il diedrale contiene al più $2n$ elementi.

Sia ρ la rotazione di centro il centro dell' n-agono e angolo $\frac{2\pi}{n}$ osserviamo che $\rho \in D_n$ inoltre anche

$$e = \rho^0, \rho, \ldots, \rho^{n-1} \in D_n$$

inoltre sono tutti distinte infatti ρ^i manda il vertice 1 nel vertice i quindi se $i \neq j(\mod n)$ allora $\rho^i \neq \rho^j$ Sia σ una riflessione rispetto ad un asse di simmetria del n-agono allora sicuramente $\sigma^2 = e$ e

$$\sigma, \sigma\rho, \ldots, \sigma\rho^{n-1} \in D_n$$

inoltre sono tutte distinte tra loro

$$\sigma\rho^i = \sigma\rho^j \quad \Rightarrow \quad \sigma\sigma\rho^i = \sigma\sigma\rho^j \quad \Rightarrow \quad \rho^i = \rho^j$$

ma abbiamo precedentemente osservato che $\rho^i \neq \rho^j$ se $i \neq j(\mod n)$ Inoltre

$$\rho^i = \sigma\rho^j \quad \forall i \forall j$$

infatti ρ viene rappresentata da una matrice con determinante 1 invece σ con una matrice con determinante -1.

D_n ha al più $2n$ elementi, avendo trovato $2n$ suoi elementi distinti possiamo concludere dicendo che

$$|D_n| = 2n$$

Osservando che $\sigma\rho\sigma = \rho^{-1}$ possiamo considerare

$$D_n =< \rho, \sigma | \rho^n = e,\ \sigma^2 = e, \quad \sigma\rho = \rho^{-1}\sigma >$$

2.1 I sottogruppi del diedrale

- Il sottogruppo $C_n =< \rho >$ è un sottogruppo ciclico di ordine n
- Dentro C_n gli unici sottogruppi sono quelli di ordine m tale che $m|n$ ed inoltre esiste un solo sottogruppo di ogni ordine
- Per il teorema 1.5, un sottogruppo Z deve o essere contenuto in C_n (in questo caso io abbiamo già considerato) oppure $|Z| = 2|Z \cap C_n|$
  Consideriamo
  $$\forall m \quad m|n \quad Z \cap C_n =< \rho^m >$$
  e scegliamo $\sigma\rho^i \in Z - C_n$.
  Per ogni scelta di m, i trovo un preciso sottogruppo Z di ordine $\frac{2n}{m}$
  Se $m \neq m'$ allora $o(Z) \neq o(Z')$ quindi i sottogruppi generati da scelte differenti di m sono distinti.
  Poichè $K \cap C_n =< \rho^m >$ e $\sigma\rho^i \in Z$ allora
  $$K = \{\rho^{hm}, \sigma\rho^{i+hm}\}_{h=0,\dots\frac{n}{m}-1}$$
  Fissato m ottengo gli stessi sottogruppi se e solo se $i \equiv i' \pmod m$ dunque per ogni m ho esattamente m sottogruppi.

  Verifichiamo che K è chiuso per il prodotto
  $$\rho^{hm} \cdot \sigma\rho^{i+h'm} = \sigma\rho^{i+(h'-h)m}$$
  $$\sigma\rho^{i+hm} \cdot \rho^{h'm} = \sigma\rho^{i+(h+h')m}$$
  $$\sigma\rho^{i+hm} \cdot \sigma\rho^{i+h'm} = \rho^{-i-hm}\rho^{i+h'm} = \rho^{(h'-h)m}$$

Riassumendo il numero dei sottogruppi di D_n è

$$\text{numero di divisori di n} + \sum_{m|n} m$$

2.2 I sottogruppi normali del diedrale

Prima di andare a catalogare i sottogruppi normali diamo un'importante definizione

Definizione 2.1. Sia G un gruppo.
Diciamo che $H < G$ è caratteristico in G se

$$\forall \varphi : G \to G \text{ isomorfismo} \quad \varphi(H) = H$$

Osservazione 1. I sottogruppi caratteristici sono normali infatti $C_g : G \to G$ è un isomorfismo. Se H è caratteristico allora $gHg^{-1} = C_g(H) = H$

Proposizione 2.1. *Sia G un gruppo e $H < N \lhd G$ con H caratteristico in N allora: $H \lhd G$*

Dimostrazione. Poichè N è normale in G allora preso $g \in G$

$$C_g : N \to N \text{ è un isomorfismo}$$

ora usando il fatto che H è caratteristico in N vale $C_g(H) = H$ dunque H è normale in G □

Dal fatto che in C_n esiste un solo sottogruppo per ogni ordine possibile, $H < C_n$ è caratteristico in C_n (un isomorfismo manda H in un sottogruppo di C_n con lo stesso ordine di H) dunque normale in G.

Da quanto visto precedentemente gli altri sottogruppi di D_n sono della forma

$$H =< \rho^m, \sigma\rho^i >$$

dove gli elementi sono

$$\rho^a \quad a \equiv 0 \pmod m$$
$$\sigma\rho^b \quad b \equiv i \pmod m$$

Vediamo se $K \lhd G$
Coniugando rispetto a ρ^c

$$\rho^c \sigma \rho^b \rho^{-c} = \sigma \rho^{b-2c}$$

se $m \neq 1, 2$ allora K non è normale.
In particolare se $m = 2$ allora n è pari.
Riassumendo:

- Se n è dispari i sottogruppi normali sono:
  - D_n
  - $\{0\}$
  - $K < C_n$
- Se n è pari i sottogruppi normali sono
  - D_n
  - $\{0\}$
  - $K < C_n$
  - $< \rho^2, \sigma >$
  - $< \rho^2, \sigma\rho >$

2.3 Centro

Un elemento del diedrale si può esprimere come $\rho^i\sigma$ oppure ρ^i esso si trova nel centro se commuta con entrambi i generatori.

- $\rho^i\sigma$ non appartiene al centro infatti

$$\rho\left(\rho^i\sigma\right)\rho^{-1} = \rho\rho^i\rho\sigma = \rho^{i+2}\sigma$$

  dunque $2 \not\equiv 0 \mod$ infatti $n \geq 3$ (abbiamo definito il diedrale come le isometrie di un poligono)

- ρ^i commuta con ρ, vediamo quando commuta con l'altro generatore

$$\sigma\rho^i\sigma = \rho^{-i}$$

  dunque l'elemento sta nel centro se $2i \equiv 0 \mod n$ da cui se n dispari la soluzione è $i = 0$ se n pari ci sono 2 soluzioni 0 e $\frac{n}{2}$

$$Z(D_n) = \begin{cases} \{e\} \text{ se } n \text{ dispari} \\ \{e, \rho^{\frac{n}{2}}\} \text{ se } n \text{ pari} \end{cases}$$

3 Classificazione dei gruppi di ordine 8

Sia G un gruppo tale che $|G| = 8$.
Ci sono elementi di ordine maggiore di 2?

no Per il lemma precedente $G \cong (\mathbb{Z}_2)^3$

si **Ci sono elementi di ordine 8?**

si G è un gruppo ciclico generato da un elemento di ordine 8 dunque $G \cong \mathbb{Z}_8$

no Dunque esiste un elemento di ordine 4.
Sia N il sottogruppo ciclico generato da quell'elemento, allora $N \cong \mathbb{Z}_4$.
Ora essendo l'indice di N in G uguale a 2, N è normale.
Fuori da N esistono elementi di ordine 2?

si $G \cong \mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_2$

$$\varphi :\ \mathbb{Z}_2 \to Aut\left(\mathbb{Z}_4\right) = \left(\mathbb{Z}_4\right)^\star \cong \left(\{\pm 1\}, \cdot\right) \cong \left(\mathbb{Z}_2, +\right)$$

Ci sono 2 possibilità

· φ è l'omorfismo banale $\varphi(1) = Id_{\mathbb{Z}_4}$ in questo caso

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

· φ è tale che $\varphi(1) = 1$ ovvero -1 di $(Z_4)^\star$.
$\varphi(1)$ è l'automorfismo che manda un elemento nel suo inverso.
Sia g un generatore di $\mathbb{Z}_4$ dunque $o(g) = 4$ e viene codificato da $(1, 0)$ Sia h un generatore di $\mathbb{Z}_2$ dunque $o(g) = 2$ e viene codificato da $(0, 1)$

$$hgh^{-1} = hgh = (0,1)(1,0)(0,1) = (-1,0) = g^{-1}$$

dunque

$$G =< g\,h \,|\, hgh^{-1} = g^{-1},\ g^4 = e,\ h^2 = e >= D_4$$

no In $G - N$ ci sono solamente elementi di ordine 4
Sia $N =< g >$ e sia $h \in G - N$, poniamo $H =< h > \cong \mathbb{Z}_4$.
Consideriamo l'omomorfismo

$$\psi :\ H \to Aut(N) \qquad h \to C_h$$

Ora $Aut(N) \cong (Z_4)^\star \cong \mathbb{Z}_2$.

· Se $\psi(1) = 0$ allora $C_h = Id$ da cui $hgh^-1 = g$ dunque $hg = gh$.
Allora $N \subseteq C(g)$ ed inoltre $h \in C(g)$ ovvero $|C(g)| \geq 5$.
Per il teorema di Lagrange concludiamo che $C(g) = G$ e in modo analogo $C(h) = G$.
Con la stessa osservazione notiamo che $Z(G) = G$ ovvero G è abeliano, mostriamo che ciò è assurdo

$$gh \notin N \text{ infatti } h \notin N \quad \Rightarrow \quad (gh)^2 \notin N$$

$$(gh)^2 = g^2 h^2$$

Ora $g^2 \in N$ è l'unico elemento di ordine 2 quindi $h^2 = g^2$ da cui

$$(gh)^2 = g^4 = e \notin N \text{ assurdo essendo } N < G$$

- $\psi(1) = -1$ ovvero $hgh^{-1} = g^{-1}$.
  Il gruppo in esame è così composto
  6 elementi di ordine 4:

$$g,\ g^{-1},\ h,\ h^{-1},\ gh,\ (gh)^{-1}$$

1 elemento di ordine 1:

$$g^2 = h^2 = (gh)^2$$

L'identità.
Cambiando nome agli elementi ponendo $1 = e$

$$i = g$$

$$-1 = g^2$$

$$j = h$$

$$k = gh$$

Osserviamo che

$$i^2 = h^2 = k^2 = -1$$

da cui poichè $-1 \in Z(G)$ basta studiare le regole di moltiplicazione tra i, j, k

$$(ij)(ji) = ij^2 i = -i^2 = 1$$

dunque ji è l'opposto di ij ovvero $ji = -k$.
In modo analogo si prova che

$$ki = j \qquad ik = -j$$

$$jk = i \qquad kj = i$$

Questo gruppo prende il nome di gruppo dei quaternioni indicato con Q_8.
Osserviamo che Q_8 non è abeliano e in particolare $Z(Q_8) = 1, -1$

4 Normalizzatore del gruppo ciclico di una permutazione

Sia $\sigma \in S_n$ denotiamo con $N(\sigma) = N(<\sigma>)$ e con $Aut(\sigma) = Aut(<\sigma>)$
Consideriamo l'omomorfismo

$$\varphi: N(\sigma) \to Aut(\sigma) \quad \rho \to \varphi_\rho \text{ dove } \varphi_\rho(\sigma^i) = \rho\sigma^i\rho^{-1}$$

φ è ben definita infatti se $\rho \in N(\sigma)$ allora $\rho\sigma^i\rho^{-1} \in <\sigma>$.
Osserviamo che $\ker\varphi = C(\sigma)$ da cui

$$\frac{N(\sigma)}{C(\sigma)} \cong |Im\,\varphi| \quad \Rightarrow \quad |N(\sigma)| = |Im\,\varphi| \cdot |C(\sigma)|$$

Esempio 4.1. *Normalizzatore in S_5 di $\sigma = (1, 2, 3, 4, 5)$.*
Osserviamo che $<\sigma> \cong \mathbb{Z}_5$ dove l'isomorfismo è dato mandando $\sigma^i \to i$ per ogni $i = 0, \dots, 5$
Dunque $Aut(\sigma) \cong \mathbb{Z}_5^\star \cong \mathbb{Z}_4$.
Sia ψ un automorfismo di $<\sigma>$ tale che $\psi(\sigma) = \sigma^2$ Sia

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = (2, 3, 5, 4)$$

dunque per come abbiamo definito τ otteniamo $\psi = \varphi_\tau$.
Possiamo usare un argomentazione analoga per dimostrare $\forall\psi \in Aut(\sigma)$ $\exists\tau \in N(\sigma)$ si ha $\psi = \varphi_\tau$ ovvero φ è suriettiva da cui

$$|N(\sigma)| = |C(\sigma)| \cdot \phi(o(\sigma))$$

Mostriamo che in generale l'omomorfismo è surgettivo e dunque vale l'espressione per la cardinalità del normalizzatore.
Sia $\sigma \in S_n$ con $\sigma = c_1 \cdots c_k$ scritta in cicli disgiunti, sia $l = o(\sigma) = m.c.m(o(c_1), \dots, o(c_k))$
Consideriamo l'automorfismo che manda σ in σ^i con i e l coprimi.
Essendo i cicli disgiunti, commutano dunque

$$\sigma^i = c_1^i \cdots c_k^i$$

Ora essendo $M.C.D(l, i) = 1$ segue che $\forall j = 1, \dots, k$ $M.C.D(i, o(c_j)) = 1$ da cui c_j e c_j^i hanno la stessa lunghezza dunque sono coniugati e la mappa φ è surgettiva.

Mostriamo molto di più:

Proposizione 4.2. *Sia G un gruppo e $N \lhd G$.*
Sia π la naturale proiezione e s una sua inversa sinistra allora

$$G \cong N \rtimes Im\,s$$

Dimostrazione. Dal primo teorema di isomorfismo segue

$$|G| = |N| \cdot \left|\frac{G}{N}\right|$$

Posto $H = Im\,s$ e poichè s è iniettiva (è un inversa sinistra) $|G| = |N| \cdot |H|$
Osserviamo ora che $H \cap N = \{e\}$ infatti:

$$g \in N \quad \Leftrightarrow \quad \varphi(g) = e$$

$$g \in H \quad \Leftrightarrow \quad g = s(a) \text{ con } a \in \frac{G}{N}$$

da cui $e = \varphi(g) = \varphi(g(s(a))$ ma s è inversa sinistra dunque $e = a$ e poichè s è iniettiva $g = s(a) = e$.

