Algebra I

A.A. 2023-2024

SIMONE SACCANI

TEORIA DEI GRUPPI

Richiami

Sia G gruppo

Def. G si dice ciclico se $\exists g \in G$ tale che $G = \langle g \rangle$, dove $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

Teorema Sia G un gruppo ciclico, $G = \langle g \rangle$, allora
(1) Se $|G| = +\infty$, allora $G \cong \mathbb{Z}$
(2) Se $|G| = n < +\infty$, allora $G \cong \mathbb{Z}/n\mathbb{Z}$

DIMOSTRAZIONE

Sia $\varphi : \mathbb{Z} \longrightarrow G$
$i \longmapsto g^i$

φ è un omomorfismo. $\varphi(0) = g^0 = e$

$\varphi(i+j) = g^{i+j} = g^i \cdot g^j = \varphi(i) \cdot \varphi(j)$

φ è surgettivo per costruzione

(1) Se $|G| = +\infty$, φ è iniettivo, infatti:
$i \in \ker\varphi \iff g^i = e$
Se fosse $i \neq 0$, allora $\text{ord}(g) \mid |i|$, ma $\text{ord}(g) = +\infty$ ↯
Quindi $\ker(\varphi) = \{0\}$ e perciò φ è un isomorfismo: $G \cong \mathbb{Z}$

(2) Se $|G| = n$, allora $\ker\varphi = n\mathbb{Z}$, infatti
$n = |G| = |\langle g \rangle| = \text{ord}(g)$ e $i \in \ker\varphi \iff g^i = e$
Quindi $\ker\varphi = n\mathbb{Z}$. Per il I teorema di isomorfismo:
$\mathbb{Z}/n\mathbb{Z} \cong G$ □

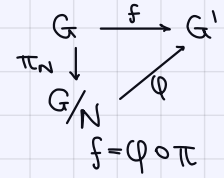
Esempio
- Σ_n: radice n-esima primitiva
  $|\langle \Sigma_n \rangle| = n$ $\quad \langle \Sigma_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$ $\quad \Sigma_n$ radice n-esima di 1 $\quad \xi_n^n = 1 = \xi_n^0$
- S_n non è ciclico (non è abeliano)
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle (1,0), (0,1) \rangle$ è abeliano ma non è ciclico

Def. Dato $S \subseteq G$ sottoinsieme, $\langle S \rangle = \{s_1 \cdots s_n \mid s_i \in S \cup S^{-1}\}$ dove $S^{-1} = \{s^{-1} \mid s \in S\}$

Esempio $S_3 = \langle (1,2), (123) \rangle$ non commutano
$\mathbb{Z}/6\mathbb{Z} = \langle \bar{3}, \bar{2} \rangle$ commutano

I teorema di omomorfismo

Data $f: G \longrightarrow G'$, con $N \triangleleft G$ $N \subseteq \ker f$
esiste un'unica φ che fa commutare il diagramma
con $\operatorname{Im} f = \operatorname{Im} \varphi$ e $\ker \varphi = \ker f / N$
Inoltre, se $N = \ker f$, φ è iniettiva.



DIMOSTRAZIONE

$f(g) = \varphi \circ \pi(g) = \varphi(gN)$
l'unica possibilità è porre $\varphi(gN) = f(g)$

(1) φ è ben definita: $gN = xN \longrightarrow f(g) = \varphi(gN) = \varphi(xN) = f(x)$
$\longrightarrow x \in gN : x = gn \in N \subseteq \ker f \longrightarrow f(x) = f(gn) = f(g) f(n) = f(g)$

(2) φ è omomorfismo: $\varphi(gN \cdot hN) = \varphi(ghN) = f(gh) = f(g) f(h) = \varphi(gN) \varphi(hN)$

(3) $\ker \varphi = \{gN \mid \varphi(gN) = f(g) = e\} = \{gN \mid g \in \ker f\} = \ker f / N$
$\operatorname{Im} \varphi = \{\varphi(gN) \mid g \in G\} = \{f(g) \mid g \in G\} = \operatorname{Im} f$

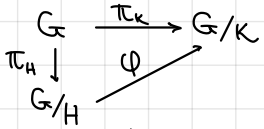
Se $N = \ker f$: $\ker \varphi = \ker f / N = \{N\} \longrightarrow \varphi$ è iniettiva □

II teorema di omomorfismo

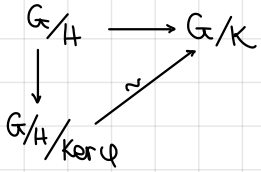
G gruppo, $H, K \triangleleft G$ con $H \subseteq K$. Allora
$\frac{G/H}{K/H} \cong G/K$

DIMOSTRAZIONE

Considero $\pi_K : G \longrightarrow G/K$
$H \subseteq \ker \pi_K = K$
Dal I th. di omomorfismo



π_K è surgettiva $\Longrightarrow$ φ è surgettiva e $\ker \varphi = \frac{\ker \pi_K}{H} = K/H$
Di nuovo, per il I th. di omomorfismo



cioè $\frac{G/H}{K/H} \cong G/K$ □

III teorema di omomorfismo

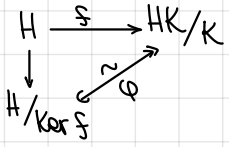
$H, K \triangleleft G$, allora
$\frac{H}{H \cap K} \cong \frac{HK}{K}$

DIMOSTRAZIONE

$f : H \longrightarrow HK/K$
$h \longmapsto hK$

- f è ben definita
- f è omo: $f(xy) = xyK = xKyK = f(x) f(y) \quad \forall x, y \in H$

Applico il I th. di omomorfismo a f:
da cui $\operatorname{Im} \varphi = \operatorname{Im} f$



$\ker f = \{x \in H \mid xK = K\} = \{x \in H \mid x \in K\} = H \cap K$
$\operatorname{Im} f = \{xK \mid x \in H\} = \{xyK \mid x \in H, y \in K\} = HK/K$
Quindi $\frac{H}{H \cap K} \cong \frac{HK}{K}$ □

Teorema di corrispondenza

G gruppo, $N \lhd G$, $\pi_N : G \longrightarrow G/N$
π_N induce una corrispondenza biunivoca tra i sottogruppi di G che contengono N e i sottogruppi di G/N. Questa corrispondenza conserva la normalità e l'indice di sottogruppo.

DIMOSTRAZIONE

(1) Sia $X = \{H < G \mid N \subset H\}$ e $Y = \{\mathcal{H} < G/N\}$

$$X \longrightarrow Y$$
$$H \xmapsto{\alpha} \pi_N(H)$$
$$\pi_N^{-1}(\mathcal{H}) \xmapsto{\beta} \mathcal{H}$$

- α è ben definita: $N \subseteq H < G \qquad \pi_N(H) = H/N < G/N$
  π_N manda sottogruppi in sottogruppi
- β è ben definita: $\beta(\mathcal{H}) = \pi_N^{-1}(\mathcal{H}) < G$ perché controimmagine di un sgr via omomorfismo
  $N = \pi_N^{-1}(\bar{e}) \subset \pi_N^{-1}(\mathcal{H})$
- $\alpha \circ \beta(\mathcal{H}) = \alpha \pi_N^{-1}(\mathcal{H}) = \pi_N \pi_N^{-1}(\mathcal{H}) = \mathcal{H}$ (π_N è surgettiva)
- $\beta \circ \alpha(H) = \pi_N^{-1} \pi_N(H) = \pi_N^{-1}(H/N) = \{x \in G \mid \pi_N(x) = xN \in H/N\} = \{x \in G \mid x \in H/N\} =$
  $= \{x \in G \mid xN = hN \text{ per qualche } h \in N\} = \{x \in G \mid x \in HN = H\} = H$

(2) $N \subseteq H < G$: $H \lhd G \iff \alpha(H) = \pi_N(H) = H/N \lhd G/N$

($\Longrightarrow$) ok perché π_N è surgettiva

($\Longleftarrow$) ok perché la controimmagine mediante omomorfismo di un sgp normale è un sgp normale

(3) $H \in X \quad [G : H] = [G/N : \alpha(H) = H/N]$

Se $H \lhd G$, segue dal II teorema di omomorfismo

$[G : H] = \#\{xH \mid x \in G\} \qquad [G/N : H/N] = \#\{\bar{x} H/N \mid \bar{x} \in G/N\}$

$$xH \xmapsto{T} \bar{x} H/N$$

- T è ben definita: $xH = yH \Rightarrow \bar{x} H/N = \bar{y} H/N$
  $y = xh, h \in H \qquad yN H/N = \bar{y} H/N = \overline{xh} H/N = \bar{x} H/N$
  $\bar{x} H/N \overset{=}{\bar{h}} H/N$
- T è iniettiva: $\bar{x} H/N = \bar{y} H/N \Rightarrow \bar{x} \in \bar{y} H/N \Rightarrow \bar{x} = \bar{y}\bar{h} \Rightarrow xN = yhN$
  $\Rightarrow x \in yhN \Rightarrow x = yhn$ ($hn \in H$) $h \in H, n \in N \Rightarrow x \in yH \Rightarrow xH = yH$
- T è surgettiva: $\forall \bar{x} = xN \in G/N \qquad T(xH) = \bar{x} H/N$

□

esempio $\mathbb{Z}$ ha sottogruppi $\{n\mathbb{Z}\}_{n \in \mathbb{N}}$

$m\mathbb{Z} \subset n\mathbb{Z} \iff n \mid m$

$$\mathbb{Z} \xrightarrow{\pi_n} \mathbb{Z}/n\mathbb{Z}$$

$X = \{d\mathbb{Z} \mid d\mathbb{Z} \supset n\mathbb{Z}\} = \{d\mathbb{Z} \mid d \mid n\}$

$\mathbb{Z}/n\mathbb{Z}$ ha un unico sottogruppo di ordine d $\forall d \mid n, d > 0$

se $d \mid n$, $d\mathbb{Z} \supset n\mathbb{Z}$: $d\mathbb{Z}/n\mathbb{Z}$ è il sgr di ordine n/d

Automorfismi

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

esempio $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$

DIMOSTRAZIONE

$F: \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathbb{Z}/n\mathbb{Z}^*$

$f \longmapsto f(\bar{1})$

F è ben definita: $f(\bar{1}) \in \mathbb{Z}/n\mathbb{Z}^*$

$f: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$\bar{1} \longmapsto \bar{a}$

f è iniettivo $\iff \mathrm{ord}\,\bar{a} = \mathrm{ord}\,\bar{1} = n \iff a \in \mathbb{Z}/n\mathbb{Z}^*$

F è iniettiva: se $f \neq g \Rightarrow F(f) \neq F(g)$ cioè $f(\bar{1}) \neq g(\bar{1})$

Se fosse $f(\bar{1}) = g(\bar{1})$ allora $f(\bar{x}) = xf(\bar{1}) = xg(\bar{1}) = g(\bar{x})\ \forall x \in \mathbb{Z}/n\mathbb{Z}$ ↯

F è surgettiva: $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}^*\ \exists f \in \mathrm{Aut}(G)$ t.c. $F(f) = \bar{a}$ cioè $f(\bar{1}) = \bar{a}$

Se definisco f estendendo $f(\bar{1}) = \bar{a}$, cioè $f(\bar{x}) = xf(\bar{1})$, ottengo un automorfismo □

esempio $\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$

DIMOSTRAZIONE

$f: \mathbb{Z} \longrightarrow \mathbb{Z}$

$1 \longmapsto a$

$n \longmapsto \underbrace{(a+\dots+a)}_{|n| \text{ volte}} \cdot \mathrm{sgn}(n)$

$f(n+m) = f(n) + f(m)$

$\ker f = \{b \mid ab = 0\} \begin{cases} \{0\} & \text{se } a \neq 0 \\ \mathbb{Z} & \text{se } a = 0 \end{cases}$

f è surgettivo $\iff 1 \in \mathrm{Im}\, f = \langle a \rangle$

cioè $1 = na$ ha soluzione $\iff a = \pm 1$

esempio $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$

$G = (\mathbb{Z}/p\mathbb{Z})^n$ è automaticamente un $\mathbb{F}_p$-spazio vettoriale di dimensione n con prodotto per scalare $v \in (\mathbb{Z}/p\mathbb{Z})^n$ $\bar{\lambda} \in \mathbb{Z}/p\mathbb{Z}$ $\bar{\lambda} \cdot v = \underbrace{v + v + \dots + v}_{\lambda \text{ volte}}$

$\varphi: G \longrightarrow G$ omomorfismo di gruppi $\iff$ applicazione lineare

$\mathrm{Aut}(G) = \{\text{applicazioni lineari invertibili } G \to G\} =$

$= \{(\varphi(e_1), \dots, \varphi(e_n)) \text{ dove } \varphi(e_1), \dots, \varphi(e_n) \text{ sono lin. ind. su } \mathbb{F}_p\}$

Consideriamo la matrice M di tale φ, rispetto alle basi canoniche

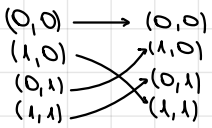
$$M = \left(\begin{array}{c|c|c|c|c} v_1 & v_2 & v_3 & \dots & v_n \end{array}\right)$$

$v_1 \neq 0$	$p^n - 1$
$v_2 \in \mathbb{F}_p^n \setminus \mathrm{Span}(v_1)$	$p^n - p$
$v_3 \in \mathbb{F}_p^n \setminus \mathrm{Span}(v_1, v_2)$	$p^n - p^2$
$\vdots$	
$v_n \in \mathbb{F}_p^n \setminus \mathrm{Span}(v_1, \dots, v_{n-1})$	$p^n - p^{n-1}$

$\Rightarrow \#\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

$\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = GL_n(\mathbb{F}_p)$

esempio $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong S_3 \cong GL_2(\mathbb{F}_2)$



Automorfismi interni

Def. Dato G gruppo e $g \in G$, si definisce il **coniugio**

$$\varphi_g : G \longrightarrow G$$
$$x \longmapsto gxg^{-1} \quad \text{coniugato di } x$$

Proposizione (1) $\forall g \in G \quad \varphi_g \in \mathrm{Aut}(G)$
(2) $\mathrm{Inn}(G) = \{\varphi_g \mid g \in G\} \trianglelefteq \mathrm{Aut}\, G$
(gruppo degli automorfismi interni)

DIMOSTRAZIONE

(1) $\varphi_g : G \longrightarrow G$
$x \longmapsto gxg^{-1} \in G$

φ_g è un omomorfismo

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

φ_g è iniettivo:
$\ker \varphi_g = \{x \in G \mid gxg^{-1} = e\}$ cioè $gx = g$ quindi $x = e$

φ_g è surgettivo:
$y \in G \ \exists x \in G$ t.c. $\varphi_g(x) = gxg^{-1} = y$ cioè $x = g^{-1}yg$

(2) Da (1) $\mathrm{Inn}\, G \subseteq \mathrm{Aut}\, G$

$\mathrm{Inn}\, G$ è un gruppo:

- $\varphi_e = id \in \mathrm{Inn}\, G$
- $\varphi_g \in \mathrm{Inn}\, G \Rightarrow (\varphi_g)^{-1} = \varphi_{g^{-1}}$
  $(\varphi_g)^{-1}(gxg^{-1}) = x = \varphi_{g^{-1}}(gxg^{-1})$
- $\varphi_g \circ \varphi_h = \varphi_{gh} \in \mathrm{Inn}\, G$
  $\varphi_g \circ \varphi_h(x) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}$

$\mathrm{Inn}\, G$ è normale: $\forall f \in \mathrm{Aut}\, G \ \forall \varphi_g \in \mathrm{Inn}\, G \quad f\varphi_g f^{-1} \in \mathrm{Inn}\, G$

$$f\varphi_g f^{-1}(x) = f(gf^{-1}(x)g^{-1}) = f(g) \times f(g^{-1}) = f(g) \times (f(g))^{-1} = \varphi_{f(g)} \in \mathrm{Inn}\, G \quad \square$$

<u>OSS</u> $H \trianglelefteq G \iff H$ è invariante per automorfismi interni
$\forall \varphi_g \quad \varphi_g H \subseteq H$

Def. $H < G$ si dice **caratteristico** se H è invariante per automorfismi
cioè se $\forall f \in \mathrm{Aut}\, G \Rightarrow f(H) \subset H$

<u>OSS</u> H caratteristico $\Rightarrow H$ normale

Se H è l'unico sottogruppo di un certo ordine in G,
allora $f(H) = H \ \forall f \in \mathrm{Aut}\, G$ (perché $|f(H)| = |H|$)

<u>esempio</u> in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \{0\}$ non è caratteristico

proposizione $\operatorname{Inn} G \cong G/Z(G)$

DIMOSTRAZIONE

$\Phi: G \longrightarrow \operatorname{Inn} G$

$g \longmapsto \varphi_g$

Φ è omomorfismo

$\Phi(gh) = \varphi_{gh} = \varphi_g \circ \varphi_h = \Phi(g) \circ \Phi(h)$

Φ è surgettivo per definizione

$\ker \Phi = \{g \mid \varphi_g = id_G\} = \{g \mid gx = xg\} = Z(G)$

cioè $\varphi_g(x) = gxg^{-1} = x \quad \forall x \in G$

Per il I teorema di omomorfismo

$\operatorname{Inn} G \cong G/Z(G)$ □

<u>Oss</u> $G/Z(G)$ ciclico $\Rightarrow$ G abeliano

DIMOSTRAZIONE

Sia $G/Z(G) = \langle gZ(G) \rangle$. Dati $g_1, g_2 \in G$, si ha:

$g_1 Z(G) = g^{k_1} Z(G)$ e $g_2 Z(G) = g^{k_2} Z(G)$ per certi $k_1, k_2 \in \mathbb{Z}$, da cui

$g^{-k_1} g_1 Z(G) = Z(G) \iff g^{-k_1} g_1 \in Z(G)$, cioè

$\exists z_1 \in Z(G) \cdot g_1 = g^{k_1} z_1$ e analogamente $g_2 = g^{k_2} z_2$

Ora $g_1 g_2 = g^{k_1} z_1 g^{k_2} z_2 = g^{k_1} g^{k_2} z_1 z_2 = g^{k_1+k_2} z_1 z_2 = g^{k_2+k_1} z_2 z_1 =$

$= g^{k_2} g^{k_1} z_2 z_1 = g^{k_2} z_2 g^{k_1} z_1 = g_2 g_1$, cioè G è abeliano □

<u>Oss</u> Se $G/Z(G)$ ciclico $\Rightarrow$ G abeliano $\Rightarrow$ $G/Z(G) = \{\bar{e}\}$

$\operatorname{Inn} G$ ciclico $\Rightarrow$ G abeliano $\Rightarrow$ $\operatorname{Inn} G = \{id\}$

<u>esempio</u> $\operatorname{Aut}(S_3) \cong S_3$

DIMOSTRAZIONE

$\operatorname{Inn} S_3 \cong S_3/Z(S_3) \cong S_3$ (↑)

$Z(S_3)$ è banale: se fosse $|Z(S_3)| = 6$ allora $Z(S_3) = S_3$ ma S_3 non è abeliano;

se fosse $|Z(S_3)| = 2$ o 3 allora $|S_3/Z(S_3)| = 3$ o 2 quindi è ciclico, cioè

S_3 è abeliano ↯ $\Rightarrow |Z(S_3)| = 1 \Rightarrow Z(S_3) = \{id\}$

$S_3 \cong \operatorname{Inn} S_3 \trianglelefteq \operatorname{Aut} S_3$

<u>Claim</u> $|\operatorname{Aut} S_3| \leq 6 \Rightarrow \operatorname{Aut} S_3 \cong S_3$

- S_3 è generato dai 2-cicli τ_1, τ_2, τ_3
- gli automorfismi conservano gli ordini degli elementi

$\forall f \in \operatorname{Aut} S_3 \quad f(\tau_i) = \tau_j \longrightarrow f$ permuta 3 di (al più 3! possibilità) □

sottogruppi caratteristici e automorfismi

Lemma Dato $G = H \times K$ con H, K finiti, se $(|H|, |K|) = 1$, allora $H \times \{1\}$ e $\{1\} \times K$ sono caratteristici in G.

DIMOSTRAZIONE

Sia $\varphi \in \mathrm{Aut}\, G$ e $g = (h, 1)$, da cui $\mathrm{ord}\, g = (\mathrm{ord}\, h, \mathrm{ord}\, 1) = \mathrm{ord}\, h$

Ora $\varphi(g) = (h_1, k_1)$

Poiché $\varphi \in \mathrm{Aut}\, G$ $\quad \mathrm{ord}\, \varphi(g) = (\mathrm{ord}\, h_1, \mathrm{ord}\, k_1) = \mathrm{ord}\, g = \mathrm{ord}\, h$

Quindi $\mathrm{ord}\, k_1 \mid \mathrm{ord}\, h \mid |H|$ e $\mathrm{ord}\, k_1 \mid |K|$, quindi $\mathrm{ord}\, k_1 = 1 \Rightarrow k_1 = 1$

Perciò $\varphi(H \times \{1\}) \subseteq H \times \{1\}$; l'uguaglianza segue per cardinalità.

Analogo per $\{1\} \times K$ □

proposizione Dati due gruppi finiti H, K, $\mathrm{Aut}(H \times K) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ se e solo se $H \times \{1\}$ e $\{1\} \times K$ sono caratteristici in $H \times K$

DIMOSTRAZIONE

$\Leftarrow$. preso $\varphi \in \mathrm{Aut}(H \times K)$, poiché $H \times \{1\}$ è caratteristico, ha senso considerare $\varphi_{|H \times \{1\}} : H \times \{1\} \xrightarrow{\cong H} H \times \{1\} \xrightarrow{\cong H}$, analogo per $\{1\} \times K$

Definiamo quindi

$$f : \mathrm{Aut}(H \times K) \longrightarrow \mathrm{Aut}(H) \times \mathrm{Aut}(K)$$
$$\varphi \longmapsto (\varphi_H, \varphi_K) \quad \text{dove} \quad \varphi_H(h) = \varphi_{|H \times \{1\}}(h, 1) \ \text{e} \ \varphi_K(k) = \varphi_{|\{1\} \times K}(1, k)$$

e al contrario

$$g : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \longrightarrow \mathrm{Aut}(H \times K)$$
$$(\varphi_H, \varphi_K) \longmapsto \varphi : H \times K \longrightarrow H \times K$$
$$(h, k) \longmapsto (\varphi_H(h), \varphi_K(k))$$

Si verifica che:

- $f \circ g = \mathrm{id}$ e $g \circ f = \mathrm{id}$
- f e g sono omomorfismi

$\Rightarrow$: Utilizzando l'isomorfismo g, $\varphi \in \mathrm{Aut}(H \times K)$ può essere scritto come $(\varphi_H, \varphi_K) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, quindi

$\varphi(H \times \{1\}) = (\varphi_H(H), \varphi_K(1)) = H \times \{1\}$ quindi $H \times \{1\}$ è caratteristico in $H \times K$. Analogo per $\{1\} \times K$. □

corollario Se $(m, n) = 1$, vale $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$, e quindi $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/mn\mathbb{Z})$, cioè $\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^* \cong \mathbb{Z}/mn\mathbb{Z}^*$

Azioni di gruppo su un insieme

Sia G gruppo, X insieme

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

$$\Phi : G \longrightarrow S(X)$$
$$g \longmapsto \varphi(g) \quad (= \varphi_g = g\cdot)$$

dove $\varphi_g : X \longrightarrow X$
$$x \longmapsto g\cdot x$$

esempio (1) Se $X = G$, il coniugio è un'azione di G su G

$$G \longrightarrow \operatorname{Inn} G < S(G)$$
$$g \longmapsto \varphi_g \text{ (coniugio)}$$

(2) V $\mathbb{K}$-sp.v.

$$\mathbb{K}^* \longrightarrow S(V)$$
$$\lambda \longmapsto \varphi_\lambda : v \longmapsto \lambda v$$

Oss Φ azione di G su X definisce una relazione di equivalenza su X

$x \sim y \iff \exists g \in G \quad \varphi_g x = y$

- riflessiva: $x \sim x$ $\quad \varphi_e(x) = x$
- simmetrica: $x \sim y$ $\quad \varphi_g(x) = y$ $\quad g \in G$
  $y \sim x$ $\quad \varphi_{g^{-1}}(y) = x$
- transitiva: $x \sim y$ $\quad y \sim z \Longrightarrow x \sim z$

Def. $\operatorname{orb}_G(x) = [x] = \{y \in X \mid x \sim y\}$ classe di equivalenza

Vale quindi: $X = \bigcup_{x \in R} \operatorname{orb}(x)$

esempio (1) $X = G$ $\quad \operatorname{orb}(x) = \{gxg^{-1} \mid x \in G\}$ = Classe di coniugio di x

(2) $X = V$, $G = \mathbb{K}^*$

$$\operatorname{orb}(v) = \{\varphi_\lambda(v) \mid \lambda \in \mathbb{K}^*\} = \{\lambda v \mid \lambda \in \mathbb{K}^*\} = \begin{cases} \langle v \rangle \setminus \{0\} & \text{se } v \neq 0 \\ \{0\} & \text{se } v = 0 \end{cases}$$

Def. $\operatorname{St}(x) = \{g \in G \mid \varphi_g(x) = x\}$

Oss $\operatorname{St}(x) \leq G$

Infatti: $\cdot\ \varphi_e(x) = x \ \forall x \in X \Longrightarrow e \in \operatorname{St}(x)$

$\cdot$ se $g_1, g_2 \in \operatorname{St}(x) \Longrightarrow g_1 g_2 \in \operatorname{St}(x)$, infatti

$$\varphi_{g_1 g_2}(x) \overset{\varphi \text{ omomorfismo}}{=} \varphi_{g_1} \circ \varphi_{g_2}(x) = \varphi_{g_1}(x) = x \Longrightarrow g_1 g_2 \in \operatorname{St}(x)$$

$\cdot$ se $g \in \operatorname{St}(x) \longrightarrow g^{-1} \in \operatorname{St}(x)$, infatti

$$\varphi_{g^{-1}}(x) = \varphi_{g^{-1}} \circ \varphi_g(x) = \varphi_{g^{-1}g}(x) = \varphi_e(x) = x$$

esempio (1) $\operatorname{St}(x) = \{g \in G \mid gxg^{-1} = x\} = Z_G(x)$

(2) $\operatorname{St}(0) = \mathbb{K}^*$ $\quad v \neq 0$ $\quad \operatorname{St}(v) = \{1\}$

Lemma orbita-stabilizzatore Se G è un gruppo finito, $\phi: G \to S(X)$ un'azione, allora $\forall x \in X \quad |G| = |orb(x)|\,|St(x)|$

DIMOSTRAZIONE

Vale $|G| = [G : St(x)] \cdot |St(x)|$

Basta dimostrare che $|orb(x)| = [G : St(x)]$

F: $orb(x) \longrightarrow$ classi laterali sx di $St(x)$

$y = \varphi_g(x) \longmapsto gSt(x)$

F è ben definita: $F(y)$ dipende da y e non da g

$y = \varphi_g(x) = \varphi_h(x) \implies gSt(x) = hSt(x)$

$\varphi_{h^{-1}g} = \varphi_{h^{-1}}\varphi_g(x) = x \implies h^{-1}g \in St(x) \implies gSt(x) = hSt(x)$

F è iniettiva: $gSt(x) = hSt(x) \implies \varphi_g(x) = \varphi_h(x)$

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

quindi $\varphi_h(x) = \varphi_h \circ \varphi_{h^{-1}} \circ \varphi_g(x)$

F è surgettiva: ovvio □

Abbiamo $X = \bigcup_{x \in R} orb(x)$, quindi, nel caso finito, $|X| = \sum_{x \in R} |orb(x)|$

Se considero l'azione di coniugio ($X = G$)

$G \longrightarrow S(G)$

$g \longmapsto \varphi_g : x \longmapsto gxg^{-1}$

con $St(x) = Z_G(x)$ e $orb(x) = C_x$ (classe di coniugio)

vale $|G| = |C_x|\,|Z_G(x)| \quad \forall x$

<u>Oss</u> $C_x = \{x\} \iff x \in Z(G) \iff Z_G(x) = G$

Quindi vale $|G| = \sum_{x \in R} |C_x|$

Nel caso di G gruppo finito, otteniamo la seguente formula

Formula delle classi $$|G| = \sum_{x \in R} \frac{|G|}{|Z_G(x)|} = \sum_{x \in Z(G)} 1 + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|} = |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

Applicazioni

(1) Il centro di un p-gruppo è non banale

DIMOSTRAZIONE

$|G| = p^k$, $k > 0$, p primo; $|Z(G)| = p^h$ con $0 \le h \le k$ (TS: $|Z(G)| \neq 1$)

$p^k = |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \rightsquigarrow p \mid \frac{|G|}{|Z_G(x)|}$ per $x \in R \setminus Z(G)$

$\implies p \mid \Sigma = pV$

Quindi $|Z(G)| = p^k - pV \implies p \mid |Z(G)|$ □

(2) Un gruppo di ordine p^2 è sempre abeliano ($G \cong \mathbb{Z}/p^2\mathbb{Z}$ oppure $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$)

DIMOSTRAZIONE

$$|Z(G)| = \begin{cases} 1 & \text{assurdo perché } G \text{ è un } p\text{-gruppo} \\ p & \text{no perché altrimenti } G/Z(G) \text{ ciclico} \implies G \text{ abeliano} \\ p^2 & \end{cases}$$

□

Azioni transitive

Def. G **agisce transitivamente** su X se esiste un'unica orbita, ossia se
$\forall x,y \in X \ \exists g \in G \quad g \cdot x = y$

Lemma Sia G un gruppo finito, $H < G$, allora
$\bigcup_{g \in G} gHg^{-1} \neq G$ a meno che $H = G$.

DIMOSTRAZIONE

Sto unendo $|G|$ insiemi, ma quanti sono distinti?

$xHx^{-1} = yHy^{-1} \iff y^{-1}xHx^{-1}y = H \iff y^{-1}xH(y^{-1}x)^{-1} = H$

$\iff y^{-1}x \in N_G(H) \iff x \in yN_G(H) \iff xN_G(H) = yN_G(H)$

Ogni insieme gHg^{-1} compare $|N_G(H)|$ volte

Per evitare ripetizioni, sia R un insieme di rappresentanti: $\bigcup_{g \in G} gHg^{-1} = \bigcup_{g \in R} gHg^{-1}$

Ora $|R| = |G| / |N_G(H)|$ e $|gHg^{-1}| = |H|$

Perciò $\left| \bigcup_{g \in R} gHg^{-1} \right| \leq \frac{|G|}{|N_G(H)|} \cdot |H| \leq |G|$

↑ c'è l'identità in ogni gHg^{-1}

C'è uguaglianza solo se:
- $|R| = 1 \Rightarrow N_G(H) = G \Rightarrow H \lhd G$
- $\left| \bigcup_{g \in G} gHg^{-1} \right| \leq \frac{|G|}{|G|} \cdot |H| \leq |H| \Rightarrow H = G$ □

Proposizione Sia G un gruppo finito che agisce transitivamente su X:
(i) $\forall x,y \in X \quad Stab(x) \cong Stab(y)$
(ii) $|X| \geq 2$: $\exists g \in G$ che agisce su X senza punti fissi

DIMOSTRAZIONE

(i) Per ipotesi, dati $x,y \in X$, $\exists g \in G$ t.c. $y = g \cdot x$

$Stab(y) = \{h \in G \mid h \cdot y = y\} = \{h \in G \mid h \cdot g \cdot x = g \cdot x\} = \{h \in G \mid g^{-1} \cdot h \cdot g \cdot x = x\} =$

$= \{h \in G \mid g^{-1}hg \in Stab(x)\} = \{h \in G \mid h \in gStab(x)g^{-1}\} = gStab(x)g^{-1}$

quindi $Stab(x)$, $Stab(y)$ sono coniugati (e perciò isomorfi).

(ii) g agisce senza punti fissi $\iff g \notin \bigcup_{x \in X} Stab(x)$

Fissando $x_0 \in X$, poiché l'azione è transitiva, equivale a $g \notin \bigcup_{h \in G} Stab(h \cdot x_0)$

$\iff g \notin \bigcup_{h \in G} hStab(x_0)h^{-1}$

Basta dire $\bigcup_{h \in G} hStab(x_0)h^{-1} \neq G$ per il lemma

Se $Stab(x_0)$ fosse G, $|Orb(x_0)| = \frac{|G|}{|Stab(x_0)|} = 1 = |X|$ ↯ □

Teorema di Cauchy Dato G gruppo finito
Se p è un primo t.c. $p \mid |G|$ allora
$\exists x \in G \quad \text{ord}(x) = p$

DIMOSTRAZIONE (1)

G abeliano $\quad |G| = pn$

Per induzione su n, cerco $y \in G$ con $p \mid \text{ord}(y)$ $\left(\text{ord}\, y^k = \frac{\text{ord}\, y}{(k, \text{ord}\, y)} \right)$

- $n = 1$ ovvio
- $x \in G$, $\langle x \rangle \trianglelefteq G$, $x \neq e$
  - $p \mid |\langle x \rangle| \longrightarrow$ una potenza di x ha ordine p
  - $p \nmid |\langle x \rangle| : |G/\langle x \rangle| = pm$ con $m < n$

  Per ipotesi induttiva $\exists \bar{y} = y\langle x \rangle$ con $\text{ord}\, \bar{y} = p$
  $y \in G$ t.c. $\pi(y) = \bar{y}$ dove $\pi : G \longrightarrow G/\langle x \rangle$
  Abbiamo $p = \text{ord}\, \bar{y} \mid \text{ord}\, y \Rightarrow$ una potenza di y ha ordine p

G qualsiasi $\quad |G| = pn$

Per induzione su n

- $n = 1$: ovvio
- Suppongo la tesi vera per gruppi di ordine pm con $1 \leq m < n$

  $\exists H \leq G \;\; p \mid |H| \Rightarrow |H| = pm$ con $m < n \longrightarrow$ per hp. ind $\exists x \in H$ ord $x = p$
  $\forall H \leq G \;\; (|H|, p) = 1$

  Formula delle classi: $pn = |G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$
  $p \nmid |Z_G(x)|$ perché è un sgr proprio $\forall x \in R \setminus Z(G)$
  Quindi $p \mid \frac{|G|}{|Z_G(x)|}$ $\forall x \in R \setminus Z(G)$

  $\Rightarrow p \mid |Z(G)|$ allora non è un sgr proprio $\Rightarrow G = Z(G)$
  $\Rightarrow G$ abeliano e vale il caso precedente $\square$

Oss Lagrange: se $H < G \Rightarrow |H| \mid |G|$
Il viceversa è falso: A_4 non ha sottogruppi di ordine 6

DIMOSTRAZIONE (2)

Sia $X = \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = e_G\}$, con $|X| = n^{p-1}$
C'è un'azione di $\mathbb{Z}/p\mathbb{Z}$ su X: l'elemento $i \in \mathbb{Z}/p\mathbb{Z}$ agisce mandando
$(g_1, \dots, g_p) \longmapsto (g_{i+1}, g_{i+2}, \dots, g_{i+p})$ (indici letti modulo p)
è un'azione: $X \ni (g_1, \dots, g_p) \xmapsto{1} (g_2, g_3, \dots, g_p, g_1) \in X$
$g_1(g_2 \cdots g_p) = e \longrightarrow (g_2 g_3 \cdots g_p) g_1 = e$

Consideriamo le orbite di questa azione
$|\text{Orb}(x)| = |\mathbb{Z}/p\mathbb{Z}| / |\text{Stab}(x)| = \{1, p\}$
Le orbite di lunghezza 1 corrispondono ad elementi $x = (x_1, x_2, \dots, x_p)$ con $x_1 = x_2 = \dots = x_p$ e $e = x_1 x_2 \cdots x_p = x_1^p$,
cioè sono $x = (g, g, \dots, g)$ con $g^p = e$ ovvero $\text{ord}(g) \in \{1, p\}$
Quindi c'è l'orbita di $(e, e, \dots, e)$ e poi le orbite corrispondenti agli elementi di ordine p

$|X| = \sum_{x \in R} |\text{Orb}(x)| = 1 + \#\{\text{elementi di ord } p\} + p \cdot \#\{\text{orbite di lunghezza } p\}$
$\Rightarrow |X| - 1 \equiv \#\{\text{elementi di ord } p\} \pmod p$
$-1 \equiv n^{p-1} - 1 \equiv \#\{\text{elementi di ord } p\} \pmod p$
$\Rightarrow \#\{\text{elementi di ord } p\} \neq 0$ (perché $0 \not\equiv -1 \pmod p$) $\square$

corollario (Piccolo teorema di Fermat) Dato p primo, se $p \nmid n$, allora
$$n^{p-1} \equiv 1 \pmod p$$

DIMOSTRAZIONE

$G = \mathbb{Z}/n\mathbb{Z}$ con $p \nmid n$

$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 + \dots + g_p = 0\}$

$\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ come prima, $|X| = n^{p-1}$

le orbite di lunghezza 1 è quella banale $(0,0,\dots,0)$

perché $p \cdot g \equiv 0 \ (n) \iff g \equiv 0 \ (n)$

$n^{p-1} = |X| = 1 + p \cdot \#\{\text{orbite di lunghezza } p\}$

$\Rightarrow n^{p-1} \equiv 1 \pmod p$ □

Teorema di cayley Ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni.
Se $|G| = n$, $G \hookrightarrow S_n$

DIMOSTRAZIONE

$\lambda: G \hookrightarrow S(G)$ (rappresentazione regolare sinistra)

$g \longmapsto \varphi_g : x \longmapsto gx$

Buona definizione di λ: $\lambda(g) = \varphi_g \in S(G)$?

$\varphi_g : x \longmapsto gx$: iniettiva $gx = gy \longrightarrow x = y$

suriettiva $y \in G \quad gx = y \longrightarrow x = g^{-1}y$

λ è omomorfismo : $\lambda(g_1 g_2) = \lambda(g_1) \circ \lambda(g_2)$

$\varphi_{g_1 g_2} \qquad \varphi_{g_1} \circ \varphi_{g_2}$

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

λ è iniettiva: $\ker \lambda = \{g \in G \mid \varphi_g = id\} = \{e\}$

perché $\varphi_g(e) = g \Rightarrow g = e$ □

Oss $G = \{x_1, \dots, x_n\}$ $g = x_i$ $\operatorname{ord} g = d \mid n$

$\varphi_g(x_1) = g x_1$

$(x_1, g x_1, g^2 x_1, \dots, g^{m-1} x_1)$ con $g^m x_1 = x_1 \longrightarrow g^m = id \longrightarrow m = d$

Quindi, in generale:

$|G| = n$ $\quad G \hookrightarrow S_n$

$\operatorname{ord} g = d$, $n = dk$ $\quad g \longrightarrow k$ d-cicli

esempio $\mathbb{Z}/6\mathbb{Z} \hookrightarrow S_6 = S(\{0,1,2,3,4,5\})$

$g = \bar{2}$, $\operatorname{ord} \bar{2} = 3$

$\bar{2} \longmapsto \varphi_{\bar{2}}$: $0 \mapsto 2$, $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 0$, $5 \mapsto 1$

$\bar{2} \longmapsto (0,2,4)(1,3,5)$ (2 3-cicli)

Oss $H \leq G$

$H \trianglelefteq G \iff H$ è unione di classi di coniugio di G

$\Updownarrow$

$\forall h \ ghg^{-1} \in H \ \forall g \in G \iff C_h \subseteq H \iff H = \bigcup_{h \in H} C_h$

esempio Se $H \leq G$ $\quad |G| = \sum_{x \in R} |C_x| = |Z(G)| + \sum_{x \in R \setminus Z(G)} |C_x|$

$$|H| = \sum_{h \in R \cap H} |C_h| = \sum_{h \in H \cap Z(G)} 1 + \sum_{h \in T} \frac{|G|}{|Z_G(h)|} = |H \cap Z(G)| + \sum_{h \in T} \frac{|G|}{|Z_G(h)|} \quad \text{dove } T = (R \setminus Z(G)) \cap H$$

esempio G, $X = \{\text{sottogruppi di } G\}$

$\varphi : G \longrightarrow S(X)$

$g \longmapsto \varphi_g : H \longrightarrow gHg^{-1}$

- $\varphi_g \in S(X)$ è biiettiva
- φ è omomorfismo: $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$

  $H \longmapsto g_1 g_2 H g_2^{-1} g_1^{-1} \quad H \longmapsto g_2 H g_2^{-1} \longmapsto g_1 g_2 H g_2^{-1} g_1^{-1}$
- $orb(H) = \{gHg^{-1} \mid g \in G\} = \{\text{coniugati di } H\}$

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

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

Quindi:

$|G| = |orb(H)| \, |N_G(H)|$

#coniugati di H in G $= [G : N_G(H)]$

proposizione Sia G gruppo finito, $N < G$ di indice p primo. Supponiamo che p sia il più piccolo primo che divide $\#G$. Allora $N \trianglelefteq G$

Oss Se $N < G$ ha indice 2, questo si applica e otteniamo un fatto già noto

DIMOSTRAZIONE

Cerco di costruire un omomorfismo di cui N sia il nucleo.

