# GRUPPI

## Generatori

$G$ gruppo, $x_1, \dots, x_n \in G$

$\langle x_1, \dots, x_n \rangle$ = sottogp generato da $x_1, \dots, x_n$

= il più piccolo sgp di $G$ che contiene $x_1, \dots, x_n$

$$= \bigcap_{\substack{H < G \\ H \ni x_1, \dots, x_m}} H$$

Oss Sia $S = \langle x_1, \dots, x_m \rangle$. $x_1 \cdot x_1$, $x_1^k \in S$

$x_1^{k_1} \cdot x_2^{k_2} \cdots x_m^{k_n} \in S$ $k_1, \dots, k_m \in \mathbb{Z}$

$$\underline{x_1 x_2 x_1 x_2 x_1 x_2 \dots x_1 x_2} \in S$$

S deve contenere tutti i prodotti finiti della forma

$$\{ g_1^{\pm 1} g_2^{\pm 1} g_3^{\pm 1} \dots g_r^{\pm 1} \}, \text{ dove } g_i \in \{x_1, \dots, x_n\}$$

$$x_1^3 x_2^3 x_1$$

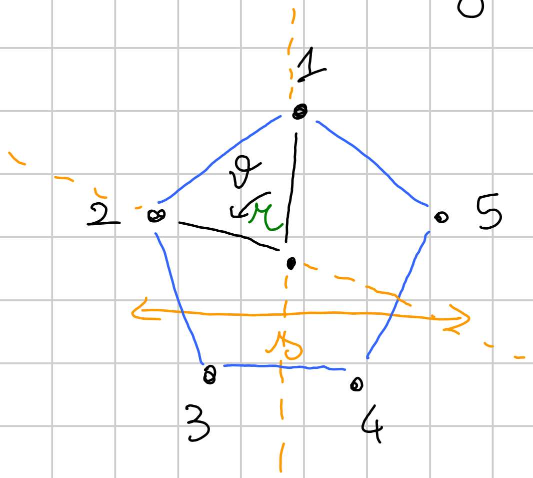
$$\langle x_1, \dots, x_n \rangle = \{ g_1^{\pm 1} \dots g_r^{\pm 1} \mid \overset{r \geq 0}{\text{ogni}} \ g_i \text{ e' uno fra } x_1, \dots, x_n \}$$

$$x^{\pm 1} x^{\pm 1} \dots x^{\pm 1} = x^h$$

Diremo che $x_1, \dots, x_n$ <u>generano G</u> se $\langle x_1, \dots, x_n \rangle = G$

# GRUPPO DIEDRALE

$n \geq 2$. Consideriamo nel piano un poligono regolare con centro l'origine ed $n$ vertici



$D_n$ = gruppo diedrale su $n$ vertici

= l'insieme delle isometrie del piano che mandano il poligono in sé

Esempi di elementi: $r$, la rotaz. antioraria di $\frac{2\pi}{n}$ radianti

$s$, la simmetria $x \mapsto -x$

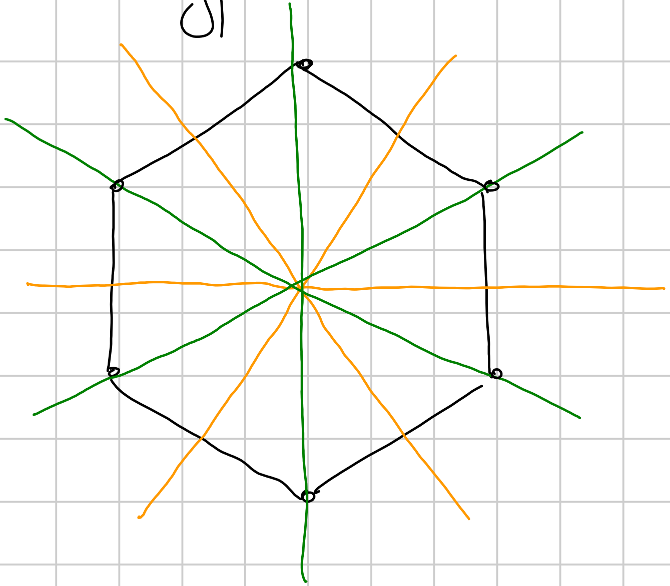
$$\langle r, s \rangle = \{ id, r, r^2, r^3, \dots, r^{n-1}$$