$\square$

Tornando al caso dei normalizzatori si ha

$$G \cong N \rtimes \left(\mathbb{Z}_{o(\sigma)}\right)^{\star}$$

5 Non semplicità di un gruppo

Proposizione 5.1. *Sia G gruppo finito e $H < G$ con indice n*

$$|G| \geq \frac{n!}{2} \quad \Rightarrow \quad G \textit{ non è semplice}$$

Dimostrazione. Facciamo agire G sull'insieme X delle classi laterali per moltiplicazione a sinistra, tale azione risulta non banale, dunque poichè $|X| = n$ esiste un omomorfismo non banale

$$\psi : G \to S_n$$

- Se $Im\psi \subseteq A_n$ possiamo considerare $\tilde{\psi}$ la restrizione del codominio di ψ

  $$\tilde{\psi} : G \to A_n$$

  Da $|G| \geq |A_n|$ segue che $\tilde{\psi}$ non è iniettiva dunque il suo nucleo è un sottogruppo non banale (azione non banale) normale in G

- Se $Im\psi \nsubseteq A_n$, posta P la funzione parità di $S_n \to \mathbb{Z}_2$ segue che $P \circ \psi$ è surgettiva, dunque $(P \circ \psi)^{-1}(0)$ è un sottogruppo di G di indice 2 dunque normale

□

Proposizione 5.2. *Sia G un insieme che agisce in modo non banale su un insieme di n elementi*

$$|G| \not| n! \quad \Rightarrow \quad G \textit{ non semplice}$$

Dimostrazione. Poichè G agisce in modo non banale su un insieme di n elementi allora esiste un omomorfismo non banale

$$\psi : G \to S_n$$

ora se ψ fosse iniettiva $|G| = |Im\psi|$ ma per Lagrange ciò è assurdo infatti $Im\psi$ è un sottogruppo di S_n ma la sua cardinalità non divide quella dell'ordine

Esempio 5.3 (Gruppo di ordine 112).
Sia P un 2-Sylow, ora dai teoremi di Sylow $n_2 = 1, 7$.
Se $n_2 = 1$ allora P è normale ed il gruppo non è semplice.
Supponiamo, dunque, che $n_2 = 7$, dunque G agisce sui p-Sylow da cui

$$X = \{P, g_1P, \ldots, g_6P\}$$

L'azione di G su X determina un omomorfismo non banale

$$\phi : G \to S_7$$

dunque $\ker \phi \neq G$

- *Se $Im\,\phi \not\subseteq A_7$ allora $\varphi^{-1}(A_7) \lhd G$ infatti posso considerare la composizione segno $\circ\varphi$, tale mappa risulta suriettiva dunque $\varphi^{-1}(A_7)$ ha indice 2 da cui è normale in G*
- *se $Im\,\phi \subseteq A_7$ allora posso restringere l'omo*

  $$\tilde{\varphi} : G \to A_7$$

  tale omomorfismo non può essere iniettivo infatti $|G|$ non divide A_7 da cui $\ker \tilde{\varphi} \neq \{e\}$ *è il sottogruppo normale cercato.*

Esempio 5.4 (Gruppo di ordine 144).
Osserviamo che $144 = 2^4 3^2$.
Studiamo il numero dei 3-Sylow, esso può essere 1, 4 o 16

- *se $n_3 = 1$ allora il 3-Sylow è normale*
- *se $n_3 = 4$ allora G agisce sui 3-Sylow ma $|G|$ non divide 4! dunque esiste un sottogruppo normale non banale*
- *se $n_3 = 16$, allora*
  - *Se i 3-Sylow si intersecano a 2 a 2 in modo banale allora in G esistono $16 \cdot 8$ elementi con ordine che dividono 3 da cui il $2 - Sylow$ è normale*
  - *Se esistono P_1, P_2 3-Sylow tale che $|P_1 \cap P_2| = 3$, in questo caso $N(P_1) = 9$ (un gruppo di ordine p^2 è abeliano).*
    Studiamo $N(P_1 \cap P_2)$
    * *Tale sottogruppo ha più di 9 elementi, contiene sia elementi di P_1 che di P_2*
    * *Se $|N(P_1 \cap P_2) = 18$ allora $P_1 \lhd N(P_1 \cap P_2)$ da cui $|N(P_1) \geq 18$ il che è assurdo.*
    * *Se $|N(P_1 \cap P_2) = 36$ allora tale sottogruppo ha indice 4 e poichè $|G|$ non divide 4! G non è semplice.*
    * *Se $|N(P_1 \cap P_2) = 36$ allora tale sottogruppo ha indice 2 dunque normale*

6 Gruppi pqr

6.1 Studio degli automorfismi dei gruppi pq

Sia H un gruppo di ordine pq con $p < q$ primi, allora dalla classificazione dei gruppi di ordine pq sappiamo che

- $H = \mathbb{Z}_p \times \mathbb{Z}_q$ dunque $Aut(H) = (\mathbb{Z}_{pq})^\star$ quindi $|Aut(H)| = (p-1)(q-1)$
- $H = \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ con $\varphi : \mathbb{Z}_p \to \mathbb{Z}_q^\star$ tale che $\varphi(1) = m$ tale che $o(m) = p$.
  Sia x un generatore di $\mathbb{Z}_p$ e y un generatore di $\mathbb{Z}_q$.
  Ora poichè φ esprime come avviene il coniugio nel gruppo otteniamo: $xyx^{-1} = y^m$ da cui abbiamo le seguenti relazioni

  $$x^p = y^q = e \quad xyx^{-1} = y^m$$

  Vogliamo costruire $f : H \to H$ isomorfismo.
  Dunque, una condizione necessaria è che mandi i generatori in elementi dello stesso ordine.
  Poichè $\mathbb{Z}_q$ è normale gli unici elementi di ordine q sono

  $$y,\, y^2, \ldots,\, y^{q-1}$$

  mentre tutti gli altri elementi, tranne e, devono avere ordine p (poichè il gruppo H non è abeliano non può essere ciclico dunque non esiste elementi con ordine pq) quindi gli elementi di ordine p sono

  $$\begin{array}{cccc} x & x^2 & \cdots & x^{p-1} \\ xy & x^2y & \cdots & x^{p-1}y \\ \vdots & & & \vdots \\ xy^{q-1} & x^2y^{q-1} & \cdots & x^{p-1}y^{q-1} \end{array}$$

  Osserviamo che x^2y^b coniuga y nello stesso modo indifferentemente dalla scelta di b

  $$\left(xy^b\right) y \left(xy^b\right)^{-1} = x(y^byy^{-b})x^{-1} = xyx^{-1}$$

  Osserviamo, inoltre che ponendo $f(x) = x^b$ e $f(y) = y$ otteniamo

  $$f(x)f(y)f\left(x^{-1}\right) = x^byx^{-b} = y^{bm^2}$$

  Dunque con questa scelta di $f(x)$ non rispettiamo la relazione infatti $am^2 \not\equiv am \pmod{q}$
  Invece ponendo $f(y) = y^a$ e $f(x) = x$ otteniamo

  $$xy^ay^{-1} = y^{am}$$

  dunque tale scelta rispetta le relazioni.
  Unendo le osservazioni precedenti, otteniamo che n possibile automorfismo deve essere una funzione del tipo

  $$x^ay^b \to \left(xy^i\right)^a \left(y^j\right)^b \text{ con } i = 0, \ldots, q-1 \quad j = 1, \ldots, q-1$$

  Tale funzione mantiene l'ordine dei generatori, verifichiamo che è un omomorfismo

  $$\left(x^ay^b,\, x^cy^d\right) \xrightarrow{\cdot} x^ay^bx^cy^d = x^{a+c}\left(x^{-c}y^bx^c\right)y^d = x^{a+c}y^{bm^{-c}+d}$$

  ora applicando f otteniamo $(xy^i)^{a+c}\, y^{j\left(bm^{-c}+d\right)}$

  $$\left(x^ay^b,\, x^cy^d\right) \xrightarrow{f} \left(\left(xy^i\right)^a y^{jb}, \left(xy^i\right)^c y^{jd}\right) \xrightarrow{\cdot} \left(xy^i\right)^{a+c} y^{j\left(bm^{-c}+d\right)}$$

  quindi f è un'automorfismo da cui $|Aut(H)| = q(q-1)$

Sia $|G| = pqr$ con $p < q < r$ primi e P, Q, R rispettivamente il p, q, r-Sylow. Possiamo allora dire che

1. R è normale
2. Esiste in G un sottogruppo normale di ordine qr
3. Se $q \not| p - 1$ allora Q è normale

1. R è un sottogruppo normale.
   Dal secondo e terzo teorema di Sylow

   $$n_r = \begin{cases} 1 \\ pq \end{cases}$$

   infatti $p \not\equiv 1 \pmod r$ essendo $r > p$ e per motivi analoghi $q \not\equiv 1 \pmod r$.
   Se $n_r = 1$ allora R è normale.
   Supponiamo che $n_r = pq$ dunque esistono $(r-1)pq$ elementi di ordine r.

   Uno tra il p-Sylow ed il q-Sylow deve essere normale, se così non fosse $n_p \geq q$ e $n_q \geq r$ da cui

   $$|G| \geq pq(r-1) \text{ (ordine r) } + (q-1)r \text{ (ordine q) } + (p-1)q \text{ (ordine p) } > pqr \quad \textit{assurdo}$$

   Dunque almeno uno tra P e Q deve essere normale da cui $H = PQ$ è un sottogruppo, tale sottogruppo è caratteristico in G (dunque normale) infatti fuori da H ci sono elementi di ordine r.
   Dunque $G = H \rtimes R$, sia $\psi : R \to Aut(H)$, per quanto precedentemente osservato:

   - $H = \mathbb{Z}_p \times \mathbb{Z}_q$ allora $|Aut(H)| = (p-1)(q-1)$.
     $r \not| (p-1)$ e $r \not| (q-1)$ dunque ψ è banale
   - $H = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ allora $|Aut(H)| = q(q-1)$.
     Anche in questo caso allora ψ è banale

   Dunque tutti gli elementi di R commutano con gli elementi di R e H ovvero $Z(R) = G$ allora R è normale (l'ipotesi $n_r = pq$ non si realizza mai)

2. In G esiste un sottogruppo normale di ordine qr.
   Come sappiamo R è normale dunque $N = QR$ è un sottogruppo, inoltre tale sottogruppo ha indice p da cui $N \lhd G$

3. Se $q \not| (r-1)$ allora il q-Sylow è normale.
   Dalla classificazione dei gruppi qr osserviamo che $N = R \rtimes Q = R \times Q$.
   Ora Q è caratteristico in N allora dalla proposizione 2.1 $Q \lhd G$

7 A_n

7.1 Semplicità

Lemma 7.1. *Sia H un sottogruppo di S_n, allora si possono verificare due differenti situazioni*

- $H < A_n$
- $|H \cap A_n| = \frac{1}{2}|H|$

Dimostrazione. Supponiamo che esista in H una permutazione con dispari allora se consideriamo l'omomorfismo

$$\phi : H \to \mathbb{Z}_2 \quad \sigma \to P(\sigma)$$

è suriettiva dunque $\ker \phi = H \cap A_n$ ha indice 2 (da cui la tesi) □

Corollario 7.2. *In A_5*

1. *Tutti i 3-cicli sono coniugati*
2. *Tutte le doppie trasposizioni sono coniugate*
3. *I 5-cicli si dividono in 2 classi di coniugio*

Dimostrazione.

1. Sia σ un 3-ciclo e siano a, b i 2 elementi lasciati fissi da σ dunque $(a, b) \in Stab_{S_5}(\sigma)$. Per il lemma precedente

$$|Stab_{A_5}(\sigma)| = \frac{1}{2}|Stab_{S_5}(\sigma)| \quad \Rightarrow \quad orb_{A_5}(\sigma) = orb_{S_5}(\sigma)$$

2. Sia $\sigma = (a, b)(c, d)$ scritta in cicli disgiunti.
   Ora $(a, b) \in Stab_{S_5}(\sigma)$ dunque per motivi analoghi al caso precedente σ ha la stessa orbita in S_5 che in A_5

3. Sia σ un 5-ciclo.

$$Stab_{S_5}(\sigma) = \frac{|S_5|}{|orb(\sigma)|} = 5$$

   dunque $Stab_{S_5}(\sigma) =< \sigma >\subseteq A_n$ dunque

$$|orb_{A_5}(\sigma)| = \frac{1}{2}|orb_{S_5}(\sigma)|$$

   ovvero esistono 2 orbite

□

Teorema 7.3. *$\forall n \geq 5$ A_n è semplice*

Dimostrazione. Consideriamo il caso $n = 5$.
Supponiamo che esista $N \lhd A_5$ con $N \neq \{e\}$.

- N contiene una 3-ciclo dunque tutti i 3-cicli.
  Osserviamo inoltre che $(1, 3, 2)(2, 4, 3) = (1, 3)(2, 4)$ quindi N contiene tutte le doppie trasposizioni che generano tutto A_5
- N contiene tutte le doppie trasposizioni, dunque $N = A_5$

- N contiene $(1,2,3,4,5)$ dunque anche $(1,4,3,5,2) = (1,2)(3,4)(1,2,3,4,5)(1,2)(3,4)$ dunque N contiene tutto A_5

Un sottogruppo normale di A_n diverso da $\{e\}$ deve necessariamente contenere tutto A_5.