Considero l'azione di G sull'insieme G/N data da

$g \cdot (g'N) = gg'N$

Verifica: $(g_1 g_2) \cdot (g'N) = g_1 \cdot (g_2 \cdot g'N)$

$e \cdot g'N = g'N$

Questa azione è un omomorfismo $\quad \psi : G \longrightarrow Big(G/N)$

$g \longmapsto (g'N \longmapsto gg'N)$

$Big(G/N) \cong S_p$

$|G/N| = [G : N] = p$

$Im\,\psi < S_p \implies \#Im\,\psi \mid p!$

$\#Im\,\psi = \#G/_{Ker\,\psi} = \frac{\#G}{\#Ker\,\psi} \mid \#G = p^e (q_1^{e_1} \cdots q_k^{e_k}) \quad q_i > p$

$\implies Im\,\psi \mid (p!, \#G) = p$

Non può essere $\#Im\,\psi = 1$, perché se $g \notin G/N$, $g \cdot N \neq N$

Quindi $\#Im\,\psi = p$

$\implies Ker \trianglelefteq G$ di indice p

Cerchiamo un contenimento tra N e $Ker\,\psi$:

se $g \in Ker\,\psi$, $g \cdot N = N$ (la permutazione data da g è l'identità, e in particolare fissa N)

$\iff g \in N$

$\implies Ker\,\psi \subseteq N$, ma hanno la stessa cardinalità, quindi $Ker\,\psi = N$

□

Teorema di Poincaré Dato un gruppo finito G, se $H<G$ e $[G:H]=n$, allora esiste $N \trianglelefteq G$ tale che:
(1) $N < H < G$
(2) $n \mid [G:N] \mid n!$

DIMOSTRAZIONE
Consideriamo l'azione:
$$\psi: G \longrightarrow Big(G/H) \cong S_{|G/H|} = S_n$$
$$g \longmapsto \psi_g : g'H \longmapsto gg'H$$
Ora $\ker\psi \trianglelefteq G$
- $\ker\psi < H$, infatti: $g \in \ker\psi \iff \psi(g) = id \Rightarrow \psi(g)(H) = H \iff gH = H \iff g \in H$
- $[G:\ker\psi] = \#G/\ker\psi = \#\mathrm{Im}\,\psi \mid n! = |S_n|$
  $[G:\ker\psi] \mid \#G$ (n)
  Inoltre $\ker\psi \leq H \leq G$, quindi $n = [G:H] \mid [G:\ker\psi]$ □

esempio G di ordine $3 \cdot 5 \cdot 7$, H sottogruppo di ord 21
$\Rightarrow \exists N \trianglelefteq G$ $[G:N] \mid |G/H|! = 5!$
$[G:N] \mid |G| = 3 \cdot 5 \cdot 7$
$\Rightarrow [G:N] \in \{1, 3, 5, 15\}$

Lemma Dati $g_1, g_2 \in G$ con $\mathrm{ord}\,g_1 = m$, $\mathrm{ord}\,g_2 = n$, $(m,n)=1$ e $g_1g_2 = g_2g_1$
allora $\mathrm{ord}(g_1g_2) = \mathrm{mcm}(m,n) = mn$

DIMOSTRAZIONE
$(g_1g_2)^k = e$ $\qquad g_1g_2g_1g_2\cdots g_1g_2 = g_1^k g_2^k = e$
$\iff g_1^k = g_2^{-k} \in \langle g_1\rangle \cap \langle g_2\rangle = \{e\}$
$\iff g_1^k = e = g_2^k \iff m \mid k$ e $n \mid k \iff mn \mid k$
Quindi $\mathrm{ord}(g_1g_2) = mn$ □

esempio **Gruppi di ordine 15**
Sia G t.c. $|G| = 15$, allora G è ciclico
DIMOSTRAZIONE
$\exists g \in G$ $\mathrm{ord}(g) = 5$ per Cauchy
$N = \langle g\rangle$, $|N| = 5$ e $[G:N] = 3$ che è il più piccolo primo che divide 15 $\Rightarrow N \trianglelefteq G$
Definisco $\Phi: \mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(N)$ (ha senso perché $N \trianglelefteq G$)
$$\varphi_x \longmapsto \varphi_{x|N}$$
$N \subseteq Z(G) \iff \mathrm{Im}\,\Phi = \{id\}$
$\mathrm{Inn}(G) \cong G/Z(G)$ è un gruppo di ordine $|15$
$\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}^* \cong \mathbb{Z}/4\mathbb{Z}$
$\Rightarrow \#\mathrm{Im}\,\Phi \mid (\#\mathrm{Aut}\,N, \#\mathrm{Im}\,G) \mid (4, 15) = 1$
$\Rightarrow \mathrm{Im}\,\Phi = \{id\} \Rightarrow N \subseteq Z(G)$
$|G/Z(G)| \in \{1, 3\} \Rightarrow G/Z(G)$ ciclico $\Rightarrow G$ abeliano
Qui si applica il lemma con g_1 el. di ord. 5 e g_2 di ord. 3
$\Rightarrow |\langle g_1g_2\rangle| = 15 \Rightarrow G = \langle g_1g_2\rangle$

Gruppo derivato

Def. Dato un gruppo G e $x,y \in G$, il commutatore di x e y è $[x,y] = xyx^{-1}y^{-1}$.
Si chiama **sottogruppo derivato di G** (o sottogruppo dei commutatori) il sottogruppo:

$$G' = \langle \{[x,y] \mid x,y \in G\} \rangle < G$$

Lemma $S \subseteq G$ caratteristico $\Rightarrow \langle S \rangle$ è caratteristico

DIMOSTRAZIONE
Dato $\varphi \in \mathrm{Aut}\, G$, $\varphi(\langle S \rangle) = \langle \varphi(S) \rangle = \langle S \rangle$ □

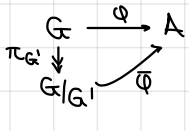
proposizione Dato G gruppo, valgono:
(1) G' è caratteristico in G
(2) G/G' è abeliano
(3) dato A abeliano e $\varphi \in \mathrm{Hom}(G,A)$, allora $G' \subseteq \ker\varphi$

DIMOSTRAZIONE
(1) Sia $\varphi \in \mathrm{Aut}(G)$, basta mostrare φ manda i generatori di G' in G'.
$\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x),\varphi(y)^{-1}] \in G'$
Inoltre $[x,y] = \varphi([\varphi^{-1}(x),\varphi^{-1}(y)])$
(2) dati $x,y \in G$, $xG' \cdot yG' = yG' \cdot xG' \iff xyG' = yxG'$, che equivale a $xyx^{-1}y^{-1} \in G'$, cioè $[x,y] \in G'$
(3) Dato $\varphi \in \mathrm{Hom}(G,A)$, $\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = e_A$
$\Rightarrow G' \subseteq \ker\varphi$ □

Oss Per il I teorema di omomorfismo, G/G' è il "più grande" quoziente abeliano di G, ossia G' è il "più piccolo" sottogruppo di G che produce un quoziente abeliano. In questo senso, G' misura quanto è abeliano il gruppo G.

corollario Dato A gruppo abeliano, si ha
$$\mathrm{Hom}(G,A) \longleftrightarrow \mathrm{Hom}(G/G',A)$$

DIMOSTRAZIONE
$\mathrm{Hom}(G,A) \longleftrightarrow \mathrm{Hom}(G/G',A)$
dato $\varphi : G \to A$, per (3) $G' \subseteq \ker\varphi$, quindi
per il I teorema di omomorfismo
$\exists!\ \overline{\varphi} : G/G' \to A$ che fa commutare il diagramma



data $\overline{\varphi} \in \mathrm{Hom}(G/G',A)$, si ha $\overline{\varphi} \circ \pi_{G'} \in \mathrm{Hom}(G,A)$ □

proposizione $|G| = 2d$ con d dispari $\Rightarrow \exists$ un sottogruppo di ordine d

DIMOSTRAZIONE

Consideriamo l'immersione di Cayley $\Phi : G \hookrightarrow S_{2d}$

Voglio costruire $H = \Phi^{-1}(A_{2d})$

$[G : \Phi^{-1}(A_{2d})] \leq 2$

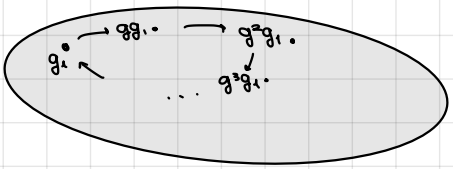
$\Phi(G) \cap A_{2d} = \begin{cases} \Phi(G) & \text{se } \Phi(G) \subseteq A_{2d} \\ \text{un sgp di indice 2 di } \Phi(G) & \end{cases}$

$\frac{\Phi(G)}{\Phi(G) \cap A_{2d}} = \frac{K}{K \cap A_{2d}}$ $\quad sgn : K \longrightarrow \{\pm 1\}$

$= \frac{K}{\ker(sgn|_K)} \cong Im(sgn|_K) = \begin{cases} \{1\} \\ \{\pm 1\} \end{cases}$

Dobbiamo escludere $\Phi(G) \cap A_{2d} = \Phi(G)$, cioè $\Phi(G) \subseteq A_{2d}$

OSS



Gli elementi del ciclo di g_1 sono

$g^0 g_1, gg_1, g^2g_1, \dots, g^{ord(g)-1}g_1$

$\Rightarrow$ tutti i cicli hanno lunghezza $ord(g)$

Come trovo una permutazione dispari in $\Phi(G)$?

Se g ha ordine k, $\Phi(g) = \underbrace{(k\text{-ciclo}) \cdots (k\text{-ciclo})}_{|G|/k}$

$sgn(\Phi(g)) = \begin{cases} 1 \text{ se } k \text{ è dispari} \\ (-1)^{\frac{2d}{k}} = -1 \text{ se } k \text{ è pari} \end{cases}$

Basta prendere $g \in G$ $ord(g) = 2$ (Cauchy) $\square$

proposizione Dato G gruppo e $H \leq G$ t.c. $[G:H] = 2$, se $K < G$ allora $[K : H \cap K] \in \{1, 2\}$

DIMOSTRAZIONE

- se $K \subseteq H$, allora $H \cap K = K$ e $[K : H \cap K] = 1$
- se $K \not\subseteq H$, considero $\pi_H : G \longrightarrow G/H \cong \mathbb{Z}/2\mathbb{Z}$
  $g \longmapsto gH$

quindi $\pi_H(K) = G/H$, e inoltre $\ker \pi_{H|K} = \ker \pi_H \cap K = H \cap K$

Quindi, per il I teo. di omo.

$K/K \cap H \cong G/H \cong \mathbb{Z}/2\mathbb{Z} \Longrightarrow [K : K \cap H] = 2$ $\square$

Prodotto diretto

Lemma $H, K \trianglelefteq G$, $H \cap K = \{e\}$
allora $hk = kh \quad \forall h \in H, k \in K$

DIMOSTRAZIONE

$$hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})}_{\in K}\underbrace{k^{-1}}_{\in K} \in K$$

$$= \underbrace{h}_{\in H}\underbrace{(kh^{-1}k^{-1})}_{\in H} \in H$$

$$\Rightarrow hkh^{-1}k^{-1} \in H \cap K = \{e\} \Rightarrow hkh^{-1}k^{-1} = e \quad \square$$

Teorema G gruppo, $H, K \leq G$
(1) $H \cap K = \{e\}$
(2) $HK = G$
Allora $G \cong HK$

Oss $G = G_1 \times G_2 \qquad H = G_1 \times \{e_2\}$
$H, K \leq G \qquad K = \{e_1\} \times G_2$
$HK = \{(x, e_2)(e_1, y) = (x, y) \mid x \in G_1, y \in G_2\} = KH$

DIMOSTRAZIONE

$$f : H \times K \longrightarrow G$$
$$(h, k) \longmapsto hk$$

Claim : f è isomorfismo

- f è omo : $f((h_1,k_1)(h_2,k_2)) = f((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 \overset{\text{lemma}}{=} h_1k_1h_2k_2 = f((h_1,k_1))\, f((h_2,k_2))$
- f è surgettiva per (2)
- f è iniettiva : $\ker f = \{(h,k) \in HK \mid f(h,k) = hk = e\} = \{(e,e)\}$
  $h = k^{-1} \in H \cap K \Rightarrow h = e, k = e$ $\square$

esempio Un gruppo di ordine p^2 è isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ oppure a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

DIMOSTRAZIONE

$|G| = p^2 \Rightarrow G$ abeliano

G < ciclico : $G \cong \mathbb{Z}/p^2\mathbb{Z}$
non ciclico : tutti gli elementi $\neq e$ hanno ordine p

$x \in G \setminus \{e\} : |\langle x \rangle| = p$
$y \in G \setminus \langle x \rangle : |\langle y \rangle| = p$
$\langle x \rangle = H, \langle y \rangle = K$
$G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
$\langle x \rangle \cap \langle y \rangle = \{e\}$
$|\langle x \rangle \langle y \rangle| = \frac{|\langle x \rangle|\,|\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = p^2 \Rightarrow HK = p^2$ $\square$

Prodotto semidiretto

Def Dati H, K gruppi, $\varphi : K \longrightarrow Aut(H)$ omomorfismo (K agisce su H per automorfismi)
si dice **prodotto semidiretto** di H e K via φ, $H \rtimes_\varphi K$,
l'insieme prodotto cartesiano $H \times K$ con l'operazione definita da

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

Proposizione $H \rtimes_\varphi K$ è un gruppo

DIMOSTRAZIONE

(e_H, e_K) è l'identità

$$(h,k)(h',k') = (\underbrace{h\varphi_k(h')}_{\in H},\ \underbrace{kk'}_{\in K})$$

$$(h,k)^{-1} = (\varphi_{k^{-1}}(h^{-1}),\ k^{-1})$$

...

Oss $H \rtimes_\varphi K = H \times K \iff \varphi$ è l'omomorfismo banale ($\varphi_k = id_H\ \ \forall k \in K$)

Oss $H \times \{e_K\},\ \{e_H\} \times K < H \rtimes_\varphi K$

$$(h,e_K)(h',e_K) = (h\,\varphi_{e_K}(h'),\ e_K) = (hh',\ e_K)$$

$H \times \{e_K\} \triangleleft H \rtimes_\varphi K$

$H \rtimes_\varphi K \longrightarrow K$

$(h,k) \longmapsto k$ è un omomorfismo con nucleo $H \times \{e_K\}$

Abbiamo trovato che in $H \rtimes_\varphi K = G$

$H \times \{e_K\} \triangleleft G$, $\{e_H\} \times K < G$ e $(H \times \{e_K\}) \cap (\{e_H\} \times K) = (e_K, e_H)$

Teorema Dato G gruppo con $H \triangleleft G$, $K < G$ tali che

(1) $G = HK$

(2) $H \cap K = \{e\}$

allora $G \cong H \rtimes_\varphi K$ dove

$\varphi : K \longrightarrow Aut(H)$ con $\varphi_k(h) = khk^{-1}\ \ \forall h \in H, \forall k \in K$

DIMOSTRAZIONE

$F : H \rtimes_\varphi K \longrightarrow G$

$(h,k) \longmapsto hk$

$$F((h,k)(h',k')) = F((h\varphi_k(h'), kk')) = h\varphi_k(h')kk' = hkh'k^{-1}kk' = hkh'k' = F((h,k))\,F((h',k'))$$

F è surgettiva perché $HK = G$

F è iniettiva perché $H \cap K = \{e\}$

$\ker F = \{(h,k) \mid hk = e\}$ cioè $h = k^{-1} \in H \cap K$

□

esempio $S_n \cong A_n \rtimes_\varphi \langle (1,2) \rangle$

- $A_n \trianglelefteq S_n$, $\langle (1,2) \rangle < S_n$
- $S_n = A_n \langle (1,2) \rangle$
- $A_n \cap \langle (1,2) \rangle = \{id\}$

Per il teorema, $\varphi : \langle (1,2) \rangle \longrightarrow A_n$

$$(1,2) \longmapsto \varphi_{(1,2)} : \sigma \longmapsto (1,2)\sigma(1,2)$$

esempio $D_n \cong \langle r \rangle \rtimes_{\varphi_s} \langle s \rangle \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$

- $\langle r \rangle \trianglelefteq D_n$, $\langle s \rangle < D_n$
- $D_n = \langle r \rangle \langle s \rangle$
- $\langle r \rangle \cap \langle s \rangle = \{id\}$

$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$

$\overline{1} \longmapsto \varphi_{\overline{1}} : [1]_n \longmapsto [-1]_n$

$n = p_1^{e_1} \cdots p_r^{e_r}$ $\quad \mathbb{Z}/n\mathbb{Z}^* \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}^* \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}^*$

per $p \neq 2$ $\quad \mathbb{Z}/p^e\mathbb{Z}^* \cong \mathbb{Z}/\phi(p^e)\mathbb{Z}$

esempio In D_n, $s^a r^b \cdot s^c r^d = s^{a+c} r^{(-1)^c b + d}$

$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

Cerchiamo un sottogruppo $N \trianglelefteq D_n$ e $H < D_n$ t.c. $N \cap H = \{e\}$ e $NH = D_n$

$N = R \trianglelefteq D_n$ e $H = \langle s \rangle$:

$R \cap \langle s \rangle = \{e\}$, $\langle s \rangle R = D_n$

$\Rightarrow D_n \cong R \rtimes_\varphi \langle s \rangle \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$

φ: coniugio $\qquad \psi : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/n\mathbb{Z})$

La φ è l'azione di coniugio

$$H \longrightarrow Aut(N)$$

$$x \longmapsto \varphi_{x|_N} : n \longmapsto xnx^{-1}$$

$$\langle s \rangle \longrightarrow Aut(R) \cong \mathbb{Z}/n\mathbb{Z}^* \qquad \varphi_s(r) = srs^{-1} = r^{-1}$$

$$s \longmapsto (r \longmapsto r^{-1}) \longleftrightarrow (-1)$$

Partendo da $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z}$, posso prendere

$$\psi : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$$

$$1 \longmapsto (x \longmapsto -x) \longleftrightarrow (-1)$$

$G = \mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$

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

$\psi(a)$ = moltiplicazione per $(-1)^a$

equivale a $s^a r^b \cdot s^c r^d = s^{a+c} r^{(-1)^c b + d}$

proposizione H, K gruppi, $\varphi: K \to Aut(H)$, $\psi: K \to Aut(H)$ omomorfismi
Se esistono $\alpha \in Aut(H)$, $\beta \in Aut(K)$ tali che
$$\alpha \circ \varphi_k \circ \alpha^{-1} = \psi_{\beta(k)} \quad \forall k \in K$$
allora $H \times_\varphi K \cong H \times_\psi K$

DIMOSTRAZIONE

$F: H \times_\varphi K \longrightarrow H \times_\psi K$
$(h,k) \longmapsto (\alpha(h), \beta(k))$

$F((h,k)(h',k')) = F(h\varphi_k(h'), kk')) = (\alpha(h\varphi_k(h')), \beta(kk')) =$
$= (\alpha(h)\,\alpha(\varphi_k(h')), \beta(k)\beta(k')) = (\alpha(h)\psi_{\beta(k)}(\alpha(h')), \beta(k)\beta(k')) =$
$= (\alpha(h), \beta(k))(\alpha(h'), \beta(k')) = F((h,k))F((h',k'))$

iniettività e surgettività seguono □

Classificazione dei gruppi di ordine pq

Siano p, q primi con $q > p$

Se $p \nmid q-1$ esisiste un unico gruppo di ordine pq, che è quindi isomorfo a $\mathbb{Z}/pq\mathbb{Z}$

Se $p \mid q-1$ esistono, a meno di isomorfismo, due gruppi di ordine pq:
$\mathbb{Z}/pq\mathbb{Z}$ e $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$

DIMOSTRAZIONE

$|G| = pq$

Per Cauchy, $\exists x \in G$ ord $x = q$, $\exists y \in G$ ord $y = p$

$H = \langle x \rangle \cong \mathbb{Z}/q\mathbb{Z}$ e $K = \langle y \rangle \cong \mathbb{Z}/p\mathbb{Z}$

$H \triangleleft G$ perché ha indice il più piccolo primo

$G = HK$

$H \cap K = \{e\}$ per questioni di ordine

$\Rightarrow G \cong \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z}$ dove $\varphi: \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$

$\varphi_a: [1]_p \longmapsto [a]_{q-1}$

dove ord $[a]_{q-1} = \begin{cases} 1 \longrightarrow \text{prodotto diretto} \\ p \text{ che esiste solo se } p \mid q-1 \text{ e in tal caso ne ho } \phi(p) = p-1 \end{cases}$

Se $p \mid q-1$, gli elementi di ordine p di $\mathbb{Z}/(q-1)\mathbb{Z}$ sono
$px \equiv 0 \ (q-1) \longrightarrow x \equiv 0 \ \left(\frac{q-1}{p}\right)$
cioè $x = k\left[\frac{q-1}{p}\right]$ per $k = 1, \dots, p-1$

Dico che tutte queste φ danno gruppi isomorfi

$\varphi_\ell: \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$
$[1]_p \longmapsto \ell\left[\frac{q-1}{p}\right]_{q-1} \qquad \ell = 1, \dots, p-1$

$\mathbb{Z}/q\mathbb{Z} \times_{\varphi_1} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \times_{\varphi_\ell} \mathbb{Z}/p\mathbb{Z}$

$\alpha([1]_q) = [1]_q$
$\beta([1]_p) = [\ell]_p$

Basta verificare la formula con $k = [1]_p$

$\alpha\varphi_{[1]}\alpha^{-1} = \psi_{\beta[1]} = \psi_{[\ell]_p}$

Definisco $\varphi = \varphi_\ell$ $\psi = \varphi_1$

$(\varphi_\ell)_{[1]_p} = \ell\left[\frac{q-1}{p}\right] \qquad (\varphi_1)_{[\ell]_p} = \ell\left[\frac{q-1}{p}\right]$ □

criterio (sufficiente) di isomorfismo tra prodotti semidiretti

Siano H, N gruppi, $\varphi: H \longrightarrow Aut(N)$, $f \in Aut(H)$. Allora
$N \times_\varphi H \cong N \times_{\varphi \circ f} H$

DIMOSTRAZIONE

Considero $g: N \times_\varphi H \longrightarrow N \times_{\varphi \circ f} H$
$(n,h) \longmapsto (n, f^{-1}(h))$

Verifichiamo che g è un isomorfismo:

- biettivo: l'inversa è $(n,h) \longmapsto (n, f(h))$
- omomorfismo:

$$g((n_1,h_1) \cdot_\varphi (n_2,h_2)) = g((n_1,h_1)) \cdot_{\varphi \circ f} g((n_2,h_2))$$
$$\Leftrightarrow g((n_1 \varphi_{h_1}(n_2), h_1 h_2)) = (n_1, f^{-1}(h_1)) \cdot_{\varphi \circ f} (n_2, f^{-1}(h_2))$$
$$\Leftrightarrow (n_1 \varphi_{h_1}(n_2), f(h_1 h_2)) = (n_1 (\varphi \circ f)(f^{-1}(h_1))(n_2), f^{-1}(h_1) f^{-1}(h_2)) = (n_1 \varphi_{h_1}(n_2), f^{-1}(h_1 h_2))$$

□

Conseguenza

Siano p, q primi distinti, $q < p$ e $|G| = pq$.

- $q \nmid p-1 \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ciclico
- $q \mid p-1 \Rightarrow n_p = 1$, quindi il p-Sylow è normale
  $G \cong P \times_\varphi Q$ dove Q è un q-Sylow

  Se φ è banale, $G \cong \mathbb{Z}/pq\mathbb{Z}$

  Se φ è non banale: $\varphi: Q \longrightarrow Aut(P)$
  $\mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}^*$
  $1 \longmapsto y$ di ordine q

  Se ho un'altra φ, questa manderà 1 in $y_2 = y^k$ con $(q,k)=1$ e $1 \le k < q$
  $\langle y \rangle = \langle y_2 \rangle$ unico sgp di ordine q in $\mathbb{Z}/p\mathbb{Z}^*$

  Abbiamo $\varphi: \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}^*$, $\varphi_2: \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}^*$
  $1 \longmapsto y$ $\quad$ $1 \longmapsto y^k$

  $\mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times_{\varphi_2} \mathbb{Z}/q\mathbb{Z}$

  perché $\varphi_2 = \varphi \circ f$ con $f: \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$
  $1 \longmapsto k$

  Infatti $\varphi_2 = \varphi \circ f \Leftrightarrow \varphi_2(1) = \varphi \circ f(1)$
  $\Leftrightarrow y^k = \varphi(k) = y^k$

Oss φ non banale $\Rightarrow \mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/q\mathbb{Z}$ non abeliano

esempio Il gruppo non abeliano di ordine 21

$G = \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

con $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/7\mathbb{Z})$

$1 \longmapsto (x \longmapsto kx)$

Oss $x \longmapsto kx \longmapsto k^2x \longmapsto k^3x = x$

$\Rightarrow k = 1, 2, 4$

Che ordine hanno gli elementi di G?

1 : c'è solo l'identità $(0,0)$

3 : 14

7 : 6 $(a,0)$ con $a \neq 0$

21 : non ci sono, perché sarebbe ciclico

G non è abeliano : $(0,1)(1,0)(0,1)^{-1} = \varphi(1)((1,0)) = (2,0) \neq (1,0)$

$(a,b) \cdot (a,b) = (a+\varphi_b(a), b+b) = (a+2^b a, 2b)$

$(a,b)^3 = (a+2^b a, 2b)(a,b) = (a+2^b a+\varphi_{2b}(a), 3b) = ((1+2^b+2^{2b})a, 0) \stackrel{?}{=} (0,0)$

Due casi : se $b=0$ questo è $(3a, 0)$

se $b \neq 0$ questo è $(7a, 0) = (0,0)$

$(a,b)^3 = 0$ a meno che $b=0$

Quindi gli elementi di ordine 3 sono $2 \cdot 7 = 14$

Oss $G = \langle x, y \mid x^7 = e, y^3 = e, yxy^{-1} = x^2 \rangle$

Teorema di struttura dei gruppi abeliani finiti

$G(p) = \{x \in G \mid \text{ord}\, x = p^k \text{ per qualche } k\}$ componente di p-torsione

- $G(p) < G$

  $x, y \in G(p) \quad x+y \in G(p)$

  Infatti $\text{ord}(x+y) \mid [\text{ord}\, x, \text{ord}\, y] = p^h$

- $G(p)$ è caratteristico in G

  perché gli automorfismi conservano gli ordini degli elementi

Teorema 1 Se G è un gruppo abeliano con $|G| = p_1^{e_1} \cdots p_r^{e_r}$, $p_i \neq p_j$, allora

$$G \cong G(p_1) \times \cdots \times G(p_r)$$

la decomposizione di G come prodotto di p-gruppi di ordine tra loro coprimi è unica

DIMOSTRAZIONE

Esistenza: $|G| = p_1^{e_1} \cdots p_s^{e_s}$ con $p_i \neq p_j$

Per induzione su s:

- $s = 1$: $G = G(p_1)$
- Supponiamo la tesi vera per i gruppi di cardinalità

  $s \geq 2 \quad |G| = mm' \quad$ con $m, m' > 1$ e $(m, m') = 1$

  Dico che $G \cong mG \times m'G$

  (i) $mG, m'G \trianglelefteq G$

  $mG < G$: $mx + my = m(x+y) \in mG$

  la normalità è ovvia perché G è abeliano

  (ii) $mG + m'G = G$

  $\subseteq$: ovvia

  $\supseteq$: $(m, m') = 1 \Rightarrow \exists h, k \in \mathbb{Z}$ t.c. $hm + km' = 1 \Rightarrow hmg + km'g = g$

  cioè $g = m(hg) + m'(kg) \quad \forall g \in G \Rightarrow g \in mG + m'G$

  (iii) $mG \cap m'G = \{0\}$

  $g \in mG \cap m'G$: $g = mx = m'y$, $x, y \in G$

  $m'g = m'mx = 0 \Rightarrow \text{ord}\, g \mid m'$

  $mg = mm'y = 0 \Rightarrow \text{ord}\, g \mid m \Rightarrow \text{ord}\, g \mid (m, m') = 1$

  quindi $\text{ord}\, g = 1$, cioè $g = 0$

  Ora $mG = G_{m'} = \{x \in G \mid m'x = 0\}$

  $\subseteq$: chiaro, perché se $mg \in mG \Rightarrow m'mg = 0 \Rightarrow mg \in G_{m'}$

  $\supseteq$: $x \in G_{m'}$: $x = mhx + m'kx = mhx \Rightarrow x \in mG$

  Quindi $G \cong G_{m'} \times G_m$

  $G_m < G$ e $G_m \neq \{0\}$ perché $m \neq 1$ (Cauchy)

  $$\prod_{i=1}^{s} p_i^{e_i} = |G| = |G_m||G_{m'}| = \prod_{p_i \mid m} p_i^{e_i} \prod_{p_j \mid m'} p_j^{e_j} = mm'$$

  G_m e $G_{m'}$ verificano l'ipotesi induttiva:

  $$G_m = \prod_{p_i \mid m} G(p_i) \quad \text{e} \quad G_{m'} = \prod_{p_j \mid m'} G(p_j)$$

  e quindi

  $$G \cong G_m \times G_{m'} \cong \prod_{i=1}^{s} G(p_i)$$

Unicità: $G \cong G(p_1) \times \cdots \times G(p_s)$

$\cong H_1 \times \cdots \times H_s \quad$ con H_i p_i-gruppo $\Rightarrow H_i \subseteq G(p_i)$

ma $|G| = \prod |G(p_i)| = \prod |H_i| \Rightarrow |H_i| = |G(p_i)| \Rightarrow H_i = G(p_i)$ □

Teorema 2 Se G è un p-gruppo abeliano, allora esistono e sono univocamente determinati $r_1 \geq r_2 \geq \dots \geq r_t$ tali che

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

DIMOSTRAZIONE

Esistenza: $|G| = p^n$

Per induzione su n

- $n=1$: $G \cong \mathbb{Z}/p\mathbb{Z}$
- Supponiamo la tesi vera per n

Sia $x_1 \in G$ un el. di ordine massimo

$\operatorname{ord} x = p^{r_1}$: se $r_1 = n \implies G \cong \mathbb{Z}/p^n\mathbb{Z}$

$0 < r_1 < n$: sia la proiezione al quoziente

$$\pi : G \longrightarrow G/\langle x_1 \rangle \cong \langle \bar{x}_2 \rangle \times \dots \langle \bar{x}_t \rangle \quad \text{con } |\langle \bar{x}_i \rangle| = p^{r_i} \text{ e } r_2 \geq r_3 \geq \dots \geq r_t$$

Lemma Sia G un p-gruppo abeliano e $x_1 \in G$ un elemento di ordine massimo:
$\forall \bar{x} \in G/\langle x_1 \rangle \quad \exists y \in \pi^{-1}(\bar{x})$ con $\operatorname{ord} y = \operatorname{ord} \bar{x}$

Oss sempre $\operatorname{ord} \bar{x} = \operatorname{ord} \pi(y) \mid \operatorname{ord} y$

DIMOSTRAZIONE

$\pi : G \longrightarrow G/\langle x_1 \rangle$ con x_1 di ord max in G

$\bar{x} \in G/\langle x_1 \rangle \quad \pi^{-1}(\bar{x}) = y + \langle x_1 \rangle$, cioè $\pi(y) = \bar{x}$

Dico che $\exists a$ t.c. $\operatorname{ord}(y + a x_1) = \operatorname{ord}(\bar{x}) = p^r$ con $r \leq r_1$

Sappiamo che $p^r \mid \operatorname{ord}(y + a x_1)$

Basta vedere che $p^r (y + a x_1) = 0$

Ora $\pi(p^r y) = p^r \bar{x} = 0 \implies p^r y \in \langle x_1 \rangle \implies p^r y = b x_1$

$0 = p^{r_1 - r}(p^r y) = p^{r_1 - r} b x_1 = 0 \implies p^r \mid b \implies b = p^r b_1$

Affermo che $y - b_1 x_1$ ha ordine p^r, infatti:

$p^r (y - b_1 x_1) = p^r y - p^r b_1 x_1 = 0$ □

Per il lemma $\exists x_2, \dots, x_t \in G$ t.c. $\operatorname{ord} x_i = \operatorname{ord} \bar{x}_i = p^{r_i}$

Sia $H = \langle x_2, \dots, x_t \rangle$

$\pi : G \longrightarrow G/\langle x_1 \rangle \cong \langle \bar{x}_2 \rangle \times \dots \times \langle \bar{x}_t \rangle$

$a_2 \bar{x}_2 + \dots + a_t \bar{x}_t \longmapsto (a_2 \bar{x}_2, \dots, a_t \bar{x}_t)$

$\pi|_H : \langle x_2, \dots, x_t \rangle \xrightarrow{\sim} G/\langle x_1 \rangle \cong \langle \bar{x}_2, \dots, \bar{x}_t \rangle$

- è surgettiva perché $\pi(x_i) = \bar{x}_i$
- $\ker \pi|_H = \{ h \in H \mid \pi(h) = 0 \}$

$h = a_2 x_2 + \dots + a_t x_t \longmapsto a_2 \bar{x}_2 + \dots + a_t \bar{x}_t = (a_2 \bar{x}_2, \dots, a_t \bar{x}_t) = 0$

$\implies a_i \bar{x}_i = 0 \ \forall i \implies a_i \equiv 0 \ (p^{r_i}) \implies a_i x_i = 0 \implies h = 0$

$\implies H \cong \langle \bar{x}_2 \rangle \times \dots \times \langle \bar{x}_t \rangle \cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle$

Dico che $G \cong \langle x_1 \rangle \times H \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \dots \times \langle x_t \rangle$

(i) $\langle x_1 \rangle, H \trianglelefteq G$

(ii) $\langle x_1 \rangle + H = G$

$\subseteq$: ovvio

$\supseteq$: $x \in G \quad \pi(x) = a_2 \bar{x}_2 + \dots + a_t \bar{x}_t \implies \pi(x - a_2 x_2 - \dots - a_t x_t) = 0$

$\implies x - a_2 x_2 - \dots - a_t x_t \in \langle x_1 \rangle \implies x = a_1 x_1 + a_2 x_2 + \dots + a_t x_t$

(iii) $\langle x_1 \rangle \cap H = \{0\}$

$\pi(h) \neq 0 \ \forall h \in H \setminus \{0\}$ e $\pi(a x_1) = 0 \ \forall a$

$z \in \langle x_1 \rangle \cap H \implies z = 0$

Unicità: $|G| = p^n$

Per induzione su n:

- $n=1$: $G \cong \mathbb{Z}/p\mathbb{Z}$
- sia $G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t}\mathbb{Z} \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{k_s}\mathbb{Z}$ con $r_1 \geq \dots \geq r_t$, $k_1 \geq \dots \geq k_s$

  Ora $G_p = \{g \in G \mid pg = 0\}$ è caratteristico e contiene tutti gli elementi con con ordine che divide p, cioè $G_p \cong (\mathbb{Z}/p\mathbb{Z})^e$ con e numero di fattori, quindi

  $G_p \cong (\mathbb{Z}/p\mathbb{Z})^t \cong (\mathbb{Z}/p\mathbb{Z})^s \iff t = s$

  A questo punto $|pG| = p^{n-t}$ e

  $pG \cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t-1}\mathbb{Z} \cong \mathbb{Z}/p^{k_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{k_t-1}\mathbb{Z}$

  ma per ipotesi induttiva la scrittura è unica:

  $r_i - 1 = k_i - 1 \ \forall i = 1, \dots, t \iff r_i = k_i \ \forall i = 1, \dots, t$ □

Teorema di struttura dei gruppi abeliani finiti

Sia G un gruppo abeliano finito. Allora

$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_s\mathbb{Z}$

e questa decomposizione è unica se $n_{i+1} \mid n_i \ \forall i = 1, \dots, s-1$

DIMOSTRAZIONE

Esistenza: $|G| = n = p_1^{e_1} \cdots p_s^{e_s}$

$G \overset{T1}{\cong} G(p_1) \times \dots \times G(p_s) \overset{T2}{\cong} \mathbb{Z}/p_1^{r_{11}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{r_{1t_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{r_{s1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}$

Sia $t = \max\{t_1, \dots, t_s\}$. Posso estendere le decomposizioni in modo siano tutte t, eventualmente con $r_{ij} = 0$ se $j > t_i$

Per il teorema cinese

$G \cong \mathbb{Z}/p_1^{r_{11}}p_2^{r_{21}} \cdots p_s^{r_{s1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{r_{1t}}p_2^{r_{2t}} \cdots p_s^{r_{st}}\mathbb{Z} = \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_t\mathbb{Z}$

Abbiamo $r_{j,t+1} < r_{ij}$.

È chiaro che $n_{i+1} \mid n_i \ \forall i = 1, \dots, t-1$

Unicità: se fosse anche $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_t\mathbb{Z}$ con $m_{i+1} \mid m_i$

Riapplicando il CRT, troverei una componente di p-torsione con due decomposizioni distinte ↯ □

esempio $G = \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \cong$

$\cong \mathbb{Z}/2 \times \mathbb{Z}/13 \times \mathbb{Z}/13^2 \times \mathbb{Z}/2^3 \times \mathbb{Z}/2^3 \times \mathbb{Z}/3 \cong$

$\cong (\mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/13^2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}) \cong$

$\cong \mathbb{Z}/2^3 \cdot 3\, 13^2\mathbb{Z} \times \mathbb{Z}/2^3\, 13\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Teorema $\mathbb{Z}/n\mathbb{Z}^*$ è ciclico $\iff$ $n = 2, 4, p^e, 2p^e$ con p primo dispari, $e \geq 1$

DIMOSTRAZIONE

($\Rightarrow$) $\mathbb{Z}/n\mathbb{Z}^*$ è ciclico : $n = ab$ $(a,b) = 1$

$\mathbb{Z}/n\mathbb{Z}^* = \mathbb{Z}/a\mathbb{Z}^* \times \mathbb{Z}/b\mathbb{Z}^*$
(ord $\varphi(a)$, ord $\varphi(b)$)

$\mathbb{Z}/a\mathbb{Z}^*$ e $\mathbb{Z}/b\mathbb{Z}^*$ devono essere ciclici e $(\varphi(a), \varphi(b)) = 1$

Siccome $\varphi(a) = \begin{cases} 1 \\ \text{pari} \end{cases}$

Quindi $\varphi(a) = 1 \Rightarrow a = 1, 2$

$\Rightarrow n = p^e$ o $n = 2p^e$ con p dispari
↳ devo escludere $p = 2$, per $e \geq 3$

Infatti $\mathbb{Z}/8\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/2^e\mathbb{Z}$ ha un sgp isomorfo a $\mathbb{Z}/8\mathbb{Z}$ $e \geq 3$

$\mathbb{Z}/p^e\mathbb{Z}^*$ ha un sgp isomorfo a $\mathbb{Z}/8\mathbb{Z}^*$ quindi non è ciclico

($\Leftarrow$) $\mathbb{Z}/2\mathbb{Z}^*$, $\mathbb{Z}/4\mathbb{Z}^*$ sono ciclici

$\mathbb{Z}/2p^e\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z}^* \times \mathbb{Z}/p^e\mathbb{Z}^* \cong \mathbb{Z}/p^e\mathbb{Z}^*$

Devo vedere che $\mathbb{Z}/p^e\mathbb{Z}^*$ è ciclico

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

Dico che $\exists x \in G$ ord $x = p-1$, $\exists y \in G$ ord $y = p^{e-1}$

$\Rightarrow$ ord $xy = (p-1)p^{e-1}$ perché $(p-1, p^{e-1}) = 1$ $\Rightarrow$ G ciclico

Cerco x:

$\pi : \mathbb{Z}/p^e\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ omo

$[a]_{p^e} \longmapsto [a]_p$

$\pi| : (\mathbb{Z}/p^e\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ ciclico

$[a] \longmapsto [a]$

$(a, p^e) = 1 \iff (a, p) = 1$: dà buona definizione e sorgettività

$\Rightarrow \exists [x]_p \in (\mathbb{Z}/p\mathbb{Z})^*$ ord $[x]_p = p-1$

$[x]_{p^e} \in \mathbb{Z}/p^e\mathbb{Z}^*$

$p-1 = \text{ord } [x]_p = \text{ord } \pi([x]_{p^e}) \mid \text{ord } [x]_{p^e}$

$\Rightarrow$ in $\langle [x]_{p^e} \rangle$ c'è un elemento di ord $p-1$

Cerco y:

$[1+p] \in \mathbb{Z}/p^e\mathbb{Z}^*$ ha ordine p^{e-1}

Dimostro per induzione su k: $[1+p]^{p^k} \equiv 1 + p^{k+1} \quad (p^{k+2})$

- $k = 0$: $1+p \equiv 1+p \quad (p^2)$
- $[1+p]^{p^{k+1}} = \sum_{i=0}^{p^{k+1}} \binom{p^{k+1}}{i} 1^{p^{k+1}-i} p^i = 1 + p \cdot p^{k+1} + p^2 \cdot p^{k+1} \cdot (\ldots) \equiv 1 + p^{k+2} \quad (p^{k+3})$

Quindi:

$(1+p)^{p^{e-2}} \equiv 1 + p^{e-1} \not\equiv 1 \quad (p^e)$

$(1+p)^{p^{e-1}} \quad 1 + p^e \quad (p^{e+1})$

$\equiv 1 \quad (p^e)$

$\Rightarrow \text{ord}_{\mathbb{Z}/p^e\mathbb{Z}^*} (1+p) = p^{e-1}$ □

esercizio $\mathbb{Z}/2^m\mathbb{Z}^* \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{m-2}\mathbb{Z}$

Teorema di Sylow

- **Lagrange**: G gruppo finito
  $\forall H \leq G \Rightarrow |H| \mid |G|$
- **Cauchy**: p primo, $p \mid |G| \Rightarrow \exists x \in G : \text{ord}\, x = p$, cioè $|\langle x \rangle| = p$
- G ciclico: $\forall d \mid |G| \quad \exists! H \leq G \quad |H| = d$
- G abeliano: $d \mid |G| \Rightarrow \exists H \leq G \quad |H| = d$

DIMOSTRAZIONE

$G \cong G(p_1) \times \dots \times G(p_r)$

$H \cong H(p_1) \times \dots \times H(p_r)$

esempio $G = \mathbb{Z}/32 \times \mathbb{Z}/27 \times \mathbb{Z}/54$

$|G| = 2^6 \cdot 3^6$

$d = 2^4 \cdot 3^2$

$2\mathbb{Z}/32\mathbb{Z} \times 9\mathbb{Z}/27\mathbb{Z} \times {}^{18}\mathbb{Z}/_{54}\mathbb{Z}$

Oss Il teorema di Lagrange non si inverte in generale

esempio A_4 non ha sottogruppi di ordine 6

Per assurdo, sia $H < A_4$ con $|H| = 6$: allora $H \trianglelefteq A_4$

Per Cauchy, contiene el. di ord 2 e ord 3

e poiché $H \trianglelefteq A_4$ contiene le loro classi di coniugio in A_n

$\text{ord}\, \sigma = 2$, $\sigma \in H < A_4$: $\sigma = (ab)(cd) \Rightarrow Cl_{A_n}(\sigma) < H$

$Cl_{S_n}(\sigma) = \{(12)(34), (13)(24), (14)(23)\} = Cl_{A_n}(\sigma)$

$\Rightarrow Cl_{A_n}(\sigma) < H$

$\Rightarrow H$ ha un sgp di ordine 4, V_4

ma $4 \nmid 6$ ↯

Def. Se $|G| = p^n m$ con $(p, m) = 1$, p primo

allora $H < G$, $|H| = p^n$ si dice p-sottogruppo di Sylow o p-Sylow

Lemma G p-gruppo, $H \lneq G \Rightarrow H \lneq N_G(H)$

DIMOSTRAZIONE

Sia $|G| = p^n$

Se $H \not\supseteq Z(G) \longrightarrow Z(G) < N(H) \Rightarrow N(H) \not\supseteq H$

Se $H \supseteq Z(G)$, per induzione su n

- $n = 1$: $G \cong \mathbb{Z}/p\mathbb{Z}$, $G \not\supseteq H \cong \{e\} \Rightarrow H \lneq N(H) = G$
- supponiamo la tesi vera per n

Considero $\bar{G} = G/Z(G)$ e $\pi : G \longrightarrow \bar{G}$ ($Z(G) \neq \{e\}$ perché G è un p-gruppo)

Sia $\bar{H} = \pi(H) \lneq \bar{G}$: per ipotesi $\bar{H} \lneq N_{\bar{G}}(\bar{H})$

Ora $\pi^{-1}(\bar{H}) = HZ(G) = H$

Affermo $\pi^{-1}(N_{\bar{G}}(\bar{H})) = N_G(H)$:

$g \in \pi^{-1}(N_{\bar{G}}(\bar{H})) \iff gZ \in N_{\bar{G}}(\bar{H}) \iff gZ \cdot HZ \cdot g^{-1}Z = HZ$

$\iff gHg^{-1} = H \iff g \in N_G(H)$

Quindi $H = \pi^{-1}(\bar{H}) \lneq \pi^{-1}(N_{\bar{G}}(\bar{H})) = N_G(H)$ □

Teorema di Sylow

G gruppo finito, $|G| = p^n m$, p primo, $(p,m) = 1$

(ESISTENZA) $\forall \alpha \ 1 \le \alpha \le n \quad \exists H \le G \quad |H| = p^\alpha$

(INCLUSIONE) $\forall \alpha \ 1 \le \alpha \le n$ ogni sottogruppo di ordine p^α è contenuto in un sottogruppo di ordine $p^{\alpha+1}$

(CONIUGIO) Due qualsiasi p-sottogruppi di Sylow di G sono coniugati

(NUMERO) $n_p = \#$ p-sgr di Sylow di G

$n_p \mid |G|$, $n_p \equiv 1 \ (p)$, $n_p = [G : N_G(S)]$

DIMOSTRAZIONE

Esistenza: Fisso α

Consideriamo $\mathcal{M} = \{X \le G \mid |X| = p^\alpha\}$

$$|\mathcal{M}| = \binom{p^n m}{p^\alpha} = \frac{p^n m \,(p^n m - 1)\cdots(p^n m - p^\alpha + 1)}{p^\alpha (p^\alpha - 1)\cdots(p^\alpha - p^\alpha + 1)} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$$

$p^{n-\alpha}$; $\frac{p^n m - i}{p^\alpha - i}$ non è divisibile per p

se $i = p^k \ell$ con $k < \alpha$, $(\ell, p) = 1$: $p^n m - p^k \ell = p^k (p^{n-k} m - \ell)$

$p^\alpha - p^k \ell = p^k (p^{\alpha-k} - \ell)$

Quindi $p^{n-\alpha} \parallel |\mathcal{M}|$

Consideriamo $\Phi : G \longrightarrow S(\mathcal{M})$

$g \longmapsto \varphi_g : X \longrightarrow gX$

$$p^{n-\alpha} m = |\mathcal{M}| = \sum_{i \in I} |orb(X_i)|$$

$\exists i$ t.c. $p^{n-\alpha+1} \nmid |orb(X_i)| = \frac{|G|}{|Stab(X_i)|} = \frac{p^n m}{|Stab(X_i)|} \Rightarrow p^\alpha \mid |Stab(X_i)| = s \ge p^\alpha$

$j : Stab(X_i) \longrightarrow X_i$

$y \longmapsto yx$ con $x \in X_i$ fissato

j è iniettiva per la legge di cancellazione

$\Rightarrow s = |Stab(X_i)| \le |X_i| = p^\alpha$

$\Rightarrow |Stab(X_i)| = p^\alpha$, $Stab(X_i) < G$

Inclusione: S p-Sylow di G, $|S| = p^n$

$|H| = p^\alpha$ con $0 \le \alpha \le n$

$X = \{$classi laterali di S in $G\}$ $\quad \# X = [G : S] = m$

$\Theta : H \longrightarrow S(X)$

$h \longmapsto \varphi_h : gS \longmapsto hgS$

$$m = \#X = \sum_i orb(g_i S) = \sum_i \frac{|H|}{|St_H(g_i S)|} = \sum_i p^{k_i} \quad \text{con } 0 \le k_i \le \alpha$$

$\Rightarrow \exists i$ t.c. $k_i = 0$ $\quad H = St_H(g_i S)$

$\forall h \in H \quad hg_iS = g_iS \Rightarrow h \in g_i S g_i^{-1} \Rightarrow H < g_i S g_i^{-1}$

e $g_i S g_i^{-1}$ è un p-Sylow

Coniugio: se $|H| = p^n$ $H < g_i S g_i^{-1} \Rightarrow H = g_i S g_i^{-1}$, quindi i p-Sylow sono coniugati