$$s, sr, sr^2, sr^3, \dots, sr^{n-1},$$

$$srs, \quad srsr, \quad sr^2sr^3, \dots \}$$

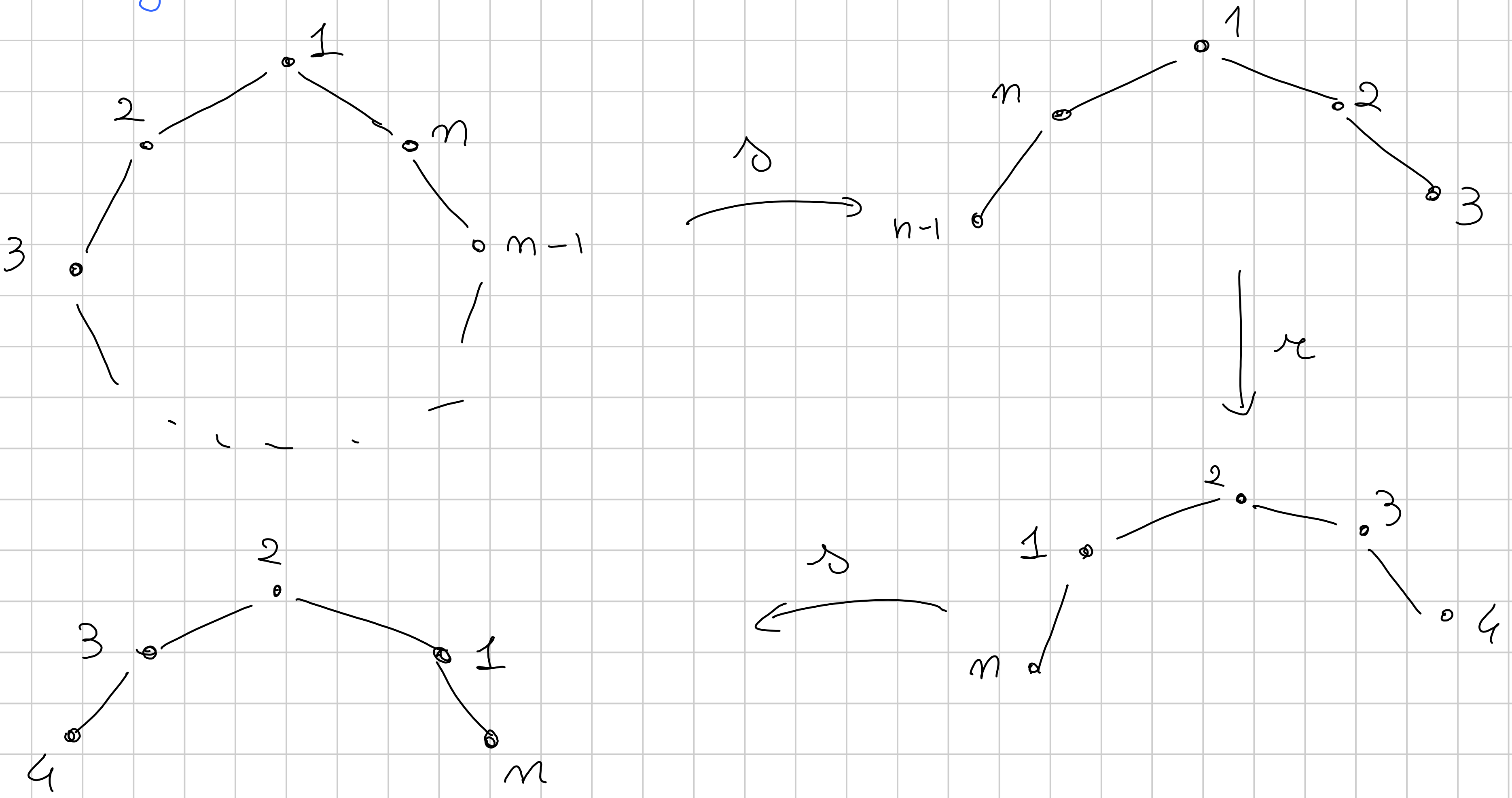
**Def** $\langle r \rangle =: R$, detto il sottogp delle rotazioni