Supponiamo adesso che A_{n-1} sia semplice e mostriamo che A_n è semplice.
Sia
$$G_i = \{\sigma \in A_n \,|\, \sigma(i) = i\} \quad \Rightarrow \quad G_i \cong A_{n-1}$$
Sia $\{e\} \neq N \lhd A_n$ allora $N \cap G_i \lhd G_i$
$$G_i \text{ semplice} \quad \Rightarrow \quad N \cap G_i = \begin{cases} G_i \\ \{e\} \end{cases}$$
Se $G_i \cap N = G_i$ per un certo i allora ciò succede per tutti gli i infatti G_i e G_j sono coniugati.
Ora se $N \cap G_i$ $\forall i$ otteniamo che $N = A_n$ infatti nell'unione dei G_i sono contenuti tutti i 3-cicli, ma i 3-cicli generano A_n.
Supponiamo $N \cap G_i = \{e\}$ $\forall i = 1, \dots, n$ allora
$$\sigma \in N \backslash \{e\} \quad \Rightarrow \quad \sigma(i) \neq i \quad \forall i$$
da ciò segue che
$$\sigma, \tau \in N \quad \sigma(i) = \tau(i) \quad \Rightarrow \quad \left(\tau^{-1}\sigma\right)(i) = i \quad \Rightarrow \quad \tau^{-1}\sigma = e \quad \Rightarrow \quad \sigma = \tau$$
Supponiamo

$\sigma \in N \quad \sigma = c_1 c_2 \dots c_r$ scritto in cicli disgiunti ordinati per lunghezza decrescente $l_1 \geq l_2 \geq \dots \geq l_r$

Se $l_1 \geq 3$ sia
$$c_1 = (i_1, i_2, i_3, \dots)$$
e
$$A_n \ni \rho = (i_3, j, k) \text{ dove } j, k \notin \{i_1, i_2, i_3\}$$
Sia
$$c_1' = \rho c_1 \rho^{-1} = (i_1, i_2, j, \dots) \quad \Rightarrow \quad c_1'(i_1) = c_1'(i_1) = i_2 \quad \Rightarrow \quad c_1' = c_1$$
Ora $c_1'(i_2) = j$ mentre $c_1(i_2) = i_3 \neq j$ assurdo
Se $l_1 = 2$.
Sia
$$\sigma = (i,j)(k,l)\dots \quad \rho = (l,p,q) \text{ con } p, q \notin \{i,j,k,l\}$$
Allora
$$\sigma' = \rho\sigma\rho^{-1} \quad \sigma(i) = \sigma'(i) = j \quad \Rightarrow \quad \sigma = \sigma'$$
Ora $\sigma(k) = l \neq \sigma'(k) = p$
Dunque abbiamo dimostrato che σ deve avere tutti cicli di lunghezza 1 dunque $\sigma = \{e\}$

$\square$

7.2 Sottogruppi di indice n

Definizione 7.1. Si dice che un gruppo G agisce in modo transitivo su un insieme X se

$$\forall y_1, y_2 \in X \quad \exists g \in G \quad g \centerdot y_1 = y_2$$

o in modo equivalente X si partiziona in una sola orbita

Lemma 7.4. *Supponiamo $n \geq 5$ e che A_n agisca in modo transitivo su X. Allora, se l'azione non è banale*

$$|X| \geq n$$

Dimostrazione. Sia $|X| = m$ ora l'azione di A_n su X determina un omomorfismo non banale:

$$\varphi : \ A_n \to S_n$$

Se $m < n$ allora $m! < \frac{n!}{2}$ dunque φ non è iniettiva, ciò è assurdo, infatti essendo A_n semplice e φ non banale $Ker\,\varphi = \{e\}$

□

Lemma 7.5. *Sia $n \geq 5$ e $H < A_n$*

$$[A_n \ : \ H] = n \quad \Rightarrow \quad H \cong A_{n-1}$$

Dimostrazione. Consideriamo l'azione di A_n su $X = \{H, g_1 H, \ldots, g_{n-1} H\}$ data dalla moltiplicazione a sinistra, tale azione è transitiva dunque non banale.
Consideriamo l'omomorfismo, non banale

$$\varphi : \ A_n \to S_n$$

Se $Im\,\varphi \not\subseteq A_n$ allora

$$|Im\,\varphi \cap A_n| = \frac{1}{2}|Im\,\varphi| \quad \Rightarrow \quad [Im\,\varphi : Im\,\varphi \cap A_n] = 2 \quad \Rightarrow \quad Im\,\varphi \cap A_n \lhd Im\,\varphi$$

Dunque $A_n \cap \varphi^{-1}(A_n) \lhd A_n$.
Ora $[A_n : A_n \cap \varphi^{-1}(A_n)] = 2$ ma ciò è assurdo data la semplicità di A_n.
Dunque $Im\varphi \subseteq A_n$ e data l'iniettività di φ si ha l'uguaglianza da cui $\varphi : \ A_n \to A_n$ è isomorfismo.
Ora $\phi(H) \subseteq Stab(H)$ infatti se $h \in H$ allora $h \centerdot H = H$ (l'azione è la moltiplicazione a sinistra).
Ora $Stab(H) \cong A_{n-1}$ infatti sono quelle permutazioni dell'insieme X che fissano H.
Ora essendo φ iniettiva $|\phi(H)| = \frac{(n-1)!}{2}$ quindi $H \cong A_{n-1}$ □

Lemma 7.6. *Sia $n > 7$.*
Sia $H < A_n$, come sappiamo, $H \cong^{\varphi} A_{n-1}$.
Se c è un 3-ciclo di A_{n-1} allora anche $\varphi(c)$ è un 3-ciclo di A_n

Dimostrazione.

$$C_{A_{n-1}}(c) =< c > \times K$$

dove $K \cong A_{n-4}$ è il gruppo delle permutazioni che lasciano fissi gli elementi del 3-ciclo.
Supponiamo $n - 4 \geq 5$ dunque K è semplice.
Chiamiamo O l'orbita di $\varphi(K)$ in $1, \ldots, n$.
Per il lemma 7.4 si ha $|O| = n - t \geq n - 4$.
Consideriamo ora l'azione di $\varphi(c)$ in O

- Se $\varphi(c)$ non muove nessun elemento di O allora $\varphi(c)$ è un 3-ciclo.
  $\varphi(c)$ può muovere solo 4 elementi e ha ordine 3

- Se $\varphi(c)$ muove qualche elemento di O allora deve muovere tutti gli elementi di O.
  Sia $x \in O$ un elemento mosso da $\varphi(c)$ dunque

  $$\exists y \neq x \in O \quad y = \varphi(c) \centerdot x$$

  $$\forall o \in O \quad \exists k \in \varphi(K) \quad k \centerdot x = o$$

  dunque poichè c e K commutano

  $$\varphi \centerdot o = \varphi \centerdot (k \centerdot x) = k \centerdot (\varphi(c) \centerdot x) = k \centerdot y$$

  Dunque le orbite di $\varphi(c)$ in 0 sono $\frac{n-t}{3}$ avendo c ordine 3 inoltre $\varphi(K) \cong A_{n-4}$ agisce su queste orbite dunque per il lemma 7.4

  $$\frac{n-t}{3} \geq n - 4 \quad \Rightarrow \quad n \leq 6$$

  tale richiesta è assurda infatti avevamo supposto $n - 4 > 5$

Dunque per $n > 9$ abbiamo dimostrato il teorema; resta da dimostrare il caso di $n = 8$.
Sia $c = (1, 2, 3) \in A_7$ dunque

$$C_{A_7}(1, 2, 3) \cong< (1, 2, 3) > \times A_4$$

dentro lo stabilizzatore di c ci sono $3 \cdot 9 - 1 = 26$ elementi di ordine 3 Supponiamo, per assurdo, che $\varphi(c)$ sia un doppio 3-ciclo per esempio $((1, 2, 3)(4, 5, 6) \in A_8)$

$$C_{S_8}(\varphi(c)) =< (1, 2, 3), (4, 5, 6), (7, 8) > \rtimes < (1, 4)(25)(36) >$$

che contiene 8 elementi di ordine 3, φ, per motivi di "spazio", non può mandare un 3-ciclo in un doppio 3-ciclo. □

Osservazione 2. Il lemma precedente vale anche per $n = 5$ infatti in A_5 gli unici elementi di ordine 3 sono i 3-cicli

Osservazione 3. Siano $H_2 =< (1, 2, 3), (1, 2, 4) >$, $H_1 =< (1, 2, 3)(3, 4, 5) >$ e $H =< (1, 2, 3), (4, 5, 6) >$.
I 3 gruppi generati sono differenti infatti H_1 è A_4, H_2 è più di A_4 mentre H è un gruppo abeliano

Teorema 7.7. *Sia $n \geq 5$ e $n \neq 6$.*
Sia $H < A_n$

$$H \cong A_{n-1} \quad \Rightarrow \quad H = Stab_{A_n}(i) \text{ per un certo } i = 1, \dots, n$$

Dimostrazione. Consideriamo il caso $n = 7$.
Consideriamo l'azione di A_7 sull'insieme $\{1, \dots, 7\}$.
Ora $H \cong A_6$ ha orbite, per il lemma 7.4, di almeno 6 elementi.
H non può avere un orbita di 7 elementi infatti $7 \not| \frac{6!}{2}$.
Ora $H \subseteq Stab(i)$ ma hanno lo stesso ordine quindi vale l'uguaglianza.

Sia $n \neq 7$ per il lemma 7.6 e l'osservazione 2 φ manda un 3-ciclo in un 3-ciclo se $n = 5$ φ manda un 3-ciclo in un Per l'osservazione precedente, inoltre, φ preserva il numero di elementi in comune tra 2 differenti 3-cicli infatti se hanno numero di elementi in comune diversi generano gruppi diversi.
Consideriamo dunque

$$\varphi : \ A_{n-1} \to H < A_n$$

$$(1, 2, 3) \to (x_1, x_2, x_3)$$

$$(1, 2, 4) \to (x_1, x_2, x_4)$$

$$\vdots$$

$$(1, 2, n-1) \to (x_1, x_2, x_{n-1})$$

con x_i tutti distinti.
Ora $(1, 2, i)$ al variare di i generano tutto A_{n-1} quindi

$$\varphi(A_{n-1}) \subseteq Stab(y) \quad y \neq x_i \quad \forall i = 1, \dots, n-1$$

Inoltre i 2 insiemi hanno la stessa cardinalità dunque sono uguali.

7.3 Automorfismi di A_n

Teorema 7.8. *Sia $n \geq 5$ con $n \neq 6$ allora*

$$Aut(A_n) \cong S_n$$

Dimostrazione. Per il teorema 7.7 un sottogruppo di indice n è $Stab_{A_n}(i)$ per un certo i, dunque un automorfismo di A_n permuta gli stabilizzatori di un elemento tra loro ovvero.
È ben definita l'azione del gruppo $Aut(A_n)$ sull'insieme $Stab_{A_n}(i)$ per $i = 1, \dots n$.
Dunque tale azione induce un omomorfismo:

$$\vartheta : \; Aut(A_n) \to S_n$$

Sia $\psi \in Aut(A_n)$ e posto $\vartheta(\psi) = \sigma$ si ha

$$\forall i = 1, \dots n \quad \psi\left(Stab_{A_n}(i)\right) = Stab_{A_n}(\sigma(i))$$

La suriettività di ϑ deriva da questa uguaglianza insiemistica

$$\forall \tau \in S_n \quad \tau \, Stab_{A_n}(i) \, \tau^{-1} = Stab_{A_n}(\tau(i))$$

Mostriamo solo l'inclusione $\subseteq$.
$\forall \sigma \in Stab_{A_n}(i)$ si ha $\sigma(i) = i$ dunque

$$(\tau\sigma\tau^{-1})(\tau(i)) = \tau(\sigma(i)) = \tau(i) \quad \Rightarrow \quad \tau\sigma\tau^{-1} \in Stab_{A_n}(\tau_i)$$

Mostriamo che tale mappa è iniettiva, sia $\psi \in \ker \vartheta$ dunque $\psi\left(Stab_{A_n}(i)\right) = Stab_{A_n}(i)$ da cui

$$(1,2,3) \in \bigcap_{j \geq 4} Stab_{A_n}(j) = \{e, (1,2,3), (1,3,2)\}$$

ora $\psi(1,2,3) \neq e$ essendo ψ un automorfismo preserva l'ordine.
Supponiamo per assurdo, dunque, che $\psi(1,2,3) = (1,3,2)$.
Per motivi analoghi, si possono verificare 2 situazioni

- $\psi(1,2,4) = (1,2,4)$

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

  ma ciò è assurdo ψ manda un elemento di ordine 3 in un elemento di ordine 2

- $\psi(1,2,4) = (1,4,2)$

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

  Ma ciò è assurdo poichè ψ non preserva $Stab_{A_n}(1)$

Dunque era assurda l'ipotesi $\psi(1,2,3) \neq (1,2,3)$.
In modo analogo si prova che ψ calcolata in un 3-ciclo è un 3-ciclo dunque poichè i 3-cicli generano A_n $\psi = id_{A_n}$ da cui ϑ iniettiva

$\square$

8 Automorfismi di S_n

Definizione 8.1. Un automorfismo interno di un gruppo G è un automorfismo indotto da un elemento $g \in G$ tramite coniugio.
Il gruppo degli automorfismi interni si denota con $inn(G)$
In modo equivalente $Inn(G)$ è l'immagine dell'omomorfismo

$$C : G \to Aut(G) \quad g \to C_g$$

dove $C_g(h) = ghg^{-1}$

Osservazione 4. Se $n \geq 3$ $S_n \cong Inn(S_n)$.
La mappa $C : S_n \to Inn(S_n)$ è per definizione suriettiva, mostriamo che è iniettiva.
Sia $\sigma \in \ker C$ dunque $C_\sigma = Id$ ovvero

$$\sigma\tau\sigma^{-1} = \tau \, \forall \tau \in S_n \quad \Leftrightarrow \quad \sigma \in Z(S_n) = \{e\}$$