Per concludere l'inclusione, basta mostrare che se $\mathcal{G}$ è un p-gruppo e $H \le \mathcal{G}$ con $|H| = p^\alpha$

$\Rightarrow H$ è contenuto in un sottogruppo di ordine $p^{\alpha+1}$

Per il lemma, $H \trianglelefteq N_{\mathcal{G}}(H)$. Ora $N_{\mathcal{G}}(H)/H$ è un p-gruppo non banale

e per Cauchy $\exists \bar{x} \in N_{\mathcal{G}}(H)/H : ord \bar{x} = p$

Per corrispondenza, $\pi^{-1}(\langle \bar{x} \rangle)$ contiene H e ha ordine $p^{\alpha+1}$

dove $\pi : N_{\mathcal{G}}(H) \longrightarrow N_{\mathcal{G}}(H)/H$ è la proiezione al quoziente

Numero :

$n_p = [G : N_G(S)] \Rightarrow n_p \mid |G|$

$X = \{p\text{-Sylow}\}$

$\phi : S \longrightarrow S(X)$

$g \longmapsto \phi_g : S' \longmapsto gS'g^{-1}$

$orb(S) = \{S\}$

Inoltre se $orb(S') = \{S'\} \Rightarrow S' = S$

Infatti $orb(S') = \{S'\} \Rightarrow S \subseteq N_G(S')$

$SS' < G \Rightarrow |SS'| = \frac{|S||S'|}{|S \cap S'|} = \frac{p^n \cdot p^n}{|S \cap S'|} \Rightarrow |S \cap S'| = p^n \Rightarrow S = S'$

$n_p = \#X = \sum_{i \in I} |orb(S_i)| = \sum_{i \in I} p^i$

↳ c'è un unico addendo 1 perché c'è un'unica orbita banale

$\Rightarrow n_p \equiv 1 \ (p)$ □

Classificazione dei gruppi di ordine 12

$|G| = 12 = 2^2 \cdot 3$

Per Sylow, $\exists P_2, P_3$

Uno tra P_2 e P_3 è normale in G

- Se $P_3 \trianglelefteq G$ ok
- Se $P_3 \not\trianglelefteq G \Rightarrow n_3 \equiv 1 \ (3) \Rightarrow n_3 \geq 4$

  $\Rightarrow$ ho almeno 8 elementi di ordine 3

  $\Rightarrow$ restano 4 el. : P_2 è unico $\Rightarrow P_2 \trianglelefteq G$

$P_2 P_3 = G$ per cardinalità

$P_2 \cap P_3 = \{e\}$

$\Rightarrow G \cong P_2 \times P_3$ o $G \cong P_3 \rtimes P_2$

Se $P_2 \trianglelefteq G$: $P_2 \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases}$

$\mathbb{Z}/4\mathbb{Z} \times_\varphi \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$

$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$

$\overline{1} \longmapsto id$

$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$

$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$

$\overline{1} \longmapsto id$ $\quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\overline{1} \longmapsto s, s^2$ $\quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \cong A_4$

Se $P_3 \trianglelefteq G$

$\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong D_6$

$\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$

$(0,1) \longmapsto \overline{1}$

$(1,0) \longmapsto \overline{1}$

$(1,1) \longmapsto \overline{0}$

$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$

$\varphi : \mathbb{Z}/4\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$

$\overline{1} \longmapsto [1]$

Oss $n_p = 1 \iff$ un p-Sylow è normale

DIMOSTRAZIONE

($\Longrightarrow$) è l'unico del suo ordine, quindi è caratteristico

($\Longleftarrow$) P un p-Sylow normale. Gli altri sono $gPg^{-1} = P$ e quindi è l'unico $\square$

Classificazione dei gruppi di ordine 15

$\#G = 15$

$n_3 \equiv 1 \ (3) \quad n_3 \mid 3 \cdot 5 \implies n_3 = 1$

$n_5 \equiv 1 \ (5) \quad n_5 \mid 3 \cdot 5 \implies n_5 = 1$

$\implies G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$

Classificazione dei gruppi di ordine 45

$|G| = 45$

$n_3 \equiv 1 \ (3) \quad n_3 \mid 5 \implies n_3 = 1$

$n_5 \equiv 1 \ (5) \quad n_5 \mid 9 \implies n_5 = 1$

$$\implies G \cong P_3 \times P_5 \cong \begin{cases} \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{cases}$$

Classificazione dei gruppi di ordine $3 \cdot 5 \cdot 17$

$|G| = 3 \cdot 5 \cdot 17$

$n_3 \equiv 1 \ (3) \quad n_3 \mid 5 \cdot 17 \implies n_3 \in \{1, 85\}$

$n_5 \equiv 1 \ (5) \quad n_5 \mid 3 \cdot 17 \implies n_3 \in \{1, 51\}$

$n_{17} \equiv 1 \ (17) \quad n_{17} \mid 3 \cdot 5 \implies n_{17} = 1$

Sia P_{17} l'unico 17-Sylow

Dico che $P_{17} \subseteq Z(G)$

$\frac{N(H)}{Z(H)} \hookrightarrow \mathrm{Aut}(H)$

Applichiamolo a P_{17}:

$\frac{G}{C_G(P_{17})} \hookrightarrow \mathrm{Aut}(P_{17}) \cong \mathbb{Z}/16\mathbb{Z}$

$\implies \# \frac{G}{C_G(P_{17})} \mid (16, 3 \cdot 5 \cdot 17) = 1 \implies C_G(P_{17}) = G$

Ora considero $\frac{G}{Z(G)}$, che ha cardinalità $1, 3, 5, 15$

$\implies G/Z(G)$ ciclico $\implies G$ abeliano

$\implies G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$

Classificazione dei gruppi di ordine 8

- Abeliani: $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$
- Non abeliani: D_4, Q_8

Se non è abeliano, non può avere solo elementi di ordine 2 (sarebbe $(\mathbb{Z}/2\mathbb{Z})^3$), quindi:

$\exists a \in G$ con $\operatorname{ord} a = 4$: $\langle a \rangle = \{e, a, a^2, a^3\} \triangleleft G = \langle a \rangle \cup b\langle a \rangle$

$G = \{e, a, a^2, a^3, ba, ba^2, ba^3\} = \langle a, b \rangle$

$\operatorname{ord} b = \begin{cases} 2 \\ 4 \end{cases}$

$bab^{-1} \in \langle a \rangle \quad \Rightarrow \quad bab^{-1} = \begin{cases} a & \longleftarrow \text{no perché sarebbe abeliano} \\ a^3 = a^{-1} \end{cases}$

- Se $\operatorname{ord} b = 2$, $b^2 = e$, $a^4 = e$, $bab^{-1} = a^{-1}$

  $G \cong D_4$

  $\varphi: \begin{matrix} a \mapsto r \\ b \mapsto s \end{matrix}$ si estende ad un unico omomorfismo $G \to D_4 : a^i b^j \mapsto r^i s^j$ perché le relazioni vengono preservate

  Infatti basta vedere: $\varphi(a)^4 = id$, $\varphi(b)^2 = id$, $\varphi(b)\varphi(a)\varphi(b)^{-1} = \varphi(a)^{-1}$ cioè $srs^{-1} = r^{-1}$
- Se $\operatorname{ord} b = 4$

  $\langle a, b \mid a^4 = e, b^4 = e, ba = a^3 b \rangle$

  $b^2 = ba^j \rightarrow b = a^j$ ↯ $\quad \Rightarrow b^2 = a^2$

  Quindi $G \cong Q_8$

  $\begin{matrix} a \mapsto i \\ b \mapsto j \end{matrix}$

  Infatti $ba = a^3 b \longrightarrow ji = i^3 j = -ij$

Classificazione dei gruppi di ordine 30

$30 = 2 \cdot 3 \cdot 5 = 2d$ con $d = 15$ dispari $\qquad \mathbb{Z}/30\mathbb{Z}$, $D_5 \times \mathbb{Z}/3\mathbb{Z}$, $D_3 \times \mathbb{Z}/5\mathbb{Z}$, D_{15}

$\Rightarrow \exists H \triangleleft G \ |H| = 15$; $\exists y \in G \ \operatorname{ord} y = 2$

$\Rightarrow G \cong H \times_\varphi \langle y \rangle$

$H = \langle x \rangle \cong \mathbb{Z}/15\mathbb{Z}$

$G = \langle x, y \mid x^{15} = e, y^2 = e, yxy^{-1} = \varphi_y(x) \rangle$

$\varphi \quad \langle y \rangle \longrightarrow \operatorname{Aut}(\langle x \rangle) \cong \mathbb{Z}/15\mathbb{Z}^* \cong \mathbb{Z}/3\mathbb{Z}^* \times \mathbb{Z}/5\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$y \longmapsto \varphi_y$ · deve avere ord 1 o 2 $\sim$ 3 el. id

· $x \mapsto x^\ell$ $(\ell, 15) = 1$

$\begin{cases} \ell \equiv \pm 1 \ (3) \\ \ell \equiv \pm 1 \ (5) \end{cases} \Rightarrow \begin{cases} \ell \equiv 1 \ (3) \\ \ell \equiv 1 \ (5) \end{cases} \vee \begin{cases} \ell \equiv -1 \ (3) \\ \ell \equiv 1 \ (5) \end{cases} \vee \begin{cases} \ell \equiv 1 \ (3) \\ \ell \equiv -1 \ (5) \end{cases} \vee \begin{cases} \ell \equiv -1 \ (3) \\ \ell \equiv -1 \ (5) \end{cases}$

$\ell \equiv 1 \ (15)$ $\qquad \ell \equiv -4 \ (15)$ $\qquad \ell \equiv 4 \ (15)$ $\qquad \ell \equiv -1 \ (15)$

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

$\mathbb{Z}/30\mathbb{Z}$ $\qquad D_3 \times \mathbb{Z}/5\mathbb{Z}$ $\qquad D_5 \times \mathbb{Z}/3\mathbb{Z}$ $\qquad D_{15}$

· $yxy^{-1} = x^4$

$yx^3y^{-1} = (yxy^{-1})^3 = x^{12} \neq x^3$

$\not\exists$ di ord 5

$\operatorname{ord} x^5 = 3$

$yx^5y^{-1} = (yxy^{-1})^5 = x^{20} = x^5$

$x, y \in Z(x^5) \Rightarrow Z(x^5) = G \quad \Rightarrow x^5 \in Z(G)$

$\langle x \rangle \cong \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \langle x^5 \rangle \times \langle x^3 \rangle$

Classificazione dei gruppi non semplici di ordine ≤ 100

$|G| \leq 100$

- A_5 semplice, $|A_5| = 60$, $\mathbb{Z}/p\mathbb{Z}$ p primo
- $|G| = pq$ p, q primi
  se $p = q$: G abeliano, non semplice
  se $p < q$: $n_q \equiv 1 \ (q)$, $n_q \mid p \Rightarrow n_q = 1$
- $|G| = 2d$ d dispari $\longrightarrow \exists H < G$ di indice 2, quindi G non è semplice (a meno che $|G| = 2$)
- $|G| = 4p$ p primo ≥ 5 : $n_p \equiv 1 \ (p)$, $n_p \mid 4 \Rightarrow n_p = 1$
- $|G| = 48 = 2^4 \cdot 3$

  Sia P_2 un 2-sylow di indice 3
  $\Rightarrow$ per Poincaré, $\exists N \lhd G$, $N \leq P_2$ $\quad [G : N] \mid 3! = 6$
  $N \neq G$ perché $N \leq P_2$
  $N \neq \{e\}$ perché ha indice ≤ 6

- Cardinalità "interessanti" : 56, 60, 72, 80
- $|G| = 56 = 7 \cdot 2^3$

  $n_7 \in \{1, 8\}$, $n_2 \in \{1, 7\}$
  Se $n_7 = 8$, ho $P_1, \dots, P_8$ 7-Sylow
  La loro unione contiene $1 + 8 \cdot 6 = 49$ elementi
  Un 2-Sylow Q sarà contenuto in $G \setminus (P_1 \cup \dots \cup P_8) \cup \{e\}$, che ha cardinalità 8
  $\Rightarrow Q = (G \setminus \bigcup_{i=1}^{8} P_i) \cup \{e\}$
  $\Rightarrow$ il 2-Sylow è unico quindi normale
- $|G| = 72 = 2^3 \cdot 3^2$

  $n_2 \in \{1, 3, 9\}$, $n_3 \in \{1, 4\}$
  Sia $n_3 = 4$, voglio costruire un'azione "interessante" : passo considerare
  $G \curvearrowright \{3\text{-Sylow}\}$ per coniugio
  $X = \{P_1, \dots, P_4\}$ insieme di 3-Sylow
  $g \in G, P_i \in X$: $g \cdot P_i = g P_i g^{-1}$
  L'azione è un omomorfismo $\psi : G \longrightarrow \mathrm{Big}(X) \cong S_4$
  Quest'azione è transitiva per Sylow
  Sia $N = \ker \psi$
  - $N \neq G$: se $N = G$, ψ manda nell'identità, cioè $\forall g \in G$ coniugare per g fissa ciascuno dei 3-Sylow, che contraddice la transitività
  - $N \neq \{e\}$: per il I th. di omo. $G/\ker\psi = G/N \hookrightarrow S_4$
    $\frac{72}{|N|} = |G/N| \leq 24 \Rightarrow |N| \geq 3$
- $|G| = 80 = 5 \cdot 2^4$

  $n_2 \in \{1, 5\}$
  $n_5 \in \{1, 16\}$
  Oss Si può fare notando che "non c'è spazio"
  Sia $n_2 = 5$. Considerando l'azione di coniugio sui suoi 2-Sylow costruisco $\psi : G \longrightarrow S_5$
  Allora $N = \ker\psi \lhd G$, e $|G|/|\ker\psi| \mid 120 \Rightarrow |\ker\psi| \neq 1$

Oss Sia G semplice, $|G| \neq 2$ e $\psi : G \longrightarrow S_n$ un omomorfismo. Allora $\psi(G) \leq A_n$

$$\ker\psi = \begin{cases} G & \mathrm{Im}\,\psi = \{id\} \leq A_n \\ \{e\} & \psi : G \xrightarrow{\sim} \mathrm{Im}\,\psi \ \text{(perché iniettivo)} \end{cases}$$

$\mathrm{Im}\,\psi \cap A_n$ è un sottogruppo normale di $\mathrm{Im}\,\psi \cong G$
se $\mathrm{Im}\,\psi \cap A_n = \mathrm{Im}\,\psi \Rightarrow \mathrm{Im}\,\psi \leq A_n$
se $\mathrm{Im}\,\psi \cap A_n = \{e\} \Rightarrow \#G = \frac{\#\mathrm{Im}\,\psi}{\#\,\mathrm{Im}\,\psi \cap A_n} = [\mathrm{Im}\,\psi : \mathrm{Im}\,\psi \cap A_n] \leq 2$, caso non interessante

- $|G|=60$, G semplice $\Rightarrow G \cong A_5$

  $60 = 2^2 \cdot 3 \cdot 5$

  Se $G = A_5$: $n_5 = 6$, $n_3 = \frac{1}{2}\binom{5}{3} \cdot 2 = 10$, $n_2 = 5$

  V_4 è un 2-Sylow di A_5

  $n_2 \in \{1,3,5,15\}$, $n_3 \in \{1,4,10\}$, $n_5 \in \{1,6\}$

  Casi per n_2:

  - $n_2 = 3$: voglio trovare un assurdo

    l'azione sui 3 2-Sylow dà $G \longrightarrow S_3$

    e il suo Ker è un sottogruppo normale non banale

  - $n_2 = 5$: l'azione di G sui 2-Sylow dà

    $\psi : G \longrightarrow S_5$

    $\ker \psi = \{e\}$ (azione transitiva) $\Rightarrow \psi : G \hookrightarrow S_5$

    Per l'osservazione precedente, $\psi : G \hookrightarrow A_5$

    che è un isomorfismo per cardinalità

  - $n_2 = 15$: per ragioni di cardinalità, $\exists\ P_1, P_2$ 2-Sylow

    con $|P_1 \cap P_2| > 1 \Rightarrow |P_1 \cap P_2| = 2$

    Sia $H = P_1 \cap P_2$ e $K = N_G(H)$

    Osserviamo che : $H \subseteq K$, $P_1, P_2 \subseteq K$ perché P_1, P_2 sono abeliani $\Rightarrow H \lhd P_i \Rightarrow P_i \subseteq K$

    $4 \mid \#K$, $\#K \geq 6$, $\#K \mid 60$

    $\Rightarrow \#K \in \{4, 12, 20, 60\}$

    Se $\#K = 60$, $N_G(H) = G$ quindi $H \lhd G$ ↯

    Se $\#K = 20$, per Poincaré ho un sottogruppo normale di indice ≤ 6 ↯

    Se $\#K = 12$, l'azione sulle classi laterali $G \curvearrowright (G/K) : g \cdot g_1 K = g g_1 K$

    fornisce un omomorfismo non banale (azione transitiva) $\psi : G \longrightarrow S_5$

    e come sopra si conclude $G \cong A_5$ ↯

Gruppi (non) semplici di ordine 144

$|G| = 144 = 3^2 \cdot 2^4$ non è semplice

Per assurdo G semplice

$n_2 \in \{1,3,9\}$

$n_3 \in \{1,4,16\}$

Se $n_2 = 3$ o $n_3 = 4$, guardo l'azione sui 2-Sylow o 3-Sylow,

cioè ho un omomorfismo $\psi : G \longrightarrow S_3$ o S_4, il cui nucleo

non è G (azione transitiva) e non è $\{id\}$ (cardinalità)

Quindi $n_2 = 9$, $n_3 = 16$

Non è possibile che tutti i 3-Sylow si intersechino banalmente a 2 a 2:

dovrebbero $16 \cdot 8 = 128$ elementi di ordine 3 o 9, e il 2-Sylow sarebbe unico.

Siano allora P_1, P_2 due 3-Sylow con $|P_1 \cap P_2| = 3$

Sia $K = N_G(P_1 \cap P_2) = N_G(H)$:

- $P_1, P_2 \subseteq K$
- $9 \mid \#K$, $\#K \geq 15$
- $\#K \in \{18, 36, 72, 144\}$

  ↳ $K \lhd G$ (ha indice 2)

  ↳ no per Poincaré

K contiene $P_1 P_2$: $|P_1 P_2| = \frac{|P_1| \cdot |P_2|}{|P_1 \cap P_2|} = 27 > 18$

Gruppi di ordine 75

$|G|=75 \qquad \#Z(G)=?$

- $\#Z(G) \in \{1,3,5,15,25,75\}$
- $\#Z(G) = 75$ ok
- $\#Z(G) \neq 25, 15, 5$, altrimenti $G/Z(G)$ sarebbe ciclico

C'è un unico 5-Sylow P_5. Scegliamo un 3-Sylow P_3

$\Rightarrow G \cong P_5 \rtimes P_3$

Due casi: $P_5 \cong \mathbb{Z}/5^2\mathbb{Z}$ o $P \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

(1) Se $P_1 \cong \mathbb{Z}/5^2\mathbb{Z}$, $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/5^2\mathbb{Z}) \cong \mathbb{Z}/20\mathbb{Z}$ $\Rightarrow \varphi$ è banale

$\Rightarrow G \cong \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/75\mathbb{Z}$

(2) Se $P_1 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut((\mathbb{Z}/5\mathbb{Z})^2) = GL_2(\mathbb{F}_5)$

$\#GL_2(\mathbb{F}_5) = (5^2-1)(5^2-5) = 24 \cdot 20 = 480$

Se φ è banale, $G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Se φ è non banale, chiamo $M = \varphi(1) \in GL_2(\mathbb{F}_5)$

Studio $Z(G)$ in questo caso

Sia $(v,i) \in Z((\mathbb{Z}/5\mathbb{Z})^2 \times_\varphi \mathbb{Z}/3\mathbb{Z})$

$v \in (\mathbb{Z}/5\mathbb{Z})^2$, $i \in \mathbb{Z}/3\mathbb{Z}$

L'elemento $(v,i) \in Z(G)$ se e solo se

$(v,i)\cdot(w,j) = (w,j)\cdot(v,i) \quad \forall (w,j) \in G$, se e solo se

$(v,i)\cdot(0,1) = (0,1)\cdot(v,i)$

$(v,i)\cdot(w,0) = (w,0)\cdot(v,i) \quad \forall w \in (\mathbb{Z}/5\mathbb{Z})^2$

Calcoliamo questi prodotti:

$(v + \varphi_i(0), i+1) = (0 + \varphi_1(v), i+1)$

$(v, i+1) = (Mv, i+1) \iff Mv = v$

$(v + \varphi_i(w), i) = (w + \varphi_0(v), i)$

$(v + M^i w, i) = (w+v, i) \iff v + M^i w = w + v \iff M^i w = w \quad \forall w$

$\iff M^i = I \iff i = 0 \in \mathbb{Z}/3\mathbb{Z}$

Quindi gli elementi nel centro sono $(v,0)$ tale che $Mv = v$

$\rightarrow$ Sono (in biezione con) l'autospazio di M relativo a 1 $\Rightarrow Z(G) = 5^k$

Non può essere 5 o 25, quindi $|Z(G)| = 1$

Classificazione dei gruppi di ordine 105

$105 = 3 \cdot 5 \cdot 7$

$\mathbb{Z}/105\mathbb{Z}$ e $(\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z}$

$n_3 \in \{1, 7\}$

$n_5 \in \{1, 21\}$

$n_7 \in \{1, 15\}$

Se valesse $n_5 = 21$, $n_7 = 15$, avrei

$21 \cdot 4 + 15 \cdot 6 > 105$ ass. di ord 5 o 7

Siano P_5 un 5-Sylow e P_7 un 7-Sylow.

Siccome almeno uno dei due è normale, $H := P_5 P_7 < G$ e $H \cong \mathbb{Z}/35\mathbb{Z}$ e $H \lhd G$ perché ha indice il più piccolo primo

Quindi $G \cong \mathbb{Z}/35\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

dove $\varphi: \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/35\mathbb{Z}^* \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

$(0, \bar{2}_4)$

Ci sono 3 φ possibili $\varphi_1 : 1 \longmapsto 1 \in (\mathbb{Z}/35\mathbb{Z})^*$

$\varphi_2 : 1 \longmapsto y$

$\varphi_3 : 1 \longmapsto y^2$

Ora $\varphi_3 = \varphi_2 \circ [2]$ dove $[2] : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$

$x \longmapsto 2x$

Quindi i prodotti semidiretti con φ_2 e φ_3 sono isomorfi

$\mathbb{Z}/35\mathbb{Z} \rtimes_{\varphi_2} \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z} \rtimes_\psi \mathbb{Z}/3\mathbb{Z})$

$(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}) \rtimes_{\varphi_2} \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z} \rtimes_\psi \mathbb{Z}/3\mathbb{Z})$

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

è omomorfismo:

$g(((a_1, b_1), c_1)((a_2, b_2), c_2)) = (a_1, (b_1, c_1)) \cdot (a_2, (b_2, c_2))$

$g((a_1, b_1) + \varphi_2(c_1)(a_2, b_2)), c_1 + c_2) \quad (a_1 + a_2, (b_1 + \psi_{c_1}(b_2), c_1 + c_2))$

$(a_1 + a_2, (b_1 + \varphi_2(c_1)(b_2), c_1 + c_2))$

che sono uguali se prendo $\psi = \pi_{\mathbb{Z}/7\mathbb{Z}^*} \circ \varphi_2$

Presentazioni di gruppi

Def. Il gruppo libero su n generatori è

$$F_n = \langle x_1, \dots, x_n \rangle = \{ x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \cdots x_{i_k}^{\pm 1} \mid i_j \in \{1, \dots, n\} \}$$

con l'operazione di concatenazione

esempio $F_1 = \langle x_1 \rangle = \{ x_1^{\pm 1} x_1^{\pm 1} \cdots x_1^{\pm 1} \} = \{ x_1^k \mid k \in \mathbb{Z} \} \cong \mathbb{Z}$

$F_2 = \langle x_1, x_2 \rangle = \langle x, y \rangle \ni xxyxy^{-1}$ ha inverso $yx^{-1}y^{-1}x^{-1}x^{-1}$

Proprietà universale

$$\begin{aligned} \mathrm{Hom}(F_n, G) &\longleftrightarrow \{(g_1, \dots, g_n) \in G\} \\ \varphi &\longmapsto (\varphi(x_1), \dots, \varphi(x_n)) \\ \varphi(x_i) = g_i &\longleftarrow\!\shortmid (g_1, \dots, g_n) \end{aligned}$$

esempio $D_n = \langle r, s \rangle$

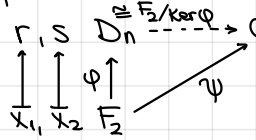
$$\begin{aligned} \varphi : F_2 &\twoheadrightarrow D_n \\ x_1 &\longmapsto r \\ x_2 &\longmapsto s \end{aligned}$$

Chi sarà $\ker\varphi$? Contiene x_1^n perché $\varphi(x_1^n) = \varphi(x_1)^n = r^n = id$,

e anche x_2^2 e $x_2 x_1 x_2 x_1$ che è mandato in $srsr = id$

Vale in effetti che $\ker\varphi$ è il più piccolo sgp normale che contiene $x_1^n, x_2^2, x_2 x_1 x_2 x_1$

Supponiamo di voler definire un omomorfismo



$\psi(x_1) = x, \psi(x_2) = y$ $\quad \ker\psi \ni x_1^n, x_2^2, x_2 x_1 x_2 x_1$

$\Longrightarrow \ker\psi \supseteq \ker\varphi$

Def. La **presentazione di un gruppo** G è

$$\langle x_1, \dots, x_n \mid r_1 = r_2 = \dots = 1 \rangle$$

dove $r_i \in F_n$.

Si interpreta così: c'è un omomorfismo surgettivo

$$\begin{aligned} \varphi : F_n &\longrightarrow G \\ x_1 &\longmapsto x_1 \\ &\vdots \\ x_n &\longmapsto x_n \end{aligned}$$

tale che $\ker\varphi$ è il più piccolo sottogruppo normale di F_n che contiene $r_1, r_2, \dots$

esempio

$D_n = \langle r, s \mid r^n = s^2 = srsr = 1 \rangle$

$\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1 \rangle$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle x, y \mid x^2 = y^2 = [x, y] = 1 \rangle$

$(\mathbb{Z}/2\mathbb{Z})^3 = \langle x, y, z \mid x^2 = y^2 = z^2 = [x, y] = [y, z] = [x, z] = 1 \rangle$

Gruppo delle permutazioni

$(S_n, \circ)$ è un gruppo

Data $\sigma \in S_n$: $\langle\sigma\rangle \hookrightarrow S_n = S(\{1,\dots,n\})$
$\langle\sigma\rangle$ agisce su $X=\{1,\dots,n\}$ per inclusione
Quindi $X = \bigcup_{x \in R} orb(x)$
dove $orb(x) = \{\sigma^i(x) \mid i \in \mathbb{Z}\}$

I cicli delle permutazioni sono le orbite, viste come insieme ordinato
$(x, \sigma x, \sigma^2 x, \dots, \sigma^{m-1} x)$ $\quad m = \min\{j \mid \sigma^j x = x\}$

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

DIMOSTRAZIONE
$\sigma \in S_n \quad \langle\sigma\rangle \hookrightarrow S_n$
determina univocamente le orbite
Ogni orbita si considera come insieme ordinato.
Questa scrittura è unica a meno della scelta del primo elemento dell'orbita
(ogni k-ciclo ha k scritture diverse) □

corollario I 2-cicli (trasposizioni) generano S_n $\forall n$
(equivalentemente, ogni permutazione è prodotto di trasposizioni)

DIMOSTRAZIONE
Basta vederlo per i cicli
$(1,\dots,k) = (1,k)(1,k-1)\cdots(1,2)$
$i \mapsto i+1$ $(i<k)$ $\quad i \mapsto 1 \mapsto i+1$
$k \mapsto 1$ $\quad k \mapsto 1$ □

Fatti:
- Cicli disgiunti commutano
- L'ordine di un k ciclo è k
- L'ordine di una permutazione è il mcm delle lunghezze dei suoi cicli (nella sua scrittura "unica" come prodotto di cicli disgiunti)

esempio S_4 $\quad 4! = 24$

tipo			
1		id	1
2		(a b)	$\binom{4}{2}\frac{2!}{2} = 6$
3		(a b c)	$\binom{4}{3}\frac{3!}{3} = 8$
4		(a b c d)	$\binom{4}{4}\frac{4!}{4} = 3! = 6$
2+2		(a b)(c d)	$\frac{1}{2!}\binom{4}{2}\binom{2}{2}\frac{2!}{2}\frac{2!}{2} = 3$

In generale $\#\{k\text{-cicli di } S_n\} = \binom{n}{k}\frac{k!}{k} = \binom{n}{k}(k-1)!$

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

La scrittura di una permutazione come prodotto di trasposizioni non è unica, non è unico il numero di trasposizioni, ma questo è sempre pari o sempre dispari

Proposizione La mappa $\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}$

$$\sigma \longmapsto \operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

è un omomorfismo di gruppi

Inoltre $\operatorname{sgn}(a\,b) = -1$

Siccome un k-ciclo è prodotto di $k-1$ trasposizioni

$$\operatorname{sgn}(k\text{-ciclo}) = (-1)^{k-1}$$

DIMOSTRAZIONE

(1) sgn è ben definita:

a denominatore vi sono tutte le possibili coppie $i-j$ in $\{1,\dots,n\}$ (con $i<j$)

e anche a numeratore a meno dell'ordine, poiché σ è biiettiva

quindi $\operatorname{sgn}(\sigma) \in \{\pm 1\}$

(2) sgn è un omomorfismo: $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$

$$\operatorname{sgn}(\sigma\circ\tau) = \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i-j} = \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i-j} = \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau)$$

(3) $\operatorname{sgn}(a\,b) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i-j}$

Se $\{i,j\} \cap \{a,b\} = \emptyset$: $\frac{\sigma(i)-\sigma(j)}{i-j} = 1$

Se $\{i,j\} = \{a,b\}$: $\sigma(a) = b$, $\sigma(b) = a$ $\quad \frac{b-a}{a-b} = -1$

Se $\{i,a\} \circ \{i,b\}$ $\quad \frac{\sigma(i)-\sigma(a)}{i-a} \cdot \frac{\sigma(i)-\sigma(b)}{i-b} = \frac{i-b}{i-a} \cdot \frac{i-a}{i-b} = 1$

$\Rightarrow \operatorname{sgn}\{(a\,b)\} = -1$ □

Def Una permutazione $\sigma \in S_n$ si dice **pari** se $\operatorname{sgn}(\sigma) = 1$, **dispari** se $\operatorname{sgn}\sigma = -1$

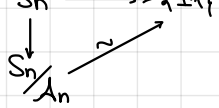
Quindi k-ciclo è dispari $\iff k$ è pari

Def Dato l'omomorfismo $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$, si definisce il **gruppo alterno**:

$A_n = \ker \operatorname{sgn}$ (permutazioni pari)

Oss $A_n \lhd S_n$ e $[S_n : A_n] = 2$

Infatti



Classi di coniugio di S_n

Teorema Due permutazioni sono coniugate in S_n se e solo se hanno lo stesso tipo

DIMOSTRAZIONE

$\Leftarrow$ $\sigma, \rho \in S_n$ dello stesso tipo

Scopo: mostrare che $\exists \eta \in S_n$ t.c. $\sigma = \eta \rho \eta^{-1}$

$\rho = (a_1, \dots, a_{k_1})(b_1, \dots, b_{k_2}) \cdots (z_1, \dots, z_{k_t})$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \ \eta$

$\sigma = (a'_1, \dots, a'_{k_1})(b'_1, \dots, b'_{k_2}) \cdots (z'_1, \dots, z'_{k_t})$

$\eta \rho \eta^{-1}(a'_i) = \eta \rho(a_i) = \eta(a_{i+1}) = a'_{i+1} = \sigma(a'_i)$

$\Rightarrow$ Il coniugio è un omomorfismo, quindi basta vedere che il coniugato di un k-ciclo è un k-ciclo

$\eta (a_1, \dots, a_k) \eta^{-1}$ con $\eta(a_i) = \alpha_i \ \forall i$

sia $c \notin \{\alpha_1, \dots, \alpha_k\} \rightarrow \exists b$ t.c. $\eta(b) = c \rightarrow b \notin \{a_1, \dots, a_k\}$

$\eta (a_1, \dots, a_k) \eta^{-1} = (\alpha_1, \dots, \alpha_k)$

$\alpha_i \mapsto a_i \mapsto a_{i+1} \mapsto \alpha_{i+1}$

$c \mapsto b \mapsto b \mapsto c$ □

Oss Se $\eta \sigma \eta^{-1} = \rho$ e $\tau \sigma \tau^{-1} = \rho$

allora $\tau^{-1} \eta \sigma \eta^{-1} \tau = \tau^{-1} \rho \tau = \sigma \implies \tau^{-1} \eta \in Z_{S_n}(\sigma)$

Viceversa, $\tau \in \eta Z_{S_n}(\sigma) \implies \tau \sigma \tau^{-1} = \eta \gamma \sigma \gamma^{-1} \eta^{-1} = \eta \sigma \eta^{-1}$

$\tau = \eta \gamma$ con $\gamma \in Z_{S_n}(\sigma)$

Gli elementi x t.c. $x \sigma x^{-1} = \rho$ sono esattamente quelli di una classe laterale di $Z_{S_n}(\sigma)$

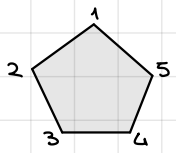
esempio Sottogruppo di S_5

Consideriamo $\sigma = (12345)$, $\tau = (25)(34)$, $G = \langle \sigma, \tau \rangle$

$\tau \sigma \tau^{-1} = (25)(34)(12345)(25)(34) = (\tau(1), \tau(2), \tau(3), \tau(4), \tau(5)) = (15432) = \sigma^{-1}$

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

$\sigma \rightsquigarrow r$, $\tau \rightsquigarrow s$: $srs^{-1} = r^{-1}$ gruppo diedrale



D_5 agisce su $\{1,2,3,4,5\}$

$D_5 \longrightarrow S_5$

$s \longmapsto (25)(34)$

$r \longmapsto (12345)$

Sottogruppo derivato di S_n

In generale, vale:

$[(i,j),(j,k)] = (i\,k\,j)$ se i,j,k sono tre indici distinti

$\Rightarrow$ S_n' contiene tutti i 3-cicli

proposizione (1) $\langle \{(i,j)(k,l) \mid i\neq j, k\neq l\} \rangle = A_n$

(2) $\langle \{(i,j,k) \mid i,j,k \text{ distinti}\} \rangle = A_n$

DIMOSTRAZIONE

(1),(2) $\langle \dots \rangle \subseteq A_n \iff$ le doppie trasposizioni (risp. i 3-cicli) sono in A_n

Per l'altra inclusione:

(1) $\sigma \in A_n \Rightarrow \sigma = (\tau_1\tau_2)\cdots(\tau_{2k-1}\tau_{2k}) \in$ Sgp generato $(i,j)(k,l)$ $i\neq j, k\neq l$

(2) Basta far vedere che ogni $(i,j)(k,l)$ $i\neq j, k\neq l$ sta nel sottogruppo generato dai 3-cicli:

se $|\{i,j\}\cap\{k,l\}| = 2 \Rightarrow (i,j)(k,l) = id$ che è $(123)^3$

$|\{i,j\}\cap\{k,l\}| = 1 \Rightarrow (i,j)(j,l) = (i,l,j)$

$|\{i,j\}\cap\{k,l\}| = 0$, considero $(i,j)(k,l) = (i,j)(j,k)(j,k)(k,l) = (i,k,j)(j,l,k)$ □

Dunque per S_n':

- ogni $(i,j,k) \in S_n' \Rightarrow A_n = \langle\{(i,j,k)\}\rangle \subseteq S_n'$
- voglio dire che $S_n' \subseteq A_n \iff \forall x,y\ [x,y] \in A_n$
  $\iff \operatorname{sgn}(xyx^{-1}y^{-1}) = 1$ (facendo il conto o osservando che sgn è un omo verso un gruppo abeliano è t.c. $S_n' \subseteq \ker \operatorname{sgn}$)

cioè $S_n' = A_n$

corollario Dato H abeliano

$\operatorname{Hom}(S_n, H) = \operatorname{Hom}(S_n/S_n', H) = \operatorname{Hom}(S_n/A_n, H) = \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, H)$

Sottogruppi transitivi abeliani di S_n

Def. $G < S_n$ si dice transitivo se l'azione naturale di G su $\{1,\dots,n\}$ è transitiva, cioè se $\forall i,j \in \{1,\dots,n\}$ esiste $\sigma \in G$ t.c. $\sigma(i) = j$

proposizione Se $G < S_n$ è transitivo e abeliano, allora $|G| = n$

DIMOSTRAZIONE

Il lemma orbita stabilizzatore ci dice $n = |\mathrm{Orb}(i)| = \frac{|G|}{|\mathrm{Stab}(i)|}$

La tesi equivale a $\mathrm{Stab}_G(i)$ è banale $\forall i$

Siccome l'azione è transitiva, $\mathrm{Stab}(i)$ e $\mathrm{Stab}(j)$ sono coniugati $\forall i,j$

Poiché G è abeliano $\mathrm{Stab}(i) = \mathrm{Stab}(j)$ $\forall i,j$

Allora, presto $\sigma \in \mathrm{Stab}(1) = \mathrm{Stab}(2) = \dots = \mathrm{Stab}(n)$, si ha $\sigma = id$

$\Rightarrow |\mathrm{Stab}(\sigma)| = 1$ □

Oss $V_4 = \{id, \overset{\sigma_2}{(12)(34)}, \overset{\sigma_3}{(13)(24)}, \overset{\sigma_4}{(14)(23)}\} < S_4$

$V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\sigma_j(1) = j$

Classi di coniugio in A_n

Oss $\mathcal{C}_{A_n}(\sigma) = \{\tau\sigma\tau^{-1} \mid \tau \in A_n\} \subseteq \{\tau\sigma\tau^{-1} \mid \tau \in S_n\} = \mathcal{C}_{S_n}(\sigma)$

$$\#\mathcal{C}_{A_n}(\sigma) = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|S_n|/2}{|Z_{S_n}(\sigma) \cap A_n|} = \begin{cases} \dfrac{|S_n|/2}{|Z_{S_n}(\sigma)|/2} = \dfrac{|S_n|}{|Z_{S_n}(\sigma)|} = \#\mathcal{C}_{S_n}(\sigma) & \text{se } Z_{S_n}(\sigma) \not\subseteq A_n \\ \dfrac{|S_n|/2}{|Z_{S_n}(\sigma)|} = \dfrac{1}{2}\dfrac{|S_n|}{|Z_{S_n}(\sigma)|} = \dfrac{1}{2}\#\mathcal{C}_{S_n}(\sigma) & \text{se } Z_{S_n}(\sigma) \subseteq A_n \end{cases}$$

Nel primo caso, $\mathcal{C}_{A_n}(\sigma) = \mathcal{C}_{S_n}(\sigma)$

Nel secondo caso, $\mathcal{C}_{A_n}(\sigma) \cup \mathcal{C}_{A_n}(\tau\sigma\tau^{-1}) = \mathcal{C}_{S_n}(\sigma)$ con τ permutazione dispari.

proposizione Siano $\sigma \in S_n$, $C = \mathcal{C}_{S_n}(\sigma)$, $C' = \mathcal{C}_{A_n}(\sigma)$. Supponiamo $|C'| = \frac{1}{2}|C|$

Sia $\tau \in S_n \setminus A_n$ e sia $\sigma' = \tau\sigma\tau^{-1}$

(1) $\#\mathcal{C}_{A_n}(\sigma') = \#\mathcal{C}_{A_n}(\sigma)$

(2) $\mathcal{C}_{A_n}(\sigma) \cap \mathcal{C}_{A_n}(\sigma') = \emptyset$

(3) $\mathcal{C}_{A_n}(\sigma) \cup \mathcal{C}_{A_n}(\sigma') = C$

DIMOSTRAZIONE

Oss $Z_{S_n}(\sigma') = \{\rho \mid \rho\sigma'\rho^{-1} = \sigma'\} = \{\rho \mid \rho\tau\sigma'\tau^{-1}\rho^{-1} = \tau\sigma\tau^{-1}\} = \{\rho \mid (\tau^{-1}\rho\tau)\sigma(\tau^{-1}\rho\tau)^{-1} = \sigma\} =$
$= \{\rho \mid \tau^{-1}\rho\tau \in Z_{S_n}(\sigma)\} = \{\rho \mid \rho \in \tau Z_{S_n}(\sigma)\tau^{-1}\} = \tau Z_{S_n}(\sigma)\tau^{-1}$

(1) $\#\mathcal{C}_{A_n}(\sigma') = \dfrac{|A_n|}{\#Z_{A_n}(\sigma')}$

$Z_{A_n}(\sigma') = Z_{S_n}(\sigma') \cap A_n = \tau Z_{S_n}(\sigma)\tau^{-1} \cap A_n =$

$= \tau Z_{S_n}(\sigma)\tau^{-1} \cap \tau A_n \tau^{-1} = \tau(Z_{S_n}(\sigma) \cap A_n)\tau^{-1} = \tau Z_{A_n}(\sigma)\tau^{-1}$

$\Rightarrow \#\mathcal{C}_{A_n}(\sigma') = \dfrac{|A_n|}{\#Z_{A_n}(\sigma')} = \dfrac{|A_n|}{\#Z_{A_n}(\sigma)} = \#\mathcal{C}_{A_n}(\sigma)$

(2) $\Rightarrow$ (3) per cardinalità

(2) Se $\mathcal{C}_{A_n}(\sigma) \cap \mathcal{C}_{A_n}(\sigma') \neq \emptyset \Rightarrow \mathcal{C}_{A_n}(\sigma) = \mathcal{C}_{A_n}(\sigma')$

Prendiamo $\rho \in S_n$: $\rho\sigma\rho^{-1} \in \mathcal{C}_{A_n}(\sigma)$

se $\rho \in A_n$: ok

se $\rho \notin A_n$: $\rho = \rho'\tau$ dove $\rho' \in A_n$

e $\rho\sigma\rho^{-1} = \rho'\tau\sigma\tau^{-1}\rho'^{-1} = \rho'\sigma'\rho'^{-1} \in \mathcal{C}_{A_n}(\sigma)$ ↯ □

esempio $\sigma \in S_5$ $\quad \mathcal{C}_{S_5}(\sigma) = \{$permutazioni con la stessa decomposizione in cicli$\}$

id	1	(12)	10
(12)(34)	15	(1234)	30
(123)	20	(123)(45)	20
(1234)	24		

In S_5

id	1
(12)(34)	15
(123)	20
(12345)	24

In A_5

id	1
(12)(34)	15
(123)	20
(12345)	12
(21345)	12

Centralizzatori in S_n

Strategia generale: (1) Calcolare $\#Z_{S_n}(\sigma)$ via orbita-stabilizzatore
(2) Indovinare il n° giusto di elementi

Oss Fissata $\sigma \in S_n$
$\{\tau\sigma\tau \mid \tau \in S_n\}$ è l'insieme delle permutazioni con la stessa decomposizione in cicli di σ

Oss I k-cicli in S_n sono $\binom{n}{k} \cdot \frac{k!}{k} = (k-1)!\binom{n}{k}$

esempio Sia $\sigma = (1\,2\,3)$ in S_{10}
$\#Orb(\sigma) = \#\{3\text{-cicli}\} = \binom{10}{3} 2!$
$Stab(\sigma) = \{\tau \mid \tau\sigma\tau^{-1} = \sigma\} = \{\tau \mid \tau\sigma = \sigma\tau\} = Z_{S_n}(\sigma)$
$\frac{|S_n|}{|Z_{S_{10}}(\sigma)|} = |Orb| \Rightarrow \frac{10!}{\#Z_{S_{10}}(\sigma)} = \frac{10!}{3!\cdot 7!} \cdot 2 \longrightarrow \#Z_{S_{10}}(\sigma) = 3 \cdot 7!$

$Z_{S_{10}}(\sigma) = \langle\sigma\rangle \times Stab(\{1,2,3\})$

esempio $Z_{S_5}((1\,2\,3\,4\,5))$
$\#Z_{S_5}(\sigma) = \frac{|S_5|}{|Orb(\sigma)|} = \frac{5!}{4!} = 5$
$\Rightarrow Z_{S_5}(\sigma) = \langle\sigma\rangle$

esempio $Z_{S_9}((1\,2\,3\,4)(5\,6\,7)(8\,9))$
$\#Orb(\sigma) = \binom{9}{4} 3! \binom{5}{3} 2! \cdot \binom{2}{2} \cdot 1!$

$\Rightarrow \#Z_{S_9}(\sigma) = \frac{9!}{\frac{9!}{5!4!} 3! \cdot \frac{5!}{3!2!} 2!} = 24$