**Oss** $n$ pari:



**Oss** $\det(s \cdot r^k) = \det(s) \cdot \det(r)^k = (-1) \cdot 1^k = -1$

Fatto fondamentale $srs^{-1} = r^{-1}$



$$r = \begin{pmatrix} \boxed{\cos\left(\frac{2\pi}{n}\right)} & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \boxed{\cos\left(\frac{2\pi}{n}\right)} \end{pmatrix} \qquad s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$srs^{-1} = \begin{pmatrix} \cos\left(-\frac{2\pi}{n}\right) & -\sin\left(-\frac{2\pi}{n}\right) \\ \sin\left(-\frac{2\pi}{n}\right) & \cos\left(-\frac{2\pi}{n}\right) \end{pmatrix} = r^{-1}$$

$$sr^2s^3r^{-4}s^4sr = \overbrace{\underbrace{sr^2s^{-1}}}^{= (srs^{-1})^2}\underbrace{r^{-4}}\underbrace{sr}$$

$$= \varphi_s(r^2)\, r^{-4}\, srs^{-1}s$$

$$= \varphi_s(r)^2\, r^{-4}\, \varphi_s(r)\, s$$

$$= r^{-2}\, r^{-4}\, r^{-1} s = r^{-7} s$$

$\varphi_s$ = coniugio per $s$

$$= s\, s^{-1} r^{-7} s$$

$$= s\, r^{7}$$

**Prop.** $|D_n| = 2n$ ⚠ $D_{2n}$

**Dim** Ogni $g \in D_n$ è caratterizzato da $g(1), \dots, g(n)$.

Noto $g(1) \in \{1, \dots, n\}$, $g(2)$ ha $\leq 2$ possibilità

$g(1), g(2)$ non allineati $\Rightarrow$ sono una base $\Rightarrow$ se so $g(1), g(2)$ so tutto $\Rightarrow$ al massimo $n \cdot 2$ scelte

$$\Rightarrow |D_n| \leq 2n$$

$$\left.\begin{matrix} 1, & r, & & \dots, & r^{n-1} \\ s, & sr, & sr^2, & \dots, & sr^{n-1} \end{matrix}\right\} \text{tutti distinti}$$

$$\cancel{s} r^{i} = \cancel{s} r^{j} \Rightarrow i = j \quad \square$$

**Oss** $\langle s, r \rangle = D_n$ : sono generatori!

**Oss** $r^k \cdot s = s \cdot r^{-k} \iff s r^k s^{-1} = r^{-k}$

$$(s r s^{-1})^k = r^{-k}$$

$$\shortparallel$$

$$(r^{-1})^k$$

Fatto fond: $\underbrace{\varphi_s}_{\text{coniugio per } s} (r) = r^{-1} \implies \varphi_s(r)^k = r^{-k}$

$$\shortparallel$$

$$\varphi_s(r^k) = s r^k s^{-1}$$

$$\varphi_s(x) = s x s^{-1}$$

$$s \boxed{r^2 \; s} r^3 \; s r^{-4} \; s r^5 \; s r^6 =$$

$$s \boxed{s r^{-2}} r^3 s \; r^{-4} \; s r^5 \; s r^6$$

$$r s \; r^{-4} s r^{5} s r^{6}$$

$$s r^{-1} r^{-4} s r^{5} s r^{6} = \dots = s r^{j}$$

## Sottogruppi

$H < D_n$

- $H \leq R$ : $R \cong \mathbb{Z}/n\mathbb{Z}$, ce n'è uno $\forall d \mid n$
- $H \not\leq R$

- I sottogp di $R$ sono quelli della forma $\langle r^{n/d} \rangle$, con $d \mid n$ : questo è l'unico di ordine $d$
- $H \not\leq R$.