Assumiamo $Aut(A_n) \cong A_n$

Teorema 8.1. *Se $n \geq 5$ con $n \neq 6$ allora*

$$Aut(S_n) \cong S_n$$

Dimostrazione. Consideriamo la mappa

$$\vartheta : Aut(S_n) \to Aut(A_n)$$

$$\{\psi : S_n \to S_n\} \to \{\psi_{|A_n} : A_n \to A_n\}$$

tale mappa è ben definita in quanto $A_n < S_n$ caratteristico.
Mostriamo che è iniettiva.
Sia $\psi \in \ker \vartheta$ dunque $\psi_{|A_n}$ è l'identità da cui

$$\forall i, j \quad D = \psi\left(Stab_{A_n}(i) \cap Stab_{A_n}(j)\right) = Stab_{A_n}(i) \cap Stab_{A_n}(j)$$

Osserviamo che (i, j) è l'unico elemento di ordine 2 che commuta con D.
Essendo ψ un isomorfismo, $\psi((i, j))$ deve commutare con D da cui $\psi((i, j)) = (i, j)$.
Poichè le trasposizioni generano S_n, $\psi = id_{S_n}$ da cui ϑ è iniettiva.
Mostriamo la surgettività.
Nell'immagine di ϑ è presente un sottogruppo isomorfo a S_n infatti, essendo ϑ iniettiva e è $Inn(S_n) \cong S_n$ segue $\vartheta(Inn(S_n)) \cong S_n$.
Ora $Aut(A_n) \cong S_n$ da cui $Im\vartheta = Aut(A_n)$

□

9 Un criterio per dire se un gruppo è abeliano

Proposizione 9.1. *Sia G un gruppo*

$$\frac{G}{Z(G)} \text{ ciclico} \quad \Rightarrow \quad G \text{ abeliano}$$

Dimostrazione. $\frac{G}{Z(G)} =< gZ(G) >$ per un certo $g \in G$ dunque

$$\forall x \in G \quad x = g^a h \text{ con } h \in Z(G)$$

$$\forall y \in G \quad y = g^b h' \text{ con } h' \in Z(G)$$

ora si ha

$$xy = g^a h g^b h' = g^{a+b} h h'$$
$$yx = g^b h' g^a h = g^{a+b} h' h = g^{a+b} h h'$$

10 Studio di automorfismi

Proposizione 10.1. *Se G è un gruppo con H e K sottogruppi caratteristici tali che $G = H \times K$ allora*

$$Aut(G) \cong Aut(H) \times Aut(K)$$

Osservazione 5. Questo è il caso dei gruppi abeliano in quanto esso può essere scritto come prodotto dei suoi p-Sylow che sono normali

Esempio 10.2 (Cardinalità degli automorfismi di $\mathbb{Z}_p \times \mathbb{Z}_p$ con p primo)**.**
Osserviamo che $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ è isomorfo al gruppo delle matrici invertibili 2×2 a coefficienti in $\mathbb{F}_p$.
Ora la prima colonna la possiamo scegliere in $p^2 - 1$ modi ovvero tutte le coppie tranne $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ infatti la matrice deve essere invertibile.
La seconda colonna non deve essere multipla della prima dunque la posso scegliere in $p^2 - p$ modi dunque

$$|Aut(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$$

Esempio 10.3 (Cardinalità di $Aut(\mathbb{Z}_2 \times \mathbb{Z}_4)$)**.**
Sia $\psi \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_4)$, $g_1 = (1, 0)$ e $g_2 = (0, 1)$.
g_2 deve andare in un elemento di ordine 4 dunque può andare in $2^3 - 2^2$ modi.
g_1 deve andare in un elemento di ordine 2 ma

$$< \psi(g_1) > \cap < \psi(g_2) >= \{e\}$$

ora poichè l'intersezione di ciclici è ciclica basta porre $\psi(g_1) \notin < \psi(g_2) >$.
In $< \psi(g_2) \cong \mathbb{Z}_4$ c'è un solo elemento di ordine 2 da cui$\psi(g_1)$ in $2^2 - 2$ modi.

$$|Aut(\mathbb{Z}_2 \to \mathbb{Z}_4)| = 8$$

Esempio 10.4 (Cardinalità di $Aut(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4)$)**.**
Sia $\psi \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4)$ e poniamo

$$g_1 = (1, 0, 0)$$

$$g_2 = (0, 1, 0)$$

$$g_3 = (0, 0, 1)$$

g_3 può andare in un qualunque elemento di ordine 4 dunque in $2^5 - 2^3$ modi.
g_2 deve andare in un elemento di ordine 4 ma

$$< \psi(g_2) > \cap < \psi(g_3) >= \{e\}$$

poichè l'intersezione di ciclici è ciclico non deve succedere che

$$\psi(g_2) = \psi(g_3) + y \text{ con } o(y) \leq 2$$

dunque g_2 viene mandato in $2^5 - 2^3 - 2^3$ (infatti $2^5 - 2^3$ sono gli elementi di ordine 4 mentre 2^3 sono gli elementi della forma $\psi(g_2) + y$)
g_1 deve andare in un elemento di ordine 2 non contenuto in $< \psi(g_2), \psi(g_3) >$ dunque in $2^3 - 2^2$ modi

Esempio 10.5 (Cardinalità di $Aut(\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9)$).
g_3 deve andare in un elemento di ordine 9 dunque in $3^5 - 3^3$ modi
$< \psi(g_2) > \cap < \psi(g_3) >= \{e\}$ dunque

$$3\psi(g_2) \notin < \psi(g_3) >$$

ora in $< \psi(g_3) > \cong \mathbb{Z}_9$ ci sono $\phi(9) = 6$ elementi di ordine 9 ma

$$1 \equiv 4 \equiv 7 \mod 3$$

e

$$2 \equiv 5 \equiv 8 \mod 3$$

dunque

$$\psi(g_2) \neq \begin{cases} \psi(g_3) + y \\ 2\psi(g_3) + y \end{cases} \quad \textit{con } o(y) = 1, 3$$

quindi g_2 può andare in $3^5 - 3^3 - 2 \cdot 3^3$.
g_1 può andare in $3^3 - 3^2$ elementi di ordine 3 non inclusi nei generati da $\psi(g_2)$ e $\psi(g_3)$

Parte II

Teoria di Galois

11 Nozioni sui polinomi

In questa sezione riportiamo alcune nozioni sui polinomi fornite nel corso di Aritmetica

Definizione 11.1 (Contenuto e polinomi primitivi)**.**
Sia $p(x) = a_0 + a_1 x + \cdots + a_n x_n$ un polinomio, definiamo il contenuto di p come

$$c(p) = M.C.D.(a_0, \ldots, a_n)$$

Un polinomio è detto primitivo se ha contenuto 1

Lemma 11.1 (di Gauss)**.** *Il prodotto di 2 polinomi primitivo è primitivo*

Proposizione 11.2. *Sia p un polinomio primitivo in $\mathbb{Z}[x]$*

$$p \text{ irriducibile in } \mathbb{Q}[x] \quad \Leftrightarrow \quad p \text{ irriducibile in } \mathbb{Z}[x]$$

Proposizione 11.3. *Sia $p \in \mathbb{Q}[x]$ con $\deg p \leq 3$ allora*

$$p \text{ non ha radici} \quad \Leftrightarrow \quad p \text{ irriducibile}$$

Proposizione 11.4. *Se $f \in \mathbb{Z}_p$ è irriducibile allora f è irriducibile anche in $\mathbb{Z}[x]$*

Proposizione 11.5. *Sia $p(x) \in \mathbb{Z}[x]$ con $p(x) = a_0 + a_1 x + \cdots + a_n x^n$.*
Allora le radici in $\mathbb{Q}$ di p sono della forma $\frac{a}{b}$ con $a | a_0$ e $b | a_n$

Proposizione 11.6 (Criterio di Eisenstein)**.**
Sia $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$.
Se esiste p primo tale che

- *p non divide a_n*
- *p divide $a_0, \ldots, a_{n-1}$*
- *p^2 non divide a_0*

Allora $p(x)$ è irriducibile

Corollario 11.7. *Per ogni primo p il polinomio*

$$g(x) = x^{p-1} + \ldots x + 1$$

è irriducibile in $\mathbb{Q}[x]$

Dimostrazione. Osserviamo che

$$g(x) = \frac{x^p - 1}{x - 1}$$

quindi

$$g(x+1) = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k$$

tale polinomio è irriducibile per Eisenstein dunque anche g lo è infatti la funzione che manda $h(x) \to h(x+1)$ è un isomorfismo di anelli.

□

12 Lezione del 22 Novembre

Esempio 12.1. $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ *è di Galois?.*
Il polinomio $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ è irriducibile per Eisenstein, dunque è il polinomio minimo di $\sqrt[3]{2}$.
Ora $\mathbb{Q}(\sqrt[3]{2})$ non è il campo di spezzamento di p infatti p possiede radici non reali, dunque l'estensione non è di Galois

Esempio 12.2. *Trovare il campo di spezzamento $\mathbb{K}$ di $x^3 - 2$ e studiare* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$

Sia ζ_3 radice di $x^3 - 1$ diversa da 1 dunque

$$\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$$

Ora poichè $\sqrt[3]{2} \in \mathbb{K}$ allora $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.
Osserviamo che $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \subseteq S_3$ infatti permuta le radici di $x^3 - 1$ ed un elemento che fissa tutte e 3 le radici è l'identità.
Ora $\mathbb{Q} \subseteq \mathbb{K}$ ha grado 6 infatti

$$\begin{tikzcd}[column sep=small] & \mathbb{K} \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_3) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] \\ & \mathbb{Q} & \end{tikzcd}$$

infatti il polinomio minimo di ζ_3 è $x^2 + x + 1$ e quello di $\sqrt[3]{2}$ è $x^3 - 2$.
Da ciò segue che il grado di $\mathbb{K}$ su $\mathbb{Q}$ deve dividere 2 e 3 dunque $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = S_3$
Sia $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\zeta_3$ e $\alpha_3 = \sqrt[3]{2}\zeta_3^2$.
Usiamo i teoremi di corrispondenza per studiare tutti i sottocampi.
Sia $H_1 = \langle(2,3)\rangle$ dunque scambia α_2 con α_3 e fissa α_1 .
$\sqrt[3]{2} \in \mathbb{K}^{H_1}$ e poichè $\mathbb{Q}$ viene lasciato fisso si ha $K^{H_1} \subseteq \mathbb{Q}(\sqrt[3]{2})$.
Ora essendo $Q \supseteq \mathbb{K}^{H_1}$ ha grado 3 (indice di H_1 in S_3) dunque $\mathbb{K}^{H_1} = \mathbb{Q}(\sqrt[3]{2})$.
Ripetiamo il ragionamento con $H_2 = \langle(1,3)\rangle$ ottenendo che $\mathbb{K}^{H_2} = \mathbb{Q}(\zeta_3\sqrt[3]{2})$.
Invece se $H_3 = \langle(1,2)\rangle$ otteniamo $\mathbb{K}^{H_3} = \mathbb{Q}(\zeta^2\sqrt[3]{2})$.
Poichè $\mathbb{Q}(\zeta_3)$ è un sottocampo si ha $\mathbb{K}^{A_3} = \mathbb{Q}(\zeta_3)$ per esclusione infatti $\mathbb{K}^{A_3}$ ha grado 2 su $\mathbb{Q}$.
Un altro modo, sia

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)$$

osserviamo che $(1,2)(\delta) = (1,3)(\delta) = (2,3)(\delta) = -\delta$ dunque $\delta \notin \mathbb{Q}$ (non viene fissato da tutto il gruppo di Galois), inoltre $\delta \in \mathbb{K}^{A_3}$ e $\mathbb{K}^{A_3}$ ha grado 2

$$\delta = 2(1 - \zeta_3)(\zeta_3 - \zeta_3^2)(1 - \zeta_3^2)$$

ma $\zeta_3^2 = \overline{\zeta_3}$ e $(1 - \zeta_3)(1 - \zeta_3^2) = \frac{9}{4} + \frac{3}{4} \in \mathbb{Q}$ quindi $\mathbb{Q}(\delta) = \mathbb{Q}(\zeta_3(1 - \zeta_3))$.
Ora ζ_3 è radice di $1 + x + x^2$ quindi $\zeta^2 = -1 - \zeta_3$.

$$\mathbb{Q}(\delta) = \mathbb{Q}(\zeta_3(1 - \zeta_3)) = \mathbb{Q}(2\zeta_3 + 1) = \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3)$$

Possiamo riassumere quello che abbiamo detto fino ad ora con i seguenti diagrammi:
Sottogruppi di S_3

$$
\begin{tikzcd}
 & & \{e\} \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle(12)\rangle \arrow[drr, dash] & \langle(1,3)\rangle \arrow[dr, dash] & & \langle(2,3)\rangle \arrow[dl, dash] & A_3 \arrow[dll, dash, "\lhd"] \\
 & & S_3 & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & & \mathbb{K} \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\zeta_3^2\sqrt[3]{2}) \arrow[drr, dash] & \mathbb{Q}(\zeta_3\sqrt[3]{2}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash] & \mathbb{Q}(\zeta_3) \arrow[dll, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$

Esempio 12.3. *Studiare il campo di spezzamento di* $p = x^3 - x + 1$ *e il suo gruppo di Galois.*
Le uniche possibili radici sono ± 1 *quindi il polinomio è irriducibile.*
Sia $\mathbb{K}$ *il campo di spezzamento di* p *su* $\mathbb{Q}$ *e* n *il suo grado.*
Ora poichè il polinomio è irriducibile $3|n$ *ed inoltre* $n|3!$ *dunque*

- $n = 3$ *da cui* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}_3$
- $n = 6$ *da cui* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong S_3$

Poichè $p' = 3x^2 - 1$ *si annulla in* $\pm\frac{1}{\sqrt{3}}$ *inoltre*

$$p\left(\frac{1}{\sqrt{3}}\right) > 0 \quad p\left(-\frac{1}{\sqrt{3}}\right) > 0$$

quindi p *ha una radice reale e* 2 *complesse coniugate.*
$\varphi : \mathbb{C} \to \mathbb{C}$ *definito come* $\varphi(z) = \overline{z}$ *è un automorfismo di ordine* 2 *di* $\mathbb{C}$ *su* $\mathbb{Q}$*, ora* $\varphi_{|\mathbb{K}}$ *è un automorfismo (*p *ha coefficienti razionali).*
Il gruppo di Galois contiene un elemento di ordine 2 *da cui* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong S_3$

Esempio 12.4. *Studio del campo di spezzamento di* $x^3 + ax + b \in \mathbb{Q}[x]$ *e il suo gruppo di Galois.*
Siano α_1, α_2 *e* α_3 *sue radici.*
Dalle formule di Viete si ha

$$\begin{cases} \alpha_1\alpha_2\alpha_3 = -b \\ \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = a \end{cases}$$

Consideriamo come nel primo esempio

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \notin \mathbb{Q}$$

Inoltre $\Delta = \delta^2 \in \mathbb{Q}$ *infatti le permutazioni pari cambiano segno di* δ *mentre* δ^2 *no.*
Dalle formule di Viete si ottiene

$$\Delta = -4a^3 - 27b^2$$

distinguiamo 2 *differenti casi*

- *se Δ é un quadrato in $\mathbb{Q}$ allora $\delta \in \mathbb{Q}$ quindi il gruppo di Galois contiene solo permutazioni pari dunque è $\mathbb{Z}_3$*
- *se Δ non è un quadrato in $\mathbb{Q}$ allora $\delta \notin \mathbb{Q}$ quindi $\mathbb{Q}(\delta)$ è contenuto nel campo di spezzamento, ma $\mathbb{Q} \subset \mathbb{Q}(\delta)$ ha grado 2 quindi il gruppo di Galois è S_3*

Osservazione 6. Nel caso $p(x) = x^3 + ax^2 + bx + c$ allora se pongo $x_1 = x - \frac{a}{b}$ ottengo un polinomio della forma $x_1^3 + dx_1 + e$ quindi posso usare l'esempio precedente, traslando per numeri razionali, traslo le radici da cui il gruppo di Galois non viene modificato.