$\sigma_1 = (1\,2\,3\,4), \sigma_2 = (5\,6\,7), \sigma_3 = (8\,9)$
$Z_{S_9}(\sigma) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Lemma normalizzatore-centralizzatore Dato $H < G$:
(1) $Z_G(H) \trianglelefteq N_G(H)$
(2) $N_G(H)/Z_G(H) \hookrightarrow Aut(H)$

DIMOSTRAZIONE
$f : N_G(H) \longrightarrow Aut(H)$
$g \longmapsto (\varphi_g)|_H : H \xrightarrow{\sim} H$
$\ker f = \{g : \varphi_g|_H = id\} = \{g : \varphi_g(h) = h \ \forall h\} = \{g : ghg^{-1} = h \ \forall h \in H\} = Z_G(H)$ □

esempio $\sigma = (123)(456)(789)$

$C = Z_{S_9}(\sigma) \cong (\mathbb{Z}/3\mathbb{Z})^3 \rtimes S_3$

(1) $\#C = \dfrac{\#S_9}{\#\mathcal{O}_{S_9}(\sigma)} = \dfrac{9!}{\frac{1}{3!}\binom{9}{3}\cdot 2\cdot\binom{6}{3}\cdot 2\cdot\binom{3}{3}\cdot 2} = 3!\cdot 3^3$

(2) $(123)\in C$, $(456)\in C$, $(789)\in C$

$N := \langle (123), (456), (789)\rangle \cong (\mathbb{Z}/3\mathbb{Z})^3$ (σ_1, σ_2, σ_3)

$\tau\sigma\tau^{-1} = \sigma \iff \tau \in Z_{S_9}(\sigma)$

$(\tau(1)\,\tau(2)\,\tau(3))(\tau(4)\,\tau(5)\,\tau(6))(\tau(7)\,\tau(8)\,\tau(9))$

Ad esempio, $\tau = (14)(25)(36) \in C$

oppure $\rho = (147)(258)(369)$

Speranza: (i) $H = \langle \tau, \rho\rangle \cong S_3$

(ii) $N \cap H = \{id\}$

(iii) $N \lhd C$

(iv) $NH = C$

(i) $\tau\rho\tau^{-1} \stackrel{?}{=} \rho^{-1}$

$(417)(528)(639) = (369)(258)(147)$

(ii) $|N\cap H| \in \{1,3\}$

Se fosse $|N\cap H| = 3$, sarebbe $\{id, \rho, \rho^{-1}\}$

$\Rightarrow \rho \in N = \{(123)^a(456)^b(789)^c\}$ ↯

(iv) $\langle N, H\rangle \supseteq N\cdot H \quad |NH| = 27\cdot 3!$

$\Rightarrow NH = C$, $\langle N, H\rangle = C$

(iii) Sia $M = N_C(N)$: voglio vedere che $M = C$

Intanto $N \subset M$. Basta mostrare che $H \subset M$ (perché allora $C = NH \subseteq M$) e quindi basta $\rho, \tau \in M$

$\tau\sigma_1\tau^{-1} = \sigma_2 \quad \tau\sigma_2\tau^{-1} = \sigma_1 \quad \tau\sigma_3\tau^{-1} = \sigma_3$

$\rho\sigma_1\rho^{-1} = \sigma_2 \quad \rho\sigma_2\rho^{-1} = \sigma_3 \quad \rho\sigma_3\rho^{-1} = \sigma_1$

$\tau N\tau^{-1} \stackrel{?}{=} N$

$\langle \tau\sigma_1\tau^{-1}, \tau\sigma_2\tau^{-1}, \tau\sigma_3\tau^{-1}\rangle = \langle \sigma_2, \sigma_1, \sigma_3\rangle = N$

$\rho N\rho^{-1} = \langle \sigma_2, \sigma_3, \sigma_1\rangle = N$

$\Rightarrow N \lhd C$

$\Rightarrow C \cong N \rtimes_\varphi H \cong (\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\psi S_3$

$\sigma_1 \longmapsto ((1,0,0), id)$

$\sigma_2 \longmapsto ((0,1,0), id)$

$\sigma_3 \longmapsto ((0,0,1), id)$

$\tau \longmapsto ((0,0,0), (12))$

$\rho \longmapsto ((0,0,0), (123))$

$\psi : S_3 \longrightarrow \mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^3)$

$(12) \longmapsto \begin{pmatrix} (1,0,0)\mapsto(0,1,0) \\ (0,1,0)\mapsto(1,0,0) \\ (0,0,1)\mapsto(0,0,1)\end{pmatrix}$

$(123) \longmapsto \begin{pmatrix} (1,0,0)\mapsto(0,1,0) \\ (0,1,0)\mapsto(0,0,1) \\ (0,0,1)\mapsto(1,0,0)\end{pmatrix}$

esempio $\sigma = (1,2,\dots,7) \in S_7$

$N_{S_7}(\langle\sigma\rangle)/Z_{S_7}(\sigma) \hookrightarrow Aut(\langle\sigma\rangle)$ dal lemma normalizzatore/centralizzatore

$$\#Z_{S_7}(\sigma) = \frac{\#S_7}{\#Cl_{S_7}(\sigma)} = \frac{7!}{6!} = 7 \implies Z_{S_7}(\sigma) = \langle\sigma\rangle$$

$$Aut(\langle\sigma\rangle) \cong Aut(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/7\mathbb{Z}^* \cong \mathbb{Z}/6\mathbb{Z}$$

$\tau\sigma\tau^{-1} = (\tau(1), \tau(2), \tau(3), \tau(4), \tau(5), \tau(6), \tau(7)) = \begin{cases} \sigma^2 \\ \sigma^{-1} \end{cases}$

Prendiamo $\tau_1 = (1)(235)(476)$ di ord 3

$\tau_2 = (1)(2,7)(3,6)(5,4)$ di ord 2

Altrimenti, consideriamo l'azione di coniugio di S_7 su $X := \{H < S_7\}$

$$g \cdot H = gHg^{-1}$$

$N_{S_7}(\langle\sigma\rangle) = Stab(\langle\sigma\rangle)$ per questa azione

$$\implies \#N = \frac{\#S_7}{\#Orb(\langle\sigma\rangle)} = \frac{7!}{5!} = 7 \cdot 6 = 42$$

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

$\implies Orb(\langle\sigma\rangle) = \{H < S_7$ generati da un 7 ciclo$\}$

$$\#Orb(\langle\sigma\rangle) = \frac{\#\text{7-cicli}}{\phi(7)} = \frac{6!}{6} = 5!$$

Quindi $N/Z_{S_7}(\sigma) \cong \mathbb{Z}/7\mathbb{Z}^*$ per cardinalità

l'isomorfismo veniva da: dato $n \in N$,

lo mando nel coniugio per n ristretto al sottogruppo $\langle\sigma\rangle$

$$N \longrightarrow Aut(\langle\sigma\rangle) \cong (\mathbb{Z}/7\mathbb{Z})^* = \langle 3\rangle$$

$$n \longmapsto \varphi_n$$

l'automorfismo che corrisponde a 3 è $\langle\sigma\rangle \longrightarrow \langle\sigma\rangle : \sigma \longmapsto \sigma^3$

Sto cercando $n \in S_7$ t.c. $n\sigma n^{-1} = \sigma^3$

$$(n(1)\ n(2)\ \cdots\ n(7)) = (1\ 4\ 7\ 3\ 6\ 2\ 5)$$

Prendo $n = (2\ 4\ 3\ 7\ 5\ 6)$

Ora so che

- $Z_{S_7}(\sigma) = \langle\sigma\rangle \lhd N_{S_7}(\langle\sigma\rangle)$
- $n \in N \implies \langle n\rangle \cong \mathbb{Z}/6\mathbb{Z} < N_{S_7}(\langle\sigma\rangle)$
- per cardinalità: $\langle\sigma\rangle \cap \langle n\rangle = \{id\}$, $\langle\sigma\rangle\langle n\rangle = N$

Quindi $N \cong \langle\sigma\rangle \times_\varphi \langle n\rangle$ dentro S_7

$\cong \mathbb{Z}/7\mathbb{Z} \times_\psi \mathbb{Z}/6\mathbb{Z}$ dove $\psi : \mathbb{Z}/6\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/7\mathbb{Z})$

$1 \longmapsto (x \longmapsto 3x)$

(dove si usano gli isomorfismi $\langle\sigma\rangle \xrightarrow{\sim} \mathbb{Z}/7\mathbb{Z}$, $\sigma \longmapsto 1$; $\langle n\rangle \xrightarrow{\sim} \mathbb{Z}/6\mathbb{Z}$, $n \longmapsto 1$)

Sottogruppi di S_n di indice n (per $n \geq 5$)

$H < S_n$, $[S_n : H] = n \Rightarrow H \cong S_{n-1}$

Sia $\psi : S_n \longrightarrow Big(S_n/H)$ l'azione sulle classi laterali

$g \cdot g_1 H = g g_1 H$

Questo ψ è un isomorfismo: tra gruppi della stessa cardinalità

$\ker \psi = \begin{cases} id & A_n \\ x & S_n \setminus A_n \end{cases} \Rightarrow \psi$ iniettiva

$\psi(H)$ è un sottogruppo di $Big(S_n/H)$ di ordine $(n-1)!$

e $\psi(H) \subseteq \{\sigma \in Big(G/H) : \sigma(H) = H\}$

$h \in H : \psi(h) :$ $H \longmapsto H$, $g_1 H \to h g_1 H$, $\dots$, $g_{n-1} H \to h g_{n-1} H$

l'inclusione e l'uguaglianza di cardinalità dice che $\psi(H) = \{\sigma \in Big(G/H) : \sigma(H) = H\} \cong S_{n-1}$

Sottogruppi di S_5 isomorfi a D_5

Devono contenere elementi di ordine 5

$G < S_5$, $G \cong D_5$, $\sigma \in G$ un 5-ciclo

In D_5 il 5-Sylow è normale $\rightarrow \langle\sigma\rangle \lhd G \Rightarrow G \subseteq N_{S_5}(\sigma)$

$N_{S_5} \cong \mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$

Quanti sgp $\cong D_5$ contiene $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ $\quad \varphi : \mathbb{Z}/4\mathbb{Z} \longrightarrow (\mathbb{Z}/5\mathbb{Z})^*$, $1 \longmapsto 2$

$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \supseteq H$

$P_5 \subseteq H$

Tali H sono in biezione con i sottogruppi (di indice 2) $\quad \dfrac{\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}}{\mathbb{Z}/5\mathbb{Z}} \cong \mathbb{Z}/4\mathbb{Z}$ di indice 2

$\#\{D_5 \text{ in } S_5\} = \#\{\text{sgp di } S_5 \text{ di ord } 5\} = \dfrac{4!}{4} = 6$

esempio Trovare minimo n tale che S_n contiene un sottogruppo di ordine 21

Se $G \cong \mathbb{Z}/21\mathbb{Z}$, $n \geq 10$: mi servono un elemento di ord 7 ($n \geq 7$) e uno di ord 3 che commutano

Se calcolo il centralizzatore di un 7-ciclo in S_7, S_8, S_9 ha ordine $7, 7, 14 \longrightarrow$ non ci sono elementi di ordine 3

In S_{10} invece sì : $\min n = 10$

In alternativa, mi serve σ di ord 21 : $\sigma = \sigma_1 \cdots \sigma_r$ decomposizione in cicli

$21 = mcm(\ell(\sigma_1), \dots, \ell(\sigma_r))$: il minimo è $21 = mcm(3, 10) \longrightarrow n \geq 10$

Se invece G è non abeliano di ordine 21 : se $G \hookrightarrow S_n$,

G ha un elemento di ordine $7 \Rightarrow n \geq 7$

Sappiamo che $N_{S_7}(\langle(12\dots7)\rangle) \cong \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/6\mathbb{Z} \supseteq \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

Oss $C < B \Rightarrow A \rtimes_\varphi C \subseteq A \rtimes_\varphi B$

In generale $D \rtimes_\varphi B$ con $D \subseteq A$ potrebbe non avere senso (funziona se $\varphi(B)$ preserva D)

Oss $N_{S_7}(\langle\sigma\rangle)$ ha ordine $2 \cdot 21 \Rightarrow$ contiene un sottogruppo di ordine 21

Semplicità di A_n

Def. Un gruppo G è semplice se gli unici sottogruppi normali sono $\{e\}$ e G stesso

Oss G abeliano è semplice $\iff G \cong \mathbb{Z}/p\mathbb{Z}$ per p primo (o $|G|=1$)

Lemma $N \triangleleft G$, $g \in G$ t.c. $(\text{ord}\, g, [G:N]) = 1 \Rightarrow g \in N$

DIMOSTRAZIONE

$\pi : G \longrightarrow G/N$, $\ker \pi = N$

$g \longmapsto x$ con $\text{ord}\, x \mid \text{ord}\, g$ e $\text{ord}\, x \mid [G:N]$

$\Rightarrow \text{ord}\, x = 1 \Rightarrow x = N \Rightarrow g \in N$ □

Proposizione A_5 è semplice

DIMOSTRAZIONE

Sia $N \triangleleft A_5$ e $i = [A_5 : N]$

- Se $3 \nmid i \Rightarrow$ tutti i 3-cicli sono in $N \Rightarrow N = A_5$
- Se $3 \mid i$, $\#N = \frac{\#A_5}{i} \Rightarrow \#N \mid 20$

Oss Un sottogruppo normale è unione di classi di coniugio

Se N contiene un 5-ciclo (12 elementi) $\Rightarrow \#N = 20$

Ma se $\#N = 20$ contiene un el. di ord 2, cioè $(ab)(cd)$

$\Rightarrow$ contiene la classe di coniugio di 15 el. $\Rightarrow \#N \geq 1+12+15$ ↯

Se N non contiene un 5-ciclo, $5 \nmid \#N \Rightarrow \#N \mid 4$,

o $\#N = 1$, cioè $N = \{e\}$, oppure $2 \mid \#N$

quindi ha un el. di ord 2, ma la classe ha 15 elementi ↯ □

Oss Sia $H \triangleleft A_n$, che contiene un 3-ciclo, allora $H = A_n$

DIMOSTRAZIONE

Mostriamo che H contiene tutti i 3-cicli

$$\#\mathcal{O}_{A_n}((1,2,3)) = \frac{\#A_n}{\#Z_{A_n}((1,2,3))} = \frac{\#S_n/2}{\#(Z_{S_n}((1,2,3)) \cap A_n)} = \frac{\#S_n/2}{\#Z_{S_n}((1,2,3))/2} =$$

($(4,5) \in Z_{S_n}((1,2,3))$)

$$= \frac{\#S_n}{\#Z_{S_n}((1,2,3))} = \#\mathcal{O}_{S_n}((1,2,3)) \Rightarrow \mathcal{O}_{A_n}((1,2,3)) = \mathcal{O}_{S_n}((1,2,3)) = \{\text{tutti i 3-cicli}\}$$ □

proposizione A_n è semplice per $n \geq 5$

DIMOSTRAZIONE

Assumiamo di sapere che A_6 è semplice

Per induzione su n

Sia $H \triangleleft A_{n+1}$ con $n \geq 6$. Consideriamo

$K_i = \{\sigma \in A_{n+1} \mid \sigma(i) = i\} \cong A_n$

allora $H \cap K_i \triangleleft K_i \cong A_n$, che è semplice

Oss $N \triangleleft G$, $K < G \Rightarrow N \cap K \triangleleft K$

Infatti $k(N \cap K)k^{-1} \subseteq N, K \Rightarrow k(N \cap K)k^{-1} \triangleleft K$

Siccome K_i è semplice, $H \cap K_i \cong \begin{cases} K_i \\ \{e\} \end{cases}$

Se $H \cap K_i = K_i$, allora $K_i \subseteq H \Rightarrow H$ contiene un 3-ciclo $\Rightarrow H = A_{n+1}$

Se invece $H \cap K_i = \{e\}$ per ogni $i = 1, \dots, n+1$, procediamo così:

supponiamo per assurdo $H \neq \{e\}$ e scegliamo $\sigma \in H \setminus \{e\}$

Sia $j = \sigma(1)$ e scegliamo $\tau = (j, k, \ell)$ un 3-ciclo con $j, k, \ell \neq 1$

Consideriamo $\sigma(\tau\sigma^{-1}\tau^{-1}) \in H$ ($\sigma \in H$, $\tau\sigma^{-1}\tau^{-1} \in H$)

$(\sigma\tau\sigma^{-1})\tau^{-1}$ è prodotto di 2 3-cicli, quindi muove al massimo 6 elementi.

Siccome siamo in A_{n+1}, $n \geq 6$, ha un punto fisso

Per l'ipotesi del nostro caso, $\sigma\tau\sigma^{-1}\tau^{-1} = id$ (l'unica permutazione in H con punti fissi)

$\Rightarrow \sigma\tau = \tau\sigma$

$\sigma\tau(1) = \tau\sigma(1) \Rightarrow j = \sigma(1) = \tau(j)$ ↯ □

Oss $N \triangleleft G$, $|N| = 2 \Rightarrow N \subseteq Z(G)$

DIMOSTRAZIONE

$N = \{e, g\}$ $\quad hNh^{-1} = N$

$\{e, hgh^{-1}\} = \{e, g\} \Rightarrow hgh^{-1} = g \ \forall h \Rightarrow g \in Z(G)$ □

Lemma $Z(S_n) = \{e\}$

DIMOSTRAZIONE

Sia $\sigma \in Z(S_n) \setminus \{id\}$: esistono $x \neq y \in \{1, \dots, n\}$ t.c. $\sigma(x) = y$

Sia $z \in \{1, \dots, n\} \setminus \{x, y\}$ e sia $\tau = (yz)$.

Allora $(\sigma\tau)(x) = y$ e $(\tau\sigma)(x) = z$ ↯ □

corollario Per $n \geq 5$, i sottogruppi normali di S_n sono $\{e\}, A_n, S_n$

DIMOSTRAZIONE

$N \triangleleft S_n \Rightarrow N \cap A_n \triangleleft A_n$ $\begin{cases} N \cap A_n = A_n \\ N \cap A_n = \{e\} \end{cases}$

(1) $A_n \subseteq N \subseteq S_N \Rightarrow N = A_n$ o $N = S_n$

(2) $1 = \#(N \cap A_n) = \begin{cases} \#N \Rightarrow N = \{id\} \\ \frac{1}{2}\#N \Rightarrow \#N = 2 \end{cases}$ ↯

□

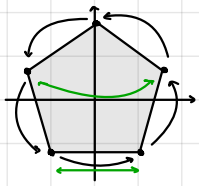
Gruppo diedrale

Def. Fissiamo $n \geq 3$ un intero.

Il gruppo diedrale su n elementi D_n è il gruppo delle isometrie del piano che mandano in sè i vertici di un n-agono regolare centrato nell'origine

NOTA Alcuni denotano con D_{2n} lo stesso gruppo

esempio

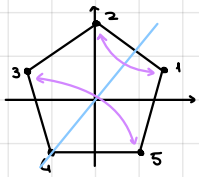


id, r = rotazione di $\frac{2\pi}{n}$,
s = simmetria rispetto all'asse verticale

Oss D_n è effettivamente un sottogruppo delle isometrie del piano:
$id \in D_n$, la composizione anche (se σ_1 e σ_2 mandano i vertici nei vertici, anche $\sigma_1 \circ \sigma_2$ lo fa) e l'inversa pure.
Chiamiamo $v_1, \dots, v_n$ i vertici. Prendo $\sigma \in D_n$
$\{\sigma(v_1), \dots, \sigma(v_n)\} = \{v_1, \dots, v_n\} \Rightarrow \sigma$ è una permutazione di $v_1, \dots, v_n$
Quindi anche l'inversa lo è e manda vertici in vertici.

Alcuni elementi di D_n: $id, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}$

esempio

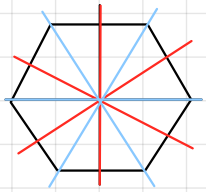


sr : $1 \mapsto 2$
$2 \mapsto 1$
$3 \mapsto 5$
$4 \mapsto 4$
$5 \mapsto 3$

In generale, sr^k è la simmetria rispetto ad un opportuno asse

Oss $\det(sr^k) = \det(s) \cdot \det(r)^k = (-1)(1)^k = -1$
$s = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$

Oss



Nel caso n pari, ci sono due tipi diversi di simmetrie

proposizione $|D_n| = 2n$

DIMOSTRAZIONE
Prendiamo $\sigma \in D_n$ e vediamo "cosa fanno" $\sigma(v_1)$ e $\sigma(v_2)$, dove v_1 e v_2 sono due vertici adiacenti [v_1, v_2 sono base di $\mathbb{R}^2$ e σ è un'applicazione lineare: se conosco $\sigma(v_1)$ e $\sigma(v_2)$ ho determinato σ]
$\sigma(v_1) = v_i$ $\sigma(v_2) = v_{i+1}$ o v_{i-1}
Ci sono $\leq n$ scelte per $\sigma(v_1)$ e ≤ 2 scelte per $\sigma(v_2)$ una volta fissato $\sigma(v_1)$
$\Rightarrow |D_n| \leq 2n$
D'altra parte: $1, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$ sono $2n$ elementi
Sono distinti: • $r^i \neq sr^j$ (det diverso)
• r^i distinti $(0 \leq i \leq \text{ord}(r) - 1)$
• sr^i distinti: $sr^i = sr^j \iff r^i = r^j$
(oppure guardo i punti fissi)

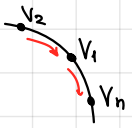
□

Oss $D_n = \langle s, r \rangle$ $\quad \langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ $\quad \langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$

proposizione $srs^{-1} = r^{-1}$

DIMOSTRAZIONE (1)

Sia v_1 un vertice fissato da s



$srs^{-1}(v_1) = sr(v_1) = s(v_2) = v_n$

$srs^{-1}(v_2) = sr(v_n) = s(v_1) = v_1$

$\Rightarrow srs^{-1}$ e r^{-1} coincidono su v_1 e v_2 $\Rightarrow srs^{-1} = r^{-1}$

DIMOSTRAZIONE (2)

$$r = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \qquad r^{-1} = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \qquad s = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$$

$srs^{-1} = srs = r^{-1}$ □

Sottogruppi di D_n

$R := \langle r \rangle$ sottogruppo delle rotazioni

$H \subseteq R$: per ogni $d \mid n$ esiste un unico sottogruppo di ordine d, $R_d = \langle r^{\frac{n}{d}} \rangle$

proposizione $H \leq G$, $[G:H] = 2 \Rightarrow H$ normale

DIMOSTRAZIONE

Tutte le classe laterali hanno la stessa cardinalità

Sono H e $G \setminus H$ (sia a dx che a sx) $\Rightarrow H$ normale

In alternativa, $gHg^{-1} = H \iff gH = Hg$

- Se $g \in H$: $gH = H = Hg$
- Se $g \notin H$: $gH = G \setminus H = Hg$ □

Quindi $R \triangleleft D_n$ perché ha indice 2.

def. Dato G gruppo e $H < G$, il normalizzatore di H in G è

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

Proprietà

In generale

- $N_G(H) < G$
- $H < N_G(H)$: $hHh^{-1} = H \quad \forall h \in H$
- $H \triangleleft N_G(H)$
- $N_G(H)$ è il massimo (per inclusione) sottogruppo di G in cui H è normale

  (Se $K < G$, $K \geq H$, e $H \triangleleft K$, allora $\forall k \in K$ si ha $kHk^{-1} = H$

  $\Rightarrow k \in N_G(H) \Rightarrow K \subseteq N_G(H)$)

Oss $H \triangleleft G \iff N_G(H) = G$

Oss La funzione $\varphi_s : D_n \longrightarrow D_n$ il coniugio per s è un automorfismo
$x \longmapsto sxs^{-1}$

$\varphi_s(r^k) = \varphi_s(r)^k$, cioè $sr^k s^{-1} = (srs^{-1})^k$

Quindi, alternativamente, $R \lhd D_n \iff N_{D_n}(R) = D_n$

$N_{D_n}(R) \supseteq R$

ma se $N_{D_n}(R)$, perché $SRS^{-1} = S\{r^k\}S^{-1} = \{sr^k s^{-1}\} = \{(srs^{-1})^k\} = \{(r^{-1})^k\} = R$

Allora $N_{D_n}(R) = D_n$

Lemma $|H_1H_2| = \dfrac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}$

DIMOSTRAZIONE

$\varphi : H_1 \times H_2 \longrightarrow H_1H_2$

$(h_1, h_2) \longmapsto h_1h_2$

Fissato $g = h_1h_2 \in H_1H_2$, contiamo le coppie (h_1', h_2') t.c. $\varphi((h_1', h_2')) = g$

$h_1'h_2' = h_1h_2 \iff \underbrace{h_1^{-1}h_1'}_{\in H_1} = \underbrace{h_2(h_2')^{-1}}_{\in H_2} \in H_1 \cap H_2$

$(h_1' = h_1x, h_2' = x^{-1}h_2) \longleftarrow\!\shortmid x$

C'è una bigezione fra $\varphi^{-1}(h_1h_2)$ e $H_1 \cap H_2$

$\Rightarrow |H_1H_2| = \dfrac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}$ □

Lemma $H_1, H_2 < G$ Vale che $H_1H_2 < G \iff H_1H_2 = H_2H_1$

DIMOSTRAZIONE (gruppi finiti)

$\Leftarrow$: L'ipotesi è $\forall h_1 \in H_1, \forall h_2 \in H_2 \ \exists h_1' \in H_1, \exists h_2' \in H_2$ t.c. $h_1h_2 = h_2'h_1'$ e viceversa.

Verifichiamo che H_1H_2 è chiuso per prodotto

$(h_1h_2) \cdot (h_1'h_2') = h_1(h_2h_1')h_2' = \underbrace{h_1h_1''}_{\in H_1}\underbrace{h_2''h_2'}_{\in H_2} \in H_1H_2$

$\Rightarrow$: Se H_1H_2 è un sottogruppo, $\forall h_1 \in H_1, \forall h_2 \in H_2$, contiene $h_1^{-1} \cdot h_2^{-1}$

$\Rightarrow (h_1^{-1}h_2^{-1})^{-1} \in H_1H_2 \Rightarrow h_2h_1 \in H_1H_2 \Rightarrow H_2H_1 \subseteq H_1H_2$

Poiché hanno la stessa cardinalità, $H_2H_1 = H_1H_2$ □

Sottogruppi H di D_n, $H \not\subseteq R$:

Consideriamo la proiezione $\pi : D_n \longrightarrow D_n/R \cong \mathbb{Z}/2\mathbb{Z}$

$(D_n \xrightarrow{\det} \{\pm 1\})$

$\pi(H) = \mathbb{Z}/2\mathbb{Z}$ (se fosse $\pi(H) = \{0\}$, avrei $H \subseteq \ker\pi = R$)

Studiamo $H \cap R = H \cap \ker\pi = \ker(\pi_{|H} : H \longrightarrow \mathbb{Z}/2\mathbb{Z})$

Per il I teorema di omomorfismo. $H/H\cap R \cong \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow \dfrac{|H|}{|H\cap R|} = 2 \Rightarrow |H \cap R| = \dfrac{|H|}{2}$ e $H \cap R = \langle r^d \rangle$ $|H\cap R| = \dfrac{n}{d}$ con $d \mid n$

Ora $H \cap R \leq H$, cioè $H = \langle r^d, sr^h \rangle$

Verifica: $|\langle r^d, sr^h \rangle| = 2\,|\langle r^d \rangle| = 2\frac{n}{d}$

Affermo che $\langle r^d, sr^h \rangle = \langle sr^h \rangle \langle r^d \rangle := \{ g_1 g_2 \mid g_1 \in \langle sr^h \rangle, g_2 \in \langle r^d \rangle \}$

$\langle r^d, sr^h \rangle \leq \langle r^d \rangle < sr^h >$

Basta mostrare

- $r^d, sr^h \in \langle r^d \rangle \langle sr^h \rangle$: ovvio
- $\langle r^d \rangle \langle sr^h \rangle$ è un gruppo $\iff \langle r^d \rangle \langle sr^h \rangle = \langle sr^h \rangle \langle r^d \rangle$

  $\iff R = \langle sr^h \rangle^{-1} R \langle sr^h \rangle$ vero perché $R \lhd D_n$

L'uguaglianza segue per cardinalità: infatti il termine a dx ha cardinalità $\frac{n}{d} \cdot 2$ e il termine a sx ha cardinalità multipla di $\frac{n}{d}$, quindi coincidono e sono $2\frac{n}{d}$

Lemma $C < N < G$ con $N \lhd G$ e C caratteristico in N allora $C \lhd G$

DIMOSTRAZIONE

Un sgp normale $N \lhd G$ è un sgp t.c. $\forall \varphi_g \in \mathrm{Inn}\, G$ soddisfa $\varphi_g(N) = N$. Un sgp $C < N$ è caratteristico se $\forall \psi \in \mathrm{Aut}\, N$ vale $\psi(C) = C$

Devo dire che $\forall \varphi_g \in \mathrm{Inn}\, G$ vale $\varphi_g(C) = C$

$\varphi_g|_N : N \longrightarrow N$ $(N \lhd G)$ è un automorfismo di N

$\varphi_g(C) = \varphi_g|_N(C) = C$ □

In D_n: $\langle r^d \rangle < R \lhd D_n$ e $\langle r^d \rangle$ è caratteristico (perché è l'unico del suo ordine)

Quindi $\langle r^d \rangle \lhd D_n$

A mano, basta mostrare $r^h \langle r^d \rangle r^{-h} = \langle r^d \rangle$

$sr^h \langle r^d \rangle (sr^h)^{-1} = \{ sr^h r^{dk} r^{-h} s \} = \{ sr^{dk} s \} = \{ r^{-dk} \} = \langle r^d \rangle$

Oss $\langle r^d, sr^h \rangle = \langle r^d, sr^{h+d} \rangle = \langle r^d, sr^{h+2d} \rangle = \dots$

Posso assumere $0 \leq h < d$

Oss $H_1 = \langle r^{d_1}, sr^{h_1} \rangle \stackrel{?}{=} \langle r^{d_2}, sr^{h_2} \rangle = H_2$ $\quad d_1, d_2 \mid n$

$H_1 = H_2 \Rightarrow H_1 \cap R = \langle r^{d_1} \rangle = H_2 \cap R = \langle r^{d_2} \rangle \Rightarrow d_1 = d_2$

Gli elementi di $H_1 = \langle sr^{h_1} \rangle \langle r^{d_1} \rangle$ sono $1 \cdot r^{kd_1}$, $sr^{h_1} \cdot r^{kd_1}$

e gli elementi di H_2 sono $1 \cdot r^{kd_1}$, $sr^{h_2} \cdot r^{kd_1}$

$sr^{h_1} \cdot r^{kd_1} = sr^{h_2} \cdot r^{k'd_1} \Rightarrow h_1 + kd_1 \equiv h_2 + k'd_1 \pmod n$

$\Rightarrow h_1 + kd_1 \equiv h_2 + k'd_1 \pmod{d_1} \Rightarrow h_1 = h_2 \pmod{d_1} \Rightarrow h_2 = h_1$

Quindi, riassumendo:

Proposizione I sottogruppi di D_n sono nella forma:

(1) $\langle r^d \rangle$ con $d \mid n$

(2) $\langle r^d, sr^h \rangle$ con $d \mid n$ e $0 \leq h < d$

Tali sottogruppi sono tutti distinti.

Ci chiediamo se $\langle r^d, sr^h \rangle$ sia un sottogruppo normale

Oss $H \triangleleft G \iff N_G(H) = G \iff N_G(H)$ contiene un insieme $g_1, \dots, g_n$ di generatori di G
$\iff g_i H g_i^{-1} = H \quad \forall i = 1, \dots, n$

Oss $h\langle g_1, \dots, g_n \rangle h^{-1} = \langle hg_1h^{-1}, \dots, hg_nh^{-1} \rangle$

Ora:

$$r\langle r^d, sr^h \rangle r^{-1} = \langle r^d, rsr^h r^{-1} \rangle \overset{rs = sr^{-1}}{=} \langle r^d, sr^{h-2} \rangle = \langle r^d, sr^h \rangle$$

$\iff h \equiv h-2 \pmod d \iff 2 \equiv 0 \pmod d$

Se $d = 1$: $\langle r, s \rangle = D_n$

$d = 2$ (n pari) : $\langle r^2, s \rangle, \langle r^2, sr \rangle$

$$s\langle r^d, sr^h \rangle s^{-1} = \langle r^{-d}, ssr^h s^{-1} \rangle = \langle r^d, sr^{-h} \rangle = \langle r^d, sr^h \rangle$$

$\iff h \equiv -h \pmod d$ soddisfatto se $d = 1, 2$

Classi di coniugio di D_n

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

$$|\mathcal{O}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|} = \frac{|G|}{|C_G(x)|}$$

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

Ora, per $G = D_n$, $x = r$: $\underbrace{D_n \supseteq C_G(r) \supseteq R}_{2}$

Se fosse $C_G(r) = D_n \Rightarrow r \in Z(G) \Rightarrow rs = sr \iff sr^{-1} = sr \iff r = r^{-1}$ falso per $n \geq 3$

Quindi $C_G(r) = R$ e $|\mathcal{O}(r)| = |D_n| / |R| = 2$

$\Rightarrow \mathcal{O}(r) = \{ r, srs^{-1} \} = \{ r, r^{-1} \}$

Analogamente si mostra $\mathcal{O}(r^k) = \{ r^k, r^{-k} \}$

Oss Se n è pari e $x = r^{\frac{n}{2}}$, $\mathcal{O}(x) = \{ r^{\frac{n}{2}}, r^{-\frac{n}{2}} \} = \{ r^{\frac{n}{2}} \}$

e quindi $r^{\frac{n}{2}} \in Z(D_n)$, infatti :

$$1 = \frac{|D_n|}{|C_G(x)|} \Rightarrow C_{D_n}(x) = D_n \Rightarrow x \in Z(D_n)$$

Consideriamo ora $\mathcal{O}(sr^h) \ni g(sr^h)g^{-1}$. Abbiamo due casi.

- $g \in R$, $g = r^k$, perciò $r^k sr^h r^{-k} = sr^{h-2k}$
- $g \notin R$, $g = sr^k$, perciò $sr^k sr^h (sr^k)^{-1} = s^2 r^{h-2k} s^{-1} = sr^{2k-h}$

Quindi $\mathcal{O}(sr^h) = \{ sr^{h-2k}, sr^{2k-h} \mid k \in \mathbb{Z} \}$

Omomorfismi di D_n

proposizione Sia G gruppo. C'è una bigezione

$$\mathrm{Hom}(D_n, G) \longleftrightarrow \{(x,y) \in G \times G \mid x^n = e_G,\ y^2 = e_G,\ yxy = x^{-1}\}$$
$$\varphi \longmapsto (\varphi(r), \varphi(s)) \qquad yxyx = e$$
$$\varphi(s^a r^b) = y^a x^b \longmapsto (x,y)$$

DIMOSTRAZIONE

1) Se $\varphi: D_n \longrightarrow G$ è omo, detti $x = \varphi(r)$, $y = \varphi(s)$

$$\varphi(r)^n = \varphi(r^n) = \varphi(\mathrm{id}) = e_G$$
$$\varphi(s)^2 = \varphi(s^2) = \varphi(\mathrm{id}) = e_G$$
$$\varphi(srsr) = \varphi(s)\varphi(r)\varphi(s)\varphi(r) = \varphi(\mathrm{id}) = e$$

2) $s^a r^b = s^{a'} r^{b'} \iff \begin{cases} a \equiv a' & (2) \\ b \equiv b' & (n) \end{cases}$

$y^a x^b \quad y^{a'} x^{b'}$

$$\Longrightarrow y^{a'} x^{b'} = y^{a+2h} x^{b+nk} = y^a x^b$$

Quindi abbiamo definito una funzione

- è un omomorfismo

$$\varphi(s^a r^b)\,\varphi(s^c r^d) = y^a x^b y^c x^d$$

Oss c pari: $s^a r^b s^c r^d = s^a r^{b+d} = s^{a+c} r^{b+d}$

c dispari: $s^a r^b s^c r^d = s^a r^b s r^d = s^a s r^{-b} r^d = s^{a+c} r^{-b+d}$

$$s^a r^b s^c r^d = s^{a+c} r^{(-1)^c b + d}$$

$$\Longrightarrow \varphi(s^a r^b s^c r^d) = \varphi(s^{a+c} r^{(-1)^c b + d}) = y^{a+c} x^{(-1)^c b + d}$$

Sappiamo che $yxy = x^{-1}$, perciò per induzione deduciamo che in G vale $yx^b = x^{-b}y \quad \forall b \in \mathbb{Z}$

Perciò $y^a x^b \cdot y^c x^d = y^{a+c} x^{(-1)^c b + d}$

3) Le due applicazioni sono una l'inversa dell'altra $\square$

Gruppo dei quaternioni

Il gruppo dei quaternioni è

$$Q_8 = \langle i, j \mid i^4 = e,\ i^2 = j^2,\ ij = j^3 i \rangle$$

Segue che $\text{ord}(i) = \text{ord}(j) = 4$

Inoltre $Q_8 = \langle i \rangle \langle j \rangle$, quindi

$$|Q_8| = \frac{|\langle i \rangle|\,|\langle j \rangle|}{|\langle i \rangle \cap \langle j \rangle|} = \frac{4 \cdot 4}{2} = 8$$

$$\Rightarrow Q_8 = \{1, i, i^2, i^3, j, i^2 j, ij, i^3 j\}$$

Sottogruppi di Q_8

ordine 1 : $\{1\} \triangleleft Q_8$

ordine 2 : $\langle i^2 \rangle \triangleleft Q_8$ $\quad i^2 = -1$

ordine 4 : $\langle i \rangle, \langle j \rangle, \langle ij \rangle \triangleleft Q_8$

$$(ij)^2 = ijij = ijj^3 i = i^2$$

$\Rightarrow Q_8$ è un gruppo non abeliano con tutti i sottogruppi normali

Posto convenzionalmente $ij = k$: $\quad Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Il prodotto è dato da

Oss $Z(Q_8) = \langle i^2 \rangle$

Infatti $\langle i^2 \rangle \subseteq Z(Q_8)$ e

$$|Z(Q_8)| = \begin{cases} 1 & \lightning \text{ perché } Q_8 \text{ è un } p\text{-gruppo} \\ p & \\ p^2 \longrightarrow Q_8/Z(Q_8) \text{ ciclico} & \lightning \\ p^3 \longrightarrow Z(Q_8) = Q_8 & \lightning \end{cases}$$

$$\Rightarrow Z(Q_8) = \langle i^2 \rangle$$

TEORIA DEGLI ANELLI

Def. Un **anello** è una terna $(A,+,\cdot)$ tale che
- $(A,+)$ è un gruppo abeliano
- $\cdot$ è associativa
- valgono le leggi distributive a destra e sinistra:
  $a(b+c)=ab+ac \qquad (a+b)c=ac+bc \qquad \forall a,b,c\in A$

Def. Un anello $(A,+,\cdot)$ è **commutativo** se il prodotto è commutativo.
Un anello si dice **con unità** se $1\in A$ (elemento neutro del prodotto).

Def. $(A,+,\cdot)$ è un **campo** se è un anello e $A^*=A\setminus\{0\}$ è un gruppo abeliano

Def. $x\in A$ si dice **divisore di 0** se $\exists\, y\in A, y\neq 0$ t.c. $xy=0$
A si dice **dominio di integrità** se $D=\{\text{divisori di zero di } A\}=\{0\}$

Def. $x\in A$ si dice **invertibile** se $\exists\, y\in A \quad xy=yx=1$
$A^*=\{x\in A \mid x \text{ è invertibile in } A\}$

esempio $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\ \mathbb{Z}/n\mathbb{Z},\ A[x]$ con A anello, $\mathbb{Z}[i],\ \mathbb{Z}[\sqrt{a}]$

proposizione Sia A anello commutativo con unità. Allora:
(1) $(A^*,\cdot)$ è un gruppo
(2) $A^*\cap D=\emptyset$
(3) se A è un anello finito, allora $A=A^*\cup D$

DIMOSTRAZIONE
(1) chiaro
(2) Sia $x\in A^*\cap D \Rightarrow \exists\, y\in A$ t.c. $xy=1$, $\exists\, z\in A, z\neq 0 : xz=0$
$z=1\cdot z=xyz=xzy=0\cdot y=0$ ↯
$\Rightarrow A^*\cap D=\emptyset$
(3) $A^*\cup D\subseteq A$ è chiaro.
Sia $x\in A$: se $x\in D$, ho finito
Se $x\in A\setminus D$, definisco l'omomorfismo
$\varphi_x : a \longrightarrow xa$
Poiché $x\notin D$, $\ker\varphi_x=\{0\}$, quindi $A\cong \mathrm{Im}\varphi_x \Rightarrow A=\mathrm{Im}\varphi_x$,
da cui $1\in\mathrm{Im}\varphi_x$, ossia $\exists\, y\in A, y\neq 0$ t.c. $xy=1$, quindi $x\in A^*$ □

corollario Un dominio finito è un campo.