**Oss** $\underbrace{R \lhd D_n}_{\text{indice } 2}$, e $D_n / R \simeq \mathbb{Z}/2\mathbb{Z}$

$\pi : D_n \longrightarrow D_n / R.$

Se $H \not\subseteq R$, $\pi(H) = D_n/R$, perché se $h \in H \setminus R$

allora $\pi(h) \neq id$

$\ker \pi|_H = (\ker \pi) \cap H = R \cap H$

1° teo di isom (applicato a $\pi|_H$) : $\dfrac{H}{R \cap H} \simeq \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow \quad |R \cap H| = \frac{1}{2} |H|$

$H \supseteq \langle r^k \rangle, \; s \cdot r^h$ dove $\langle r^k \rangle = R \cap H$

Affermo che $H = \underbrace{\langle r^k \rangle}_{|H|/2} \cdot \underbrace{\langle s \cdot r^h \rangle}_{2}$ $\quad \supseteq$ + cardinalità

$$(sr^h)^2 = s\underleftarrow{r^h s}r^h = s s r^{-h} r^h = id$$

$$hK = Kh \qquad hKh^{-1} = K$$

Ricordiamoci $H \cdot K$ è sgp $\iff$ $H \cdot K = K \cdot H$, e questo è vero se almeno uno dei 2 è normale, oppure più generalmente se $H \subseteq \underbrace{N_G(K)}_{\text{normalizz. in } G \text{ di } K}$

Verifichiamo che $sr^h \in N_{D_n}(\langle r^k \rangle)$

$$\iff \quad sr^h \langle r^k \rangle (sr^h)^{-1} \subseteq \langle r^k \rangle$$

Mi sto chiedendo se $sr^h \cdot r^{mk} \cdot sr^h \in \langle r^k \rangle$ per ogni $m \in \mathbb{Z}$

$$s \cdot s \cdot r^{-h-mk} \cdot r^h = r^{-mk} \in \langle r^k \rangle$$

Def. $H_{k,h} = \langle r^k, sr^h \rangle = \langle r^k \rangle \langle sr^h \rangle$

$k \mid n, \quad 0 \leq h < k$

Oss $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$

$\boxed{\subseteq}$ $sr^h = (sr^{h+k}) \cdot (r^k)^{-1}$

$\boxed{\supseteq}$ $r^k \in$ gp di sinistra per def.

$sr^{h+k} \in$ " " " perché lo posso scrivere nella forma $(sr^h) \cdot (r^k)$

$\Rightarrow$ il gp di sx contiene i generatori del gp di dx

$\Rightarrow$ per definizione di sgp. generato, $sx \supseteq dx$.

**Teo** I sgp di $D_n$ sono:

I • $\langle r^k \rangle$ per $k \mid n$

II • $\langle r^k, sr^h \rangle$ per $k \mid n$ e $0 \leq h < k$

Questi sono tutti distinti.

**Dim** Abbiamo già visto che ogni sgp è di uno di questi due tipi. Verifichiamo che sono tutti diversi.

- Due sgp di tipo I, $\langle r^k \rangle = \langle r^m \rangle \iff k = m$

  Cardinalità: $n/k = n/m$

- Uno di tipo I e uno di tipo II sono diversi (uno è $\subseteq R$ ed uno no)

- Due di tipo II: $\langle r^k, sr^h \rangle = \langle r^m, sr^\ell \rangle$

Intersecando con R: $\langle r^k \rangle = \langle r^m \rangle \Rightarrow k = m$

$$sr^h \in \langle r^m, sr^\ell \rangle = \langle sr^\ell \rangle \langle r^m \rangle$$

$$\cancel{s}r^h = \cancel{s}r^\ell \cdot (r^m)^t$$

$$\Rightarrow h \equiv \ell + mt \pmod{n}$$

$$\Rightarrow h \equiv \ell \pmod{m} \quad \text{perché } m \mid n$$

$$\begin{array}{l} 0 \le h < K \\ 0 \le \ell < \overset{\parallel}{m} \end{array} \longrightarrow h = \ell$$

$\square$

**Lemma** $A \leq B \leq G$ con $B \trianglelefteq G$ e $A$ caratt. in $B$.

Allora $A \trianglelefteq G$.