Proposizione 12.5. *Se n è primo, un n-ciclo è una trasposizione generano S_n*
Se n non è primo $(1, 2, \dots, n)$ e $(1, 2)$ generano S_n

Esempio 12.6. $p(x) = x^4 - 4x - 2$
Tale polinomio è irriducibile per Eisenstein.
Ora $f' = 5x^4 - 4$ da cui si annulla in 2 punti, dallo studio del segno di f nei punti di massimo e minimo osservo che p ha 3 radici reali e 2 complesse coniugate.
Posto $\mathbb{K}$ il campo di spezzamento si ha $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \subseteq S_5$.
Poichè il polinomio è irriducibile si ha $5|o(G)$ dunque$G$ contiene un 5-ciclo.
Il coniugio ristretto a $\mathbb{K}$ fissa 3 radici dunque G contiene una trasposizione.
Ora $G = S_5$

13 Lezione del 27-29 Novembre

Esempio 13.1. *Calcolare il grado del polinomio minimo di ζ_5 su $\mathbb{Q}(i)$*

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_5, i) \arrow[dl, dash, "\star"'] \arrow[dr, dash, "\circ"] & \\
\mathbb{Q}(\zeta_5) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

A noi interessa il grado $\circ$, studiamo il grado $\star$.
Tale grado è 1 se $i \in \mathbb{Q}(\zeta_5)$ altrimenti tale grado è 2.
In modo equivalente ci chiediamo se esiste un estensione del genere

$$\begin{tikzcd}
\mathbb{Q}(\zeta_5) \arrow[d, dash, "2"'] \\
\mathbb{Q}(i) \arrow[d, dash, "2"'] \\
\mathbb{Q}
\end{tikzcd}$$

Poichè $G = \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \mathbb{Z}_4$ esiste una sola sottoestensione di grado 2.
Sia $\varphi \in G$ dunque deve mandare una radice di $x^4 + x^3 + x^2 + x + 1$ in un altra radice dunque

$$\varphi(\zeta_5) = \zeta_5^j \quad j = 1, 2, 3, 4$$

Ma tale automorfismo deve avere ordine 4 quindi l'unico sottogruppo di indice 2 è

$$H = \{id, \varphi_4 : \zeta_5 \to \zeta_5^4\}$$

Ora $\omega = \zeta_5 + \zeta_5^{-1} \in \mathbb{Q}(\zeta_5)^H$, inoltre $\zeta_5 + \zeta_5^{-1} \notin \mathbb{Q}$ infatti

$$p(x) = (x - \zeta_5)\left(x - \zeta_5^{-1}\right) = x^2 - \omega x + 1$$

Se $\omega \in \mathbb{Q}$ allora $p(x)$ sarebbe un polinomio in $\mathbb{Q}(x)$ con ζ_5 come radici ovvero l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$ avrebbe grado minore o uguale a 2, il che è assurdo.
Dunque

$$\begin{tikzcd}
\mathbb{Q}(\omega) \arrow[d, dash, "\geq 2"] & \subseteq & \mathbb{Q}(\zeta_5)^H \arrow[dll, dash, "2"] \\
\mathbb{Q} & &
\end{tikzcd}$$

Da cui $\mathbb{Q}(\omega) = \mathbb{Q}(\zeta_5)^H$.
Osserviamo inoltre che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ è reale in quanto

$$\omega + \omega^2 = \zeta_5 + \zeta_5^4 + \zeta_5^2 + \zeta_5^3 + 2 = 1$$

dunque ω è radice di $x^2 + x - 1$ che ha $\Delta = \sqrt{5}$.
Concludiamo che $\mathbb{Q}(i)$ non è il sottocampo dell'estensione da cui

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_5, i) \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & \\
\mathbb{Q}(\zeta_5) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

ovvero il grado di ζ_5 su $\mathbb{Q}(i)$ è 4

Un altro modo per risolvere il problema era considerare i polinomi ciclotomici.
$i = \zeta_4$ *inoltre* $\zeta_4\zeta_5 = \zeta_{20}$ *da cui essendo* $\phi(20) = 8$ *otteniamo*

$$\begin{tikzcd}[column sep=small]
& \mathbb{Q}(\zeta_{20}) = \mathbb{Q}(i,\zeta_5) \arrow[dl, dash, "4"'] \arrow[dd, dash, "8"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(i) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\zeta_5) \arrow[dl, dash, "4"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Esempio 13.2. $\mathbb{Q}(\sqrt{2})$ *e* $\mathbb{Q}(\sqrt{3})$ *non sono isomorfi.*
Poichè le estensioni fissano $\mathbb{Q}$ *se 2 campi sono isomorfi allora poichè 2 è un* $\square$ *in* $\mathbb{Q}$ $(\sqrt{2})$ *allora lo deve essere anche in* $\mathbb{Q}(\sqrt{3})$ *ovvero*

$$2 = (a + b\sqrt{3})^2 \quad \Rightarrow \quad 2 = a^2 + 3b^2 + 2ab\sqrt{3} \quad a, b \in \mathbb{Q}$$

Ora $\{1, \sqrt{3}\}$ *sono una base di* $\mathbb{Q}(\sqrt{3})$ *come spazio vettoriale su* $\mathbb{Q}$ *dunque*

$$(2 - a^2 - 3b^2) \cdot 1 + 2ab\sqrt{3} = 0 \Rightarrow ab = 0$$

se $a = 0$ *allora* $2 = 3b^2$ *ovvero* $\frac{2}{3}$ *è un* $\square$ *in* $\mathbb{Q}$ *il che è assurdo.*
se $b = 0$ *allora* $2 = a^2$ *ovvero 2 è un* $\square$ *in* $\mathbb{Q}$ *il che è assurdo*

Lemma 13.3. $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}(\sqrt{d}) \Leftrightarrow cd$ *è un* $\square$ *in* $\mathbb{Q}$

Dimostrazione. $\Leftarrow$ $\sqrt{cd} \in \mathbb{Q}$ dunque $\sqrt{d} \in \mathbb{Q}(\sqrt{c})$
$\Rightarrow$ Se uno tra c e d è un $\square$ in $\mathbb{Q}$ allora lo sono entrambi dunque lo è anche il loro prodotto.
Supponiamo che c non è un $\square$ in $\mathbb{Q}$ allora poichè $\sqrt{d} \in \mathbb{Q}(\sqrt{c}$ si ha $d = (a + b\sqrt{c})^2$ con $a, b \in \mathbb{Q}$.
Essendo $\{1, \sqrt{c}\}$ una base segue $ab = 0$ dunque $a = 0$ (c non è un $\square$ in $\mathbb{Q}$)
Dunque

$$b^2c = d \quad \Leftrightarrow \quad b^2c^2 = dc \quad \Rightarrow \quad cd \text{ è un } \square \text{ in } \mathbb{Q}$$

$\square$

Proposizione 13.4 (Biquadratiche)**.**
Sia $p(x) = x^4 + ax^2 + b$*. Trovare il suo campo di spezzamento* $\mathbb{K}$ *e il gruppo di Galois.*

Poniamo $y = x^2$ *allora* $p(y) = y^2 + ay + b$*.*
Ora le 2 radici di $p(y)$ *sono*

$$\omega_1 = \frac{-a + \sqrt{\Delta}}{2} \quad \omega_2 = \frac{-a - \sqrt{\Delta}}{2} \quad \Delta = a^2 - 4b$$

dunque

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}, \sqrt{\omega_2}) \arrow[d, dash, "1{,}2"] \\
\mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}) \arrow[d, dash, "1{,}2"] \\
\mathbb{Q}(\sqrt{\Delta}) \arrow[d, dash, "1{,}2"] \\
\mathbb{Q}
\end{tikzcd}$$

Detto $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ osserviamo che $G < S_4$ (permuta le radici) ovvero G è contenuto in un 2-Sylow ovvero in D_4.
Dunque

- *Il grado è 1 si ha $G = \{e\}$*
- *Il grado è 2 si ha $G = \mathbb{Z}_2$*
- *Il grado è 4 si ha $G = \mathbb{Z}_4$ oppure $\mathbb{Z}_2^2$*
- *Il grado è 8 si ha $G = D_4$*

Passiamo ora al vero studio dell'estensione

- *Δ è un $\square$ in $\mathbb{Q}$.*
  $p(x) = (x^2 - c)(x^2 - d)$ da cui abbiamo

$$\begin{tikzcd}
 & \mathbb{K} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{c}) \arrow[dr, dash] & & Q(\sqrt{d}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

  - *c o d sono $\square$ in Q*
    - *$b = cd$ è un $\square$ in $\mathbb{Q}$ allora $G = \{e\}$*
    - *b non è un $\square$ in $\mathbb{Q}$ dunque d non è un $\square$ in $\mathbb{Q}$ da cui $G = \mathbb{Z}_2$*
  - *c e d non sono $\square$ in $\mathbb{Q}$*
    - *b è un $\square$ in $\mathbb{Q}$ allora $G = \mathbb{Z}_2$*
    - *b non è un $\square$ in $\mathbb{Q}$ allora $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.*
      Ci sono 2 sottoestensioni di grado 2 $\mathbb{Q}(\sqrt{c})$ e $\mathbb{Q}(\sqrt{d})$ dunque in G ci devono essere 2 sottogruppi di indice 2 ovvero $G \neq \mathbb{Z}_4$

- *Δ non è un $\square$ in $\mathbb{Q}$*

$$\begin{tikzcd}
 & \mathbb{K} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}) \arrow[dr, dash, "\star"'] & & \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_2}) \arrow[dl, dash, "\star"] \\
 & \mathbb{Q}(\sqrt{\Delta}) \arrow[d, dash, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

  Ora $\star = 1, 2$.
  $\star = 2$ se e solo se $p(x)$ è irriducibile in $\mathbb{Q}$ in quanto se l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ avesse grado 4 allora ω_1 ha grado 4 su $\mathbb{Q}$ dunque p sarebbe il suo polinomio minimo.

  - *p è irriducibile su $\mathbb{Q}$ (eq. $\sqrt{\omega_1}, \sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta})$)*

* $b=\omega_1\omega_2$ *non è* $\Box$ *in* $\mathbb{Q}(\sqrt{\Delta})$ *allora* $G=D_4$
Studiamo come agisce D_4 *sulle radici* $\{\sqrt{\omega_1}, -\sqrt{\omega_1}, \sqrt{\omega_2}, -\sqrt{\omega_2}\}$.
Essendo le 4 *radici non linearmente indipendenti devo identificando le radici opposte con vertici opposti del quadrato posso considerare* $G=D_4$

$$\begin{array}{ccc} \sqrt{\omega_1} & \text{———} & \sqrt{\omega_2} \\ | & & | \\ -\sqrt{\omega_2} & \text{———} & -\sqrt{\omega_1} \end{array}$$

Analizziamo i vari sottogruppi del diedrale per trovare le varie sottoestensioni.
Chiamiamo r *una rotazione di* $\pi/4$ *e* s *una simmetria per il punto medio di* 2 *lati opposti.*
I sottogruppi normali sono $\langle r\rangle$, $\langle r^2, s\rangle$ $\langle r^2, rs\rangle$ *di ordine* 4 *e* $\langle r^2\rangle$ *di ordine* 2.
$\sqrt{\Delta b}\in\mathbb{K}^{\langle r\rangle}$ *inoltre* $\sqrt{\Delta b}\notin\mathbb{Q}$ *in quanto* $\sqrt{b}\notin\mathbb{Q}(\sqrt{\Delta})$.
Ora $\langle r\rangle$ *ha indice* 2 *dunque* $\mathbb{K}^{\langle r\rangle}=\mathbb{Q}(\sqrt{\Delta b})$.
$\sqrt{b}=\sqrt{\omega_1\omega_2}\in\mathbb{K}^{\langle r^2,s\rangle}$ *ora* $\sqrt{b}\notin\mathbb{Q}$ *e per discorsi di grado* $\mathbb{K}^{\langle r^2,s\rangle}=\mathbb{Q}(\sqrt{b})$
$\sqrt{\Delta}\in\mathbb{K}^{\langle r^2,rs\rangle}$, $\sqrt{\Delta}\notin\mathbb{Q}$ *dunque* $\mathbb{K}^{\langle r^2,rs\rangle}=\mathbb{Q}(\sqrt{\Delta})$.
Poichè in D_4 *esiste un solo sottogruppo di ordine* 4 *ne segue che* $\mathbb{K}^{\langle r^2\rangle}=\mathbb{Q}(\sqrt{\Delta},\sqrt{b})$.
Manca da studiare i 4 *sottogruppi generati dalle simmetrie*