Def $I \subseteq A$ è un **ideale** se $(I,+)$ è un gruppo abeliano
e $\forall a \in A \ \forall x \in I \quad ax \in I$

Def Dato $S \subseteq A$ sottoinsieme, l'**ideale generato** da S è
$$(S) = \bigcap_{\substack{I \subseteq A \\ \text{ideale} \\ S \subseteq I}} I$$
(A fa parete dell'intersezione e l'intersezione di ideali è ideale)

Oss $(S) = \{ \sum_{i=1}^{n} a_i s_i \mid n \in \mathbb{N}, a_i \in A, s_i \in S \} = J$

DIMOSTRAZIONE
($\subseteq$) Basta osservare che J è un ideale di A che contiene S
($\supseteq$) Vero in quanto ogni ideale di A che contiene S contiene J.
Infatti se I è un ideale di A che contiene S, allora $s_i \in I \ \forall s_i \in S$
e $\sum a_i s_i \in I$ perché I è un ideale $\Rightarrow J \subseteq I$
$\Rightarrow J \subseteq \cap I = (S)$

Def Un **ideale principale** è un ideale della forma
$$(s) = \{as \mid a \in A\} = sA$$

esempio $\mathbb{Z}$: $(3) = 3\mathbb{Z}$
$\mathbb{Q}[x]$: $(x^2-1) = \{ (x^2-1)p(x) \mid p(x) \in \mathbb{Q}[x] \}$

esempio $\mathbb{Z}$: $(5,21) = \{5t+21s \mid t,s \in \mathbb{Z}\} = \mathbb{Z}$

Oss Gli ideali di $\mathbb{Z}$ sono tutti principali
$$(n_i)_{i \in I} = (\text{mcd}\{n_i \mid i \in I\})$$

Oss $\mathbb{K}[x]$ è a ideali principali

esempio $\mathbb{Z}[x]$: $(2,x)$ non è principale

operazioni con gli ideali

Sia A anello commutativo con unità

I, J ideali di A $(I, J \trianglelefteq A)$

- Somma $I+J = (i+j \mid i \in I, j \in J)$
- Intersezione $I \cap J$
- Prodotto $IJ = (ij \mid i \in I, j \in J)$
- Radicale $\sqrt{I} = \{a \in A \mid \exists n \geq 1 \text{ t.c. } a^n \in I\}$
- Colon $I:J = \{r \in A \mid rJ \subseteq I\}$

Oss $I+J = \{i+j \mid i \in I, j \in J\}$ è già un ideale:

$(i_1+j_1)+(i_2+j_2) = (i_1+i_2)+(j_1+j_2) \in I+J$

$a(i_1+j_1) = ai_1 + aj_1 \in I+J$

Oss $\sqrt{I}$ è un ideale

DIMOSTRAZIONE

- $x \in \sqrt{I} \Rightarrow \exists n \; x^n \in I \Rightarrow a^n x^n \in I \Rightarrow ax \in \sqrt{I}$
- $x, y \in \sqrt{I} \Rightarrow \exists n, m \; x^n, y^m \in I \Rightarrow (x+y)^M = \sum_{i=0}^{M} \binom{M}{i} x^i y^{M-i}$

  Se $M = m+n-1$, in ogni addendo c'è un fattore x^n o y^m

  $\Rightarrow$ è multiplo di un elemento in $I \Rightarrow (x+y)^M \in I$ □

Fatto $IJ \subseteq I \cap J$

esempio $A = \mathbb{Z}$ $I = (m)$ $J = (n)$

- $I+J = (m)+(n) = (m,n) = (d)$ dove $d = \text{mcd}(m,n)$
- $IJ = (m)\cdot(n) = (mn)$

  Infatti $I = \{am \mid a \in \mathbb{Z}\}$, $J = \{bn \mid b \in \mathbb{Z}\}$

  $IJ = \{abmn \mid a, b \in \mathbb{Z}\} = (mn)$
- $I \cap J = (m) \cap (n) = (\text{mcm}(m,n))$

  $x \in (m) \cap (n) \iff m \mid x \wedge n \mid x \iff \text{mcm}(m,n) \mid x$
- $I = (n) = (p_1^{e_1} \cdots p_r^{e_r})$

  $\sqrt{I} = (p_1 \cdots p_r)$

  $x \in \sqrt{I} \iff \exists n \geq 1 \text{ t.c. } x^n \in (p_1^{e_1} \cdots p_r^{e_r})$

  $\iff p_1^{e_1} \cdots p_r^{e_r} \mid x^n \Rightarrow p_1 \mid x^n, \ldots, p_r \mid x^n \Rightarrow p_1 \mid x, \ldots, p_r \mid x \Rightarrow p_1 \cdots p_r \mid x \Rightarrow x \in (p_1 \cdots p_r)$

  Viceversa, $x \in (p_1 \cdots p_r)$, allora $x \in \sqrt{I}$ perché

  $p_1^{e_1} \cdots p_r^{e_r} \mid x^{e_1+\cdots+e_r} \Rightarrow x^{e_1+\cdots+e_r} \in (n)$
- $(m)\cdot(n) = \{r \in \mathbb{Z} \mid r(n) = (rn) \subseteq (m)\}$

  $r \in (m):(n) \iff (rn) \subseteq (m) \iff m \mid rn \iff rn \equiv 0 \; (m)$

  $\iff r \equiv 0 \; \left(\frac{m}{(m,n)}\right)$

  $(m):(n) = \left(\frac{m}{(m,n)}\right)$

esempio $A = \mathbb{F}_5[x]$ $I = (x^2+1)$ $J = (x^3-1)$

$I+J = (x^2+1, x^3-1) = (1)$

$IJ = ((x^2+1)(x^3-1))$

$I \cap J = IJ$

Oss $I+J = (1) \Rightarrow IJ = I \cap J$

Concretamente: $p(x) \in I \cap J \iff x^2+1 \mid p(x)$, $x^3-1 \mid p(x)$

Siccome $(x^2+1, x^3-1) = 1$, concludo che $(x^2+1)(x^3-1) \mid p(x)$

Proposizione Sia A anello. Vale:
$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

DIMOSTRAZIONE

$\sqrt{IJ} \subseteq \sqrt{I \cap J}$ perché $IJ \subseteq I \cap J$

Oss $I_1 \subseteq I_2 \Longrightarrow \sqrt{I_1} \subseteq \sqrt{I_2}$

Per il viceversa, sia $x \in \sqrt{I \cap J}$. Allora $\exists n$ t.c. $x^n \in I \cap J$

Devo mostrare che $\exists m$ t.c. $x^m \in IJ$

$m = 2n$: $x^{2n} = x^n \cdot x^n \in IJ \Longrightarrow x \in \sqrt{IJ}$ □

Def. Il **nilradicale** di un anello A è:
$$\sqrt{(0)} = \{a \in A \mid a^n = 0\}$$

Oss $\sqrt{(0)} \subseteq P$ per ogni ideale primo P

$x \in \sqrt{(0)} \Rightarrow \exists n$ t.c. $x^n = 0 \in P \Rightarrow x \in P$

Teorema $\sqrt{(0)} = \bigcap_{P \text{ primo}} P$

Quozienti

Def. Dato A anello e $I \trianglelefteq A$ ideale, definiamo il quoziente

$A/I = \{a+I \mid a \in A\}$ con somma $(a+I)+(b+I) = (a+b)+I$

e prodotto $(a+I)\cdot(b+I) = ab+I$

$(A/I, +, \cdot)$ è un anello

Def. Dati due anelli A, B, $f: A \to B$ è omomorfismo di anelli se

$f(a+b) = f(a)+f(b)$

$f(ab) = f(a)\cdot f(b)$

Se A e B sono anelli con unità, vale anche

$f(1_A) = 1_B$

<u>Oss</u> $\pi : A \to A/I$ è omomorfismo di anelli

Proposizione Gli ideali di A sono esattamente i nuclei di omomorfismi di anelli definiti su A

DIMOSTRAZIONE

- $\forall \varphi : A \to B$ omomorfismo, $\ker\varphi$ è ideale di A

  $\ker\varphi < A$ e $\forall a \in A \ \forall x \in \ker\varphi \longrightarrow ax \in \ker\varphi$

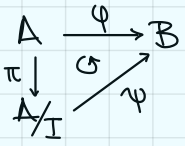
  infatti $\varphi(ax) = \varphi(a)\varphi(x) = 0$
- $\forall J \trianglelefteq A$ ideale, $J = \ker\pi_J$ dove $\pi_J : A \to A/J$ □

I teorema di omomorfismo A, B anelli, $\varphi : A \to B$ omomorfismo

$\forall I \trianglelefteq A$, $I \subseteq \ker\varphi$ $\exists!$ omomorfismo di anelli $\psi : A/I \to B$ tale che il diagramma commuta

Inoltre $\operatorname{Im}\psi = \operatorname{Im}\varphi$

e ψ è iniettiva $\iff \ker\varphi = I$



DIMOSTRAZIONE

È il I teorema di omomorfismo di gruppi con la verifica che l'unico omomorfismo di gruppi ψ che fa commutare il diagramma è anche un omomorfismo di anelli.

$\psi(\pi_I(a)) = \varphi(a)$ cioè $\psi(a+I) = \varphi(a)$

$\psi((a+I)(b+I)) \overset{?}{=} \psi(a+I)\cdot\psi(b+I)$

$\psi(ab+I) = \varphi(ab) = \varphi(a)\cdot\varphi(b)$

□

Lemma Sia $f: A \to B$ omomorfismo di anelli. Allora:
(1) $\forall J \subseteq B$ ideale, $f^{-1}(J)$ è un ideale di A
(2) se f è surgettivo, $\forall I \subseteq A$ ideale, $f(I)$ è ideale di B

DIMOSTRAZIONE
(1) Sappiamo che $f^{-1}(J)$ è sottogruppo di B. Verifichiamo che vale l'assorbimento.
$x = f^{-1}(y) \in f^{-1}(J)$, $a \in A$: $ax \xrightarrow{f} f(ax) = f(a)y = y' \in J$ perché J è ideale
quindi $ax \in f^{-1}(J)$
(2) Sappiamo che $f(I)$ è sottogruppo di B. Verifichiamo che vale l'assorbimento:
$f(x) \in f(I)$, $b \in B$: poiché f è surgettiva, $\exists a \in A$: $f(a) = b$
quindi $bf(x) = f(\underset{\in I}{ax}) \in f(I)$ □

Teorema di corrispondenza Sia $I \subseteq A$ ideale, $\pi: A \to A/I$
π induce una corrispondenza biunivoca tra gli ideali di A/I e gli ideali di A che contengono I
Questa corrispondenza preserva l'ordinamento di inclusione, l'indice di sottogruppo, ideali primi e ideali massimali

DIMOSTRAZIONE
So che $\{H < A \mid I \subseteq A\} \xrightarrow{\alpha} \{\mathcal{H} \mid \mathcal{H} < A/I\}$ è biiettiva
$H \longmapsto \pi(H) = H/I$
$J \subseteq A$ con $J \supseteq I$, $\pi(J)$ è un ideale di A/I
$\{J \subseteq A \text{ ideale} \mid J \supseteq I\} \longrightarrow \{\mathcal{J} \subseteq A/I \text{ ideale}\}$
$J \longmapsto \pi(J)$ è ideale
l'iniettività si conserva
la surgettività si conserva per (1) del lemma
$\mathcal{J}$ $\exists H < A$ sottogruppo t.c. $\pi(H) = \mathcal{J}$
$\Rightarrow H = \pi^{-1}(\mathcal{J}) \overset{(1)}{\Rightarrow} H$ è ideale

$I \subseteq J \subseteq A$
$A/J \cong A/I \,/\, J/I$ dove $J/I = \pi(J)$
quindi J è primo $\iff J/I$ è primo
J è massimale $\iff J/I$ è massimale □

Oss $\varphi: A \to B$ omomorfismo surgettivo
$B \cong A/I$ $I = \ker \varphi$
$\pi_I: A \to A/I \overset{\varphi}{\cong} B$

DEF. Il prodotto diretto di due anelli A e B è l'insieme $A \times B$ dotato delle operazioni

$(a_1,b_1)+(a_2,b_2)=(a_1+a_2, b_1+b_2) \qquad (a_1,b_1)\cdot(a_2,b_2)=(a_1a_2, b_1b_2)$

Teorema cinese per anelli Sia A anello commutativo con unità e siano $I, J \subseteq A$ ideali. Allora:

$$f: A \longrightarrow A/I \times A/J$$
$$a \longmapsto (a+I, a+J)$$

f è omomorfismo di anelli e $\ker f = I \cap J$

Inoltre $(I,J)=A \iff f$ surgettiva

e in tal caso $I \cap J = (IJ)$

Oss Generalizza $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \iff (m,n)=1$

DIMOSTRAZIONE

f è un omomorfismo: ovvio

$\ker f = \{a \in A \mid f(a)=(a+I, a+J)=(I,J)\} = \{a \in A \mid a+I=I, a+J=J\} =$
$= \{a \in A \mid a \in I, a \in J\} = I \cap J$

($\Rightarrow$) $(I,J)=A$

$\exists i \in I, j \in J$ t.c. $i+j=1$

Voglio vedere che

$\forall a,b \in A \ \exists x \in A$ t.c. $f(x)=(a+I, b+J)$

Considero $x=bi+aj$

$f(x)=(bi+aj+I, bi+aj+J)=(aj+I, bi+J) \underset{\substack{\uparrow \\ j=1-i,\, i=1-j}}{=} (a+I, b+J)$

($\Leftarrow$) f surgettiva

$\exists i \in A$ t.c. $f(i)=(I, 1+J)$, cioè $i \in I$, $i+J=1+J \iff 1-i \in J$

$\Rightarrow 1-i=j \in J \Rightarrow 1=i+j$ con $i \in I, j \in J$

$\Rightarrow (I,J)=A$ □

corollario Se $(I,J)=A$, $A/IJ \cong A/I \times A/J$

esempio $\frac{\mathbb{Q}[x,y]}{(x-y, x^3+y^3-x)}$ come prodotto di campi

TCR: $\frac{A}{IJ} \cong \frac{A}{I} \times \frac{A}{J}$ se $I+J=(1)$

Per il 2° teorema di isomorfismo: $\frac{A}{I+J} = \frac{A/I}{I+J/I}$ $I=(x-y)$, $J=(x^3+y^3-x)$

Lemma $\frac{\mathbb{Q}[x,y]}{(x-y)} \cong \mathbb{Q}[x]$

DIMOSTRAZIONE

$\varphi : \mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[x]$

$p(x,y) \longmapsto p(x,x)$

- φ è surgettiva $g(x) = \varphi(g(x))$
- $(x-y) \subseteq \ker\varphi$ chiaro

$(x-y) \supseteq \ker\varphi$: sia $p(x,y) \in \ker\varphi$

$$p(x,y) = \sum a_{ij} x^i y^j = \sum a_{ij} x^i (y^j - x^j + x^j) =$$
$$= \sum a_{ij} x^{i+j} + (y-x)q(x,y)$$
$$0 = \varphi(p(x,y)) = \sum a_{ij} x^{i+j} + (x-x)q(x,x)$$
$$\Rightarrow y-x \mid p(x,y) \Rightarrow p(x,y) \in (x-y)$$

Per il I teorema di omomorfismo:

$$\frac{\mathbb{Q}[x,y]}{(x-y)} = \frac{\mathbb{Q}[x,y]}{\ker\varphi} \cong \mathrm{Im}\,\varphi = \mathbb{Q}[x] \qquad \square$$

$$\frac{\mathbb{Q}[x,y]}{(x-y, x^3+y^3-x)} \cong \frac{\mathbb{Q}[x,y]/(x-y)}{(x-y, x^3+y^3-x)/(x-y)} \cong \frac{\mathbb{Q}[x]}{(0, 2x^3-x)} \cong \frac{\mathbb{Q}[x]}{(x(2x^2-1))} \cong \frac{\mathbb{Q}[x]}{(x)(2x^2-1)}$$
$$\overset{TCR}{\cong} \frac{\mathbb{Q}[x]}{x} \times \frac{\mathbb{Q}[x]}{(x^2-1/2)} \cong \mathbb{Q} \times \mathbb{Q}(1/\sqrt{2}) \cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2})$$

Proposizione: interpolazione di Lagrange Dati $x_1 < \dots < x_n \in \mathbb{R}$, $y_1, \dots, y_n \in \mathbb{R}$, allora $\exists!\, p(x) \in \mathbb{R}[x]$ con $\deg p(x) \le n-1$ t.c. $p(x_i) = y_i$ per $i = 1, \dots, n$

DIMOSTRAZIONE

Se p_1, p_2 hanno questa proprietà, $p_1(x) - p_2(x)$ si annulla in $x_1, \dots, x_n$

$\Rightarrow p_1(x) - p_2(x) \in ((x-x_1)\cdots(x-x_n))$

Sia $I = ((x-x_1)\cdots(x-x_n))$. Studiamo $\mathbb{R}[x]/I$

$$\frac{\mathbb{R}[x]}{((x-x_1)\cdots(x-x_n))} \cong \frac{\mathbb{R}[x]}{(x-x_1)\cdot\ldots\cdot(x-x_n)} \cong \frac{\mathbb{R}[x]}{I_1} \times \cdots \times \frac{\mathbb{R}[x]}{I_n} \cong \mathbb{R} \times \cdots \times \mathbb{R}$$

$I_j = (x-x_j)$, $I_j + I_{j'} = (1)$ per $j' \neq j$

l'isomorfismo $\frac{\mathbb{R}[x]}{(x-x_1)\cdots(x-x_n)} \xrightarrow{\sim} \mathbb{R} \times \cdots \times \mathbb{R}$

$\overline{p(x)} \longmapsto (p(x_1), \dots, p(x_n))$

$(y_1, \dots, y_n)$ $\square$

Ideali primi e massimali

Def. Sia $(\mathcal{F}, \subseteq)$ un insieme parzialmente ordinato (poset)
$X \subseteq \mathcal{F}$ un **maggiorante** per X è $A \in \mathcal{F}$ t.c. $B \subseteq A \ \forall B \in X$
$A \in \mathcal{F}$ si dice **massimale** se $\forall B \in \mathcal{F} \quad A \subseteq B \Longrightarrow B = A$

esempio $\mathcal{F} = \{\text{ideali propri di un anello } R\}$
$(\mathcal{F}, \subseteq)$ è un poset e gli elementi massimali di $\mathcal{F}$ sono gli ideali massimali di R

Def. $A \in \mathcal{F}$ è un **massimo** se $\forall B \in \mathcal{F} \ B \subseteq A$
Dato $(\mathcal{F}, \subseteq)$, una **catena** di $\mathcal{F}$ è un sottoinsieme di $\mathcal{F}$ totalmente ordinato
$(\mathcal{F}, \subseteq)$ si dice **induttivo** se ogni catena di $\mathcal{F}$ ammette un maggiorante in $\mathcal{F}$

Lemma di Zorn Sia $(\mathcal{F}, \subseteq)$ un poset induttivo non vuoto.
Allora $\mathcal{F}$ ha almeno un elemento massimale

Consideriamo ora $\mathcal{F} = \{I \subsetneq A \mid I \text{ ideale}\} : \{0\} \in \mathcal{F}$
$(\mathcal{F}, \subseteq)$ è un ordinamento parziale

Def. Un ideale proprio $M \in \mathcal{F}$ si dice **massimale**
se è un elemento massimale rispetto al contenimento,
cioè $\forall I \subseteq A \quad M \subseteq I \subseteq A$ si ha $I = M$ o $I = A$

Def. Un ideale proprio $I \in \mathcal{F}$ si dice **primo** se
$\forall x, y \in A \quad xy \in I$ si ha $x \in I \vee y \in I$

Lemma di Krull Ogni ideale proprio di un anello A è contenuto in un ideale massimale

DIMOSTRAZIONE
Sia $\mathcal{F} = \{I \subseteq J \subsetneq A \mid J \text{ ideale}\}$ · $(\mathcal{F}, \subseteq)$ poset e $I \in \mathcal{F}$
Claim: $\mathcal{F}$ è induttivo $\Longrightarrow \exists M \in \mathcal{F}$ el. massimale in $\mathcal{F}$
Dico che M è un ideale massimale di A
Se fosse $M \subseteq L \subsetneq A$, allora $I \subseteq M \subseteq L \subsetneq A$, cioè $L \in \mathcal{F}$
quindi per la massimalità di M, $L \subseteq M \Longrightarrow M = L$
$(\mathcal{F}, \subseteq)$ è induttivo.
Sia $X = \{J_\lambda\}_{\lambda \in \Lambda}$ catena
Sia $J = \bigcup_{\lambda \in \Lambda} J_\lambda$: dico che $J \in \mathcal{F}$; inoltre $\forall \lambda \ J_\lambda \subseteq J$
- $I \subset J_\lambda \subset J$
- $1 \notin J = \bigcup_{\lambda \in \Lambda} J_\lambda$ (altrimenti esisterebbe λ t.c. $1 \in J_\lambda$ ↯)
- J è ideale di A: $x, y \in J = \bigcup_{\lambda \in \Lambda} J_\lambda$, $x \in J_{\lambda_1}, y \in J_{\lambda_2}$, $J_{\lambda_1} \subseteq J_{\lambda_2}$
  quindi $x, y \in J_{\lambda_2} \Longrightarrow x + y \in J_{\lambda_2} \subset J$
  $a \in A \quad ax \in J_{\lambda_1} \subseteq J$

□

corollario (1) Ogni anello possiede ideali massimali
(2) Ogni elemento non invertibile di A è contenuto in un ideale massimale

DIMOSTRAZIONE
(1) A anello, (0) è ideale di A
Per la proposizione $\exists M \subsetneq A$ ideale massimale t.c. $(0) \subseteq M$
$\Rightarrow A$ ha ideali massimali
(2) $x \in A \setminus A^* \iff (x) \subsetneq A \implies (x) \subseteq M$ ideale massimale di A
$\Rightarrow x \in M$ □

proposizione Sia $I \subsetneq A$ ideale
(1) I è primo $\iff A/I$ è un dominio
(2) I è massimale $\iff A/I$ è un campo
(3) I massimale $\implies I$ primo

DIMOSTRAZIONE
(1) I primo $\iff \forall x,y \in A \; xy \in I \implies x \in I \vee y \in I$
A/I dominio $\iff (x+I)(y+I) = xy+I = I \iff x+I = I \vee y+I = I$
$xy \in I \iff x \in I \vee y \in I$
(2) I massimale $\iff$ gli unici ideali di A/I sono $(\bar{0})$ e A/I (per corrispondenza)
$\iff \forall x \in A/I \; x \neq 0 \;\; x$ è invertibile
$(\Rightarrow)$ per (2)
$(\Leftarrow)$ J ideale di A/I : $J = \langle \underset{\neq(\bar{0})}{(\bar{0})} \rangle \implies \exists x \in J, x \neq 0, x$ è invertibile $\implies J = A/I$
$\iff A/I$ è un campo
(3) I massimale $\iff A/I$ campo $\implies A/I$ dominio $\implies I$ primo □

esempio $\mathbb{Z}$: $n\mathbb{Z}$ è primo $\iff \mathbb{Z}/n\mathbb{Z}$ dominio
$n\mathbb{Z}$ massimale $\iff \mathbb{Z}/n\mathbb{Z}$ campo
(0) è primo ma non massimale
$n\mathbb{Z}$ è primo $\iff n\mathbb{Z}$ è massimale

esercizio ideali di $\mathbb{Z} \times \mathbb{Z}$
$\langle (1,1) \rangle$ è un ideale?

esempio $\mathbb{Z}[i]$: ideali primi (0), (π) con π primo di $\mathbb{Z}[i]$
$\mathbb{Z}[x]$: (x) è primo ma non massimale

Oss (x) è primo, $(x) \neq 0 \iff x$ è un elemento primo di A
DIMOSTRAZIONE
$x \mid ab \iff ab \in (x) \iff a \in (x) \vee b \in (x) \iff x \mid a \vee x \mid b$ □

esempio $A=\mathbb{Q}[x,y]$ $I=(x-1,y-1)$ $J=(1-xy)$

Dimostrare che $J\subseteq I$ e che I è massimale

$I\cap J=J$

$J\subseteq I \iff 1-xy\in I \iff \exists a(x,y), b(x,y)$ t.c. $1-xy=a(x,y)(x-1)+b(x,y)(y-1)$

$\overset{x=1}{\Longrightarrow}$ $1-y=a(1,y)\cdot 0+b(1,y)(y-1)$

Se scrivo $b(x,y)=\dots+(x-1)^2b_2(y)+(x-1)b_1(y)-1$

$1-xy=-y(x-1)+(-1)(y-1)$

Provo la divisione con resto

$x(-y)+1 \;:\; (x-1) = -y$ con resto $-y+1$

I è massimale $\iff \mathbb{Q}[x,y]/(x-1,y-1)$ è un campo

Cerco $\varphi: \mathbb{Q}[x,y]\longrightarrow K$ campo con $\ker\varphi=I$, $\operatorname{Im}\varphi=K$

Considero $\varphi: \mathbb{Q}[x,y]\longrightarrow\mathbb{Q}$

$p(x,y)\longmapsto p(1,1)$ è certamente surgettivo

Mostriamo che $\ker\varphi=I$

$\supseteq$: $\varphi(x-1)=0$, $\varphi(y-1)=0$

$\subseteq$: Sia $p(x,y)\in\ker\varphi$. Faccio la divisione per $x-1$:

$$p(x,y)=q(x,y)(x-1)+r(y)$$

$$p(x,y)=\sum_{i,j=0}^{d}a_{ij}x^iy^j=\sum_{i,j=0}^{d}a_{ij}(x^{i-1}+1)y^j=\sum_{i,j=0}^{d}a_{ij}y^j+\sum_{i,j=0}^{d}a_{ij}(x-1)(x^{i-1}+x^{i-2}+\dots+1)y^j$$

$$\Rightarrow q(x,y)=\sum_{i,j=0}^{d}a_{ij}(x^{i-1}+x^{i-2}+\dots+1)y^j \qquad r(y)=\sum_{i,j=0}^{d}a_{ij}y^j=p(1,y)$$

Oss $p(x)=(x-1)q(x)+r \Rightarrow r=p(1)$

Sostituisco $x=y=1$

$0=p(1,1)=(1-1)q(1,1)+r(1) \Longrightarrow r(1)=0 \overset{\text{Ruffini}}{\Longrightarrow} r(y)=(y-1)s(y)$

Quindi $p(x,y)=(x-1)q(x,y)+(y-1)s(y)\in(x-1,y-1)$

Anello delle frazioni di un dominio

Def. Sia A un dominio di integrità
Un sottoinsieme $S \subsetneq A$ con: • $0 \notin S$
• $1 \in S$
• $\forall x,y \in S \quad xy \in S$
si chiama **parte moltiplicativa di A**

Def. Dato un dominio A e una sua parte moltiplicativa S,
l'**anello delle frazioni di A** è
$S^{-1}A = A \times S / \sim = \{ \frac{a}{s} \mid a \in A, s \in S \} / \sim$
dove $(a,s) \sim (b,t)$ se $at = bs$

Oss $S = A \setminus \{0\}$ parte moltiplicativa $\iff$ A dominio

esempio $S^{-1}\mathbb{Z} = \{ \frac{a}{s}, a,s \in \mathbb{Z}, s \neq 0 \} / \sim = \mathbb{Q}$

Dotiamo $S^{-1}A$ di due operazioni:
$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ $\quad$ $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

proposizione $(S^{-1}A, +, \cdot)$ è un anello commutativo con unità

DIMOSTRAZIONE
Verifichiamo la buona definizione
$\frac{a}{s} = \frac{a_1}{s_1}$, $\frac{b}{t} = \frac{b_1}{t_1}$ cioè $as_1 = a_1 s$ e $bt_1 = b_1 t$

$\left.\begin{aligned} \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \\ \frac{a_1}{s_1} \cdot \frac{b_1}{t_1} &= \frac{a_1 b_1}{s_1 t_1} \end{aligned}\right\} = \iff ab s_1 t_1 = st a_1 b_1$ ok □

esempio $\mathbb{Z}$, $S = \{10^k\}_{k \geq 0}$
$S^{-1}\mathbb{Z} = \{ \frac{n}{10^k}, n \in \mathbb{Z}, k \geq 0 \}$

proposizione $f: A \longrightarrow S^{-1}A$
$a \longmapsto \frac{a}{1}$ è un omomorfismo iniettivo

DIMOSTRAZIONE
$f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$
$f(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b)$
$f(1) = \frac{1}{1}$ è l'identità di $S^{-1}A$
$\ker f = \{ a \in A \mid \frac{a}{1} = \frac{0}{1} \}$ cioè $a \cdot 1 = 0 \cdot 1 = 0 \Rightarrow a = 0$
quindi $\ker f = \{0\}$ □

proposizione $S^{-1}A^* = \{\frac{a}{s} \in S^{-1}A \mid \exists t \in A : at \in S\}$

DIMOSTRAZIONE

($\supseteq$) $\frac{a}{s} = \frac{at}{st}$ quindi $\frac{st}{at} \in S^{-1}A$

$\frac{a}{s} \cdot \frac{st}{at} = \frac{1}{1} \Rightarrow \frac{a}{s} \in S^{-1}A^*$

($\subseteq$) $\frac{a}{s} \in S^{-1}A^* \Rightarrow \exists\, \frac{b}{u} \in S^{-1}A$ $(b \in A, u \in S)$ t.c.

$\frac{a}{s} \cdot \frac{b}{u} = \frac{1}{1}$ $ab = su$

$\frac{a}{s} = \frac{ab}{sb} \in S$ $\frac{sb}{ab} \in S^{-1}A$ □

def. Dato un dominio A, definiamo il **campo dei quozienti di A**

$S^{-1}A = Q(A)$ dove $S = A \setminus \{0\}$

proposizione Il campo dei quozienti di A, $S^{-1}A = Q(A)$ con $S = A \setminus \{0\}$ è un campo ed è il più piccolo campo che contiene A

DIMOSTRAZIONE

$S^{-1}A$ è un campo $\iff S^{-1}A^* = S^{-1}A \setminus \{\frac{0}{1}\}$

($\subseteq$) ovvio

($\supseteq$) $\frac{a}{s} \in S^{-1}A^*, a \neq 0 \Rightarrow a \in S \Rightarrow \frac{s}{a} \in S^{-1}A$ $\frac{a}{s} \cdot \frac{s}{a} = 1$

Sia K un campo t.c. $A \subset K$

$\forall s \in A, s \neq 0$, $\frac{1}{s} \in K$

cioè $\forall s \in S$ $\frac{1}{s} \in K$ inoltre $\forall a \in A$ $a \in K \Rightarrow \frac{a}{s} \in K$

Quindi $S^{-1}A \subseteq K$ □

esempio $n\mathbb{Z}$ ideale di $\mathbb{Z}$

$\mathbb{Q}$ $S^{-1}(n\mathbb{Z})$ $S = \mathbb{Z} \setminus \{0\}$

$n=0$: $(\bar{0})$ — $\mathbb{Q}$

def. Un anello con un unico ideale massimale si dice **anello locale**

proposizione Sia A dominio, P ideale di A

(1) $S = A \setminus P$ è una parte moltiplicativa di A $\iff$ P è un ideale primo

(2) $S^{-1}A = A_P$ (localizzato di A a P) è un anello locale, con ideale massimale $PA_P = S^{-1}P$

DIMOSTRAZIONE

(1) $0 \notin S$ perché $0 \in P$ $\forall P$; $1 \in S$ perché $1 \notin P$ $\forall P$ primo

$(x, y \in S \Rightarrow xy \in S) \iff (xy \notin S \Rightarrow x \notin S \vee y \notin S) \iff (xy \in P \Rightarrow x \in P \vee y \in P)$

(2) La tesi equivale a $(S^{-1}A)^\times = S^{-1}A \setminus S^{-1}P$

($\supseteq$) Sia $\frac{a}{b} \in S^{-1}A \setminus S^{-1}P$, cioè $a \in A \setminus P$, $b \in S = A \setminus P$

Allora $\frac{b}{a} \in S^{-1}A \setminus S^{-1}P$ e $\frac{b}{a} \cdot \frac{a}{b} = 1 \Rightarrow \frac{a}{b} \in (S^{-1}A)^\times$

($\subseteq$) Sia $\frac{a}{b} \in (S^{-1}A)^\times$: $\exists\, \frac{c}{d} \in S^{-1}A$ t.c. $\frac{a}{b} \cdot \frac{c}{d} = 1 \iff ac = bd$

$b, d \notin P \Rightarrow bd \notin P \Rightarrow ac \notin P \Rightarrow a, c \notin P \Rightarrow \frac{a}{b} \in S^{-1}A \setminus S^{-1}P$ □

Sia A un dominio, S una parte moltiplicativa
Dato $X \subseteq A$, poniamo $S^{-1}X \subseteq S^{-1}A$:

$$S^{-1}X = \{ \tfrac{x}{s} \mid x \in X, s \in S \}$$

Teorema (1) Gli ideali di $S^{-1}A$ sono tutti e soli i sottoinsiemi della forma $S^{-1}I$, dove I è un ideale di A
(2) Gli ideali primi di $S^{-1}A$ sono in biezione con gli ideali primi di A t.c. $P \cap S = \emptyset$
(la biezione è $P \longmapsto S^{-1}P$)

DIMOSTRAZIONE
(1) (i) Dato $I \trianglelefteq A$, $S^{-1}I \trianglelefteq S^{-1}A$
(ii) Dato $J \trianglelefteq S^{-1}A$, $\exists I \trianglelefteq A$ t.c. $J = S^{-1}I$
(i) $S^{-1}I$ è un sottogruppo additivo:

$$\frac{i_1}{s_1} + \frac{i_2}{s_2} = \frac{i_1 s_2 + i_2 s_1}{s_1 s_2} \in S^{-1}I$$

perché $s_1 s_2 \in S$ e $s_2 i_1 + s_1 i_2 \in I$
Assorbimento: dati $\frac{i}{s} \in S^{-1}I$, $\frac{a}{s} \in S^{-1}A$
devo mostrare che $\frac{i}{s} \cdot \frac{a}{s} \in S^{-1}I$: $\frac{i}{s} \cdot \frac{a}{s} = \frac{ai}{ss} \in S^{-1}I$
(ii) Sia J ideale di $S^{-1}A$
Tramite $\varphi : A \hookrightarrow S^{-1}A$, considero $A \subseteq S^{-1}A$
$a \longmapsto a/1$
Poniamo $I = \varphi^{-1}(J)$
Questo è un ideale: è un sottogruppo additivo
(perché φ è omomorfismo rispetto a $+$)
$i \in \varphi^{-1}(J)$, $a \in A$: devo dire che $a \cdot i \in \varphi^{-1}(J)$
$\iff \varphi(ai) \in J$: in effetti $\varphi(a) \cdot \varphi(i) \in J$ perché $\varphi(i) \in J$ e J è un ideale
Resta da mostrare che $S^{-1}I = J$
($\subseteq$) gli elementi di $S^{-1}I$ sono $\frac{i}{s}$.
Per definizione, $\frac{i}{1} = \varphi(i) \in J$, $\frac{1}{s} \in S^{-1}A$
Per assorbimento di J, $\frac{i}{s} = \frac{i}{1} \cdot \frac{1}{s} \in J$
($\supseteq$) Sia $j \in J \subseteq S^{-1}A$: $j = \frac{a}{s}$ per $a \in A$, $s \in S$
Per assorbimento $\frac{a}{s} \cdot \frac{s}{1} = \frac{a}{1} \in J \Rightarrow a \in I = \varphi^{-1}(J)$
Quindi $\frac{a}{s} \in S^{-1}I$

<u>Oss</u> Se A è PID, tutti i suoi ideali sono principali, e tutti gli ideali di $S^{-1}A$ sono allora della forma $S^{-1}(\alpha)$ a loro volta principali ($S^{-1}(\alpha)$ = ideale generato da α in $S^{-1}A$)

(2) Sia P un primo di A che non interseca S. Voglio dire che $S^{-1}P$ è un ideale primo di $S^{-1}A$.
Intanto $S^{-1}P \neq S^{-1}A$: in effetti, $S^{-1}P = S^{-1}A \iff 1 \in S^{-1}P \iff 1 = \frac{p}{s}$, $p \in P$, $s \in S$
$\iff P \cap S \neq 0$, ma per ipotesi $P \cap S = \emptyset$
Ora vediamo che è primo: supponiamo $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in S^{-1}P$
$\Rightarrow \exists\, p \in P, s \in S$ t.c. $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{p}{s} \iff a_1 a_2 s = s_1 s_2 p \in P$
Quindi $a_1 a_2 s \in P$, quindi almeno uno tra $a_1, a_2, s \in P$
non può essere $s \in P$, quindi $a_1 \in P \vee a_2 \in P$
Senza perdita di generalità, $a_1 \in P \Rightarrow \frac{a_1}{s_1} \in S^{-1}P$

Viceversa, voglio dire che ogni primo di $S^{-1}A$ è della forma $S^{-1}P$, P primo di A.
So già che, dato Q ideale di $S^{-1}A$, $Q = S^{-1}I$ con $I = f^{-1}(Q)$ "$= Q \cap A$".
Basta allora dire che Q primo $\Longrightarrow f^{-1}(Q)$ primo

Lemma Dato $f: A \longrightarrow B$ omomorfismo di anelli e $Q \lhd B$ primo, allora $f^{-1}(Q)$ è un ideale primo di A

DIMOSTRAZIONE

$$x \cdot y \in f^{-1}(Q) \iff f(xy) \in Q \iff f(x) \in Q \vee f(y) \in Q$$
$$\iff x \in f^{-1}(Q) \vee y \in f^{-1}(Q)$$

Oppure:

Considero $A \xrightarrow{f} B \xrightarrow{\pi} B/Q$, $\varphi = \pi \circ f$

$$\ker \varphi = \{a \in A \mid \pi \circ f(a) = 0\} = \{a \in A \mid f(a) \in Q\} = f^{-1}(Q)$$

$\frac{A}{f^{-1}(Q)} \cong \operatorname{Im}\varphi \subseteq B/Q$ che è un dominio $\Longrightarrow \operatorname{Im}\varphi$ è un dominio
$\Longrightarrow f^{-1}(Q)$ è primo □

Resta da mostrare che è una bigezione

$$\{\text{primi di } A\} \qquad \{\text{primi di } S^{-1}A\}$$
$$P \longmapsto S^{-1}P \quad (\alpha)$$
$$f^{-1}(Q) = Q \cap A \longmapsto Q \quad (\beta)$$

Nella prima parte abbiamo visto che $\alpha \circ \beta = id$. Resta $\beta \circ \alpha = id$
Devo cioè dimostrare che $f^{-1}(S^{-1}P) = P$

($\supseteq$) $p \in P$: $\frac{p}{1} \in S^{-1}P \Longrightarrow p \in f^{-1}(S^{-1}P)$

($\subseteq$) sia $a \in f^{-1}(S^{-1}P)$: $\frac{a}{1} \in S^{-1}P \Longrightarrow \exists p \in P, s \in S$ t.c. $\frac{a}{1} = \frac{p}{s}$
$\iff sa = p \in P$ — $s \in P$: no perché $P \cap S = \emptyset$; $a \in P$

□

esempio $A = \mathbb{Z}$, $S = A \setminus (2)$: consideriamo $S^{-1}A$
Gli ideali di $S^{-1}A$ sono della forma $S^{-1}I$, con $I \lhd A$.
In particolare, sono della forma $S^{-1}(n)$, $n \in \mathbb{Z}$
$n = 2^a \cdot d$ con d dispari $\Longrightarrow S^{-1}(2^a \cdot d) = S^{-1}(2^a)$

Oss $S^{-1}(1) = S^{-1}(3) = \ldots = S^{-1}A$
$S^{-1}(2) = S^{-1}(6) = S^{-1}(10) = \ldots$

Controlliamo che $m \neq n \Longrightarrow S^{-1}(2^m) \neq S^{-1}(2^n)$
questi sono gli ideali principali di $S^{-1}A$ generati da 2^m e 2^n $(m > n)$
$(2^m) = (2^n)$ in $S^{-1}A \iff 2^{m-n} = 2^m/2^n$ è invertibile
$2^{m-n} \cdot \frac{a}{d} = 1 \iff 2^{m-n} \cdot a = d$, che non ha soluzioni in $\mathbb{Z}$

Ideali massimali di $\mathbb{Z}[x]$

esempio $I=(2)$ $\qquad \frac{\mathbb{Z}[x]}{(2)} \cong \mathbb{Z}_{/2\mathbb{Z}}[x]$

il quoziente è un dominio, ma non un campo

$\Rightarrow (2)$ è primo, ma non massimale

Gli ideali che contengono (2) sono in biezione con gli ideali di $\mathbb{Z}_{/2\mathbb{Z}}[x] \cong \mathbb{F}_2[x]$.

Gli ideali di $\mathbb{F}_2[x]$ sono tutti principali.

I massimali sono generati da polinomi irriducibili

I primi sono gli stessi e (0)

$\pi: \mathbb{Z}[x] \longrightarrow \mathbb{F}_2[x]$

$\pi^{-1}(I) \longleftarrow I$

$(2,x) \longleftarrow (\bar{x})$

↳ polinomi con termine noto pari

proposizione Sia M massimale in $\mathbb{Z}[x]$

Supponiamo che $M \cap \mathbb{Z} \ni p$ primo.

Allora $M=(p, f(x))$ dove $f(x)$ mod p è irriducibile

DIMOSTRAZIONE

$M \supseteq (p) \Rightarrow$ per corrispondenza, M è massimale in $\frac{\mathbb{Z}[x]}{(p)} \overset{\pi}{\cong} \mathbb{F}_p[x]$.

Un tale ideale è della forma $(\bar{f}(x))$ dove $\bar{f}$ è irriducibile.

Dunque $M=\pi^{-1}((\bar{f}(x))) = (p, f(x))$ □

$M \lhd \mathbb{Z}[x]$ massimale. Chiamo $g: \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$

$g^{-1}(M) = M \cap \mathbb{Z}$

M massimale $\Rightarrow M$ primo $\Rightarrow g^{-1}(M)$ primo

Se $g^{-1}(M)=(p)$, p primo $\Rightarrow p \in M$ e $M=(p, f(x))$ t.c. $\overline{f(x)} \in \mathbb{F}_p[x]$ è irriducibile

Lemma Sia A un anello, $I \lhd A$.

Poniamo $I[x] = \{a_0+a_1x+\dots+a_nx^n \mid a_i \in I, \forall i=0,\dots,n\}$

$=$ ideale generato da I in $A[x]$

$$\frac{A[x]}{I[x]} = {}_{A/I}[x]$$

DIMOSTRAZIONE

$\pi: A[x] \longrightarrow {}_{A/I}[x]$ è un omomorfismo

$p(x)=a_0+a_1x+\dots+a_nx^n \longmapsto \overline{a_0}+\overline{a_1}x+\dots+\overline{a_n}x^n$

$\ker \pi = I[x]$; per il I teorema di omomorfismo $\frac{A[x]}{I[x]} = {}_{A/I}[x]$ □

$M \supseteq (p)\,\mathbb{Z}[x]$

$M \longleftrightarrow$ massimali di $\frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \cong \mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x]$

$$\pi^{-1}((\overline{g(x)})) = \{q(x) \in \mathbb{Z}[x] \text{ t.c. } \overline{q(x)} = \overline{h(x)} \cdot \overline{g(x)} \text{ in } \mathbb{Z}/p\mathbb{Z}[x]\} =$$
$$= \{q(x) \in \mathbb{Z}[x] \text{ t.c. } q(x) - h(x)\cdot g(x) = p \cdot j(x)\} = (p, g(x))$$
$$q(x) = h(x)\cdot f(x) + p\, j(x)$$

$M \cap \mathbb{Z} = \{0\}$

In questo caso, considero $S = \mathbb{Z}\setminus\{0\}$ come parte moltiplicativa di $\mathbb{Z}[x]$

So che i primi di $\mathbb{Z}[x]$ che non intersecano S sono in bigezione con i primi di $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$

<u>Oss</u> $S^{-1}\mathbb{Z}[x] = \{\frac{p(x)}{n} \mid p(x) \in \mathbb{Z}[x], n \in \mathbb{Z}\setminus\{0\}\}$

$\mathbb{Q}[x] = \{a_0 + a_1 x + \dots + a_n x^n = \frac{\tilde{a}_0 + \tilde{a}_1 x + \dots + \tilde{a}_n x^n}{d}\}$

Osservo che $S \cap M = \emptyset$

$\Rightarrow M = g^{-1}((q(x))$ dove $q(x)$ è irriducibile in $\mathbb{Q}[x]$

e $g : \mathbb{Z}[x] \hookrightarrow \mathbb{Q}[x]$

Supponiamo che $q(x)$ sia a coefficienti interi e primitivi (senza perdita di generalità)

$g^{-1}((q(x)) = \{r(x) \in \mathbb{Z}[x] \mid \frac{r(x)}{1} \in (q(x)) \ \mathbb{Q}[x]\} = \{r(x) \in \mathbb{Z}[x] \text{ t.c. } q(x) \mid r(x) \text{ in } \mathbb{Q}[x]\}$

$\underset{\text{Lemma di Gauss}}{=} \{r(x) \in \mathbb{Z}[x] \mid r(x) \mid q(x) \text{ in } \mathbb{Z}[x]\} = (q(x))\,\mathbb{Z}[x]$

<u>Oss</u> Abbiamo dimostrato che gli ideali primi P di $\mathbb{Z}[x]$ t.c. $P \cap \mathbb{Z} = \{0\}$ sono tutti e soli quelli della forma $(q(x))$ con $q(x) \in \mathbb{Z}[x]$ irriducibile e primitivo + l'ideale (0)

Dimostro ora che nessun ideale della forma $(q(x))$ è massimale

Cerchiamo di dimostrare che $\mathbb{Z}[x]/(q(x))$ non è un campo, esibendo un elemento non invertibile

Come sarebbe fatto l'inverso di un intero n in questo quoziente?

Se $\overline{n}\cdot\overline{r(x)} = \overline{1}$ in $\mathbb{Z}[x]/(q(x))$

$\Leftrightarrow n\cdot r(x) = 1 + h(x)\,q(x)$

Scegliamo $x_0 \in \mathbb{Z}$ t.c. $q(x_0) \notin \{0,1,-1\}$ e scegliamo p un fattore primo di $q(x_0)$

Dico che $n = p$ non è invertibile in $\mathbb{Z}[x]/(q(x))$:

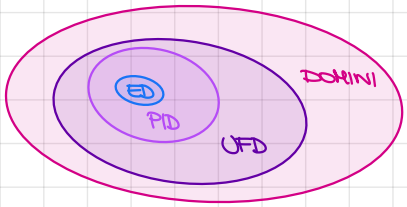
$n = p, x = x_0$: $p\cdot r(x_0) - h(x_0)\cdot q(x_0) = 1 \Rightarrow p \mid 1$ ↯

ED, PID, UFD

Def. Un dominio A si dice **dominio euclideo (ED)** se ammette una funzione grado $d: A\setminus\{0\} \longrightarrow \mathbb{N}$ tale che

(1) $d(x) \leq d(xy) \quad \forall x,y \in A\setminus\{0\}$

(2) $\forall x,y \in A \ y\neq 0 \quad \exists q,r$ tale che
$x = qy + r$ con $r = 0$ o $d(r) < d(y)$



esempio $(\mathbb{Z}, |\cdot|)$, $(\mathbb{K}[x], \deg)$
$(\mathbb{Z}[i], N)$, $(\mathbb{K}[[x]], d)$

Def. Un dominio A si dice **a ideali principali (PID)** se $\forall I \subseteq A$ ideale I è principale

Teorema Sia A un dominio euclideo
Gli elementi invertibili di A sono gli elementi di grado minimo
Gli ideali di A sono principali (ED $\Rightarrow$ PID)
e generati da un elemento di grado minimo
L'algoritmo di Euclide funziona e dà un MCD

Teorema Sia A PID.
Gli ideali primi di A sono (0) e gli ideali massimali

DIMOSTRAZIONE
Se $I=(0)$ o è massimale $\Rightarrow I$ è primo
Viceversa sia $I\neq(0)$ un ideale primo : $I=(x)$
$I=(x) \subseteq J=(y) \subsetneq A$
$\Rightarrow x = ya$, $a \in A \Rightarrow x \mid ya \Rightarrow x \mid y \vee x \mid a$
Se $x \mid y$: $y = xu \Rightarrow x = xua \Rightarrow ua = 1 \Rightarrow (x) = (xu) = (y)$
Se $x \mid a$: $a = xv \Rightarrow x = ya = yxv \Rightarrow yv = 1 \Rightarrow y$ invertibile $\Rightarrow (y) = A$ ↯ □

Proposizione (1) Siano A PID, B dominio, $\varphi: A \longrightarrow B$ omomorfismo surgettivo.
Allora φ è isomorfismo o B campo
(2) Sia A anello. Se $A[x]$ è PID, allora A è un campo.