**Dim** Sia $g \in G$. Voglio vedere che $gAg^{-1} = A \iff \varphi_g(A) = A$

Sia $\varphi_g : G \longrightarrow G$ il coniugio per $g$.

$$x \longmapsto gxg^{-1}$$

Siccome $B \trianglelefteq G$, ha senso

$$\boxed{\begin{array}{l} \varphi_g|_B : B \longrightarrow B \\ \qquad\quad b \longmapsto gbg^{-1} \end{array}} \in \operatorname{Aut}(B)$$

$\uparrow$ $B \trianglelefteq G$

Per def. di sgp. caratt., $\varphi_g(A) = A$ $\square$

**Applicazione** $\underbrace{\langle r^k \rangle \trianglelefteq R}_{\text{caratt.}} \underbrace{\trianglelefteq D_n}_{\text{normale}} \implies \langle r^k \rangle \trianglelefteq D_n$

**Oss.** $H_{k,h} \trianglelefteq D_n \iff \begin{cases} r\, H_{k,h}\, r^{-1} = H_{k,h} \\ s\, H_{k,h}\, s^{-1} = H_{k,h} \end{cases}$

$$\boxed{\Leftarrow} \quad \left.\begin{array}{l} r \in N_{D_n}(H_{k,h}) \\ s \in N_{D_n}(H_{k,h}) \end{array}\right\} \quad \underset{\underset{D_n}{\shortparallel}}{\langle r, s\rangle} \subseteq N_{D_n}(H_{k,h})$$

e un sgp $H$ è normale $\iff N_{D_n}(H) = D_n$

$$r \langle r^k, sr^h\rangle r^{-1} = \langle r^k, rsr^{h-1}\rangle = \langle r^k, sr^{h-2}\rangle$$

$$s \langle r^k, sr^h\rangle s^{-1} = \langle r^{-k}, r^h s^{-1}\rangle = \langle r^k, sr^{-h}\rangle$$

$$s(x_1^{\pm 1} x_2^{\pm 1} \cdots)s^{-1} = (sx_1s^{-1})^{\pm 1}(sx_2s^{-1})^{\pm 1} \cdots$$

Scopriamo che $H_{k,h}$ è normale $\iff \langle r^k, sr^{h-2} \rangle =$

$= \langle r^k, sr^{-h} \rangle = \langle r^k, sr^h \rangle$

$\iff h-2 \equiv -h \equiv h \pmod{k}$

$2 \equiv 0 \ (k) \implies k=1, \ k=2$

Per $k=1$, $\langle r^k, sr^h \rangle = \langle r, s \rangle = D_n$

Per $k=2$ ci sono $\langle r^2, s \rangle$ e $\langle r^2, sr \rangle$ se n è pari!

## Classi di coniugio

Classe di $r^k$:

$$g r^k g^{-1} \begin{cases} r & g \in R \\ sr^h \cdot r^k \cdot sr^h & g = sr^h \end{cases}$$

$$= s \cdot s \cdot r^{-h-k+h} = r^{-k}$$

Classe di $r^k$ $=$ $\{r^k, r^{-k}\}$ $\qquad$ $r^k = r^{-k}$ $\quad$ $r^{2k} = id$

Oss Se $n = 2\ell$, $k = \ell$, $\qquad$ Classe $(r^\ell) = \{r^\ell, r^{-\ell}\}$

$= \{r^\ell\}$

$$g x g^{-1} = x \qquad\qquad g x = x g$$

Trovato un elemento del centro! $\quad$ $r^{n/2}$ se $n$ pari

Classe di $sr^h$ $=$

$$(r^k)(sr^h)(r^{-k}) = s r^{h-2k}$$

$$(sr^k)(sr^h)(sr^k) = s r^{2k-h}$$

$$D_2 \simeq (\mathbb{Z}/_{2}\mathbb{Z})^2$$

# AUTOMORFISMI (e altro...)

Titolo nota

## Ancora sul diedrale $D_n$

$$g_1 = s^{a_1} r^{b_1} \quad \text{con} \quad a_1 \in \{0,1\} \quad b_1 \in \{0,\dots,n-1\}$$