* b *è un* $\Box$ *in* $\mathbb{Q}(\sqrt{\Delta})$
  - b *è un* $\Box$ *in* $\mathbb{Q}$
    Essendo $\sqrt{\omega_1\omega_2}\in\mathbb{Q}$ *otteniamo* $\mathbb{K}=\mathbb{Q}(\sqrt{\Delta},\sqrt{\omega_1})$.
    Se identifichiamo le radici come i vertici di un quadrato allora possiamo sicuramente dire che $r, r^3, rs, r^3s\notin G$ *in quanto non fissano* b, *per* ***esclusione*** *poichè* G *deve avere ordine* 4 *si ha* $G=\langle r^2,s\rangle\cong\mathbb{Z}_2\times\mathbb{Z}_2$

$$G=\left\{\begin{array}{ll} \alpha:\ \sqrt{\omega_1}\to-\sqrt{\omega_1} & \beta:\ \sqrt{\omega_1}\to\sqrt{\omega_2} \\ \alpha:\ \sqrt{\omega_2}\to-\sqrt{\omega_2} & \beta:\ \sqrt{\omega_2}\to\sqrt{\omega_1} \\ & \\ \alpha\beta:\ \sqrt{\omega_1}\to-\sqrt{\omega_2} & Id \\ \alpha\beta:\ \sqrt{\omega_2}\to-\sqrt{\omega_1} & \end{array}\right\}$$

    $\mathbb{K}^{\langle\alpha\rangle}=\mathbb{Q}(\sqrt{\Delta})$.
    Osserviamo che $\sqrt{\omega_1}+\sqrt{\omega_2}\in\mathbb{K}^{\langle\beta\rangle}$ *inoltre tale somma non appartiene a* $\mathbb{Q}$ *altrimenti* $x^2-(\sqrt{\omega_1}+\sqrt{\omega_2})x+\sqrt{b}$ *sarebbe il polinomio minimo di* $\sqrt{\omega_1}$ *su* $\mathbb{Q}$ *(il che assurdo poichè tale polinomio dovrebbe avere grado* 4*).*
    $\mathbb{K}^{\langle\beta\rangle}=\mathbb{Q}(\sqrt{\omega_1}+\sqrt{\omega_2})$.
    Osservo che $\delta=\sqrt{\Delta}(\sqrt{\omega_1+\omega_2})$ *viene fissato da* $\alpha\beta$ *inoltre* $\delta\notin\mathbb{Q}$.
    Se $\delta\in\mathbb{Q}$ *allora* $\sqrt{\omega_1+\omega_2}\in\mathbb{Q}(\delta)=\mathbb{K}^{\langle\alpha\rangle}$ *da cui* $\sqrt{\omega_1}=-\sqrt{\omega_2}$ *ovvero* $\omega_1=\omega_2$ *assurdo il polinomio* $p(y)$ *aveva radici distinte* Δ *non è un* $\Box$ *in* $\mathbb{Q}$
    $\mathbb{K}^{\langle\alpha\beta\rangle}=\mathbb{Q}(\sqrt{\Delta}(\sqrt{\omega_1}+\sqrt{\omega_2}))$
  - b *non è un* $\Box$ *in* $\mathbb{Q}$ *ma lo è in* $\mathbb{Q}(\sqrt{\Delta})$.
    Tale affermazione equivale a dire che $b\Delta$ *è un* $\Box$ *in* $\mathbb{Q}$ *da* $(x+y\sqrt{\Delta})^2=b$.
    Poichè $\sqrt{b\Delta}\in\mathbb{Q}$ *viene fissato, con le identificazioni usuali, si osserva che una qualsiasi simmetria non può appartenere al gruppo di Galois da cui* $G=\langle r\rangle\cong\mathbb{Z}_4$.
    Poichè esiste un solo sottogruppo di indice 2 *si ha* $\mathbb{K}^{\langle r^2\rangle}=\mathbb{Q}(\sqrt{\Delta})$

14 Lezione del 6 Dicembre

Esempio 14.1. *Trovare per quali $n \in \mathbb{Z}$ si ha $\sqrt{n} \in \mathbb{Q}(\zeta_5)$*
La domanda è equivalente a chiederci se $\mathbb{Q}(\sqrt{n})$ sia una sottoestensione dell'estensione di Galois $\mathbb{Q} \subset \mathbb{Q}(\zeta_5)$

Ora se n è un $\square$ in $\mathbb{Q}$ allora $\sqrt{n} \in \mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$.
Altrimenti $Q(\sqrt{n})$ ha grado 2 su $\mathbb{Q}$.
Dallo studio dei polinomi ciclotomici, sappiamo che $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \mathbb{Z}_5^\star \cong \mathbb{Z}_4$, dunque per corrispondenza esiste un'unica sottoestensione di grado 2 su $\mathbb{Q}$.
Studiamo come agisce il gruppo di Galois

$$\varphi : \mathbb{Z}_5^\star \to \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \quad j \to \varphi_j \text{ dove } \varphi_j(\zeta_5) = \zeta_5^i$$

Poichè $\langle 4 \rangle$ ha indice 2 in $\mathbb{Z}_5^\star$ segue che la sottoestensione di grado 2 è data da $\mathbb{K} = \mathbb{Q}(\zeta_5)^{\langle \varphi_4 \rangle}$
$\alpha = \zeta_5 + \zeta_5^{-1}$ appartiene a $\mathbb{K}$ (α è ottenuta sommando tutti i termini dell'orbita di ζ_5 rispetto all'azione di $\langle \varphi_4 \rangle$).
Osserviamo che $\alpha^2 = \zeta_5 + \zeta_5^3 + 2$ dunque

$$\alpha^2 - \alpha = \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 + 2 = 1 \quad \zeta_5 \text{ è radice di } x^4 + x^3 + x^2 + x + 1$$

ovvero α è radice del polinomio $x^2 + x - 1$ dunque $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.
Osserviamo inoltre che $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{K}$ ma hanno lo stesso grado su $\mathbb{Q}$ da cui $\mathbb{K} = \mathbb{Q}(\sqrt{5})$.
Ora $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{5})$ se e solo se $5n$ è un $\square$ in $\mathbb{Q}$.

$$\sqrt{n} \in \mathbb{Q}(\zeta_5) \quad \Leftrightarrow \quad n = a^2 \text{ o } n = 5a^2 \text{ con } a \in \mathbb{Z}$$

Esempio 14.2. *Trovare per quali $n \in \mathbb{Z}$ si ha $\sqrt{n} \in \mathbb{Q}(\zeta_7)$*
Ripercorrendo un argomentazione analoga al caso precedente dobbiamo cercare il campo fisso di un sottogruppo di indice 2 in $\mathbb{Z}_7^\star$ (ovvero un sottogruppo di ordine 3)
Ora 2 ha ordine 3 in $\mathbb{Z}_7^\star$ dunque l'unica sottoestensione di grado 2 su $\mathbb{Q}$ è $\mathbb{K} = \mathbb{Q}(\zeta_7)^{\langle \varphi_2 \rangle}$.
Considerando, come nel caso precedente, la somma degli elementi di un orbita otteniamo

$$\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$$

Poichè α ha grado 1 o 2 su $\mathbb{Q}$ calcoliamo

$$\alpha^2 = \zeta_7^2 + \zeta_7^4 + \zeta_7 + 2\zeta_7^3 + 2\zeta_7^5 + 2\zeta_7^6$$

da cui $\alpha^2 + \alpha + 2 = 0$ ovvero α è radice del polinomio $x^2 + x + 2$ che ha discriminante $\Delta = -7$, da cui $\mathbb{K} = \mathbb{Q}(\sqrt{7})$

$$\sqrt{n} \in \mathbb{Q}(\zeta_7) \quad \Leftrightarrow \quad n = a^2 \text{ o } n = -7a^2 \text{ con } a \in \mathbb{Z}$$

Andiamo ora a generalizzare i risultati generali per un qualsiasi campo $\mathbb{Q}(\zeta_p)$ con p primo. Nel seguito sarà utile la seguente definizione

Definizione 14.1 (Simbolo di Legrende)**.**
Sia p un numero primo e a un intero, allora definiamo

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ se } p|a \\ 1 \text{ se } a \text{ è } \square \mod p \\ -1 \text{ se } a \text{ non è } \square \mod p \end{cases}$$

Osservazione 7. Segue dalla definizione che

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Esempio 14.3. *Trovare per quali $n \in \mathbb{Z}$ si ha $\sqrt{n} \in \mathbb{Q}(\zeta_p)$ con p primo.*
Se n è un $\square$ in $\mathbb{Q}$ allora in modo ovvio $\mathbb{Q}(\sqrt{n}) \in \mathbb{Q}(\zeta_P)$.
Se n non è un $\square$ in $\mathbb{Q}$ allora la domanda è equivalente a chiedersi se $\mathbb{Q}(\sqrt{n})$ è una sottoestensione di grado 2 dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$
Dai polinomi ciclotomici sappiamo che il gruppo di Galois dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ è $\mathbb{Z}_p^\star$ dunque esiste un solo sottogruppo di indice 2 tale sottogruppo è

$$H = \{i \in \mathbb{Z}_p^\star \,|\, i \text{ è } \square \; mod \; p\}$$

Dunque esiste una sola sottoestensione di grado 2 $\mathbb{K} = \mathbb{Q}(\zeta_p)^H$.
Osserviamo che $\alpha = \sum_{i \in H} \zeta_p^i \in \mathbb{K}$ in quanto somma di tutti gli elementi di un orbita.

Ora $\sum_{i \in \mathbb{Z}_p^\star} \zeta_p^i = -1$ in quanto ζ_p radice del polinomio $\prod_{j=0}^{p-1} x^i$ da cui anche $\beta = \sum_{j \in \mathbb{Z}_p^\star \setminus H} \zeta_p^j \in \mathbb{K}$
Consideriamo

$$S = \alpha - \beta = \sum_{i \in H} \zeta_p^i - \sum_{i \in \mathbb{Z}_p^\star \setminus H} \zeta_p^i = \sum_{i \in \mathbb{Z}_p^\star} \left(\frac{i}{p}\right) \zeta_p^i \in \mathbb{K}$$

Il polinomio minimo di S su $\mathbb{Q}$ ha grado al massimo 2 da cui calcoliamo S^2

$$S^2 = \sum_{i,j \in \mathbb{Z}_p^\star} \left(\frac{i}{p}\right)\left(\frac{j}{p}\right) \zeta_p^{i+j} = \sum_{i,j \in \mathbb{Z}_p^\star} \left(\frac{ij}{p}\right) \zeta_p^{i+j}$$

Sia k tale che $j = ik$ allora

$$S^2 = \sum_{i,k \in \mathbb{Z}_p^\star} \left(\frac{i^2 k}{p}\right) \zeta_p^{i(1+k)} = \sum_{i,k \in \mathbb{Z}_p^\star} \left(\frac{k}{p}\right) \zeta_p^{i(1+k)} = \left(\frac{-1}{p}\right) \sum_{i \in \mathbb{Z}_p^\star} \zeta_p^{i \cdot 0} + \sum_{\substack{k \in \mathbb{Z}_p^\star \\ k \neq -1}} \left(\frac{k}{p}\right) \sum_{i \in \mathbb{Z}_p^\star} \zeta_p^{i(k+1)}$$

Ora poichè $o\left(\mathbb{Z}_p^\star\right) = p - 1$ e poichè $k + 1 \neq 0$ otteniamo

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + \sum_{\substack{k \in \mathbb{Z}_p^\star \\ k \neq -1}} \left(\frac{k}{p}\right) \sum_{j \in \mathbb{Z}_p^\star} \zeta_p^j = \left(\frac{-1}{p}\right)(p-1) + \sum_{\substack{k \in \mathbb{Z}_p^\star \\ k \neq -1}} \left(\frac{k}{p}\right)(-1)$$

dove l'ultima uguaglianza deriva dal fatto che ζ_p è radice di $\prod_{i=1}^{p-1}$.
Ora possiamo scrivere

$$S^2 = \left(\frac{-1}{p}\right) p + \sum_{k \in \mathbb{Z}_p^\star} \left(\frac{k}{p}\right)(-1)$$

Ora l'ultima sommatoria è nulla in quanto ci sono lo stesso numero di elementi che sono quadrati e che non lo sono (H ha indice 2) dunque S è radice di

$$x^2 + \left(\frac{-1}{p}\right) p$$

Dunque la sottoestensione di grado 2 è

$$\mathbb{Q}(\sqrt{p}) \qquad \textit{se } p \equiv 1 \mod 4$$

$$\mathbb{Q}(i\sqrt{p}) \qquad \textit{se } p \equiv 3 \mod 4$$

Esempio 14.4. *Problema inverso di Galois per un gruppo di ordine* 8
Consideriamo i possibili gruppi di ordine 8

- Z_8.
  Come sappiamo il gruppo di Galois di ϕ_{17} è isomorfo a $\mathbb{Z}_{17}^{\star}$, ora tale gruppo presenta un sottogruppo di indice 8 (normale essendo il gruppo abeliano) dunque nell'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta_{17})$ è presente il sottocampo $\mathbb{K}$ fissato da H dunque si ha $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \mathbb{Z}_8$

- $Z_4 \times \mathbb{Z}_2$
  Prendiamo il sedicesimo polinomio ciclotomico ϕ_{16} e come sappiamo il gruppo
  $$\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) = \mathbb{Z}_{16}^{\star} = \mathbb{Z}_4 \times \mathbb{Z}_2$$

- $\mathbb{Z}_2^3$
  Consideriamo $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ osserviamo che tale estensione ha grado 8 infatti possiamo considerare la torre
  $$\begin{tikzcd}
  \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \arrow[d, dash, "2"] \\
  \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash, "2"] \\
  \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\
  \mathbb{Q}
  \end{tikzcd}$$
  Osserviamo inoltre che tale estensione presente almeno 4 sotto-estensioni di grado 2: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5}$, $\mathbb{Q}(\sqrt{6})$ dunque il gruppo di Galois deve avere almeno 4 sottogruppi di indice 2 ovvero ordine 4 dunque possiamo concludere dicendo che è il gruppo cercato ($\mathbb{Z}_8$ ne ha 1, $\mathbb{Z}_4 \times \mathbb{Z}_2$ ne ha 3, $\mathfrak{D}_4$ ne ha 3, Q_8 ne ha 3

- D_4
  Prendiamo il polinomio $p(x) = x^4 - 1$, il suo gruppo di Galois deve essere un sottogruppo di S_4 in particolare posto $\mathbb{K}$ il suo campo di spezzamento
  $$\begin{tikzcd}
  & \mathbb{K} \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
  \mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash, "2"] & & \mathbb{Q}(\sqrt{-\sqrt{2}}) \arrow[dl, dash, "2"'] \\
  & \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] & \\
  & \mathbb{Q} &
  \end{tikzcd}$$
  Dunque il gruppo d Galois ha ordine 8 ed è contenuto in S_4 da cui è D_4

- Q_8.
  Osserviamo che $\langle -1 \rangle$ è l'unico sottogruppo di indice 2 in Q_8 dunque è normale, inoltre Q_8 quozientato tale sottogruppo è isomorfo a $Z_2 \times Z_2$.