DIMOSTRAZIONE
(1) $\frac{A}{\ker\varphi} \cong \mathrm{Im}\,\varphi = B$, dominio $\Rightarrow \ker\varphi$ primo
Quindi $\ker\varphi =$ $\{0\} \Rightarrow \varphi$ è isomorfismo ; massimale $\Rightarrow A/\ker\varphi \cong B$ campo

(2) $A[x] \longrightarrow A$
$p(x) \longmapsto p(0)$
Siccome $A \subseteq A[x]$ PID, A è un dominio
Applicando il punto (1), siccome φ non è isomorfismo, A è campo. □

def Dato A anello commutativo con unità,
$x \in A \setminus A^*$ si dice **irriducibile** se
$\forall y,z \in A \quad x = yz \implies y \in A^* \ \vee \ z \in A^*$

proposizione Sia A un dominio:
x primo $\implies x$ irriducibile

DIMOSTRAZIONE
x primo, $x = yz \quad y,z \in A$
$x \mid yz \implies x \mid y \ \vee \ x \mid z$
se $x \mid y \implies y = xu \implies x = xuz \implies uz = 1 \implies z$ è invertibile
quindi x è irriducibile $\square$

def Un dominio a fattorizzazione unica (UFD) è
un dominio A tale che $\forall x \in A \ x \notin A^* \cup \{0\}$,
x si scrive in modo "unico" come prodotto di irriducibili
(unico a meno dell'ordine dei fattori e moltiplicazione per elementi invertibili)

esempio $\mathbb{Z}$: $5 = 2 \cdot 3 = 3 \cdot 2 = (-3)(-2)$
$\mathbb{Z}[i]$: $5 = (2+i)(2-i) = (2i-1)(-2i+1)$
$\mathbb{Q}[x]$: $x^2 - 4 = (x+2)(x-2) = \left(\frac{1}{17}x + \frac{2}{17}\right)(17x - 34)$

proposizione Se A è UFD, allora in A esiste il MCD

DIMOSTRAZIONE
Siano $a,b \in A, \ a,b \neq 0$
allora $MCD(a,b) = \prod$ fattori irr. comuni con il min esponente $\square$

Oss A ED: $a,b \longrightarrow MCD$ tramite l'algoritmo di Euclide
$\longrightarrow (d, x_0, y_0) : d = MCD(a,b), \ d = ax_0 + by_0$
A PID: $(a,b) = (d)$ il generatore dell'ideale (a,b) è un mcd
$\exists x_0, y_0 \in A : ax_0 + by_0 = d$
A UFD: $a,b \longrightarrow \exists \, d = MCD(a,b)$ tramite la fattorizzazione

esempio $\mathbb{Z}[x] = (2,x) \quad MCD(2,x) = 1$
Se fosse $2a(x) + xb(x) = 1 \implies 2 \cdot \underset{\in \mathbb{Z}}{a(0)} + 0 = 1$ ↯

teorema Sia A un dominio. Sono fatti equivalenti:
(1) A è UFD
(2) (i) ogni irriducibile di A è primo
(ii) ogni catena discendente di divisibilità è stazionaria:
$\{a_n\}, \ a_{n+1} \mid a_n \ \forall n \implies \exists n_0 : a_{n_0} \sim a_m \ \forall m \geq n_0$

Oss (i) $\Leftrightarrow$ unicità della fattorizzazione
(ii) $\Leftrightarrow$ esistenza della fattorizzazione

Oss (ii) $\Leftrightarrow$ ogni catena ascendente di ideali principali è stazionaria
Infatti $\{a_n\}$ $a_{n+1} \mid a_n \ \forall n \iff (a_n) \subseteq (a_{n+1})$
$a_{n_0} \sim a_m \ \forall m \geq n_0 \iff (a_{n_0}) = (a_m)$

proposizione A PID $\Rightarrow A$ UFD

DIMOSTRAZIONE
(i) Ogni irriducibile è primo
$x \in A$ irriducibile, considero (x): è massimale $\Rightarrow$ primo $\Rightarrow x$ primo
Supponiamo $(x) \subseteq (y) \subsetneq A \Rightarrow x = ya$ $a \in A$
ma x è irriducibile $\Rightarrow$ $y \in A^*$ impossibile
$\vee$
$a \in A^* \Rightarrow (x) = (y)$

(ii) $\{(a_i)\}$ con $(a_n) \subseteq (a_{n+1})$ $\forall n$
Consideriamo $I = \bigcup_{k \geq 0} (a_k)$ è un ideale di $A \Rightarrow I = (a)$
$\Rightarrow a \in (a_{n_0}) \Rightarrow (a) \subseteq (a_{n_0}) \subseteq (a) \Rightarrow (a) = (a_{n_0})$
ma $(a) \subseteq (a_{n_0}) \subseteq (a_m) \subseteq (a)$ $\forall m \geq n_0$
quindi $(a) = (a_m)$ $\forall m \geq n_0$ □

esempio $A = K[\{x^{\frac{1}{n}}\}_{n \in \mathbb{N}}]$
non ha la proprietà (ii)
$\dots x^{\frac{1}{2^m}} \mid \dots \mid x^{\frac{1}{4}} \mid x^{\frac{1}{2}} \mid x$ e $\sqrt[2^m]{x} \cdot \sqrt[2^m]{x} = \sqrt[2^{m-1}]{x}$

esempio $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-5})$ non è UFD
perché 2 è irriducibile ma non è primo:
$N\begin{cases} 2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \\ 4 = (a^2+5b^2)(c^2+5d^2) \end{cases} \Rightarrow b = d = 0 \Rightarrow a = \pm 2, c = \pm 1$ o viceversa
quindi 2 è irriducibile
ma 2 non è primo:
$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$
ma $2 \nmid 1+\sqrt{-5}$ perché $\frac{1+\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$
$(2, 1+\sqrt{-5})$ non è principale

Teorema A UFD $\Rightarrow A[x]$ UFD

Corollario A UFD $\Rightarrow A[x_1,\dots,x_n]$ UFD

Oss A PID $\not\Rightarrow A[x]$ PID

esempio $\mathbb{Z}[x]$ non è PID

Def Dato A UFD, $f(x)\in A[x]$: $f(x)=\sum_{i=0}^{n} a_i x^i$

il **contenuto** di f è $c(f)=\mathrm{mcd}\{a_0,\dots,a_n\}$

f si dice **primitivo** se $c(f)=1$

$f=c(f)\,f'$ con f' primitivo

Lemma di Gauß A UFD, $f,g\in A[x]$, allora $c(f\cdot g)=c(f)\cdot c(g)$

DIMOSTRAZIONE

f e g primitivi, $c(f)=c(g)=1$

Per assurdo, sia $c(fg)\neq 1$

$\Rightarrow \exists\, p$ primo t.c. $p \mid c(f\cdot g)$

Sia $P=(p)$ ideale primo

$\pi: A[x] \longrightarrow A/p[x]$

$\sum a_i x^i \longmapsto \sum \bar{a}_i x^i$

$f \longmapsto \bar{f} \neq 0$

$g \longmapsto \bar{g} \neq 0$

$fg \longmapsto \overline{fg} = 0$

π è omomorfismo, quindi $0=\overline{fg}=\bar{f}\cdot\bar{g}$

è assurdo, poiché A/p è dominio $\Rightarrow A/p[x]$ dominio

Siamo ora $f,g\in A[x]$: $f=c(f)f'$, $g=c(g)g'$ con f',g' primitivi

$fg=c(fg)\,(fg)'$ con $(fg)'$ primitivo

$\Rightarrow c(fg)\,(fg)' = c(f)c(g)\,f'g'$

Considero i contenuti:

$c(\,c(fg)\,(fg)'\,) = c(fg)\,c((fg)') = c(fg)$

$c(c(f)c(g)\,f'g') = c(f)c(g)\,c(f'g') = c(f)c(g)$

□

corollario A UFD, $f,g \in A[x]$ e $c(f)=1$,
$f \mid g$ in $K[x]$ dove K è il campo dei quozienti di A.
Allora $f \mid g$ in $A[x]$

DIMOSTRAZIONE

$g(x)=f(x)h(x)$ con $h \in K[x]$

$\exists d \in A$ t.c. $h_1(x) = dh(x) \in A[x]$

$dg(x) = f(x)\, dh(x) = f(x) h_1(x)$

$d\,c(g) = c(f(x))\, c(h_1(x)) = c(h_1(x))$

$\Longrightarrow d \mid c(h_1(x)) \Longrightarrow h(x) = \frac{h_1(x)}{d} \in A[x]$ □

corollario A UFD, K campo dei quozienti di A, $f(x) \in A[x]$
$f(x) = g(x)h(x)$ in $K[x]$
Allora $\exists g_1, h_1 \in A[x]$ con $\deg g = \deg g_1$, $\deg h = \deg h_1$ tali che
$f(x) = g_1(x) h_1(x)$ in $A[x]$

DIMOSTRAZIONE

$f(x) \in A[x]$, $f(x) = g(x)h(x)$ in $K[x]$

$\exists d \in A : g_0(x) = dg(x) \in A[x]$

$f(x) = dg(x)\, d^{-1}h(x) = g_0(x)\, d^{-1}h(x)$

Scrivo $g_0(x) = c(g_0)\, g_1$ con $g_1 = g_0$ primitivo

$f(x) = g_1(x)\, \underbrace{(d^{-1}c(g)\, h(x))}_{h_1(x) \in K[x]}$

$A[x]$ $A[x]$

$\Longrightarrow g_1(x) \mid f(x)$ in $K[x]$ e g_1 primitivo

$\Longrightarrow g_1(x) \mid f(x)$ in $A[x]$ e quindi $h_1(x) \in A[x]$ □

esempio $(x^2+2x-3) = (\frac{2}{3}x - \frac{2}{3})(\frac{3}{2}x + \frac{9}{2}) = (x-1)(x+3)$

teorema A UFD, $K = Q(A)$
Gli elementi irriducibili di $A[x]$ sono:
(1) le costanti irriducibili in A
(2) f con $\deg f \geq 1$, $c(f)=1$ e f irriducibile in $K[x]$

criterio di Eisenstein

A UFD, $f(x) \in A[x]$ primitivo, $f(x) = \sum_{i=0}^{n} a_i x^i$

Sia P un ideale primo tale che:

(i) $a_n \notin P$

(ii) $a_i \in P \quad i = 0, \dots, n-1$

(iii) $a_0 \notin P^2$

Allora $f(x)$ è irriducibile in $A[x]$

DIMOSTRAZIONE

Caso $A = \mathbb{Z}$, $P = (p)$:

$f(x) \equiv a_n x^n \ (p)$

$f(x) = g(x)h(x) \implies a_n x^n = \overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x)$ in $\mathbb{F}_p[x]$

$\Rightarrow \overline{g}, \overline{h}$ sono monomi $\implies g(x) = d_m x^m + p \cdot (\dots)$

$h(x) = c_{n-m} x^{n-m} + p \cdot (\dots)$

$\Rightarrow a_0 = d_0 c_0 = p^2 \cdot (\dots)$ ↯

Caso generale:

$P \lhd A$, $P[x] = \{ p(x) = i_n x^n + \dots + i_1 x + i_0 \mid i_j \in P \} \subseteq A[x]$

$f(x) \equiv a_n x^n \quad (P[x])$

$\overline{f(x)} = \overline{a_n x^n}$ in $A[x]/P[x] \cong A/P\,[x]$

$A[x] \longrightarrow A/P\,[x]$

$\sum a_i x^i \longmapsto \sum \overline{a}_i x^i$

La dimostrazione è analoga al caso precedente perché vale:

A/I dominio $\Rightarrow$ in $A/I\,[x]$ i divisori di un monomio sono monomi

Per induzione sul grado:

D dominio $\quad b_m x^m + \dots + b_0 \in D[x]$

$c_{n-m} x^{n-m} + \dots + c_0 \in D[x]$

$b_0 c_0 = 0$

$b_0 = 0 \implies b_1 c_0 = 0$ → $b_1 = 0$ itero il processo; $c_0 = 0$ ✓

□

esempio $\mathbb{Z}[i]$: $x^4 - 5x^2 + (6+3i)x + 6 + 3i$

è $(2+i)$-Eisenstein

esempio $\mathbb{Q}[x,y] = \mathbb{Q}[x][y]$ è UFD

$I = (y^2 - x^3)$ primo

$A/I[x]$: vale $x \cdot x \cdot x = y \cdot y$

$\iff y^2 - x^3$ primo $\iff y^2 - x^3$ irriducibile

$y^2 - x^3 = p_1(x,y)\, p_2(x,y)$

Se $\deg_y p_1(x,y) = 0 \implies p_1(x,y) = p_1(x)$

$\implies p_1(x) \mid (1, -x^3) = 1 \implies p_1(x)$ è invertibile in $\mathbb{Q}[x]$

Se $\deg_y p_1(x,y) = 1$ $\quad p_1 = a(x)y + b(x)$ $\quad p_2 = c(x)y + d(x)$

$a(x)c(x) = 1 \implies a(x) = c(x) = 1$

$b(x) + d(x) = 0 \implies b(x) = -d(x)$

$y^2 - b(x)^2 = y^2 - x^3$ ↯

x è irriducibile in $A/I[x]$

non riesco a fattorizzare $\overline{x} = \overline{p_1}\,\overline{p_2}$ in A/I

$x = p_1(x,y)\, p_2(x,y) + q(x,y)(x^2 - y^3)$

proposizione (1) P ideale primo di $A \implies P[x]$ ideale primo di $A[x]$

(2) $q(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ è invertibile $\iff a_0 \in A^*, a_1, \dots, a_n \in \sqrt{0}$ (sono nilpotenti)

DIMOSTRAZIONE

(1) $\dfrac{A[x]}{P[x]} \cong A/P[x]$ è un dominio $\implies P[x]$ è primo

(2) ($\Leftarrow$) Cerchiamo un inverso

$a_0^{-1} \cdot q(x) = 1 + a_1' x + \dots + a_n' x^n$ con a_i' nilpotenti

(infatti $a_i'^k = (a_0^{-1} a_i)^k = 0$)

$1 - (a_1' x + \dots + a_n' x^n)^{mk} = 1$

$(1 + \underbrace{a_1' x + \dots + a_n' x^n}) \cdot r(x)$

Oss per $m \geq n$ si ha

$(a_1' x + \dots + a_n' x^n)^{mk} = 0$

$\sum_{i_1 + \dots + i_n = mk} \binom{mk}{i_1, \dots, i_n} (a_1' x)^{i_1} \cdots (a_n' x^n)^{i_n}$ per ogni addendo c'è un esponente $\geq k$

Oss $a_i x^i \in \sqrt{(0)} \implies a_1' x + \dots + a_n' x^n \in \sqrt{(0)}$

$\implies \exists h \geq 1$ t.c. $(a_1' x + \dots + a_n' x^n)^h = 0$

Oss $a_0^{-1} q(x) = 1 - (\overbrace{-a_1' x - \dots - a_n' x^n}^{y})$

$a_0^{-1} q(x)(1 + y + \dots + y^{h-1}) = (1 - y)(1 + y + \dots + y^{h-1}) = 1 - y^h = 1$

($\Longrightarrow$) Sia $q(x) \in A[x]^*$

Sia $r(x) \in A[x]^*$ t.c. $q(x) \cdot r(x) = 1$

$\implies a_0 r_0 = q(0) r(0) = 1 \implies a_0 \in A^*$

Sia ora P un primo di A. Consideriamo

$\overline{q(x)} \cdot \overline{r(x)} = \overline{1}$ in $\dfrac{A[x]}{P[x]} \cong A/P[x]$

$\implies \overline{q(x)}$ è invertibile in $A/P[x]$ e siccome $(A/P[x])^* = (A/P)^*$

$\overline{q(x)}$ è costante in $A/P[x]$

cioè tutti i coefficienti $a_1, \dots, a_n \in P$

$\implies a_i \in \bigcap_{P \text{ primo}} P = \sqrt{(0)}$ □

Dominio non UFD

$A = \mathbb{Z}[x]/(x^2+5)$

$A \cong \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$

$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C}$

$p(x) \longmapsto p(\sqrt{-5})$

$\ker\varphi \ni x^2+5 \implies (x^2+5) \subseteq \ker\varphi$

$\ker\varphi \subseteq (x^2+5)$: sia $q(x) \in \mathbb{Z}[x]$ t.c. $\varphi(q(x)) = 0$

$\psi : \mathbb{Q}[x] \longrightarrow \mathbb{C}$

$p(x) \longmapsto p(\sqrt{-5})$ $\quad \ker\psi = (x^2+5)$

$\implies \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, $q(x) \in \ker\psi$

$\implies q(x) \in (x^2+5)\mathbb{Q}[x]$: $q(x) = (x^2+5)r(x)$ con $r(x) \in \mathbb{Q}[x]$

Gauss $\implies x^2+5 \mid q(x)$ in $\mathbb{Z}[x] \implies q(x) \in (x^2+5)\mathbb{Z}[x]$

Per il I teorema di omomorfismo:

$$A = \frac{\mathbb{Z}[x]}{(x^2+5)} \cong \operatorname{Im}\varphi = \{a\sqrt{-5}+b \mid a,b \in \mathbb{Z}\}$$

$$\overline{p(x)} = \overline{ax+b} \longmapsto a\sqrt{-5}+b$$

Quindi A è un dominio perché $A \subseteq \mathbb{C}$ o perché (x^2+5) è primo

$A^* = ?$

$N : A \longrightarrow \mathbb{Z}_{\geq 0}$

$z = a+b\sqrt{-5} \longmapsto a^2+5b^2 = z\cdot\bar{z}$

$N(z_1z_2) = N(z_1)N(z_2)$

Se $z \in A$ è un'unità, cioè $\exists u \in A$ t.c. $zu = 1$

allora $N(z)N(u) = N(zu) = N(1) = 1 \implies N(z) = 1$

Scrivendo $z = a+b\sqrt{-5}$, scopriamo che $a^2+5b^2 = 1$, quindi $b = 0$, $a = \pm 1$

Quindi $A^* = \{\pm 1\}$

A non è UFD. Osserviamo che

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Mostriamo che 2 è irriducibile: $2 = z_1z_2$

$\implies 4 = N(2) = N(z_1)N(z_2)$

- $N(z_1) = 4$, $N(z_2) = 1 \longrightarrow z_2 = \pm 1$: $2 = (\pm 2)(\pm 1)$
- $N(z_1) = N(z_2) = 2 \longrightarrow a^2+5b^2 = 2$ non ha soluzioni in $\mathbb{Z}$

Analogamente 3 e $1 \pm \sqrt{-5}$ sono irriducibili,

quindi 6 ha due fattorizzazioni in irriducibili distinte

UFD non PID

$\mathbb{Z}[x]$ è UFD, ma non PID ($(2,x)$ non è principale)

$\mathbb{Q}[x,y]$ è UFD, ma non PID ((x,y) non è principale)

PID non ED

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \cong \frac{\mathbb{Z}[x]}{(x^2-x+5)}$$

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C}$$
$$p(x) \longmapsto p\left(\frac{1+\sqrt{-19}}{2}\right)$$

$\ker\varphi = (x^2-x+5) \implies \frac{\mathbb{Z}[x]}{(x^2-x+5)} \cong \operatorname{Im}\varphi = \left\{a+b\frac{1+\sqrt{-19}}{2} \mid a,b\in\mathbb{Z}\right\}$

Per assurdo, sia A euclideo con una funzione grado deg

Studiamo A^* $\qquad N : A \longrightarrow \mathbb{Z}$

$$a+b\omega \longmapsto (a+b\omega)(a+b\bar{\omega}) = a^2+ab(\omega+\bar{\omega})+b^2\omega\bar{\omega} =$$
$$= a^2+ab+5b^2$$

Se $z=a+b\omega$ è un'unità e u è la sua inversa

$$N(z)N(u) = N(zu) = N(1) = 1$$
$$\implies 1 = N(z) = a^2+ab+5b^2 = \left(a+\frac{b}{2}\right)^2 + \frac{19}{4}b^2$$
$$\implies b=0,\ a=\pm 1 \implies A^* = \{\pm 1\}$$

Sia ora $d := \min\{\deg z \mid z\in A\setminus\{\pm 1, 0\}\}$ e sia x t.c. $\deg x = d$

Per ogni elemento $z\in A$, facendo la divisione con il resto, trovo

$$z = xq+r \quad q\in A,\ r=0 \text{ oppure } \deg r < d \implies r = 0, \pm 1$$

Consideriamo il quoziente $A/(x)$

Questo mostra che $-1, 0, 1$ rappresentano tutti gli elementi del quoziente

$$\implies 1 < |A/(x)| \leq 3 \implies A/(x) = \mathbb{F}_2 \text{ o } \mathbb{F}_3$$

Ma $\omega\in A$, che è una radice di x^2-x+5

Allora $\bar{\omega}\in A/(x)$ è una radice dello stesso polinomio, ma

il polinomio x^2-x+5 non ha radici in $\mathbb{F}_2$ o $\mathbb{F}_3$ ↯

TEORIA DEI CAMPI

Def. Siano $K \subseteq L$ campi: diremo che L/K è un' **estensione di campi**

$\alpha \in K$

$\varphi_\alpha : K[x] \longrightarrow K[\alpha] = \{p(\alpha) \mid p(x) \in K[x]\} \subset L$

$p(x) \longmapsto p(\alpha)$

$K[x]/\ker\varphi_\alpha \cong K[\alpha]$

$\ker\varphi_\alpha$ è un ideale di $K[x]$. è principale

$K[x]/\ker\varphi_\alpha \cong K[\alpha] \subset L$ campo $\Rightarrow K[\alpha]$ è un dominio

$\Rightarrow \ker\varphi_\alpha$ è un ideale primo di $K[x]$

$\ker\varphi_\alpha = \{p(x) \in K[x] \mid p(\alpha) = 0\} =$ $\begin{cases} (0) \\ \text{massimale} : (\mu_\alpha(x)) \text{ con } \mu_\alpha(x) \text{ irriducibile} \end{cases}$

Def. Se $\ker\varphi_\alpha = (0)$, α è **trascendente** su K

Se $\ker\varphi_\alpha \neq (0)$, α è **algebrico** su K

Oss $\alpha \in L$ è algebrico su K se $\exists f(x) \in K[x]$, $f(x) \neq 0$ t.c. $f(\alpha) = 0$

potenze di α non sono tutte linearmente indipendenti su K

$\alpha \in L$ è trascendente su K se $\nexists f(x) \in K[x]$, $f(x) \neq 0$ t.c. $f(\alpha) = 0$

potenze di α $\{\alpha^i\}_{i \geq 0}$ sono linearmente indipendenti su K

Oss α è algebrico su $K \iff K[\alpha] \cong \frac{K[x]}{\ker\varphi_\alpha}$ è un campo

Quindi $K[\alpha] = \left\{\frac{p(\alpha)}{q(\alpha)} \mid p(x), q(x) \in K[x], q(\alpha) \neq 0\right\}$

esempio $\mathbb{Q}[\sqrt[3]{2}]$ $\quad \frac{1}{\sqrt[3]{2}} = \frac{\sqrt[3]{4}}{2} = p(\sqrt[3]{2})$ dove $p(x) = \frac{1}{2}x^2 \in \mathbb{Q}[x]$

$a + b\sqrt[3]{2} + c\sqrt[3]{4}$ $\quad \frac{1}{1+\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2})$ $\quad \{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$

$\ker\varphi_\alpha$ è principale, generato da un polinomio irriducibile

$\ker\varphi_\alpha = (f(x)) = (g(x))$ $\quad f(x) = u\,g(x)$ $\quad u \in K[x]^* = K^*$

Def. Il **polinomio minimo di α su K** è l'unico generatore monico di $\ker\varphi_\alpha$, $\mu_\alpha(x)$.

$K(\alpha) = K[\alpha] = K[x]/(\mu_\alpha(x))$ $\quad \mu_\alpha(x)$: · si annulla in α
· è monico
· è irriducibile su K

Sia $g \in K[x]$ con queste proprietà

$g(x) \in (\mu_\alpha(x)) \Rightarrow \mu_\alpha(x) \mid g(x)$: $g(x) = p(x)\,\mu_\alpha(x) \Rightarrow p(x) \in K^*$

$g(x)$ e $\mu_\alpha(x)$ monici $\Rightarrow p(x) = 1$

Def. Data un'estensione L/K, il **grado di L su K** è
$$[L:K] = \dim_K L$$
L/K si dice **finita** se $[L:K] < +\infty$

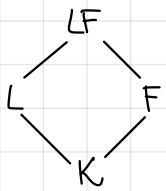
Proposizione Se $\alpha \in L$ è algebrico su K, allora
$$[K(\alpha):K] = \dim_K \frac{K[x]}{(\mu_\alpha(x))} = \deg \mu_\alpha(x)$$

DIMOSTRAZIONE
$\frac{K[x]}{(\mu_\alpha(x))} = \langle 1, x, x^2, \dots, x^{d-1} \rangle$ dove $d = \deg \mu_\alpha(x)$

Una base di $K(\alpha)$ su K è $\{1, \alpha, \dots, \alpha^{d-1}\}$
e tramite l'isomorfismo $x^i \longmapsto \alpha^i$, segue la tesi $\square$

Def. Siano $K \subseteq L$ campi, $S \subseteq L$ sottoinsieme
$K(S)$ = il più piccolo sottocampo di L che contiene K e S
$$= \bigcap_{\substack{F \subseteq L \\ S, K \subseteq F}} F = \left\{ \frac{p(s_1, \dots, s_t)}{q(s_1, \dots, s_t)} \mid p, q \text{ polinomi a coeff. in } K,\ s_i \in S,\ t \in \mathbb{N} \right\}$$

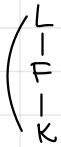
Def. Dati $L, F \subset \Omega$ campo, il **composto di L e F** è
$LF = L(F) = F(L)$



<u>Oss</u> Se $L = K(\alpha_1, \dots, \alpha_t)$, $F = K(\beta_1, \dots, \beta_s)$
$LF = K(\alpha_1, \dots, \alpha_t, \beta_1, \dots, \beta_s)$

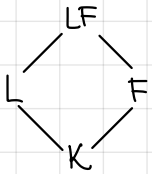
Proprietà della estensioni finite

① **Proposizione (Torri)** L/K finita $\iff$ L/F e F/K finite
$$[L:K] = [L:F] \cdot [F:K]$$



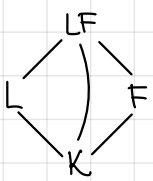
DIMOSTRAZIONE
Data $\{v_i\}_i$ base di L su F e $\{w_j\}_j$ base di F su K,
si verifica che $\{v_i w_j\}_{i,j}$ è base di L su K $\square$

② **Proposizione (Shift)** L/K finita $\Rightarrow$ LF/F finita



DIMOSTRAZIONE
$\{v_1, \dots, v_n\}$ K-base di L $\Rightarrow$ $v_1, \dots, v_n$ genera FL su F
Infatti $LF = F(L) = F(v_1, \dots, v_n)$ $(\supseteq)$ chiaro
$(\subseteq) \forall \alpha \in L : \alpha = \sum \lambda_i v_i \in F(v_1, \dots, v_n)$ $\square$

③ **Proposizione (composto)** L/K e F/K finite $\Rightarrow$ LF/K finita



DIMOSTRAZIONE
Si usa SHIFT + TORRI
$n, m \mid [LF:K] \Rightarrow [m,n] \mid [LF:K] \leq mn$ $\square$

Estensioni algebriche

Def. L/K si dice **algebrica** se $\forall \alpha \in L$, α è algebrico su K

Proposizione L/K finita $\Rightarrow$ L/K algebrica

DIMOSTRAZIONE

$\alpha \in L$: considero $\{\alpha^i\}_{i\geq 0} \subset L$

$[L:K] = n \Rightarrow \{1, \alpha, \dots, \alpha^n\}$ sono $n+1$ elementi

in uno spazio di dimensione $n \Rightarrow$ sono linearmente dipendenti

$\Rightarrow \exists \lambda_0, \dots, \lambda_n \in K$ non tutti nulli t.c. $f(x) = \sum_{i=0}^{n} \lambda_i x^i \in K[x]$ $f(\alpha) = 0$

$\Rightarrow \alpha$ è algebrico □

Il viceversa è falso.

Oss Dati $K \subset L$, $A = \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}$,

con $K \subseteq A \subseteq L$, è un campo.

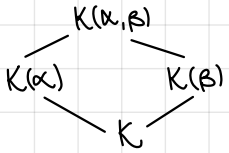
DIMOSTRAZIONE

Se $\alpha, \beta \in A \Rightarrow \alpha \pm \beta, \alpha \cdot \beta, \alpha^{-1} \in K(\alpha, \beta)$

$K(\alpha)/K$ è finita, $K(\beta)/K$ è finita

$K(\alpha,\beta)/K$ finita $\Rightarrow$ $K(\alpha,\beta)/K$ algebrica

$\Rightarrow K(\alpha,\beta) \subset A$ □



esempio $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$ è un campo

$\overline{\mathbb{Q}}/\mathbb{Q}$ è algebrica ma non è finita $[\overline{\mathbb{Q}} : \mathbb{Q}] = +\infty$

$x^n - 2$: $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ $\forall n$ $\Rightarrow$ $\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\sqrt[n]{2})}_{n} \subset \overline{\mathbb{Q}}$

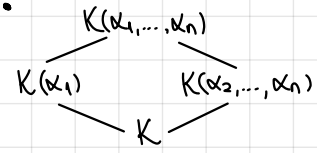
Proposizione Sia $L = K(\alpha_1, \dots, \alpha_n)$, con α_i algebrico su K

Allora $[L:K] < +\infty$

DIMOSTRAZIONE

Per induzione su n:

- $[K(\alpha_1) : K] = \deg \mu_{\alpha_1}(x) < +\infty$
-



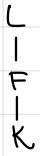
$K \subseteq K(\alpha_1) \subseteq K(\alpha_1)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n)$

Per la proprietà del composto, è finito

□

Proprietà della estensioni algebriche

① **proposizione (Torri)** L/K algebrica $\iff$ L/F e F/K algebriche



DIMOSTRAZIONE

($\Longrightarrow$) $\alpha \in L$ è algebrico su K, quindi su F

$\alpha \in F \subset L$ è algebrico su K

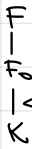
($\Longleftarrow$) $\alpha \in L$: è algebrico su F

$\Rightarrow \exists f(x) \in F[x]$, $f(x) \neq 0$, $f(\alpha) = 0$

Ora $f(x) = \sum_{i=0}^{n} a_i x^i$

Considero $K \subset K(a_0, \dots, a_n) = F_0 \subset F$

α è algebrico su F_0



$|F_0 : K| < +\infty$ perché algebrica e finitamente generata

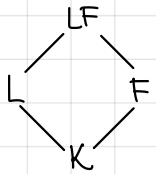
$$K \subseteq F_0 \subseteq F_0(\alpha)$$

($K \subseteq F_0$ finita, $F_0 \subseteq F_0(\alpha)$ finita)

$\Rightarrow F_0(\alpha)/K$ finita $\Rightarrow$ algebrica

$\Rightarrow \alpha$ è algebrico su K □

② **proposizione (shift)** L/K algebrica $\Longrightarrow$ LF/F algebrica

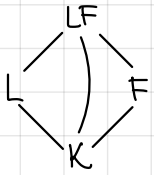


DIMOSTRAZIONE

$LF = F(L)$ $\forall \alpha \in L$ α è algebrico su K, e quindi su F

$\Rightarrow F(L)$ è algebrica perché generata da elementi algebrici □

③ **proposizione (composto)** L/K e F/K algebriche $\Longrightarrow$ LF/K algebrica



DIMOSTRAZIONE

Analoga alle estensioni finite. □

Def. Ω campo si dice **algebricamente chiuso** se
$\forall f(x) \in \Omega[x] \setminus \Omega$, f ammette una radice in Ω

Conseguenza. (1) Gli unici polinomi irriducibili di $\Omega[x]$ sono quelli di grado 1
(2) Ogni polinomio $f \in \Omega[x]$ si fattorizza
completamente in fattori irriducibili di primo grado

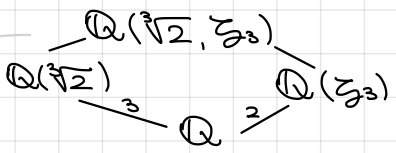
Def. Sia K un campo.
Una **chiusura algebrica** di K è un campo $\overline{K}$ algebricamente chiuso
tale che $\overline{K}/K$ sia un'estensione algebrica

Teorema Sia K un campo.
Allora K ammette una chiusura algebrica
e questa è unica a meno di isomorfismo su K.
(Se Ω_1 e Ω_2 sono due chiusure algebriche di K,
allora $\exists \varphi : \Omega_1 \xrightarrow{\sim} \Omega_2$ t.c. $\varphi|_K = id$)

Def. Sia K campo, $f(x) \in K[x]$
Il **campo di spezzamento** di $f(x)$ su K è $K(\alpha_1, \dots, \alpha_n)$,
cioè il più piccolo campo che contiene K e tutte le radici di f

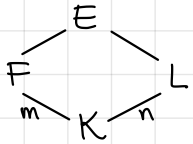
Def. Sia K un campo e $\mathcal{F} = \{f_i(x)\}_{i \in I} \subseteq K[x] \setminus K$
$\forall i \in I$, sia $\{\alpha_{ij}\}_{j=1,\dots,d_i} \subseteq \overline{K}$ l'insieme delle radici di $f_i(x)$
Il campo di spezzamento su K della famiglia $\mathcal{F}$ in $\overline{K}$ è il campo
$K(\{\alpha_{ij}\}_{i \in I, j=1,\dots,d_i}) \subseteq \overline{K}$

esempio $K = \mathbb{Q}$, $f(x) = x^3 - 2$ $\quad \alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\,\xi_3$, $\alpha_3 = \sqrt[3]{2}\,\xi_3^2$
$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2) = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$



grado pol. min. di ξ_3 su $\mathbb{Q}(\sqrt[3]{2})$ è 2
$[\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}(\sqrt[3]{2})] \geq 2 \iff \xi_3 \notin \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$
$[\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}(\sqrt[3]{2})] \leq [\mathbb{Q}(\xi_3) : \mathbb{Q}] \leq 2$

Oss



con $(m,n) = 1$
$\Rightarrow [E : K] = m \cdot n$

esempio Se $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{2})$ $(m=3)$, $L = \mathbb{Q}(\sqrt[3]{2}\,\xi_3)$ $(n=3)$
$E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\xi_3) = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ $\quad [E : \mathbb{Q}] = 6 \neq 3 \cdot 3$

esempio $K=\mathbb{Q}$, $f(x)=x^{101}-2$

$\mathbb{Q}(\sqrt[101]{2}, \sqrt[101]{2}\,\zeta_{101}, \dots, \sqrt[101]{2}\,\zeta_{101}^{100}) = \mathbb{Q}(\sqrt[101]{2}, \zeta_{101})$

teorema Sia $p(x)=a_n x^n+\dots+a_0 \in \mathbb{Z}[x]$ e $r=\frac{p}{q}\in\mathbb{Q}$, $(p,q)=1$ t.c. $p(r)=0$

Allora $p \mid a_0$ e $q \mid a_n$

esempio CdS su $\mathbb{Q}$ di x^4+3x^2+1

Radici in $\mathbb{C}$: $t=\frac{-3\pm\sqrt{5}}{2}$ $\qquad x_{1,2,3,4}=\pm\sqrt{\frac{-3\pm\sqrt{5}}{2}}$

$$\left(t-\tfrac{-3+\sqrt{5}}{2}\right)\left(t-\tfrac{-3-\sqrt{5}}{2}\right)=\left(x^2-\tfrac{-3+\sqrt{5}}{2}\right)\left(x^2-\tfrac{-3-\sqrt{5}}{2}\right)\in\mathbb{R}[x]$$

$\Longrightarrow f(x)$ irriducibile

$x_1 x_3 = 1$

$\mathbb{Q}(x_1,x_2,x_3,x_4)=\mathbb{Q}(x_1,x_3)=\mathbb{Q}(x_1)$

$\mathbb{Q}(x_1)$ | 4 | $\mathbb{Q}$

esempio $\mathbb{Q}\subseteq\mathbb{C}$

$\overline{\mathbb{Q}}=\{\alpha\in\mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$ è una chiusura algebrica di $\mathbb{Q}$

Abbiamo visto che $\overline{\mathbb{Q}}$ è un campo e che $\overline{\mathbb{Q}}/\mathbb{Q}$ è algebrico.

Sia $f(x)\in\overline{\mathbb{Q}}[x]\setminus\mathbb{Q}$

Sia $\alpha\in\mathbb{C}$ una radice di f

$\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}}(\alpha)$ (alg, alg; alg)

$\Longrightarrow \alpha$ è algebrico su $\mathbb{Q} \Longrightarrow \alpha\in\overline{\mathbb{Q}}$

$\mathbb{Q} \underset{\text{alg}}{\subseteq} K \subseteq \overline{\mathbb{Q}}$ $\qquad \overline{K}=\overline{\mathbb{Q}}$

Problema 1: $K \hookrightarrow \overline{K}$ $\qquad \alpha\in\overline{K}$

$\varphi: K(\alpha)\hookrightarrow\overline{K}$ in quanti modi?

$\varphi|_K = id$

$K(\alpha)\cong\frac{K[x]}{(\mu_\alpha(x))}$

$\alpha \longleftrightarrow x$

$\tilde{\varphi}: K[x] \longrightarrow \overline{K}$ con $\ker\tilde{\varphi}\supseteq(\mu_\alpha(x))$ (basta perché $(\mu_\alpha(x))$ è massimale)

$x\mapsto\beta$

$\frac{K[x]}{(\mu_\alpha(x))}$

$\tilde{\varphi}(\mu_\alpha(x))=\mu_\alpha(\beta)=0$

$\Longrightarrow \beta\in\overline{K}$ deve essere una radice di $\mu_\alpha(x)$

Le immersioni $\varphi: K(\alpha)\longrightarrow\overline{K}$ con $\varphi|_K=id$ sono tante quante le radici distinte di $\mu_\alpha(x)$ in $\overline{K}$.

Se $\{\alpha_1,\dots,\alpha_m\}$ sono le radici distinte di $\mu_\alpha(x)$ in $\overline{K}$

$\Longrightarrow \varphi_1,\dots,\varphi_m$ immersioni $K(\alpha)\longrightarrow\overline{K}$, $\varphi_i|_K=id$

$\varphi_i(\alpha)=\alpha_i \qquad \forall i=1,\dots,m$

Problema 2. Quante sono le radici distinte di $\mu_\alpha(x)$ in $\overline{K}$?

criterio della derivata $f(x) \in K[x]$ ha fattori multipli $\iff (f(x), f'(x)) \neq 1$

corollario $f \in K[x]$ irriducibile ha radici multiple in $\overline{K} \iff f'(x) = 0$

DIMOSTRAZIONE

f ha radici multiple in $\overline{K} \iff (f, f') \neq 1 \iff (f, f') = f$

$\iff f \mid f'$ ma $\deg f' < \deg f \iff f' = 0$ □

corollario Sia $f \in K[x]$ e $\operatorname{char} K = 0$

Se f è irriducibile, allora ha radici distinte in $\overline{K}$

esempio $K = \mathbb{F}_{p^n}$ ogni polinomio irriducibile ha derivata diversa da 0

esempio $K = \mathbb{F}_p(x)$ campo dei quozienti di $A = \mathbb{F}_p[x]$

$K[t] \ni f(t) = t^p - x$ è irriducibile in $K[t]$, infatti:

è irriducibile in $A[t]$ perché è $P = (x)$ - Eisenstein

Per il lemma di Gauß, è irriducibile in $K[t]$

$f'(t) = pt^{p-1} = 0$

$\alpha \in \overline{K}$: $f(\alpha) = \alpha^p - x = 0 \implies x = \alpha^p$

$f(t) = t^p - \alpha^p = (t - \alpha)^p$ in $\overline{K}$

def. K si dice **perfetto** se

$\forall f \in K[x]$ irriducibile, f ha radici distinte in $\overline{K}$

Oss $\operatorname{char} K = 0 \implies K$ perfetto

K finito $\implies K$ perfetto

esempio $\mathbb{Q}(\sqrt[3]{2})$ $\mu_\alpha(x) = x^3 - 2$

$\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$

$\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \overline{\mathbb{Q}}$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}$

$\sqrt[3]{2}\,\zeta_3$

$\sqrt[3]{2}\,\zeta_3^2$

$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\,\zeta_3) \cong \mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2) \cong \frac{\mathbb{Q}[x]}{(\mu_\alpha(x))}$

$K = \mathbb{Q}(\sqrt[3]{2})$, $\alpha \in \overline{\mathbb{Q}}$

$K(\alpha) \hookrightarrow \overline{\mathbb{Q}}$

Id_K fa qualche cosa di assegnato

proposizione Sia $[K(\alpha):K] = \deg \mu_\alpha(x) = n$
Ogni immersione $\varphi: K \longrightarrow \overline{K}$,
ammette esattamente n estensioni
$\varphi_1, \dots, \varphi_n : K(\alpha) \longrightarrow \overline{K}$ con $\varphi_i|_K = \varphi$

DIMOSTRAZIONE

$K(\alpha) \cong \frac{K[x]}{(\mu_\alpha(x))}$
$\alpha \longmapsto \overline{x}$

$\tilde{\varphi}: K[x] \longrightarrow \overline{K}$
$x \longmapsto \beta$

$\frac{K[x]}{(\mu_\alpha(x))}$ con $\mu_\alpha(x) \in \ker \tilde{\varphi}$

$\mu_\alpha(x) \in \ker \tilde{\varphi} \iff \tilde{\varphi}(\mu_\alpha(x)) = (\varphi\mu_\alpha)(\beta) = 0$
la condizione è che β sia una radice del polinomio $\varphi\mu_\alpha(x)$ in $\overline{K}$
$\varphi: K \hookrightarrow \overline{K}$, $\varphi(K) \cong K$: $K[x] \cong (\varphi(K))[x]$
$\Longrightarrow \deg \varphi\mu_\alpha = \deg \mu_\alpha = n$ e $\varphi\mu_\alpha(x)$ è irriducibile perché lo è $\mu_\alpha(x)$
$\Longrightarrow \#\{\tilde{\varphi}: K(\alpha) \longrightarrow \overline{K} \text{ con } \varphi_{|K} = \varphi\} = \#\{\text{radici distinte di } \varphi(\mu_\alpha)(x)\} =$
$= \deg \varphi\mu_\alpha = \deg \mu_\alpha = n$
$\varphi\mu_\alpha$ è irriducibile.