$$g_2 = s^{a_2} r^{b_2}$$

$$g_1 \cdot g_2 = s^{a_1} r^{b_1} s^{a_2} r^{b_2} = s^{a_1} s^{a_2} \underbrace{s^{-a_2} r^{b_1} s^{a_2}}_{\varphi_{s^{a_2}}(r^{b_1})} r^{b_2} = \circledast$$

$$\varphi_{s^{a_2}}(r^{b_1}) = \left(\varphi_{s^{a_2}}(r)\right)^{b_1} = \left(\left(\varphi_s\right)^{a_2}(r)\right)^{b_1}$$

$$\begin{aligned} \varphi_s : D_n &\longrightarrow D_n \\ x &\longmapsto s^{-1} x s \end{aligned}$$

$$r^{(-1)^{a_2} \cdot b_1}$$

$$\varphi_s^{2k}(r) = r \qquad \varphi_s^{2k+1}(r) = r^{-1}$$

$$(\star) = s^{a_1+a_2} \, r^{(-1)^{a_2} \cdot b_1 + b_2}$$

$$s^a r^b \rightsquigarrow (a, b)$$

Legge di gruppo $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, (-1)^{a_2} b_1 + b_2)$

Descriviamo ora $\mathrm{Hom}(D_n, G)$, $G$ gruppo qualsiasi.

$\varphi \in \mathrm{Hom}(D_n, G)$ è univoc. det. da $x = \varphi(r)$, $y = \varphi(s)$

$$\varphi(s^a r^b) = \varphi(s)^a \varphi(r)^b = y^a x^b$$

Condiz. necessarie: $\mathrm{ord}(x) \mid n$, $\mathrm{ord}(y) \mid 2 \iff \boxed{x^n = 1, \; y^2 = 1}$ Ⓘ

$$srs^{-1} = r^{-1} \quad \overset{\varphi}{\rightsquigarrow} \quad \boxed{yxy^{-1} = x^{-1}} \quad ①$$

Viceversa: se $x, y \in G$ rispettano ① e ②, allora

$$\boxed{\begin{aligned} \varphi : \quad D_n &\longrightarrow G \\ s^a r^b &\longmapsto y^a x^b \end{aligned}}$$

è un omomorfismo.

Oss: $yxy^{-1} = x^{-1} \quad \rightsquigarrow \quad y^{a_1} \cdot x^{b_1} \cdot y^{a_2} \cdot x^{b_2} =$

$$= y^{a_1+a_2} \cdot x^{(-1)^{a_2} b_1 + b_2}$$

$$\varphi(s^{a_1} r^{b_1} \cdot s^{a_2} r^{b_2}) \overset{?}{=} \varphi(s^{a_1} r^{b_1}) \cdot \varphi(s^{a_2} r^{b_2})$$

$$\varphi\left(s^{a_1+a_2}\cdot r^{(-1)^{a_2}b_1+b_2}\right) \overset{?}{=} y^{a_1}x^{b_1}\cdot y^{a_2}x^{b_2} \qquad \text{OK}$$

## $\mathrm{Aut}(D_n)$, $n>2$

$\varphi: D_n \longrightarrow D_n$ autom.

$$\varphi(r) = r^k \qquad (k,n)=1$$

$$\varphi(s) = \begin{cases} s\cdot r^h & 0\le h<n \\ r^{n/2} \end{cases}$$

No: non sarebbe né surg. né iniettiva

Verifichiamo che $(s\cdot r^h)\cdot r^k\cdot(s\cdot r^h)^{-1} \overset{?}{=} r^{-k}$ ✓

$$\overset{\shortparallel}{s\cdot \cancel{r^h}\, r^k\, \cancel{r^{-h}}\, s^{-1}} = r^{-k}.$$

Con queste scelte, $\varphi$ è surg: $\mathrm{Imm}\,\varphi \ni r^k,\ s\cdot r^h$

$$\begin{tikzcd}[row sep=small]
\mathrm{Imm}\,\varphi \supseteq \langle r^k, s\cdot r^h\rangle \\
\phantom{x} \arrow[u, phantom, "\|"] \\
D_n = \langle r, s\rangle = \langle r, s\cdot r^h\rangle
\end{tikzcd}$$