Per i teoremi di corrispondenza deve esistere un' sotto-campo $\mathbb{E}$ *con* $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$
Consideriamo il caso $\mathbb{E} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *dunque otteniamo*

$$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = \langle \sigma, \tau \rangle \text{ dove } \sigma : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \quad e\ \tau : \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases}$$

Poniamo ora $\alpha = \sqrt{\left(2-\sqrt{2}\right)\left(3-\sqrt{3}\right)}$ *e domandiamoci se* $\alpha \in \mathbb{E}$
Poichè $\alpha^2 \in E$ *possiamo considerare* $\sigma\left(\alpha^2\right)$ *ottenendo*

$$\sigma\left(\alpha^2\right) = \left(2+\sqrt{2}\right)\left(3-\sqrt{3}\right)$$

dividendo per α^2 *otteniamo*

$$\frac{\sigma\left(\alpha^2\right)}{\alpha^2} = \frac{2+\sqrt{2}}{2-\sqrt{2}} = \left(1+\sqrt{2}\right)^2$$

Supponiamo, per assurdo, $\alpha \in \mathbb{E}$ *otteniamo*

$$\frac{\sigma(\alpha)}{\alpha} = \pm\left(1+\sqrt{2}\right)$$

da cui

$$\sigma^2(\alpha) = \sigma\left(\left(1+\sqrt{2}\right)\alpha\right) = \left(1+\sqrt{2}\right)\left(1-\sqrt{2}\right)\alpha = -\alpha$$

ma ciò è assurdo in quanto σ *aveva ordine* 2, *ovvero* $\alpha \notin \mathbb{E}$.
Abbiamo dunque

$$\begin{array}{c} \mathbb{L} = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \alpha\right) \\ \Big|\,{\scriptstyle 2} \\ \mathbb{E} = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \\ \Big|\,{\scriptstyle 4} \\ \mathbb{Q} \end{array}$$

Resta da mostrare che $\mathbb{Q} \subset \mathbb{L}$ *sia un'estensione di Galois (campo di spezzamento di un polinomio separabile).*
Sia $q = x^2 - \left(2-\sqrt{2}\right)\left(3-\sqrt{3}\right)$ *il polinomio minimo di* α *su* $\mathbb{E}$.
Poichè $q \in \mathbb{E}[x]$ *possiamo considerare l'azione di* $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ *su tale polinomio, l'orbita è composta da*

$$p_1 = q = x^2 - \left(2-\sqrt{2}\right)\left(3-\sqrt{3}\right)$$

$$p_2 = q = x^2 - \left(2+\sqrt{2}\right)\left(3-\sqrt{3}\right)$$

$$p_3 = q = x^2 - \left(2-\sqrt{2}\right)\left(3+\sqrt{3}\right)$$

$$p_4 = q = x^2 - \left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)$$

Poniamo $p = p_1 p_2 p_3 p_4$, *osserviamo che tale polinomio ha grado* 8 *inoltre tale polinomio è invariante per* $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ *dunque* $p \in \mathbb{Q}[x]$.
Sia $\mathbb{K}$ *il campo di spezzamento di* p, *mostriamo che* $\mathbb{K} = \mathbb{L}$.

In modo ovvio $\alpha \in \mathbb{K}$ (è radice di p_1), mostriamo che $\sqrt{3} \in \mathbb{K}$.
Poichè $\mathbb{K}$ è il campo di spezzamento di p in particolare

$$p_1(x) = (x - a_1)(x - a_2) \text{ con } a_1, a_2 \in \mathbb{K} \quad \Rightarrow \quad -\left(2 - \sqrt{2}\right)\left(3 - \sqrt{3}\right) \in \mathbb{K}$$

$$p_2(x) = (x - a_3)(x - a_4) \text{ con } a_3, a_4 \in \mathbb{K} \quad \Rightarrow \quad -\left(2 + \sqrt{2}\right)\left(3 - \sqrt{3}\right) \in \mathbb{K}$$

Dunque anche

$$\left(2 + \sqrt{2}\right)\left(3 - \sqrt{3}\right)\left(2 - \sqrt{2}\right)\left(3 - \sqrt{3}\right) = 22 - 12\sqrt{3} \in \mathbb{K} \quad \Rightarrow \quad \sqrt{3} \in \mathbb{K}$$

In modo analogo (utilizzando $p_2(x)$ e $p_3(x)$) si mostra che $\sqrt{2} \in \mathbb{K}$.
Abbiamo provato dunque $\mathbb{L} \subseteq \mathbb{K}$.
Verifichiamo che se β è un coniugato di α allora $\frac{\beta}{\alpha} \in \mathbb{E}$ ovvero $\beta \in \mathbb{L}$.
I possibili β^2 sono $\pm\left(2 \pm \sqrt{2}\right)\left(3 \pm \sqrt{3}\right)$.
Facciamo la verifica solamente per $\beta = \left(2 - \sqrt{2}\right)\left(3 - \sqrt{3}\right)$ le altre sono analoghe

$$\frac{\beta^2}{\alpha^2} = \frac{3 + \sqrt{3}}{3 - \sqrt{3}} = \frac{\left(3 + \sqrt{3}\right)^2}{6} = \left(\frac{3 + \sqrt{3}^2}{\sqrt{3}\sqrt{2}}\right) \quad \Rightarrow \quad \beta = \pm\left(\frac{3 + \sqrt{3}}{\sqrt{2}\sqrt{3}}\right)\alpha \in \mathbb{L}$$

Dunque poichè vale un inclusione e $\mathbb{L}$ contiene tutte le radici di p possiamo concludere che $\mathbb{L} \subset \mathbb{Q}$ è un estensione di Galois.
Mostriamo adesso che il gruppo è Q_8 (contiene 6 elementi di ordine 4)
Consideriamo la mappa di restrizione

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$$

$$\phi \to \phi_{|\mathbb{E}}$$

otteniamo dunque

$$\sigma_\star \to \sigma$$

$$\tau_\star \to \tau$$

$$\mu_\star \to \sigma\tau$$

Poichè $\alpha^2 \in \mathbb{E}$ si ha

$$\frac{\sigma_\star(\alpha^2)}{\alpha^2} = \frac{\sigma(\alpha^2)}{\alpha^2} = \left(1 + \sqrt{2}\right)^2$$

dunque

$$\frac{\sigma_\star^2(\alpha)}{\alpha} = -\alpha$$

L'ordine di $\alpha_\star$ non può essere nè uno nè 2, se fosse 8 allora $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ sarebbe ciclico il che è assurdo (ha come sottogruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ che non è ciclico).
L'ordine di $\alpha_\star$ è dunque 4, dunque anche quello di $\sigma_\star^3$.
Con ragionamenti analoghi si mostra che anche $\tau_\star$, $\tau_\star^3$, $\mu_\star$ e $\mu_\star^3$ hanno ordine 4.
Il gruppo di Galois è un gruppo di ordine 8 con 6 elementi di ordine 4 dunque è il gruppo dei quaternioni

Lemma 14.5. *Sia n pari allora*
$$\phi_{2n}(x) = \phi_n(x^2)$$

Dimostrazione. Se ζ è una radice primitiva $2n$-esima dell'unità allora segue che ζ^2 è una radice primitiva n-esima dell'unità dunque: $\phi_{2n}(x)|\phi\left(x^2\right)$.
Poichè n è pari otteniamo $\phi(2n) = 2\phi(n)$ dunque i 2 polinomi ciclotomici hanno lo stesso grado, da cui l'uguaglianza. □

Esempio 14.6. *Trovare il campo di spezzamento e il gruppo di Galois del polinomio $\left(x^4 - x^2 + 1\right)\left(x^2 - 3\right)$ su $\mathbb{Q}$*
Poichè $\phi_6 = x^2 - x + 1$ per il lemma precedente otteniamo $\phi_{12} = x^4 - x^2 + 1$ da cui il campo di spezzamento del polinomio su $\mathbb{Q}$ è $\mathbb{K} = \mathbb{Q}\left(\zeta_{12}, \sqrt{3}\right) = \mathbb{Q}\left(\zeta_4, \zeta_3, \sqrt{3}\right)$.
Ora poichè ζ_3 è radice di $x^2 + x + 1$ otteniamo che $\zeta_3 \in \mathbb{Q}\left(i, \sqrt{3}\right)$.
$\mathbb{K} = \mathbb{Q}(i, \sqrt{3})$ e poichè esistono 2 sotto-estensione di grado 2 su $\mathbb{Q}$ otteniamo $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Esempio 14.7. *Trovare il campo di spezzamento del polinomio $\left(x^4 - x^2 + 1\right)\left(x^2 - 3\right)$ su $\mathbb{F}_{13}$*
Poichè in $\mathbb{F}_{13}$ si ha $4^2 = 3$ il campo contiene tutte le radici di $x^2 - 3$
Osserviamo inoltre che $\mathbb{F}_{13}$ è il campo di spezzamento del polinomio $x^{12} - 1$, ora poichè $\phi_{12}|x^{12} - 1$ si ha $x^4 - x^2 + 1$ ha tutte le radici in $\mathbb{F}_{13}$.
Il campo di spezzamento del polinomio su $\mathbb{F}_{13}$ è $\mathbb{F}_{13}$ stesso

15 Costruzione con riga e compasso

Una figura è costruibile con riga e compasso se è possibile disegnarlo solamente con queste operazioni elementari

- Tracciare una retta tra due punti
- Tracciare una circonferenza di centro un punto e passante per un altro punto
- Intersecare una circonferenza con una retta
- Intersecare due circonferenze
- Intersecare due rette

Osserviamo che per intersecare 2 circonferenze, o una retta è una circonferenza al massimo dobbiamo risolvere un equazione di secondo grado, dunque possiamo definire

Definizione 15.1. $x \in \mathbb{R}$ è costruibile se esiste un estensione $\mathbb{Q} \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n \ni x$ dove ogni singola estensione ha grado 2

In modo equivalente

Definizione 15.2. $x \in \mathbb{C}$ è costruibile se esiste un estensione $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n \ni x$ dove ogni singola estensione ha grado 2

Esempio 15.1. *Con riga e compasso non è possibile trisecare un angolo.*
Consideriamo nel piano complesso l'angolo formato da ζ_3 l'origine e ζ_3^2, tali punti sono costruibili in quanto l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3)$ ha grado 2.
Se potessimo trisecare quest'angolo allora, potremmo costruire con riga e compasso ζ_9 il che è assurdo, infatti per quanto sappiamo sui polinomi ciclotomici l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_9)$ ha grado $\phi(9) = 6$

Esempio 15.2. *Con riga e compasso non è possibile costruire un cubo con volume doppio di un cubo dato.*
Consideriamo un cubo di lato 1, se fosse possibile duplicare il cubo, allora potremmo costruire $\sqrt[3]{2}$ il che è assurdo in quanto $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}$ ha grado 3

Esempio 15.3. *Con riga e compasso non è possibile costruire un eptagono iscritto in una circonferenza.*
Se fosse possibile, allora consideriamo un eptagono iscritto in una circonferenza, i suoi vertici sono numeri complessi costruibili.
Il rapporto tra 2 vertici adiacenti sarebbe costruibile, ma tale rapporto è una radice 7-ima dell'unita primitiva, dunque ha grado 6 su $\mathbb{Q}$, il che è assurdo

Osservazione 8. Con un ragionamento analogo, si dimostra che gli unici poligoni regolari costruibili sono quelli con

$$n = 2^p \prod \text{ primi di Fermat distinti}$$

dove i primi di Fermat, sono i primi della forma $2^{2^n} + 1$

Parte III

Appendici

16 Gruppo moltiplicativo dei gruppi ciclici finiti

Osservazione 9. Abbiamo osservato nel corso di Aritmetica che

$$(\mathbb{Z}_p)^\star \cong \mathbb{Z}_{p-1}$$

Mostreremo adesso che

$$(Z_{p^\alpha})^\star \cong \mathbb{Z}_{\phi(p)}$$

ovvero che tale gruppo è ciclico se e solo se p è un primo dispari

Lemma 16.1. *Sia p un primo dispari e k un intero non nullo*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1} \text{ con } \lambda \in \mathbb{N} - \{0\} \text{ e } M.C.D(\lambda, k) = 1$$

Dimostrazione. Induzione su k.
Se $k = 1$

$$(1+p)^p = 1 + \binom{p}{1} p + \binom{p}{2} p^2 + \cdots + \binom{p}{i} p^i + \cdots + p^p$$