□

teorema Sia E/K con $[E:K] = n$
Allora ogni $\varphi: K \hookrightarrow \overline{K}$ ammette
esattamente n estensioni a E
$(\exists!\ \varphi_1, \dots, \varphi_n : E \longrightarrow \overline{K}$ t.c. $\varphi_i|_K = \varphi)$

DIMOSTRAZIONE
Per induzione su n
- $n=1$: ovvio
- $n>1$: $\exists \alpha \in E \setminus K$

$K \subsetneq K(\alpha) \subseteq E$
$\quad m \quad\quad d$
$md = n$

Se $d=1$: $E = K(\alpha)$, la tesi segue dalla proposizione precedente.
Se $1<d<n$, per la proposizione, φ ammette m estensioni a $K(\alpha)$ $\varphi_1, \dots, \varphi_m$
con $\varphi_i|_K = \varphi$
Per ipotesi induttiva, $\varphi_i: K(\alpha) \hookrightarrow \overline{K} = \overline{E}$
ammette d estensioni a E $\varphi_{i1}, \dots, \varphi_{id}$ $\varphi_{ij}|_K = \varphi_i|_K = \varphi$
$\Longrightarrow \{\varphi_{ij}\}_{i=1,\dots,m,\ j=1,\dots,d}$ sono le immersioni cercate

Sia $\psi: E \longrightarrow \overline{K}$ t.c. $\psi|_K = \varphi$
$\psi|_{K(\alpha)}: K(\alpha) \hookrightarrow \overline{K}$ e $(\psi|_{K(\alpha)})|_K = \psi|_K = \varphi$
$\Longrightarrow \psi|_{K(\alpha)} = \varphi_i$ per $i \in \{1, \dots, m\}$
ψ è un'estensione di φ
$\Longrightarrow$ per ipotesi induttiva, $\psi = \varphi_{ij}$ per $j \in \{1, \dots, d\}$

□

Def. F/K algebrica si dice **estensione normale** se $\forall \varphi: F \hookrightarrow \overline{K}$ t.c. $\varphi|_K = id$ si ha $\varphi(F) = F$

esempio $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è normale
perché $\mathbb{C} \supseteq \mathbb{Q}(\sqrt[3]{2}\,\xi_3) \supsetneq \mathbb{Q}(\sqrt[3]{2})$

esempio Tutte le estensioni di grado 2 sono normali
$L/K \quad [L:K]=2 \quad (\mathrm{char}\, K \neq 2)$
$\alpha \in L \setminus K \Rightarrow L = K(\alpha)$
$\mu_\alpha(X) = X^2 + aX + b \quad \Rightarrow \alpha_{1,2} = \frac{-a \pm \sqrt{\Delta}}{2}$
$K(\alpha_i) = K(\sqrt{\Delta}) \ni \alpha_1, \alpha_2$
$\varphi: K(\alpha) \hookrightarrow \overline{K}$ t.c. $\varphi|_K = id$
$\alpha_1 \longmapsto \begin{cases} \alpha_1 \\ \alpha_2 \end{cases} \in K(\sqrt{\Delta}) = L$

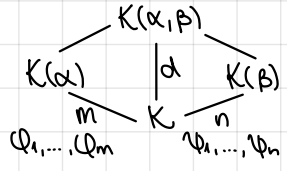
Oss E/K algebrica $\varphi: E \longrightarrow \overline{K}$ t.c $\varphi|_K = id$
$\Rightarrow \forall \alpha \in E \quad \varphi(\alpha)$ è una radice di $\mu_\alpha(X)$
$\varphi|_{K(\alpha)}: K(\alpha) \hookrightarrow \overline{K}$ è una delle immersioni che potevo costruire su $K(\alpha)$
$(\varphi|_{K(\alpha)})|_K = id \quad \Rightarrow$ manda α in una radice di μ_α

Def. I **coniugati** di $\alpha \in \overline{K}$ su K sono le radici di $\mu_{\alpha|K}(X)$

Oss L/K estensione di campi
$\varphi: L \hookrightarrow \overline{K}$ t.c. $\varphi|_K = id$
Se $K = \mathbb{Q}$, necessariamente $\varphi|_{\mathbb{Q}} = id$, perché
$\varphi(1) = 1$, $\varphi(n) = n \in \mathbb{N}$, $\varphi((-1)^2) = \varphi(-1)^2 \Rightarrow \varphi(-1) = -1$, $\varphi(-n) = -n$
$\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)} = \frac{a}{b}$

esempio $E = \mathbb{Q}(\sqrt{2}, i)$
Chi sono le immersioni $\varphi: E \hookrightarrow \overline{\mathbb{Q}}$ ($\varphi|_{\mathbb{Q}} = id$ ovvio)?
$[E:\mathbb{Q}] = 4$
$\varphi(i) = \pm i \quad x^2+1$
$\varphi(\sqrt{2}) = \pm\sqrt{2} \quad x^2-2$
$\varphi_1: \begin{matrix} i \mapsto i \\ \sqrt{2} \mapsto \sqrt{2} \end{matrix} \qquad \varphi_2: \begin{matrix} i \mapsto -i \\ \sqrt{2} \mapsto \sqrt{2} \end{matrix} \qquad \varphi_3: \begin{matrix} i \mapsto i \\ \sqrt{2} \mapsto -\sqrt{2} \end{matrix} \qquad \varphi_4: \begin{matrix} i \mapsto -i \\ \sqrt{2} \mapsto -\sqrt{2} \end{matrix}$

esempio $E = \mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$
$[\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) : \mathbb{Q}] = 4$
$\varphi: E \longrightarrow \overline{\mathbb{Q}}$
$\varphi(\sqrt{2}) = \pm\sqrt{2}$
$\varphi(\sqrt[4]{2}) = i^k \sqrt[4]{2} \quad k = 0,1,2,3$
$\varphi(\sqrt{2}) = i^2\sqrt{2} \Rightarrow \varphi(\sqrt{2}) = -\sqrt{2}$



$d < mn \Rightarrow K(\alpha) \cap K(\beta) \supsetneq K$
non tutte le scelte di $\psi|_{K(\alpha)} = \varphi_i$ funzionano
$\psi|_{K(\beta)} = \psi_j$

esempio Estensioni ciclotomiche p primo

$\mathbb{Q}(\zeta_p)/\mathbb{Q}$ è normale.

$[\mathbb{Q}(\zeta_p):\mathbb{Q}] = \deg \mu_{\zeta_p}(x) = p-1$ $\qquad \mu_{\zeta_p}(x) = \frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i$

$\forall \varphi: \mathbb{Q}(\zeta_p) \longrightarrow \overline{\mathbb{Q}} \qquad \varphi|_{\mathbb{Q}} = id$

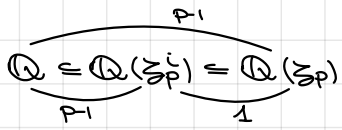
$\varphi(\mathbb{Q}(\zeta_p)) = \mathbb{Q}(\varphi(\zeta_p)) = \mathbb{Q}(\zeta_p^i)$

$\varphi(\zeta_p) = \zeta_p^i \qquad \alpha_i < p$

$\mathbb{Q}(\zeta_p^i) \subseteq \mathbb{Q}(\zeta_p)$

$[\mathbb{Q}(\zeta_p^i):\mathbb{Q}] = \deg \mu_{\zeta_p^i}(x) = \deg \mu_{\zeta_p}(x) = p-1$

$\Rightarrow \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta_p)$



Oss Se L/K è finita,

L/K è normale $\iff \forall \varphi: L \longrightarrow \overline{K}$, $\varphi|_K = id$, si ha $\varphi(L) \subseteq L$

DIMOSTRAZIONE

($\Rightarrow$) chiaro

($\Leftarrow$) $[\varphi(L):K] = [L:K]$, infatti $[L:K] = [\varphi(L)\cdot\varphi(K)] = [\varphi(L):K]$

Inoltre $\varphi(L) \subseteq L \Rightarrow \varphi(L) = L \Rightarrow L/K$ è normale $\square$

teorema L/K algebrica. Sono fatti equivalenti:

(1) L/K è normale

(2) Ogni polinomio irriducibile di $K[x]$ che ha una radice in L, ha tutte le sue radici in L

(3) L è il campo di spezzamento di una famiglia di polinomi di $K[x]$

DIMOSTRAZIONE (per L/K finita)

(1) $\Rightarrow$ (2) sia $f(x) \in K[x]$ irriducibile, α radice di $f(x)$

$f(x) = a \cdot \mu_\alpha(x) \quad a \in K^* \quad : \quad f(x) = \mu_\alpha(x)$

$K \subsetneq_d K(\alpha) \subseteq L \qquad \alpha = \alpha_1, \dots, \alpha_d$ radici di μ_α

d immersioni definite da $\varphi_i(\alpha) = \alpha_i \quad i = 1, \dots, d$

$\forall i$, φ_i si estende a L: sia $\tilde{\varphi}_i$ una di queste estensioni

Allora $\tilde{\varphi}_i|_K = \varphi_i|_K = id \qquad \tilde{\varphi}_i : L \longrightarrow \overline{K}$

Poiché L/K è normale, $\tilde{\varphi}_i(L) = L$, ma $\tilde{\varphi}_i(\alpha) = \varphi_i(\alpha) = \alpha_i \in L$

$\Rightarrow$ se $\alpha \in L$, L contiene tutte le radici di μ_α

(2) $\Rightarrow$ (3) $\forall \alpha \in L$, sia $\mu_\alpha(x) = \mu_{\alpha|K}(x)$ il suo polinomio minimo su K

Considero L_0 = campo di spezzamento su K della famiglia $\{\mu_\alpha \mid \alpha \in L\}$

$L \subseteq L_0$ perché $\forall \alpha \in L$, ho messo in L_0 tutte le radici di $\mu_\alpha = \mu_{\alpha|K} \Rightarrow \alpha \in L_0$

Per l'ipotesi, L contiene tutte le radici di $\mu_\alpha \Rightarrow L_0 \subseteq L$

(3) $\Rightarrow$ (1) $\forall \varphi: L \longrightarrow \overline{K}$, $\varphi|_K = id$ si ha $\varphi(L) = L$

Per ipotesi, L è il campo di spezzamento su K di $\mathcal{F} = \{f_i\}_{i \in I}$

sia $\{\alpha_{i1}, \dots, \alpha_{id_i}\} \subseteq \overline{K}$ l'insieme delle radici di f_i

$L = K(\{\alpha_{i1}, \dots, \alpha_{id_i}\}_{i \in I})$

$\varphi(\alpha_{ij}) = \alpha_{il} \quad \Rightarrow \varphi(L) = K(\{\varphi(\alpha_{ij}) \mid i \in I, j = 1, \dots, d_i\})$

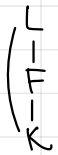
Poiché $\varphi(\alpha_{ij}) \in L$, $\varphi(L) \subseteq L$

Si ha l'uguaglianza, perché $\varphi(\{\alpha_{i1}, \dots, \alpha_{id_i}\}) = \{\varphi(\alpha_{i1}), \dots, \varphi(\alpha_{id_i})\} = \{\alpha_{ij}\}$

e perché φ è iniettiva $\square$

Proprietà delle estensioni normali

① **Proposizione (Torri)** L/K normale $\Longrightarrow$ L/F normale (in generale F/K non è normale)



DIMOSTRAZIONE

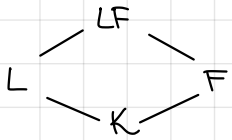
$\forall \varphi : L \longrightarrow \overline{K}$, $\varphi|_F = id \Longrightarrow \varphi|_K = id \Longrightarrow \varphi(L) = L$ □

esempio $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ (non normale; normale (x^3-2))

Oss In generale non vale il viceversa.

esempio $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ (non normale; non contiene tutte le radici del suo polinomio minimo su $\mathbb{Q}$)

② **Proposizione (Shift)** L/K normale, F/K algebrica $\Longrightarrow$ LF/F normale



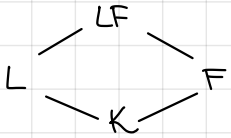
DIMOSTRAZIONE

$\varphi : LF \longrightarrow \overline{K}$ con $\varphi|_F = id$

$\varphi(LF) = \varphi(L)\varphi(F) = F\,\varphi(L) = FL$

L/K normale, $\varphi|_F = id \Rightarrow \varphi|_K = id \Rightarrow \varphi(L) = L$ □

③ **Proposizione (composto)** Se L/K e F/K sono normali, allora LF/K è normale

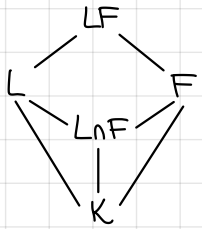


DIMOSTRAZIONE

$\varphi : LF \longrightarrow \overline{K}$, $\varphi|_K = id$

$\varphi(LF) = \varphi(L)\varphi(F) = LF$ □

④ **Proposizione (intersezione)** Se L/K e F/K normali, allora $L \cap F/K$ è normale



DIMOSTRAZIONE

$\varphi : L \cap F \longrightarrow \overline{K}$, $\varphi|_K = id$

Sia $\tilde{\varphi} : LF \longrightarrow \overline{K}$ con $\tilde{\varphi}|_{L\cap F} = \varphi$

$\varphi(L \cap F) = \tilde{\varphi}(L \cap F) = \tilde{\varphi}(L) \cap \tilde{\varphi}(F) = L \cap F$ □

Def. L/K è **separabile** se $\forall \alpha \in L$, $\mu_{\alpha|K}$ ha radici distinte in $\overline{K}$
(ha derivata diversa da 0)

Def. L/K si dice **di Galois** se è normale e separabile

<u>Oss</u> Se K è perfetto, L/K è di Galois $\iff$ L/K è normale

Se L/K è normale, $\{\varphi : L \to \overline{K} \mid \varphi_{|K} = id\} = Aut_K(L)$ è un gruppo
L/K è finita e separabile, allora $\#Aut_K(L) = [L:K]$

Se L/K è di Galois, $Gal(L/K) = Aut_K(L)$

Proposizione K campo, $f(x) \in K[x]$ irriducibile
Posto $n = \deg f(x)$ e L = c.d.s di $f(x)$ su K, allora
$n \mid [L:K] \mid n!$ e $Gal(L/K) < S_n$

DIMOSTRAZIONE
Siano $\alpha_1, \dots, \alpha_n$ le radici di $f(x)$: $L = K(\alpha_1, \dots, \alpha_n)$

$K \subseteq \underbrace{K(\alpha_1)}_{n} \subseteq L \implies n \mid [L:K]$

Se dimostro che $Gal(L/K) \hookrightarrow S_n$, allora
$[L:K] = \#Gal(L/K) \mid \#S_n = n!$

$\rho : Gal(L/K) \longrightarrow S(\{\alpha_1, \dots, \alpha_n\})$
$\varphi \longmapsto \varphi_{|\{\alpha_1, \dots, \alpha_n\}}$

ρ è ben definita perché $\varphi(\{\alpha_1, \dots, \alpha_n\}) = \{\varphi(\alpha_1), \dots, \varphi(\alpha_n)\} = \{\alpha_1, \dots, \alpha_n\}$
ρ è omomorfismo
ρ è iniettiva: se $\varphi, \psi \in Gal(L/K)$ e $\varphi \neq \psi$,
allora $\exists i : \varphi(\alpha_i) \neq \psi(\alpha_i)$ □

<u>Oss</u> L = cds di f su K
$Gal(L/K)$ agisce sulle radici di f
Se f è irriducibile, allora l'azione è transitiva
cioè, se $\alpha_1, \dots, \alpha_n$ sono le radici di f,
$\exists \varphi \in Gal(L/K) : \varphi(\alpha_i) = \alpha_j \quad \forall i,j$
Equivalentemente, $orb(\alpha_1) = \{\alpha_1, \dots, \alpha_n\}$

<u>Oss</u> L/K di Galois finita
$Gal(L/K) \longrightarrow S(L)$
$\forall \alpha \in L \quad orb(\alpha) = \{\varphi(\alpha) \mid \varphi \in Gal(L/K)\} = \{\text{radici di } \mu_{\alpha|K}\}$

$K \subseteq K(\alpha) \subseteq L$
$\mu_\alpha : \alpha_1, \dots, \alpha_n$
$\varphi_i(\alpha) = \alpha_i$
$\forall i$, sia $\tilde{\varphi}_i$ l'estensione a L di $\varphi_i \implies \tilde{\varphi}_i \in Gal(L/K)$
$orb(\alpha) \supseteq \{\tilde{\varphi}_1(\alpha), \dots, \tilde{\varphi}_n(\alpha)\} = \{\alpha_1, \dots, \alpha_n\}$

Oss $[L:K]=2 \implies Gal(L/K) \cong \mathbb{Z}/2\mathbb{Z}$

$L=K(\alpha)$ dove $\{\alpha,\alpha'\}$ sono le radici di $\mu_{\alpha}(x)$

$id: \alpha \longmapsto \alpha'$, $\sigma: \alpha \longmapsto \alpha'$

Oss $f(x) \in K[x]$ irriducibile con $\deg f(x)=3$

$L=$ cds di f su K

$f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ in $\overline{K}$: $L=K(\alpha_1,\alpha_2,\alpha_3)$

$3 \mid [L:K] \mid 3!=6$

$[L:K] = \begin{cases} 3 & Gal(L/K) \cong A_3 \cong \mathbb{Z}/3\mathbb{Z} \\ 6 & Gal(L/K) \cong S_3 \end{cases}$

esempio

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

6 | 2 | $\mathbb{Q}(\sqrt[3]{2})$ | 3 | $\mathbb{Q}$

$Gal(\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}) \cong S_3$

esempio $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. $[\mathbb{Q}(\zeta_7):\mathbb{Q}]=6$

$L=\mathbb{Q}(\overbrace{\zeta+\zeta^{-1}}^{\alpha}) \subsetneq \mathbb{Q}(\zeta)$

σ coniugio complesso

$\sigma(\zeta+\zeta^{-1})=\zeta^{-1}+\zeta$ $(\zeta=\zeta^{-1}) \implies L \subseteq \mathbb{R}$

$[L:\mathbb{Q}] \mid 6$, $\neq 6$

$[L:\mathbb{Q}] =$ • $1 \longrightarrow \zeta+\zeta^{-1}=q \in \mathbb{Q} \longrightarrow \zeta^2+1-\zeta q=0$ $\quad x^2-qx+1 \in \mathbb{Q}[x]$

ma il polinomio minimo di ζ su $\mathbb{Q}$ ha grado 6 ↯

• 2 $(\zeta+\zeta^{-1})^2+a(\zeta+\zeta^{-1})+b=0$, $a,b \in \mathbb{Q}$

$\zeta^2(\zeta^2+2+\zeta^{-2}+a\zeta+a\zeta^{-1}+b)=0$ ↯

Oppure: $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ è normale e di Galois

$Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})=\{\varphi_i\} \cong \mathbb{Z}/7\mathbb{Z}^*$

dove $\varphi_i: \mathbb{Q}(\zeta_7) \longrightarrow \overline{\mathbb{Q}}$

$\varphi_i(\zeta_7)=\zeta_7^i$

$orb(\alpha)=\{\varphi(\alpha) \mid \varphi \in Gal(L/K)\}=\{\varphi_1(\alpha),\dots,\varphi_6(\alpha)\}=$

$=\{\zeta+\zeta^{-1},\zeta^2+\zeta^{-2},\dots,\zeta^6+\zeta^{-6}\}=\{\zeta+\zeta^{-1},\zeta^2+\zeta^{-2},\zeta^4+\zeta^{-4}\}$

$\mu_{\alpha}(x)=(x-(\zeta+\zeta^{-1}))(x-(\zeta^2+\zeta^{-2}))(x-(\zeta^4+\zeta^{-4}))$

Dico che $\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}$ è di Galois

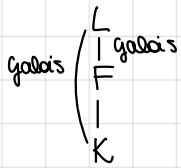
$\zeta^2+\zeta^{-2}, \zeta^4+\zeta^{-4} \in \mathbb{Q}(\zeta+\zeta^{-1})$

$\zeta^2+\zeta^{-2}=(\zeta+\zeta^{-1})^2-2$

$\zeta^4+\zeta^{-4}=(\zeta^2+\zeta^{-2})^2-2$

$\implies Gal(L/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$

Oss L/K di Galois $\Rightarrow L/F$ di Galois



$\mathrm{Gal}(L/F) < \mathrm{Gal}(L/K)$

esempio $f(x) = x^4 - 2$ Gal del c.d.s. di $f(x)$ / $\mathbb{Q}$

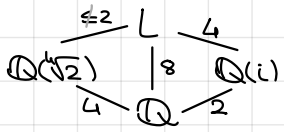
$\alpha = \alpha_1 = \sqrt[4]{2}$, $i\alpha$, $-i\alpha$, $-\alpha$

$\mathbb{Q}(\pm\alpha, \pm i\alpha) = \mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i)$

$L = \mathbb{Q}(\sqrt[4]{2}, i)$

$[L : \mathbb{Q}(\sqrt[4]{2})] = \begin{cases} 1 \\ 2 \end{cases}$ no perché $\sqrt[4]{2} \in \mathbb{R}, i \notin \mathbb{R}$

$\Rightarrow [L : \mathbb{Q}] = 8$



$\mathrm{Gal}(L/\mathbb{Q})$ è un gruppo di ordine 8

$\mathrm{Gal}(L/\mathbb{Q}) < S_4$, $\# = 8$ $\Longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \cong D_4$

$\mathrm{Gal}(L/\mathbb{Q}(i)) < \mathrm{Gal}(L/\mathbb{Q}) \cong D_4$
è ha ordine $[L : \mathbb{Q}(i)] = 4$

$\varphi : \mathbb{Q}(\sqrt[4]{2}, i) \longrightarrow \overline{\mathbb{Q}}$

$\sigma_{\pm,k}$ $i \longmapsto \pm i$

$\sqrt[4]{2} \longmapsto \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$

$\{\sigma_{+,k}\} = \mathrm{Gal}(L/\mathbb{Q}(i))$

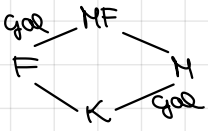
$\sigma_{+,k} = \sigma_k : \sqrt[4]{2} \longmapsto i^k\sqrt[4]{2}$

$\sigma_0 = \mathrm{id}$

$\sigma_1 : \sqrt[4]{2} \longmapsto i\sqrt[4]{2}$ $\qquad \sigma_1^2 : \sqrt[4]{2} \longmapsto i\sqrt[4]{2} \longmapsto \sigma_1(i)\,\sigma_1(\sqrt[4]{2}) = i \cdot i\sqrt[4]{2} = -\sqrt[4]{2}$

$\Rightarrow \mathrm{Gal}(L/\mathbb{Q}(i)) = \langle \sigma_1 \rangle \cong \mathbb{Z}/4\mathbb{Z}$

Oss



$\mathrm{Gal}(MF/F) \hookrightarrow \mathrm{Gal}(M/K)$

$\sigma \longmapsto \sigma|_M$

esempio $f(x)=x^7-5$ Gal del c.d.s. di $f(x)$ / $\mathbb{Q}$

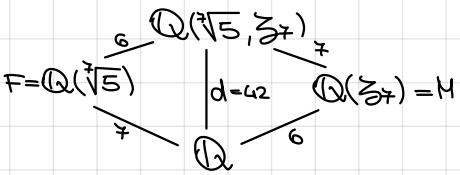
$\alpha=\sqrt[7]{5}$, $\{\zeta_7^i\sqrt[7]{5}\}_{i=0,\dots,6}$

$L=\mathbb{Q}(\alpha,\zeta\alpha,\dots,\zeta^6\alpha)=\mathbb{Q}(\alpha,\zeta_7)$

$(\subseteq)$ $\forall i,\ \zeta_7^i\in\mathbb{Q}(\alpha,\zeta_7)$

$(\supseteq)$ $\zeta_7=\frac{\zeta_7\alpha}{\alpha}\in\mathbb{Q}(\{\zeta_7^i\alpha\})$

$[6,7]\mid d\le 6\cdot 7 \Rightarrow d=6\cdot 7$



$|Gal(L/\mathbb{Q})|=42$

$H=Gal(L/F)$, $|H|=6$, $H<G$

$N=Gal(L/M)$, $|N|=7$, $N<G$

$|HN|=\frac{|H||N|}{|H\cap N|}=\frac{7\cdot 6}{1}=42 \Rightarrow HN=G$

$H=Gal(L/\mathbb{Q}(\alpha))\cong Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})\cong\mathbb{Z}/7\mathbb{Z}^*\cong\mathbb{Z}/6\mathbb{Z}$

$\sigma\longmapsto\sigma|_M$

è ben definita

è omo

è iniettiva: $\sigma|_M=id$, $\sigma|_F=id$ per hp $\Rightarrow\sigma=id$

$N\cong\mathbb{Z}/7\mathbb{Z}$, $H\cong\mathbb{Z}/7\mathbb{Z}^*$ $G=NH$

$N\trianglelefteq G$

$G\cong N\rtimes H\cong\mathbb{Z}/7\mathbb{Z}\rtimes_\varphi\mathbb{Z}/6\mathbb{Z}^*$ $\varphi:H\longrightarrow Aut N$

$\sigma:\mathbb{Q}(\alpha,\zeta_7)\longrightarrow\overline{\mathbb{Q}}$

$\sigma_{ij}:\ \zeta_7\longmapsto\zeta_7^i$ $1\le i\le 6$

$\alpha\longmapsto\zeta_7^j\alpha$ $0\le j\le 7$

[$G<S_7$: $\rho=(1\,2\dots 7)$

$N_{S_7}(\langle\rho\rangle)=\{\sigma\in S_7\mid\sigma\rho\sigma^{-1}=\rho^k\}$ ...]

$H=\{\sigma_{i0}\}=\langle\sigma_{30}\rangle$ $N=\{\sigma_{1j}\}=\langle\sigma_{11}\rangle$ perché $\sigma_{1k}=\sigma_{11}^k$

$\varphi:\langle\sigma_{3,0}\rangle\longrightarrow Aut\langle\sigma_{1,1}\rangle$

$\sigma_{3,0}\longmapsto(\sigma_{1,1}\longmapsto\sigma_{3,0}\sigma_{1,1}\sigma_{3,0}^{-1}=\sigma_{1,k}$

$\sigma_{3,0}^{-1}=\sigma_{i,0}$: $\zeta^3\longmapsto\zeta^{3i}=\zeta\Rightarrow 3i\equiv 1\ (7)\Rightarrow i\equiv 5(7)$

$\sigma_{3,0}\circ\sigma_{1,1}\circ\sigma_{5,0}=\sigma_{1,3}$

$\alpha\longmapsto\alpha\longmapsto\zeta\alpha\longmapsto\zeta^3\alpha\Rightarrow k=3$

$\Rightarrow\varphi:H\longrightarrow Aut N\cong(\mathbb{Z}/7\mathbb{Z})^*$

$\sigma_{3,0}\longmapsto\varphi_{\sigma_{3,0}}:\sigma_{1,1}\longmapsto\sigma_{1,1}^3\longleftrightarrow\overline{3}$

campi finiti

$|F| < +\infty \implies \text{char } F = p$ primo

$\mathbb{F}_p \subset F \quad [F : \mathbb{F}_p] = n \implies |F| = p^n$

Teorema $\forall p \; \forall n \; \exists!$ F campo con $|F| = p^n$ in $\overline{\mathbb{F}_p}$

DIMOSTRAZIONE

Se esiste F con $|F| = p^n$, $F \subset \overline{\mathbb{F}_p}$

$F^* = \langle \alpha \rangle$ con $\text{ord}\,\alpha = p^n - 1$, $\alpha \in \overline{\mathbb{F}_p}$

$\forall \gamma \in F^* \; \gamma^{p^n - 1} = 1 \implies \forall \gamma \in F \; \gamma^{p^n} = \gamma$

$F \subseteq \{\gamma \in \overline{\mathbb{F}_p} \mid \gamma^{p^n} = \gamma\} = \{\gamma \in \overline{\mathbb{F}_p} \mid \gamma \text{ è radice di } x^{p^n} - x\} = A$

Il polinomio $f(x) = x^{p^n} - x$ ha esattamente p^n radici (con molteplicità) in $\overline{\mathbb{F}_p}$

$f'(x) = p^n x^{p^n - 1} - 1 = -1$

$\implies$ Ogni eventuale campo con p^n el. in $\overline{\mathbb{F}_p}$ è contenuto in A, e $|A| = p^n$

Devo mostrare che $F = A$ è un campo:

$0, 1 \in F$

$\alpha, \beta \in F$: $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$

$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \in F$

...

$\implies F$ è un campo □

Quindi $\mathbb{F}_{p^n} = \{\gamma \in \overline{\mathbb{F}_p} \mid \text{radice di } x^{p^n} - x\}$

$\mathbb{F}_{p^n}$ è il cds di $x^{p^n} - x$ su $\mathbb{F}_p$

$\mathbb{F}_{p^n} / \mathbb{F}_p$ è normale e di Galois

Teorema $\text{Gal}\left(\mathbb{F}_{p^n} / \mathbb{F}_p\right) = \langle \phi \rangle$

dove $\phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n} : x \longmapsto x^p$

è l'omomorfismo di Frobenius

DIMOSTRAZIONE

$\text{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$ ha ordine n

$\phi \in \text{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$: $\phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$

$x \longmapsto x^p$ è omo di anelli

iniettivo perché $\mathbb{F}_{p^n}$ è un campo e surgettivo per cardinalità

$\phi(a) = a^p = a$ se $a \in \mathbb{F}_p$ (piccolo teorema di Fermat)

$\langle \phi \rangle < \text{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$: voglio mostrare che $\text{ord}\,\phi = n$

Sia $\text{ord}\,\phi = d \mid n$.

Allora $\forall \alpha \in \mathbb{F}_{p^n} \; \phi^d(\alpha) = \alpha^{p^d} = \alpha$

$\implies \alpha$ è radice di $x^{p^d} - x$

Il polinomio $x^{p^d} - x$ ha p^d radici in $\overline{\mathbb{F}_p}$

e ha come radice tutti i p^n elementi di $\mathbb{F}_{p^n} \implies p^n \leq p^d$

ma $d \mid n \implies n = d$ □

Oss $\overline{\mathbb{F}_p}$ contiene radici primitive k-esime di 1 solo per $p \nmid k$

Se $p \nmid k$, allora $\exists\, m \geq 1$ t.c. $p^m = 1 \bmod k$

In $\mathbb{F}_{p^m}^*$ ciclico di ordine $p^m - 1$ c'è un elemento di ordine k, perché $k \mid p^m - 1$

proposizione Siano p, q primi, $p \neq 1$

$f(x) = x^q - 1$ in $\mathbb{F}_p[x]$ si fattorizza con 1 fattore di grado 1 e $\frac{q-1}{d}$ fattori di grado $d = \operatorname{ord}_q p \pmod q$

DIMOSTRAZIONE

$f(x) = (x-1)(1 + x + \dots + x^{q-1})$

Chi sono le radici di $f(x)$ in $\overline{\mathbb{F}_p}$? Le radici dell'unità di ordine che divide q

$\mathbb{F}_p(\xi_q) = \mathbb{F}_p(\xi_q, \xi_q^2, \dots, \xi_q^{q-1})$ con ξ_q radice primitiva q-esima

$\mathbb{F}_p$

- cds: $\mathbb{F}_p(\xi_q)$
- $[\mathbb{F}_p(\xi_q) : \mathbb{F}_p] = \deg \mu_{\xi_q}(x)$
- $\mathbb{F}_p(\xi_q) = \mathbb{F}_{p^n} = \{\text{radici di } x^{p^n} - x\} = \{0\} \cup \{\text{radici di } x^{p^n - 1} - 1\}$
- $\mathbb{F}_{p^n}^* \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$

Quindi $\xi_q \in \mathbb{F}_{p^n} \iff \xi_q^{p^n - 1} = 1 \iff q \mid p^n - 1$

Il minimo n per cui questo è vero è l'ordine moltiplicativo di $p \bmod q$, d

$f(x) = (x-1)\, g_1(x)\, g_2(x) \cdots g_{\frac{q-1}{d}}(x)$

$\hookrightarrow$ pol. min di ξ_q di grado d

$\mathbb{F}_p(\xi_q) = \mathbb{F}_{p^d}$

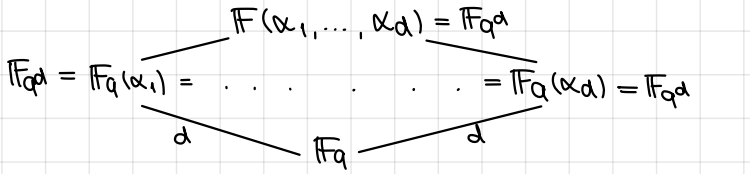
Se ξ è una qualsiasi radice di $(1 + x + \dots + x^{q-1})$, il polinomio minimo di ξ ha grado d

$\Rightarrow$ tutti i fattori irriducibili hanno grado d,

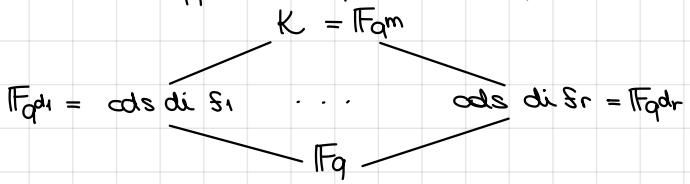
quindi $x^q - 1$ si fattorizza con 1 fattore di grado 1 e $\frac{q-1}{d}$ fattori di grado d $\square$

proposizione Sia $f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} \in \mathbb{F}_q[x]$, f_i irriducibile, $\deg f_i = d_i$
Allora il cds di $f(x)$ su $\mathbb{F}_q$ e $\mathbb{F}_{q^m}$, con $m = mcm(d_1, \dots, d_r)$

DIMOSTRAZIONE
Sia $f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} \in \mathbb{F}_q[x]$ con $q = p^n$
K cds di f
$K = \mathbb{F}_{p^s}$ poiché è un campo finito
$K \supseteq \mathbb{F}_q \iff \mathbb{F}_{p^s} \supseteq \mathbb{F}_{p^n} \iff n \mid s$: $s = n \cdot m$
$K = \mathbb{F}_{p^{nm}} = \mathbb{F}_{q^m}$
Facciamo il caso $f(x) = f_1(x)$ irriducibile, di grado d
Siano $\alpha_1, \dots, \alpha_d \in \overline{\mathbb{F}_q}$ le radici di f



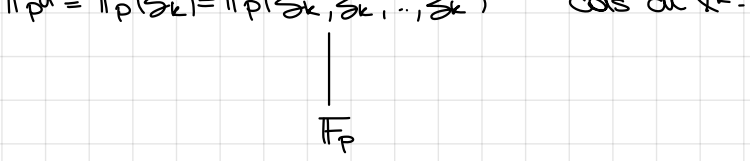
Caso generale: $f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}$ di grado $d_1, \dots, d_r$
Possiamo supporre $e_1 = e_2 = \dots = e_r = 1$



$\mathbb{F}_{q^{d_i}} \subseteq \mathbb{F}_{q^m} \implies d_i \mid m \quad \forall i$
$\implies$ il minimo m è $m = mcm(d_1, \dots, d_r)$ □

teorema Sia p primo, $n = p^m k$ con $(p, k) = 1$
Il cds di $x^n - 1$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$, dove
d è l'ordine moltiplicativo di p mod k

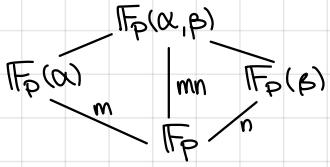
DIMOSTRAZIONE
Radici multiple $\iff (x^n - 1, nx^{n-1}) \neq 1$ in $\mathbb{F}_p[x]$
$(x^n - 1, n) \neq 1$
α^1 mod è $= 1 \iff n \neq 0$ in $\mathbb{F}_p \iff p \nmid n$
$x^{p^k} - 1 = (x^k - 1)^p$ per binomio ingenuo
Scriviamo $n = p^m k$, con $p \nmid k$: abbiamo trovato
$(x^n - 1) = (\underbrace{x^k - 1}_{\text{senza radici multiple}})^{p^m}$



Devo trovare la minima estensione $\mathbb{F}_{p^d}$ che contiene una radice primitiva k-esima $\iff k \mid |\mathbb{F}_{p^d}^*| \iff k \mid p^d - 1$
($\implies$) una radice primitiva k-esima ha ordine k, e quindi k divide l'ordine del gruppo
($\impliedby$) $\mathbb{F}_{p^d}^*$ è ciclico, quindi ha un elemento di ordine k
Quindi d = ord molt di p mod k □

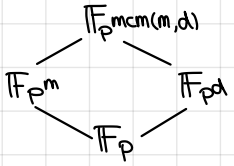
proposizione Siano $\alpha, \beta \in \overline{\mathbb{F}_p}$, con $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$, $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = n$, $(m,n) = 1$.
Allora $[\mathbb{F}_p(\alpha+\beta) : \mathbb{F}_p] = mn$

<u>Oss</u> $\mathbb{F}_p(\alpha+\beta) \subseteq \mathbb{F}_p(\alpha, \beta)$
segue $\mathbb{F}_p(\alpha+\beta) = \mathbb{F}_p(\alpha, \beta)$

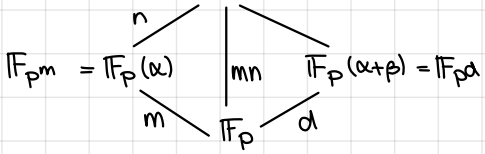


DIMOSTRAZIONE
$\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$, $\mathbb{F}_p(\beta) = \mathbb{F}_{p^n}$, $\mathbb{F}_p(\alpha+\beta) = \mathbb{F}_{p^d}$

<u>Oss</u>

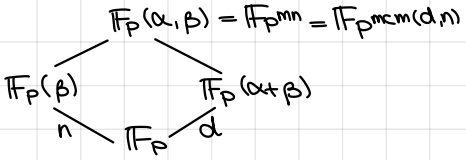


$\mathbb{F}_{p^{mcm(m,d)}} = \mathbb{F}_p(\alpha, \alpha+\beta) = \mathbb{F}_p(\alpha, \beta) = \mathbb{F}_{p^{mn}}$



$\Rightarrow mcm(m,d) = mn \implies n \mid d$

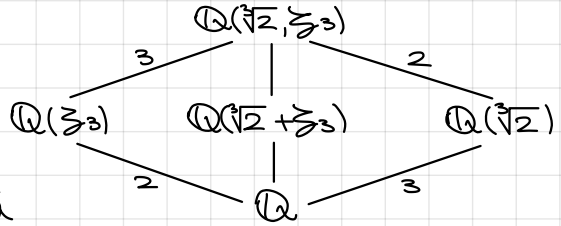
Guardando



si ottiene $m \mid d$

Quindi, poiché $(m,n) = 1$, $mn \mid d$
D'altro canto, $\mathbb{F}_p(\alpha+\beta) \subseteq \mathbb{F}_p(\alpha, \beta)$, quindi $d \mid mn \implies d = mn$ □

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



$[\mathbb{Q}(\sqrt[3]{2} + \zeta_3) : \mathbb{Q}]$ è il n° di immersioni $K \hookrightarrow \overline{\mathbb{Q}}$ che fissano K

Consideriamo le 6 immersioni di $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ in $\overline{\mathbb{Q}}$

$$\sigma_{ij} : \begin{cases} \zeta_3 \longmapsto \zeta_3^i & i = 1,2 \\ \sqrt[3]{2} \longmapsto \sqrt[3]{2}\,\zeta_3^j & j = 0,1,2 \end{cases}$$

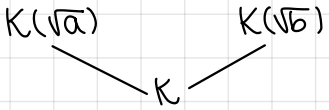
Considero $\sigma_{ij}|_K$: se sono 6 distinte, abbiamo finito.
Dobbiamo solo capire se esistono $(i,j) \neq (l,m)$ t.c.

$$\sigma_{ij}(\sqrt[3]{2} + \zeta_3) = \sigma_{lm}(\sqrt[3]{2} + \zeta_3)$$
$$\iff \zeta_3^i + \sqrt[3]{2}\,\zeta_3^j = \zeta_3^l + \sqrt[3]{2}\,\zeta_3^m$$
$$\zeta_3^i - \zeta_3^l = \sqrt[3]{2}(\zeta_3^m - \zeta_3^j)$$

Se $m = j$, segue $i = l$
Se $j \neq m$, $\dfrac{\zeta_3^i - \zeta_3^l}{\zeta_3^m - \zeta_3^j} = \sqrt[3]{2}$

che direbbe $\sqrt[3]{2} \in \mathbb{Q}(\zeta_3)$ ↯ (per gradi)

Oss Se $\mathrm{char}\, K \neq 2$



$K(\sqrt{a}) = K(\sqrt{b}) \iff \frac{a}{b}$ è un quadrato in K
$\iff ab$ è un quadrato in K

DIMOSTRAZIONE
($\Longleftarrow$) Se $\frac{a}{b} = t^2$, $t \in K^*$, allora
$K = (\sqrt{a}) = K(\sqrt{t^2 b}) = K(t\sqrt{b}) = K(\sqrt{b})$
($\Longrightarrow$) Se $[K(\sqrt{a}) : K] = [K(\sqrt{b}) : K] = 1$ è banale
Altrimenti $\sqrt{b} \in K(\sqrt{a}) \iff \exists r, s \in K$ t.c.
$\sqrt{b} = r + s\sqrt{a}$ $\qquad b = r^2 + 2rs\sqrt{a} + s^2 a$
$\sqrt{a}(2rs) = b - r^2 - s^2 a$
Se $2rs \neq 0$, $\sqrt{a} = \dfrac{b - r^2 - s^2 a}{2rs} \in K$ ↯ perché $[K(\sqrt{a}) : K] = 2$
Se $rs = 0 \Longrightarrow r = 0 \Longrightarrow \sqrt{b} = s\sqrt{a} \Longrightarrow b/a = s^2$
$\vee$
$s = 0 \Longrightarrow \sqrt{b} = r \in K$ ↯

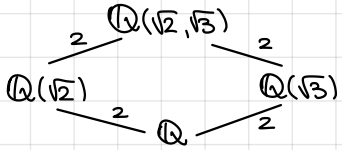
□

esempio Immersioni di $\mathbb{Q}(\sqrt{2},\sqrt{3})$ in $\overline{\mathbb{Q}}$

$\varphi : \mathbb{Q}(\sqrt{2},\sqrt{3}) \hookrightarrow \mathbb{Q}$ ne esistono $4 = [\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}]$

$\varphi : \mathbb{Q}(\sqrt{2},\sqrt{3}) \hookrightarrow \overline{\mathbb{Q}}$

$\varphi_{\pm\pm} : \begin{cases} \sqrt{2} \longmapsto \pm\sqrt{2} \\ \sqrt{3} \longmapsto \pm\sqrt{3} \end{cases}$



$\mathbb{Q}(\sqrt{2},\sqrt{3})$ è c.d.s. di $(x^2-2)(x^2-3)$

è di Galois su $\mathbb{Q}$

$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{\varphi_{++} = id, \varphi_{+-}, \varphi_{-+}, \varphi_{--}\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Chi è il polinomio minimo di $\sqrt{2}+\sqrt{3}$?

$\varphi : \mathbb{Q}(\alpha) \longrightarrow \overline{\mathbb{Q}}$

$\mathbb{Q}$

È il polinomio che ha per radici

$\{\varphi(\sqrt{2}+\sqrt{3}) \mid \varphi : \mathbb{Q}(\sqrt{2}+\sqrt{3}) \hookrightarrow \overline{\mathbb{Q}}\} = \{\varphi(\sqrt{2}+\sqrt{3}) \mid \varphi : \mathbb{Q}(\sqrt{2},\sqrt{3}) \hookrightarrow \overline{\mathbb{Q}}\}$

$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$

Oss $[L:K] = n$

$\alpha \in L$, $\varphi : L \longrightarrow \overline{K}$, $\varphi_{|K} = id$

$\{\varphi(\alpha)\}_\varphi$ = coniugati di α su K

μ_α polinomio minimo di α su K

$\mu_\alpha(\alpha) = 0 \xrightarrow{\varphi} 0 = \varphi(\mu_\alpha(\alpha)) = \mu_\alpha(\varphi(\alpha))$

Viceversa, se α' è radice di μ_α

$\varphi : K(\alpha) \longrightarrow \overline{K}$, $\varphi_{|K} = id$

$\alpha \longmapsto \alpha'$

allora φ si estende a $\tilde{\varphi} : L \longrightarrow \overline{K}$

$\alpha' = \tilde{\varphi}(\alpha) = \varphi(\alpha)$

In particolare, se L/K è di Galois.

$Gal(L/K)$ agisce in modo transitivo su {radici di μ_α}, $\forall \alpha \in L$

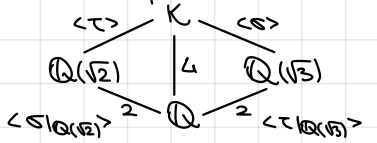
$orb(\alpha) = \{\sigma(\alpha)\}_{\sigma \in Gal(L/K)} = \{\text{radici di } \mu_\alpha\}$

L/K, $\alpha \in L$ $K \subseteq K(\alpha) \subseteq L$

$[K(\alpha):K] = \#\{\varphi(\alpha) \mid \varphi : L \longrightarrow \overline{K}, \varphi_{|K} = id\} = |O(\alpha)|$

$\mu_{\alpha/K}(x) = \prod_{\varphi(\alpha) \in O(\alpha)} (x - \varphi(\alpha))$

esempio $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$



$[K:\mathbb{Q}] = 4$

$Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\{id, \sigma, \tau, \sigma\tau\}$

$\sigma : \begin{matrix} \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} \end{matrix}$ $\tau : \begin{matrix} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto -\sqrt{3} \end{matrix}$

$\sqrt{2}+\sqrt{3}$

$\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$

$\{\varphi(\alpha)\} = \{\alpha, \sigma(\alpha), \tau(\alpha), \sigma\tau(\alpha)\} = \{\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}\}$

sono distinti perché $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ è base, quindi la scrittura è unica

$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Teorema dell'elemento primitivo

E/K estensione finita (e separabile)
Allora E/K è semplice, cioè
$\exists \alpha \in E$ t.c. $E = K(\alpha)$

DIMOSTRAZIONE

K campo finito

Se $[E:K] = d$, allora $|E| = |K|^d$

E finito $\Longrightarrow E^*$ ciclico. Sia $E^* = \langle \alpha \rangle$

E' chiaro che $E = K(\alpha)$

K campo infinito

Sia $E = K(\alpha_1, \dots, \alpha_n)$

Per induzione su n

- $n=2$: $E = K(\alpha, \beta)$

  $\varphi_1, \dots, \varphi_d : E \longrightarrow \overline{K}$, $\varphi_i|_K = id$

  Voglio trovare γ t.c. $\#\{\varphi_i(\gamma)\} = d$

  x indeterminata.

  $F(x) = \prod_{i<j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta)) \in \overline{K}[x]$

  $F(x) \neq 0$ perché, altrimenti avrei i, j t.c.