Surgettività + stessa cardinalità $\Rightarrow$ è bigettivo.

$$\# \mathrm{Aut}(D_n) = \varphi(n)\cdot n$$

$$\mathrm{Aut}(D_2) = \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

È $S_3$: posso permutare come voglio i 3 el. di ord. 2

$(\mathbb{Z}/2\mathbb{Z})^2 \simeq \mathbb{F}_2^{\ 2}$, lo sp. vett. di dim. 2 su $\mathbb{F}_2$

$(\mathbb{Z}/p\mathbb{Z})^n \simeq (\mathbb{F}_p)^n$ come sp. vett.

$$\lambda \cdot v := \underbrace{v+v+\dots+v}_{\tilde{\lambda} \text{ volte}}$$ (il risultato dipende solo da $\lambda$ e non da $\tilde{\lambda}$)

$\lambda \in \mathbb{F}_p \rightsquigarrow \tilde{\lambda} \in \mathbb{Z}$ un rappr di $\lambda \in \mathbb{F}_p$

$$\mathrm{Aut}_{Grp}\left(\mathbb{Z}/p\mathbb{Z}\right)^n = \mathrm{Aut}_{S.V.}\left(\mathbb{Z}/p\mathbb{Z}\right)^n$$

$$\overset{\rotatebox{90}{$\in$}}{\varphi} \qquad \varphi(x+y) = \varphi(x) + \varphi(y)$$

$$\overset{\rotatebox{90}{$\in$}}{\psi} \rightsquigarrow \psi(x+y) = \psi(x) + \psi(y)$$

$$\psi(\lambda \cdot x) \overset{?}{=} \lambda \cdot \psi(x)$$

$$\psi(\underbrace{x+x+\dots+x}_{\tilde{\lambda} \text{ volte}}) = \underbrace{\psi(x) + \dots + \psi(x)}_{\tilde{\lambda} \text{ volte}}$$

$$\begin{array}{c}\mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\right)\\ \wr\| \\ S_3\end{array} \simeq GL_2(\mathbb{F}_2) = \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \middle| \begin{array}{l} a,b,c,d\in\mathbb{F}_2\\ ad-bc\neq 0\end{array}\right\}$$

$$(x,y)\longmapsto(x+y,\ y)$$

trasposizioni

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \quad \underbrace{\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}}_{3\text{-ciclo}}$$

$$\#\,\mathrm{Aut}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2\right) = \#\,GL_2(\mathbb{F}_p) = \underset{\substack{\uparrow\\ \text{img. di } e_1}}{(p^2-1)}\cdot\underset{\substack{\uparrow\\ \text{img. di } e_2}}{(p^2-p)}$$

$$p^2-p = \#\,\mathbb{F}_p^2 - \#\{\text{multipli di } \varphi(e_1)\}$$

$$\#\,\mathrm{Aut}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^n\right) = (p^n-1)\cdot(p^n-p)\cdot(p^n-p^2)\ \dots\ (p^n-p^{n-1})$$

(scelte per $\varphi(e_1)$) × ... × (scelte per $\varphi(e_n)$)

Quanti sgp. di ordine $p$ in $(\mathbb{Z}/p\mathbb{Z})^n$ ? $\frac{p^n-1}{p-1}$

$$\{\text{vettori non nulli}\} \longrightarrow \{\text{sottosp. di dim } 1\}$$

$$v \longmapsto \text{Span } v$$

$$W = \text{Span}(v) = \text{Span}(\lambda v)$$

\# Sottogp di ord $p^{n-1}$ ? $=$ \# Sottosp. di CO-DIM 1

$=$ \# " " DIM 1

passo all'eqz
(o all'ortogonale)

$$0 = a_1 x_1 + \dots + a_n x_n \qquad (a_1, \dots, a_n) \in \mathbb{F}_p^n$$

$$\text{Span}(a_1, \dots, a_n) \subseteq \mathbb{F}_p^n$$

## $\mathrm{Aut}(K \times H)$

$\mathrm{Aut}(K\times H) \xhookleftarrow{i} \mathrm{Aut}(K) \times \mathrm{Aut}(H)$ : quando è iso?