Osserviamo che p^2 divide tutti i termini della sommatoria ad esclusione del primo, mentre p^3 divide tutti i termini tranne i primi 2 da cui

$$(1+p)^p = 1 + p^2 (1 + \lambda' p)$$

infatti $\binom{p}{1} = p$.
Ponendo $1 + \lambda' p = \lambda$ osserviamo che $M.C.D(\lambda, p) = 1$ dunque abbiamo la tesi.
Supponiamo, per induzione che

$$(1+p)^{p^k} = 1 + \lambda p^{k+1} \text{ con } M.C.D(\lambda, p) = 1$$

Dalla propietà delle potenze osserviamo che

$$(1+p)^{p^{k+1}} = \left(1 + \lambda p^{k+1}\right)^p = 1 + \sum_{i=1}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$

Ora p^{k+2} divide tutti i termini della sommatoria dunque

$$(1+p)^{p^{k+1}} = 1 + p^{k+2} (\lambda + up)$$

dunque poichè per ipotesi induttiva λ è primo con p posto $\lambda' = \lambda + up$ otteniamo la tesi

□

Proposizione 16.2. *Sia p un primo dispari a $\alpha \in \mathbb{N}$ con $\alpha \geq 2$ allora $(\mathbb{Z}_{p^\alpha})^\star$ è ciclico*

Dimostrazione. Poichè la cardinalità del gruppo è $p^{\alpha-1}(p-1)$, per mostrare che il gruppo è ciclico basta trovare un elemento con ordine $p^{\alpha-1}(p-1)$.
Osserviamo che $(1+p)$ ha ordine $p^{\alpha-1}$ infatti per il lemma precedente

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1 \mod p^\alpha$$

dunque l'ordine di $1+p$ divide $p^{\alpha-1}$.
Se l'ordine di $1+p$ fosse un divisore proprio di $p^{\alpha-1}$ allora

$$(1+p)^{p^{\alpha-2}} \equiv 0 \mod p^\alpha$$

ma ciò è assurdo in quanto

$$(1+p)^{p^{\alpha-2}} = 1 + p^{\alpha-1}\lambda \equiv 1 \mod p^\alpha \quad \Leftrightarrow \quad \lambda \equiv 0 \mod p^\alpha \quad \Rightarrow \quad \lambda \equiv 0 \mod p$$

Ma ciò è assurdo infatti per il lemma λ è primo con p e non è nullo.
Per concludere la dimostrazione basta trovare un elemento di ordine $p-1$ infatti se α e β commutano, hanno ordine primi tra loro allora l'ordine di $\alpha\beta$ è il prodotto degli ordini.
Consideriamo adesso l'omomorfismo

$$\psi : (\mathbb{Z}_{p^\alpha})^\star \to (\mathbb{Z}_p)^\star \quad [a]_{p^\alpha} \to [a]_p$$

Osserviamo che tale omomorfismo è ben definito (se a è inverti bile modulo p^α lo è anche modulo p) è suriettivo.
Sia x un generatore di $(\mathbb{Z}_p)^\star$.
Essendo l'omomorfismo suriettivo, esiste un $\beta \in (\mathbb{Z}_{p^\alpha})^\star$ tale che $\psi(\beta) = x$ dunque l'ordine di β deve essere un multiplo dell'ordine di x ($p-1$).
Ora esiste un $\beta' \in \langle\beta\rangle$ tale che $o(\beta') = p-1$.
$\beta'(p+1) \in (\mathbb{Z}_{p^\alpha})^\star$ inoltre tale elemento ha ordine uguale alla cardinalità del gruppo moltiplicativo, che è dunque ciclico □

Studiamo ora cosa succede quando $p = 2$, andremo a dimostrate che in questo caso (tranne nel caso 4) il gruppo moltiplicativo non è ciclico.

Lemma 16.3. *Sia $k \in \mathbb{N}$ con $k \neq 0$ allora*

$$5^{2^k} = 1 + \lambda 2^{k+2} \text{ con } \lambda \text{ dispari}$$

Dimostrazione. Induzione su k.
Per $k = 1$ osserviamo che $5^2 = 1 + 3 \cdot 2^3$.
Supponiamo che la tesi sia vera per k, mostriamo che è vera anche per $k+1$

$$5^{2^{k+1}} = \left(5^{2^k}\right)^2 = \left(1 + \lambda 2^{k+2}\right)^2 = 1 + \lambda^2 2^{2k+4} + \lambda 2^{k+3} = 1 + \lambda(1 + 2^\alpha\lambda)2^{k+3}$$

Osserviamo ora che $\lambda(1 + 2^\alpha\lambda)$ è dispari dunque otteniamo la tesi.

Proposizione 16.4. *Il gruppo $(\mathbb{Z}_{2^\alpha})^\star$ non è ciclico.*
In particolare

$$(\mathbb{Z}_{2^\alpha})^\star \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$$

Dimostrazione. Consideriamo l'omomorfismo

$$\psi : (\mathbb{Z}_{2^\alpha})^\star \to (\mathbb{Z}_4)^\star \quad [a]_{2^\alpha} \to [a]_4$$

Tale omomorfismo è ben definito e suriettivo.
Osserviamo che il $\ker\psi$ ha esattamente $2^{\alpha-2}$ elementi (l'omomorfismo è suriettivo).
Per il lemma precedente, possiamo concludere che il nucleo è ciclico, 5 appartiene al nucleo e ha ordine $2^{\alpha-2}$.
Osserviamo inoltre che $\ker\psi \lhd (\mathbb{Z}_{2^\alpha})^\star$ $\{1,-1\} \lhd (\mathbb{Z}_{2^\alpha})^\star$, inoltre $\ker\psi \cap \{1,-1\} = \{1\}$.
Per ragioni di cardinalità segue che $(\mathbb{Z}_{2^\alpha})^\star = \ker\psi\{1,-1\}$ e dato che sono entrambi normali

$$(\mathbb{Z}_{2^\alpha})^\star = \{1,-1\} \times \ker\psi \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^\alpha-2}$$

□

Possiamo adesso studiare $(\mathbb{Z}_n)^\star$.
Supponiamo infatti

$$n = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

allora come sappiamo

$$\mathbb{Z}_n \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i^{\alpha_i}}$$

ed inoltre

$$(\mathbb{Z}_n)^\star \cong \prod_{i=1}^{n} \left(\mathbb{Z}_{p_i^{\alpha_i}}\right)^\star$$

infatti se un elemento è invertibile in $\mathbb{Z}_n$ allora deve essere invertibile in ogni componente $\mathbb{Z}_{p^\alpha}$ e viceversa.

Proposizione 16.5. $(\mathbb{Z}_n)^\star$ *è ciclico solamente nei seguenti casi*

- $n = 2$
- $n = 4$
- $n = 2p^\alpha$ *con* p *primo dispari e* $\alpha \in \mathbb{N}$ *non nullo*
- $n = p^q$ *con* p *primo dispari e* $\alpha \in \mathbb{N}$

Dimostrazione. Da quanto visto precedentemente, in questi casi il gruppo moltiplicativo è ciclico.
Supponiamo adesso $n = p_1^{\alpha_1} \cdot p_n^{\alpha^n}$ con p_s, p_t primi dispari distinti.
Allora per il ragionamento precedentemente fatto

$$(Z_n)^\star \cong \left(\mathbb{Z}_{p_1^{\alpha_1}}\right)^\star \times \dots \times \left(\mathbb{Z}_{p_s^{\alpha_s}}\right)^\star \times \dots \times \left(\mathbb{Z}_{p_t^{\alpha_t}}\right)^\star \times \dots \times \left(\mathbb{Z}_{p_n^{\alpha_n}}\right)^\star$$

Ora $\left(\mathbb{Z}_{p_t^{\alpha_t}}\right)^\star \times$ e $\left(\mathbb{Z}_{p_s^{\alpha_s}}\right)^\star \times$ sono ciclici di ordine pari dunque entrambi contengono una copia isomorfa a $\mathbb{Z}_2$.
$(\mathbb{Z}_n)^\star$ dunque contiene una copia isomorfa a $\mathbb{Z}_2 \times \mathbb{Z}_2$ dunque non può essere ciclica.
Con un ragionamento analogo si mostra che $n \neq 2^\alpha p^\beta$ con $\alpha > 1$

17 Polinomi ciclotomici in caratteristica p

Proposizione 17.1. *Sia p primo e $n \in \mathbb{N}$ allora l'estensione $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ è di Galois con gruppo $\mathbb{Z}_n$*

Dimostrazione. L'estensione è di Galois in quanto è il campo di spezzamento del polinomio separabile $x^{p^n} - 1$ (ha radici distinte).
Poichè l'estensione è di Galois, il gruppo ha cardinalità $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
Osserviamo che l'omomorfismo di Frobenius

$$\mathcal{F} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \quad a \to a^p$$

è un generatore del gruppo di Galois.
Dal piccolo teorema di Fermat segue che $\mathcal{F}$ appartiene al gruppo.
Inoltre l'ordine di $\mathcal{F}$ divide n, mostriamo che è proprio n.
Supponiamo $\mathcal{F}^j = Id$ per un certo $j < n$ allora il polinomio $x^{p^j} - 1$ avrebbe p^n radici, il che è assurdo.

Da ora in avanti denotiamo con μ_n l'insieme delle radici del polinomio $x^n - 1 \in K[x]$.

Osservazione 10. μ_n è un sottogruppo moltiplicativo del campo di spezzamento di $x^n - 1$ dunque è un gruppo ciclico di ordine n,

Osservazione 11. Nel caso in cui $\mathbb{K} = \mathbb{F}_p$, $\mathbb{F}_p(\mu_n) = \mathbb{F}_{p^k}$ dunque $\mathbb{F}_p \subseteq \mathbb{F}_p(\mu_n)$ è di Galois per la proposizione precedente

Sia $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)$, possiamo considerare la restrizione di σ a μ_n dunque poichè $\mu_n = \langle \zeta \rangle$ $\sigma(\zeta) = \zeta^n$ dove ζ^a genera μ_n dunque i a e n sono coprimi.
Possiamo dunque definire la mappa

$$\vartheta : \mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p) \to (\mathbb{Z}_n)^\star$$

tale che $\vartheta(\sigma) = a$.

Proposizione 17.2. *ϑ è iniettiva.*

Dimostrazione. Sia $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)$ tale che $\vartheta(\sigma) = id$ dunque $\sigma_{|\mu_n)} = Id$ e poichè $\sigma_{|\mathbb{F}_p} = Id$ ne segue che $\sigma = Id_{\mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)}$ □

Proposizione 17.3. *Sia n primo con p.*
La mappa ϑ ha immagine $\langle p \rangle$.

Dimostrazione. Come abbiamo dimostrato $\mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)$ è generato dall'omomorfismo di Frobenius.
Ora $\vartheta(\mathcal{F}) = p$ dunque $Im\theta$ è generato da p in $(\mathbb{Z}_n)^\star$

Corollario 17.4.

$$[\mathbb{F}_p(\mu_n) : \mathbb{F}_p] = \textit{ ordine moltiplicativo di } p \textit{ in } (\mathbb{Z}_n)^\star$$

Sia $\overline{\phi_n}$ l'n-esimo polinomio ciclotomico proiettato su $\mathbb{Z}_p$

Proposizione 17.5. *Sia n primo con p.*
I fattori irriducibili di $\overline{\phi_n}$ in $\mathbb{F}_p[x]$ sono distinti a hanno grado uguale all'ordine di p in $(\mathbb{Z}_n)^\star$

Dimostrazione. $\overline{\phi_n}$ è separabile essendolo $x^n - 1$.
Sia α una radice di $\overline{\phi_n}$, α è una radice primitiva da cui

$$\mathbb{F}_p(\alpha) = \mathbb{F}_p(\mu_n)$$

Sia $f(x)$ il polinomio minimo di α su $\mathbb{F}_p$ dunque

$$\deg f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_p(\mu_n) : \mathbb{F}_p] = \text{ ordine di } p \text{ in } (\mathbb{Z}_n)^\star$$

Dunque tutti i fattori irriducibili (polinomi minimi di radici) di $\overline{\phi_n}$ hanno grado uguale all'ordine moltiplicativo di p. □

Corollario 17.6.

$$\overline{\phi_n} \text{ ‘e irriducibile in } \mathbb{F}_p[x] \quad \Leftrightarrow \quad \begin{cases} M.C.D.(p,n) = 1 \\ \langle p \rangle = (\mathbb{Z}_n)^\star \end{cases}$$

Dimostrazione. $\Rightarrow$ Se $M.C.D(p,m) = 1$ allora abbiamo la seguente relazione in $\mathbb{Z}[x]$

$$\phi_{p^r m}(x) = \frac{\phi_m\left(x^{p^r}\right)}{\phi_m\left(x^{p^{r-1}}\right)}$$

(entrambi i polinomi sono monici, quello a sinistra è irriducibile, entrambi hanno una radice in comune)
Tale relazione "letta" in $\mathbb{Z}_p[x]$ diventa

$$\overline{\phi_{p^r m}}(x) = \left(\overline{\phi_m}(x)\right)^{p^r - p^{r-1}}$$

.
Dunque $\overline{\phi_n}$ irriducibile implica n e p primi tra loro.
Se $\overline{\phi_n}$ irriducibile allora l'ordine di p in $(\mathbb{Z}_n)^\star$ è uguale al grado del polinomio ciclotomico che è $\varphi(n)$.
Dunque p è un generatore del gruppo moltiplicativo.
$\Leftarrow$ se $M.C.D(p,n) = 1$ e p genera $(\mathbb{Z}_n)^\star$ allora per la proposizione precedente i fattori irriducibili di $\overline{\phi_n}$ devono avere grado $\varphi(n)$ che è il grado del polinomio dunque è irriducibile.

Corollario 17.7. *Se* $(\mathbb{Z}_n)^\star$ *non è ciclico.*
$\overline{\phi_n}$ *si fattorizza in* $\mathbb{Z}_p[x]$ *per ogni primo* p

Osservazione 12. Il caso più piccolo è per $n = 8$ infatti $\phi(8) = x^4 + 1$ si fattorizza in ogni $\mathbb{Z}_p$ con p primo