  $\varphi_i(\alpha) + x\varphi_i(\beta) = \varphi_j(\alpha) + x\varphi_j(\beta) \Longrightarrow \varphi_i(\alpha) = \varphi_j(\alpha),\ \varphi_i(\beta) = \varphi_j(\beta)$

  $\Longrightarrow \varphi_i = \varphi_j$ con $i \neq j$ ↯

  $\deg F(x) \leq \binom{d}{2}$

  K infinito $\Longrightarrow \exists t \in K$ t.c. $F(t) \neq 0$

  $\Rightarrow$ Nessuno dei fattori di F si annulla

  $\varphi_i(\alpha) + t\varphi_i(\beta) \neq \varphi_j(\alpha) + t\varphi_j(\beta) \quad \forall i<j$

  $\gamma = \alpha + t\beta$

  $\varphi_i(\gamma) = \varphi_i(\alpha) + t\varphi_i(\beta) \neq \varphi_j(\gamma) = \varphi_j(\alpha) + t\varphi_j(\beta) \quad \forall i<j$

  $\Longrightarrow \#\{\varphi_i(\gamma)\} = d = [E:K]$

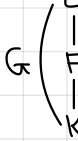
  Quindi $K(\gamma) \subseteq E \Longrightarrow K(\gamma) = E$

- PASSO INDUTTIVO

$$E = K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \overset{\text{hp.ind}}{=} K(\beta)(\alpha) = K(\beta, \alpha) \overset{n=2}{=} K(\gamma)$$

□

L/K finita e di Galois, $G = Gal(L/K)$



$\mathcal{E}_{L/K} = \{F \mid K \subseteq F \subseteq L\} \longrightarrow \mathcal{G}_{L/K} = \{H \mid H \leq G\}$

$F \longmapsto^{\alpha} Gal(L/F) < G$

$L^H \longmapsto^{\beta} H$

dove $L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\} = Fix(H)$

Oss • $Gal(L/F) < G$

• $L^H \in \mathcal{E}$, cioè è un sottocampo di L/K

$\Longrightarrow$ α e β sono ben definite

Lemma L/M di Galois, $H \leq Gal(L/M)$
Allora $L^H = M \iff H = Gal(L/M)$

DIMOSTRAZIONE

($\Longleftarrow$) $G = Gal(L/M)$

Tesi: $L^G = M$, ($\supseteq$ chiaro)

Se fosse $M \subsetneq L^G$, allora $[L^G : M] > 1$

$\Rightarrow \exists \varphi : L^G \longrightarrow L$ con $\varphi \neq id$, $\varphi_{|M} = id$

Allora φ si estende a L e quindi ad un elemento non banale di G

$\Rightarrow \tilde{\varphi} \in G$: $\tilde{\varphi}$ fissa L^G, $\tilde{\varphi}_{|L^G} = \varphi = id$ ↯

($\Longrightarrow$) $L^H = M$

$L = M(\alpha)$

$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \in L^H[x]$

Infatti, dato $h \in H$, $hf(x) = \prod_{\sigma \in H} (x - h\sigma(\alpha)) = \prod_{\rho \in H} (x - \rho(\alpha)) = f(x)$

$hf(x) = f(x) \ \forall h \in H \Rightarrow f(x) \in L^H[x] = M[x]^{H=H}$

$f(\alpha) = 0$ $\quad$ $\deg f(x) = |H|$

$\Rightarrow \mu_\alpha(x) \mid f(x)$ e $\deg \mu_\alpha(x) = [L : M] = |G|$

$\Rightarrow |G| \leq |H| \Rightarrow G = H$ □

Lemma L/K di Galois, $H < Gal(L/K)$, allora
$L^{\sigma H \sigma^{-1}} = \sigma L^H \ \forall \sigma \in G$
(Il sottocampo fissato dal coniugato di H è il coniugato di L^H)

DIMOSTRAZIONE

$L^H = \{\alpha \in L \mid \varphi(\alpha) = \alpha \ \forall \varphi \in H\}$

$\sigma L^H = \{\sigma(\alpha) \in L \mid \varphi(\alpha) = \alpha \ \forall \varphi \in H\} = \{\beta \in L \mid \varphi(\sigma^{-1}(\beta)) = \sigma^{-1}(\beta) \ \forall \varphi \in H\} =$

$= \{\beta \in L \mid \sigma\varphi\sigma^{-1}(\beta) = \beta \ \forall \varphi \in H\} = L^{\sigma H \sigma^{-1}}$ □

Teorema di corrispondenza di Galois

L/K di Galois finita

la mappa $\mathcal{E}_{L/K} \xrightarrow{\alpha} \mathcal{G}_{L/K}$

$F \longmapsto Gal(L/F)$

è biiettiva

l'inversa è $\mathcal{G}_{L/K} \xrightarrow{\beta} \mathcal{E}_{L/K}$

$H \longmapsto L^H$

Inoltre $H \triangleleft Gal(L/K) \iff L^H/K$ è normale

e in tal caso $Gal(L^H/K) \cong \frac{Gal(L/K)}{Gal(L/L^H)}$

DIMOSTRAZIONE

- $\alpha \circ \beta = id_{\mathcal{G}_{L/K}}$, $\beta \circ \alpha = id_{\mathcal{E}_{L/K}}$

  $\beta \circ \alpha(F) = \beta(Gal(L/F)) = L^{Gal(L/F)} = F$ per il lemma

  $\alpha \circ \beta(H) = \alpha(L^H) = Gal(L/L^H)$

  Devo verificare che $Gal(L/L^H) = H$

  ($\supseteq$) perché gli el. di H sono automorfismi di L che sono l'identità su L^H

  Per il lemma, se $L^H = M$, allora $H = Gal(L/M)$

  $H = Gal(L/L^H)$

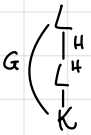
- $H \triangleleft G \iff \sigma H \sigma^{-1} = H \ \forall \sigma \in G \iff \sigma L^H = L^{\sigma H \sigma^{-1}} = L^H \ \forall \sigma \in G$

  $\iff L^H/K$ è normale

  ($\Rightarrow$) chiaro

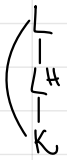
  ($\Leftarrow$) $\forall \varphi : L^H \to \overline{K}$, $\varphi|_K = id$

  φ si estende a $\sigma \in Gal(L/K) \Rightarrow \sigma(L^H) = L^H$



- Consideriamo $res : Gal(L/K) \longrightarrow Gal(L^H/K)$

  $\sigma \longmapsto \sigma|_{L^H}$



res è ben definita perché L^H/K è normale

res è anche surgettiva per il teorema di estensione degli omomorfismi

$\ker res = \{\sigma \in Gal(L/K) \mid \sigma|_{L^H} = id\} = Gal(L/L^H) = H$

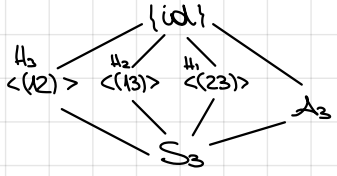
$\Rightarrow \frac{Gal(L/K)}{Gal(L/L^H)} \cong Gal(L^H/K)$ □

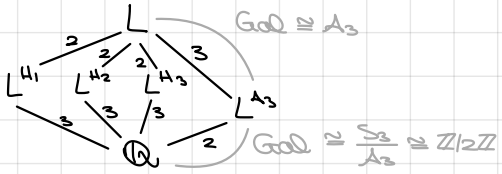
Oss $K \subset F \subset L$

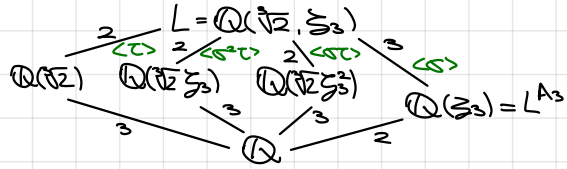
$\forall \tilde{\varphi} : L \to \overline{K}$ $\tilde{\varphi}|_K = id$ $\tilde{\varphi}F = F$

esempio $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ ods di $x^3 - 2$

$K = \mathbb{Q}$, $Gal(L/K) \cong S_3$







$Gal(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$

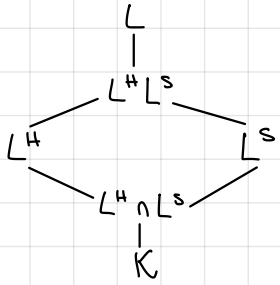
$\sigma : \begin{matrix} \sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{matrix}$, $\tau : \begin{matrix} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{matrix}$

proposizione Sia L/K di Galois finita, $H, S \leq Gal(L/K)$

(1) $L^H \subseteq L^S \iff H \supseteq S$

(2) $L^{H \cap S} = L^H L^S$

(3) $L^{\langle H,S \rangle} = L^H \cap L^S$



DIMOSTRAZIONE

$L^H = \{\alpha \in L \mid h(\alpha) = \alpha \ \forall h \in H\}$

$L^S = \{\alpha \in L \mid s(\alpha) = \alpha \ \forall s \in S\}$

(1) $H \supseteq S \implies L^H \subset L^S$

$L^H \subset L^S \subset L$

$Gal(L/L^S) = S$, $Gal(L/L^H) = H \implies S \subset H$

(2) $H \cap S \subset H, S$

$L^{H \cap S} \supseteq L^H, L^S \implies L^{H \cap S} \supseteq L^H L^S$

$L^H L^S = L^N$

$Gal(L/L^H L^S) = N = Gal(L/L^S) \cap Gal(L/L^H) = S \cap H$

$(\subseteq)$

$(\supseteq)$ $L^N \subseteq L^{H \cap S} \implies N \supseteq H \cap S$

(3) $L^{\langle H,S \rangle} = L^H \cap L^S$

$\langle H, S \rangle \supseteq H, S \implies L^{\langle H,S \rangle} \subseteq L^H \cap L^S$

$\alpha \in L^H \cap L^S$: $h\alpha = \alpha \ \forall h \in H$, $s\alpha = \alpha \ \forall s \in S$

$\forall g \in \langle H, S \rangle$: $g\alpha = \alpha$ perché g è una parola finita in H e S □

proposizione Siano L_1/K, L_2/K di Galois (finite), allora

$res: Gal(L_1 L_2/K) \longrightarrow Gal(L_1/K) \times Gal(L_2/K)$

$\sigma \longmapsto (\sigma|_{L_1}, \sigma|_{L_2})$

è iniettiva ed è surgettiva $\iff L_1 \cap L_2 = K$

DIMOSTRAZIONE

$M = L_1 L_2$: $L_1 = M^{H_1}$, $L_2 = M^{H_2}$

$G = Gal(M/K)$ $\quad H_1, H_2 \lhd G$

$G \hookrightarrow G/H_1 \times G/H_2 \qquad Gal(M^{H_1}/K) \cong G/H_1$

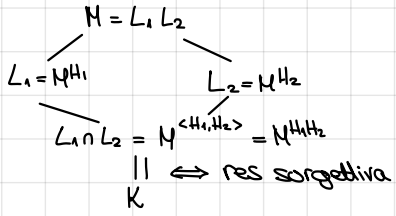
$\sigma \longmapsto (\sigma \bmod H_1, \sigma \bmod H_2)$

$\ker res = \{\sigma \in G \mid \sigma|_{L_1} = id, \sigma|_{L_2} = id\} = \{id\}$

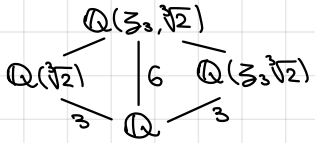
$M = L_1 L_2 = M^{H_1} M^{H_2} = M^{H_1 \cap H_2} \implies H_1 \cap H_2 = \{id\}$, $H_1, H_2 \lhd G$

$L_1 \cap L_2 = K \iff M^{H_1} \cap M^{H_2} = M^{H_1 H_2} = K \iff H_1 H_2 = G$

$\iff G \hookrightarrow G/H_1 \times G/H_2$ è surgettiva (per cardinalità) □

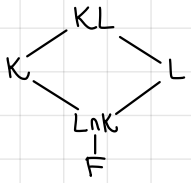


esempio



Gruppo di Galois del traslato

proposizione Sia K/F di Galois. Allora
(1) KL/L è di Galois
(2) $Gal(KL/L) \cong Gal(K/L\cap K)$



DIMOSTRAZIONE

(1) Già visto

(2) $Gal(KL/L) \xrightarrow{Res} Gal(K/F)$

$\sigma \longmapsto \sigma_K$

Notiamo che $\sigma_{K/F} = \sigma_F = id$ perché $\sigma_L = id$

$\sigma_K : K \longrightarrow \overline{K}$ ma la sua immagine è K perché K/F è di Galois

Res è iniettivo: se $\sigma \in \ker Res$, allora

$\sigma_K = id$, inoltre $\sigma_L = id \Rightarrow \sigma_{KL} = id$

il campo fissato da σ contiene K, contiene L, quindi contiene KL

Chi è l'immagine di Res? Anzi, chi è il campo fisso di tale immagine?

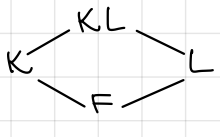
$K^I = \{x \in K \mid \forall \sigma \in I \ \sigma(x) = x\} = \{x \in K \mid \forall \sigma \in Gal(LK/L), \ \sigma_K(x) = x\} =$

$= \{x \in K \mid \forall \sigma \in Gal(LK/L) \ \ \sigma(x) = x\} = K \cap \{x \in LK \mid \forall \sigma \in Gal(LK/L) \ \sigma(x) = x\} =$

$= K \cap L = K^{Gal(K/K\cap L)}$

Dal teorema di corrispondenza, $I = Gal(K/L\cap K)$ □

corollario Sia K/F di Galois, $K\cap L = F$
Allora $[KL:F] = [K:F][L:F]$



DIMOSTRAZIONE

$Gal(KL/L) \cong Gal(K/L\cap K) = Gal(K/F)$

$[KL:L] = [K:F]$

$[KL:F] = [KL:L] \cdot [L:F] = [L:F] \cdot [K:F]$ □

proposizione $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$

DIMOSTRAZIONE

Il campo $\mathbb{Q}(\zeta_n)$

$\zeta_n :=$ qualsiasi radice primitiva n-esima di 1 in $\mathbb{C}$

- $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois: è il cds di x^n-1

  (perché le radici di x^n-1 sono ζ_n^k, $0 \le k \le n-1$)

- $\Phi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$

  $\sigma \longmapsto \overline{j}$

  $\sigma : \mathbb{Q}(\zeta_n) \hookrightarrow \mathbb{Q}(\zeta_n) \subseteq \overline{\mathbb{Q}}$

  $\sigma(\zeta_n) = \zeta_n^j$

  Bisogna verificare che $(j,n)=1$

  $\sigma : \mathbb{Q}(\zeta_n)^* \xrightarrow{\sim} \mathbb{Q}(\zeta_n)^*$

  σ induce un isomorfismo di gruppi, e quindi conserva gli ordini degli elementi

  $\Rightarrow \sigma(\zeta_n)$ è una radice primitiva n-esima di 1 $\Rightarrow \sigma(\zeta_n) = \zeta_n^j$ con $(j,n)=1$

  Φ è iniettiva, perché σ è determinata da $\sigma(\zeta_n)$ e $\sigma(\zeta_n) = \zeta_n^{\Phi(\sigma)}$

  Φ è un omomorfismo di gruppi:

  $\sigma_1(\zeta_n) = \zeta_n^{j_1}$, $\sigma_2(\zeta_n) = \zeta_n^{j_2}$ $\qquad \sigma_1\sigma_2(\zeta_n) = \zeta_n^{j_1 j_2}$

  $\Phi(\sigma_1\sigma_2) = \Phi(\sigma_1)\Phi(\sigma_2)$

- Chiamiamo $f(x)$ il polinomio minimo di ζ_n

  Fissiamo un primo p, $p \nmid n$, e consideriamo ζ_n^p

<u>Oss</u> Φ isomorfismo $\Leftrightarrow |\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg f(x) = \#\{\text{coniugati di } \zeta_n\}$

Supponiamo per assurdo ζ_n e ζ_n^p non siano coniugate,

sia $g(x)$ il polinomio minimo di ζ_n^p.

Vale $f(x)g(x) \mid x^n-1$ perché $f(x) \mid x^n-1$ (ζ_n radice di x^n-1)

$g(x) \mid x^n-1$ (ζ_n^p radice di x^n-1)

Siccome $(f(x), g(x)) = 1$ (polinomi monici irriducibili diversi)

segue $f(x)g(x) \mid x^n-1$

D'altra parte, $f(x) \mid g(x^p)$ perché $g(\zeta_n^p) = 0$

Scriviamo $g(x^p) = f(x)h(x)$ in $\mathbb{Q}[x]$, e in effetti anche in $\mathbb{Z}[x]$:

$f(x)$ è primitivo perché divide x^n-1 e $c(f(x)) \mid c(x^n-1) = 1$

<u>Oss</u> $f(x) \in \mathbb{Q}[x]$. Scelgo $d \in \mathbb{Q}$ t.c. $df(x) \in \mathbb{Z}[x]$ primitivo

$df(x) \mid x^n-1$ in $\mathbb{Q}[x]$. Per il lemma di Gauss, $\exists\, g(x) \in \mathbb{Z}[x]$

$x^n-1 = (df(x)) \cdot g(x) \Rightarrow df(x)$ è monico perché il termine di testa divide 1

$f(x) \mid g(x^p) \implies g(x^p) = f(x)h(x)$ in $\mathbb{Z}[x]$ e $f(x)g(x) \mid x^n - 1$

Riduciamo mod p: $(g(x))^p \overset{\text{in } \mathbb{F}_p}{=} g(x^p) = f(x)h(x)$ in $\mathbb{F}_p[x]$

Sia $\alpha \in \overline{\mathbb{F}_p}$ una radice di $f(x)$. Allora $g(\alpha)^p = f(\alpha)h(\alpha) = 0 \Rightarrow g(\alpha) = 0$

Da $f(x)g(x) \mid x^n - 1$, scopro che $\alpha \in \overline{\mathbb{F}_p}$ è una radice almeno doppia di $x^n - 1$

ma $(x^n - 1, nx^{n-1}) = (x^n - 1, n) = (1)$, quindi $x^n - 1$ non ha radici multiple ↯

Quindi $f(x) = g(x)$

Sia j con $(j, n) = 1$, $j > 0$. Scriviamo $j = p_1^{e_1} \cdots p_r^{e_r}$ con $p_i \mid n$

Il punto (3) dice che $\zeta_n, \zeta_n^{p_1}$ hanno lo stesso polinomio minimo,

come anche $\zeta_n^{p_1}, \zeta_n^{p_1 p_2}, \ldots$

Iterando, ζ_n e ζ_n^j hanno lo stesso polinomio minimo.

Quindi il polinomio minimo di ζ_n ha come radici almeno ζ_n^j, $(j, n) = 1$

che sono $\varphi(n)$

Quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg f(x) \geq \varphi(n)$

Quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = |\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})|$

e $\Phi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathbb{Z}/n\mathbb{Z}^*$ è un isomorfismo □

corollario $x^n - 1 = \prod_{k \mid n} \Phi_k(x)$ con $\Phi_k(x) \in \mathbb{Z}[x]$ irriducibile di grado $\varphi(k)$

DIMOSTRAZIONE

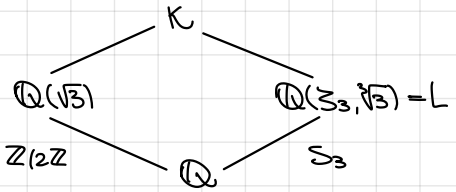
$\Phi_k(x) = \prod_{(j,k)=1} (x - \zeta_k^j) \in \mathbb{Z}[x]$ è il polinomio minimo di ogni radice k-esima □

esempio $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$ è di Galois

Voglio dire che è cds di $(x^2-3)(x^3-3)$

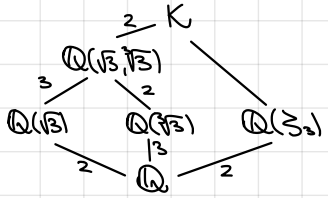
In effetti: $\mathbb{Q}(\pm\sqrt{3}, \sqrt[3]{3}, \sqrt[3]{3}\zeta_3) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \zeta_3) =$

$= \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \frac{-1+i\sqrt{3}}{2}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, i)$



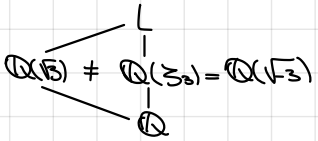
Sappiamo che $Gal(K/\mathbb{Q}) \hookrightarrow Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times S_3$

Basta dire che $\#Gal(K/\mathbb{Q}) = 12$, cioè $[K:\mathbb{Q}] = 12$



Oppure: mi basta mostrare che $\sqrt{3} \notin L$

Se $\sqrt{3} \in L$ ($\Leftrightarrow \mathbb{Q}(\sqrt{3}) \subseteq L$), $\mathbb{Q}(\sqrt{3})$ corrisponderebbe a un sottogruppo $H < Gal(L/\mathbb{Q})$ di indice 2 $\Rightarrow H = A_3$



C'è una sola estensione quadratica, che è $\mathbb{Q}(\zeta_3)$

e $\mathbb{Q}(\zeta_3) \neq \mathbb{Q}(\sqrt{3})$ perché $-3/3 \notin \mathbb{Q}^{*2}$

Troviamo tutte le estensioni quadratiche dentro K.

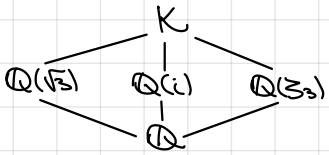
Corrispondono ai sottogruppi di $\mathbb{Z}/2\mathbb{Z} \times S_3$ di indice 2

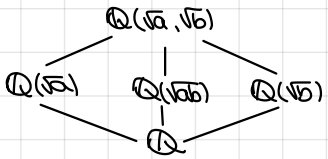
OSS $H < G$ di indice 2, $g \in G \Rightarrow g^2 \in H$

$H = (gH)^2 = g^2 H \Rightarrow g^2 \in H$

$H < G$ di indice 2 $\Rightarrow H$ contiene $\{0\} \times A_3$

Tali H sono in biiezione con i sottogruppi di indice 2 in $\frac{\mathbb{Z}/2\mathbb{Z} \times S_3}{\{0\} \times A_3} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ che sono 3.

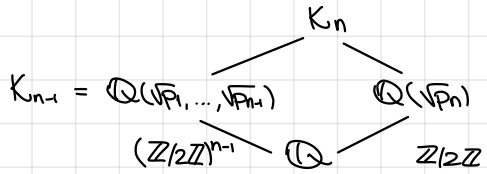




proposizione Siano $p_1, \dots, p_n$ primi distinti e $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$
Allora $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$

DIMOSTRAZIONE

Per induzione su n



$Gal(K_n/\mathbb{Q}) \leq (\mathbb{Z}/2\mathbb{Z})^{n-1} \times \mathbb{Z}/2\mathbb{Z}$

Punto cruciale: trovare tutti gli $F \subset K_{n-1}$ con $[F:\mathbb{Q}] = 2$

Contiamoli: sono i sottogruppi di indice 2 di $(\mathbb{Z}/2\mathbb{Z})^{n-1}$,
che sono $2^{n-1} - 1$

Le trovo: $\mathbb{Q}(\sqrt{p_1^{e_1} \cdots p_{n-1}^{e_{n-1}}})$ con $e_i \in \{0,1\}$ e non tutti nulli

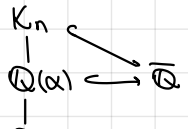
Sono distinte: $p_1^{e_1} \cdots p_{n-1}^{e_{n-1}} \cdot p_1^{f_1} \cdots p_{n-1}^{f_{n-1}} = \square$ in $\mathbb{Q}$
$\iff e_i + f_i \equiv 0 \ (2) \ \forall i \iff e_i \equiv f_i \ (2) \ \forall i$

I sottogruppi di $(\mathbb{Z}/2\mathbb{Z})^n$ di indice 2 sono $2^n - 1$
$(\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n$ $\quad H < (\mathbb{Z}/2\mathbb{Z})^n \Rightarrow H = (\mathbb{Z}/2\mathbb{Z})^{n-1}$ sottospazio vettoriale
di codimensione 1 (iperpiano)

$a_1 x_1 + \dots + a_n x_n = 0$: sono 2^n equazioni, meno l'eq.ne $0 = 0$

$\alpha := \sqrt{p_1} + \dots + \sqrt{p_n}$ è primitivo

Dobbiamo mostrare $\mathbb{Q}(\alpha) = K_n \iff [\mathbb{Q}(\alpha):\mathbb{Q}] = [K_n:\mathbb{Q}] = 2^n$
$\iff$ esistono 2^n immersioni distinte $\mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$



$\iff$ le restrizioni delle 2^n immersioni $K_n \hookrightarrow \overline{\mathbb{Q}}$
a $\mathbb{Q}(\alpha)$ sono tutte distinte

$\sigma_{\varepsilon_1 \dots \varepsilon_n} : \begin{cases} \sqrt{p_1} \longmapsto \varepsilon_1 \sqrt{p_1} \\ \vdots \\ \sqrt{p_n} \longmapsto \varepsilon_n \sqrt{p_n} \end{cases}$ con $\varepsilon_i \in \{\pm 1\}$

Dire che sono tutte distinte su $\mathbb{Q}(\alpha)$ vuol dire

$\sigma_{\varepsilon_1, \dots, \varepsilon_n}(\alpha) \neq \sigma_{\delta_1, \dots, \delta_n}(\alpha)$ se $(\delta_1, \dots, \delta_n) \neq (\varepsilon_1, \dots, \varepsilon_n)$
$\iff \varepsilon_1 \sqrt{p_1} + \dots + \varepsilon_n \sqrt{p_n} = \delta_1 \sqrt{p_1} + \dots + \delta_n \sqrt{p_n}$

Per induzione, $\sqrt{p_1}, \dots, \sqrt{p_n}$ fanno parte della base di K_n

Quindi l'uguaglianza vale $\iff \varepsilon_i = \delta_i \ \forall i$ ↯

□

Biquadratiche

proposizione Sia $p(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ irriducibile e $\Delta = a^2 - 4b$
Sia K il cols di $p(x)$ su $\mathbb{Q}$. Allora

$$Gal(K/\mathbb{Q}) \cong \begin{cases} D_4 & \text{se } \sqrt{b},\ \sqrt{b\Delta} \notin \mathbb{Q} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{se } \sqrt{b} \in \mathbb{Q} \\ \mathbb{Z}/4\mathbb{Z} & \text{se } \sqrt{b} \notin \mathbb{Q} \text{ ma } \sqrt{b\Delta} \in \mathbb{Q} \end{cases}$$

DIMOSTRAZIONE

$t := x^2 \qquad t_{1,2} = \frac{-a \pm \sqrt{a^2-4b}}{2} \qquad \Delta = a^2 - 4b$

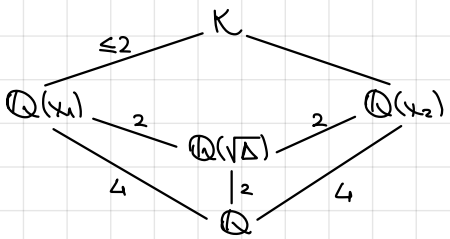
$x_1, x_2, x_3, x_4 = \pm \sqrt{\frac{-a \pm \sqrt{a^2-4b}}{2}}$

$x_1 = \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}} \qquad x_2 = \sqrt{\frac{-a-\sqrt{a^2-4b}}{2}} \qquad x_3 = -x_1,\ x_4 = -x_3$

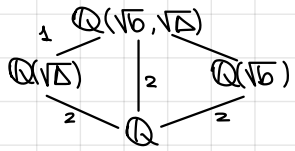
Il cols è $\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_2) = K$

$\mathbb{Q}(x_1) \supseteq \mathbb{Q}(x_1^2) = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(x_2^2) \subseteq \mathbb{Q}(x_2)$

Noto che $\sqrt{\Delta} \notin \mathbb{Q}$, altrimenti
$(t-t_1)(t-t_2)$ con $t_1, t_2 \in \mathbb{Q}$ e quindi
$p(x) = (x^2 - t_1)(x^2 - t_2)$, ma $p(x)$ è irriducibile



Vorrei capire se $\mathbb{Q}(x_1) = \mathbb{Q}(x_2) \iff \mathbb{Q}(\sqrt{\Delta})(\sqrt{t_1}) = \mathbb{Q}(\sqrt{\Delta})(\sqrt{t_2})$
$\iff t_1 \cdot t_2$ è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$
$\iff b$ è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$



Allora b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$ se e solo se:
b è un quadrato in $\mathbb{Q}$
b non è un quadrato in $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{b})$
$\iff b(a^2-4b)$ è un quadrato in $\mathbb{Q}$

$$[K : \mathbb{Q}] = \begin{cases} 4 & \text{se } b = \square \text{ o } b(a^2-4b) = \square \\ 8 & \text{altrimenti} \end{cases}$$

Se $[K:\mathbb{Q}] = 8$, $|Gal(K/\mathbb{Q})| = 8$ e $Gal(K/\mathbb{Q}) \hookrightarrow S_4$
quindi $Gal(K/\mathbb{Q}) \cong D_4$ (è un 2-Sylow di S_4)
Se $[K:\mathbb{Q}] = 4$, allora $K = \mathbb{Q}(x_1)$ e $\sigma \in Gal(K/\mathbb{Q})$
è completamente determinato da $\sigma(x_1)$.
Ci sono 4 elementi, $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ di $Gal(K/\mathbb{Q})$ e sono $\sigma(x_1) = x_i$
Cerchiamo di capire cosa fa σ_i^2
Certamente σ_3 è di ordine 2: $\sigma_3^2(x_1) = \sigma_3(-x_1) = x_1$
Guardiamo σ_2 : $x_1 \xmapsto{\sigma_2} x_2 \xmapsto{\sigma_2} \sigma_2(x_2)$

$$x_1 x_2 = \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}} \sqrt{\frac{-a-\sqrt{a^2-4b}}{2}} = \sqrt{\frac{a^2-\Delta}{4}} = \sqrt{b} \implies x_2 = \frac{\sqrt{b}}{x_1}$$

$\sigma_2(\sigma_2(x_1)) = \sigma_2(x_2) = \sigma_2(\sqrt{b}/x_1)$

Se b è un quadrato in $\mathbb{Q}$: $= \sqrt{b}/\sigma(x_1) = \sqrt{b}/x_2 = x_1$

e quindi $\sigma_2^2 = id$ e $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$

Se b non è quadrato in $\mathbb{Q}$, ma $b \cdot \Delta = c^2$ lo è:

$\sqrt{b} \cdot \sqrt{\Delta} = c \longrightarrow \sqrt{b} = c/\sqrt{\Delta}$

$x_1 = \sqrt{\frac{-a+\sqrt{\Delta}}{2}}$: $\sqrt{\Delta} = 2x_1^2 + a$, $x_2 = \sqrt{\frac{-a-\sqrt{\Delta}}{2}}$

$\sigma_2(\sqrt{\Delta}) = 2\sigma_2(x_1)^2 + a = 2x_2^2 + a = -\sqrt{\Delta}$

<u>Oss</u> Se $\sigma_2(\sqrt{\Delta}) = \sqrt{\Delta}$, si trova che tutto $Gal(K/\mathbb{Q})$ fissa $\sqrt{\Delta} \Longrightarrow \sqrt{\Delta} \in \mathbb{Q}$ ↯

Ora $\sigma_2(\sqrt{b}) = \sigma_2(c/\sqrt{\Delta}) = \frac{c}{-\sqrt{\Delta}} = -\sqrt{b}$

$\sigma_2(\sigma_2(x_1)) = \sigma_2(x_2) = \sigma_2(\sqrt{b}/x_1) = -\sqrt{b}/x_2 = -x_1$

Quindi $\sigma_2^2 = \sigma_3$ e $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$

<u>Conclusione</u>:

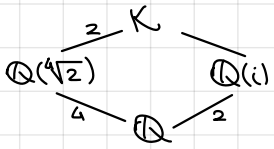
$Gal(K/\mathbb{Q})$ è : $\begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{se } b = \square \\ \mathbb{Z}/4\mathbb{Z} & \text{se } b \neq \square \text{ ma } b(a^2-4b) = \square \\ D_4 & \text{altrimenti} \end{cases}$

□

esempio Sottocampi del cols di x^4-2 su $\mathbb{Q}$

$K = \mathbb{Q}(\sqrt[4]{2}, i)$ $\quad Gal(K/\mathbb{Q}) \cong D_4$

$r: \begin{cases} \sqrt[4]{2} \longmapsto i\sqrt[4]{2} \\ i \longmapsto i \end{cases}$ $\quad s: \begin{cases} \sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ i \longmapsto -i \end{cases}$



Qual è il campo fissato da

$\langle r \rangle$: ord 4 $\longrightarrow$ ind 2 $\longrightarrow$ fissa un campo di grado 2 su $\mathbb{Q}$: $\mathbb{Q}(i)$

$\langle s \rangle$: ord 2 $\longrightarrow$ ind 4 $\longrightarrow$ fissa un campo di grado 4 su $\mathbb{Q}$: $\mathbb{Q}(\sqrt[4]{2})$

$\langle r^2 \rangle$: fissa un campo di grado 4, che contiene $\mathbb{Q}(i)$: $\mathbb{Q}(i, \sqrt{2})$

$r^2(\sqrt[4]{2}) = -\sqrt[4]{2} \longrightarrow r^2(\sqrt{2}) = \sqrt{2}$

$\langle sr \rangle$: fissa un campo di grado 4

$\beta \in K$: $\gamma = \beta + sr(\beta)$

$sr(\gamma) = sr(\beta) + (sr)^2(\beta) = \gamma$

$sr: \begin{cases} \sqrt[4]{2} \longmapsto \sqrt[4]{2}\, i \longmapsto -i\sqrt[4]{2} \\ i \longmapsto -i \end{cases}$

$\beta = \sqrt[4]{2}$, allora $\gamma = \sqrt[4]{2} - i\sqrt[4]{2}$

$K^{\langle sr \rangle} \overset{?}{=} \mathbb{Q}(\gamma)$

4 | $\quad \supseteq$ per costruzione

$\mathbb{Q}$

Polinomio minimo di γ : $\gamma^2 = \sqrt{2}(-2i)$ $\quad \gamma^4 = -8$

Se x^4+8 è irriducibile, allora $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$

e $[K^{\langle sr \rangle} : \mathbb{Q}] = [D_4 : \langle sr \rangle] = 4 \Longrightarrow \mathbb{Q}(\gamma) = K^{\langle sr \rangle}$

$\gamma/2$ annulla $(2x)^4 + 8$, equiv. $x^4 + \frac{1}{2}$

$\mathbb{Q}(\sqrt[4]{-8}) = \mathbb{Q}(\sqrt[4]{-8}/2) = \mathbb{Q}(\sqrt[4]{-1/2}) = \mathbb{Q}(\sqrt[4]{-2})$ ha grado 4 su $\mathbb{Q}$

Oss $K/\mathbb{Q}$ Galois con gruppo G, $H < G$

Preso $\beta \in K$, l'elemento $\gamma = \sum_{h \in H} h(\beta) \in K^H$

Infatti, preso $\sigma \in H$, $\sigma(\gamma) = \sum_{h \in H} \sigma h(\beta) = \sum_{\tau \in H} \tau(\beta) = \gamma$

esempio Il cols di x^6+3 su $\mathbb{Q}$

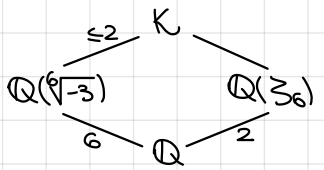
$K = \mathbb{Q}(\sqrt[6]{-3}, \zeta_6)$

$Gal(K/\mathbb{Q})$: $\sigma: \begin{cases} \sqrt[6]{-3} \longmapsto \sqrt[6]{-3}\, \zeta_6^i \\ \zeta_6 \longmapsto \zeta_6^{\pm 1} = \zeta_6^{1-i} \end{cases}$

ma $\zeta_6 = \frac{1+\sqrt{-3}}{2} = \frac{1+(\sqrt[6]{-3})^3}{2}$, sia $\alpha := \sqrt[6]{-3}$

Allora, se $\sigma(\alpha) = \alpha \cdot \zeta_6^i$, si ha necessariamente

$$\sigma(\zeta_6) = \sigma\left(\frac{1+\alpha^3}{2}\right) = \frac{1+\alpha^3 \zeta_6^{3i}}{2} = \begin{cases} \zeta_6 & \text{se } i \text{ è pari} \\ \zeta_6^{-1} & \text{se } i \text{ è dispari} \end{cases}$$



Classe di isomorfismo di $Gal(K/\mathbb{Q})$?

$\sigma_i: \begin{cases} \sqrt[6]{-3} \longmapsto \sqrt[6]{-3}\, \zeta_6^i \\ \zeta_6 \longmapsto \zeta_6^{\pm i} \end{cases}$

Se c'è un elemento di ordine 6, deve avere i dispari

(altrimenti l'intero Gal fisserebbe ζ_6)

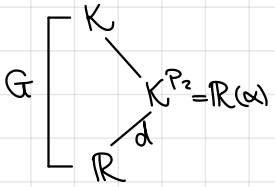
$\sigma_i(\sigma_i(\sqrt[6]{-3})) = \sigma_i(\sqrt[6]{-3}\, \zeta_6^i) = \sqrt[6]{-3}\, \zeta_6^i\, \zeta_6^{-i} = \sqrt[6]{-3}$

$\Longrightarrow$ tutti i σ_i con i dispari hanno ord 2 $\Longrightarrow$ $Gal(K/\mathbb{Q}) \cong S_3$

Teorema fondamentale dell'algebra Il cds di $f(x) \in \mathbb{C}[x]$ è $\mathbb{C}$

DIMOSTRAZIONE

$g(x) = f(x) \cdot \overline{f(x)} \in \mathbb{R}[x]$: basta vedere che il suo cds è $\mathbb{R}$ o $\mathbb{C}$



$G > P_2$ un Sylow

$d = [G : P_2]$ dispari

Sia $\mu(x)$ il pol. min. di α, di grado d

$\Rightarrow \mu(x)$ è irriducibile con una radice

(teorema dei valori intermedi)

$\Rightarrow$ ha grado 1 $\Rightarrow G = P_2$

Se $G = P_2 = \{1\}$, ok

Altrimenti: $G_n \subset_2 \dots \subset_2 G_2 \subset_2 G_1 \subset_2 G$

$\downarrow$ Galois

$\mathbb{R} \subset_2 K^{G_1} \subset_2 K^{G_2} \subset_2 \dots \subset_2 K^{G_n}$

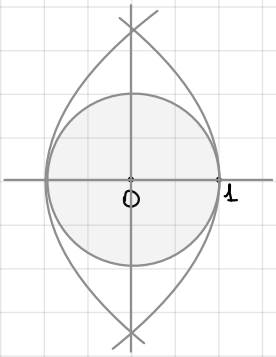
$\mathbb{R}(\sqrt{a}) = \mathbb{R}(i) = \mathbb{C}$

$\mathbb{C}$ non ha estensioni di grado 2 : $\mathbb{C}(\sqrt{z}) = \mathbb{C}$

perché $z = \rho e^{i\theta} \Rightarrow \sqrt{z} = \sqrt{\rho}\, e^{i\frac{\theta}{2}} \in \mathbb{C}$ □

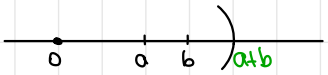
costruzioni con riga e compasso

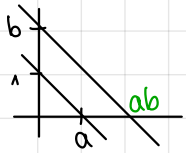
(1) Tracciare rette tra due punti costruiti
(2) Tracciare circonferenze di centro un punto costruito e di raggio uguale alla distanza tra due punti costruiti
(3) Tracciare perpendicolari e parallele ad una retta data per un punto costruito

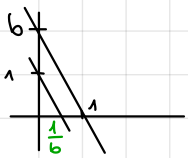


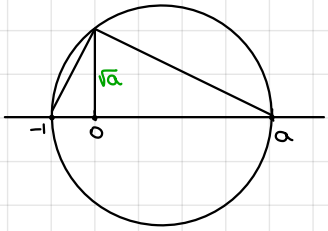
proposizione $K=\{\alpha\in\mathbb{R} \mid \alpha \text{ costruibile}\}$ è un campo, con $\mathbb{Q}\subset K$
Inoltre, $\forall \alpha\in A, \alpha>0, \sqrt{\alpha}\in A$

DIMOSTRAZIONE









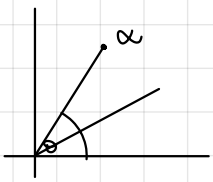
□

teorema $L=\{\alpha\in\mathbb{C} \mid \alpha \text{ costruibile}\}$ è un campo chiuso rispetto alla $\sqrt[2]{\ }$

DIMOSTRAZIONE

$\alpha = x+iy \in L \iff (x,0), (0,y)$ sono costruibile
$\beta = z+iw$

$\alpha\in L : \alpha = \rho e^{i\theta}$
$\sqrt{\rho}\in K$



□

<u>OSS</u> rette e circonferenze costruibili hanno equazioni con coefficienti costruibili

teorema $\alpha \in \mathbb{C}$, $\alpha \in L \iff$ esiste una successione finita di campi
$\mathbb{Q} = L_0 \subset L_1 \subset \dots \subset L_{n-1} \subset L_n$
con $\alpha \in L_n$ e $[L_{i+1} : L_i] = 2 \quad \forall i = 0, \dots, n-1$

DIMOSTRAZIONE

($\Rightarrow$) $\alpha \in L$: $\exists\, z_0, z_1, \dots, z_t$
dove z_i è ottenuto intersecando due rette, due circonferenze,
una retta e una circonferenza

$\alpha \in L(z_0, \dots, z_t)$
L'equazione risolvente ha grado ≤ 2, quindi
$[\mathbb{Q}(z_0, \dots, z_i) : \mathbb{Q}(z_0, \dots, z_{i-1})] \leq 2$

($\Leftarrow$) $\alpha \in L_n \supseteq_2 \dots \supseteq_2 L_1 \supseteq_2 \mathbb{Q}$
$L_{i+1} = L_i(\sqrt{\Delta_i})$, $\Delta_i \in L_i$

- $n = 0$: $L_0 = \mathbb{Q}$ e i punti $\mathbb{Q}$ sono costruibili
- Per ipotesi induttiva, gli elementi di L_{n-1} sono costruibili
  $L_n = L_{n-1}(\sqrt{\Delta})$
  $\Delta \in L_{n-1}$: è costruibile $\Rightarrow \sqrt{\Delta}$ è costruibile
  $\sqrt{\Delta} \in L$, $L_{n-1} \subset L \Rightarrow L_n = L_{n-1}(\sqrt{\Delta}) \subset L$ □

corollario α costruibile $\Rightarrow \alpha$ algebrico di grado 2^d

DIMOSTRAZIONE

$\alpha \in L_n \quad \mathbb{Q} \overset{2^d}{\subseteq} \mathbb{Q}(\alpha) \subseteq L_n \quad (2^n)$ □

Conseguenze :
- non è possibile trisecare un angolo
  se $x^3 - \alpha$, non è possibile
- non si può duplicare il cubo
  $(x^3 - 2)$

Costruzione di n-agoni regolari
n-agono costruibile $\iff \zeta_n \in L \iff [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = 2^d$

si vede con la teoria di Galois

$n = 2^a p_1^{e_1} \cdots p_r^{e_r} \qquad p_i \neq p_j, p_i \neq 2$
$\phi(n) = 2^{a-1} \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1} = 2^d$
$\Rightarrow e_i = 1 \qquad p_i = 1 + 2^{k_i}$ primo $\Rightarrow k_i = 2^{h_i}$
$p_i = 1 + 2^{2^{h_i}}$ (primi di Fermat)

Esiste una formula risolutiva per l'equazione generale di grado n in termini di operazioni di campo e $\sqrt[k]{\ }$?

Sì $\iff$ $n \leq 4$

$\alpha \in L_n$

$\mathbb{Q} = L_0 \subseteq L_1 \subseteq \dots \subseteq L_n = L$

$L_{i+1} = L_i(\sqrt[d_i]{r_i})$ con $r_i \in L_i$

Se ho le radici, L_{i+1}/L_i è di Galois, con $\mathrm{Gal}(L_{i+1}/L_i) \cong \mathbb{Z}/d_i\mathbb{Z}$

$\mathrm{Gal}(L_n/\mathbb{Q})$ ha una filtrazione di sottogruppi

$L_i = L^{H_i}$

$G = H_n \rhd \dots \rhd H_1 \rhd \{id\}$ e H_2/H_1 è ciclico

L'equazione generale di grado n ha $\mathrm{Gal} \cong S_n$

$\{e\} \lhd S_2$

$\{e\} \lhd A_3 \lhd S_3$

$\{e\} \lhd \mathbb{Z}/2\mathbb{Z} \lhd V_4 \lhd A_4 \lhd S_4$

$\{e\} \lhd \times \lhd A_n \lhd S_n$ per $n \geq 5$