$\Updownarrow$

$K\times\{1\}$ e $\{1\}\times H$ sono sottogruppi caratteristici

$\varphi_1\times\varphi_2 : K\times H \to K\times H \longleftarrow (\varphi_1 \,,\, \varphi_2)$

$(g,h) \mapsto (\varphi_1(g), \varphi_2(h))$

- Se $i$ è surgettiva, ogni autom. di $K\times H$ è un $\varphi_1\times\varphi_2$, e allora $(\varphi_1\times\varphi_2)(K\times\{1\}) = \varphi_1(K)\times\varphi_2(\{1\}) = K\times\{1\}$
- Se $K\times\{1\}$ e $\{1\}\times H$ sono caratteristici, allora dato $\varphi\in\mathrm{Aut}(K\times H) \rightsquigarrow \varphi|_{K\times\{1\}} =: \varphi_1$

$$\rightsquigarrow \quad \varphi|_{\{1\}\times H} =: \varphi_2$$

$$\varphi(g,h) = \varphi(g,1)\cdot\varphi(1,h) = (\varphi_1(g), 1)\cdot(1, \varphi_2(h))$$
$$= (\varphi_1\times\varphi_2)(g,h)$$

$K \times H$ : i fattori sono caratteristici?

$(|K|, |H|) = 1 \implies$ la risposta è sì!

$m := |K|$, $n := |H|$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$K \times \{1\} = \{ (g,h) \in K \times H$ t.c. $\operatorname{ord}(g,h) \mid m \}$

$\boxed{\subseteq}$ È il teo di Lagrange

$\boxed{\supseteq}$ $(g,h)$ di ord che $| m$

$$\left.\begin{array}{l} \mathrm{ord}(h) \mid \mathrm{mcm}(\mathrm{ord}(g), \mathrm{ord}(h)) \mid m \\ \text{Lagrange} \Rightarrow \mathrm{ord}(h) \mid n \end{array}\right\} \Rightarrow \mathrm{ord}(h) \mid (m,n) = 1$$

$$\Rightarrow h = 1 \Rightarrow (g,h) \in K \times \{1\}.$$

Cor $(m,n) = 1 \Rightarrow \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

$\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$

$\mathbb{Z} \times \{0\}$

$\{0\} \times \mathbb{Z}/n\mathbb{Z}$ : è caratt., perché è il sottoins degli el. di ord $< \infty$

$$\varphi : \begin{array}{l} (1,0) \longrightarrow (a,b) \\ (0,1) \longrightarrow (0,d) \end{array} \qquad (d,n) = 1$$

$\varphi$ surgettivo $\Longleftrightarrow$ $a = \pm 1$

$$\varphi((x,y)) = \varphi(x\cdot(1,0) + y\cdot(0,1))$$
$$= x\,\varphi(1,0) + y\,\varphi(0,1)$$
$$= (ax, bx) + (0, dy) = \underset{(1,\ 0)}{(ax,\ \underset{\shortparallel}{bx+dy})}$$

La risolubilità di $ax = 1 \Rightarrow a = \pm 1$

$$(ax, bx + dy) = (x_0, y_0)$$

$x = x_0/a$
$= a x_0$

$b \cdot a x_0 + dy \equiv y_0 \pmod n$

$y \equiv d^{-1}(y_0 - b a x_0) \pmod n$

$$\varphi((2,0)) = (2a, 2b)$$

$$\varphi((x,y)) = (ax, bx+dy) = (ax', bx'+dy')$$

$$(\pm 1, b)$$

$$(0, d)$$

Conclusione: $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \longleftrightarrow \left\{ \begin{pmatrix} \pm 1 & 0 \\ b & d \end{pmatrix} \;\middle|\; d \in (\mathbb{Z}/n\mathbb{Z})^\times \right\}$

Un autom. è $\varphi_0 : (x,y) \longmapsto (x, x+y)$

$$\varphi_0(\mathbb{Z} \times \{0\}) = \{(x,x) \mid x \in \mathbb{Z}\}$$

$$\# \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = 2 \cdot n \cdot \varphi(n)$$

## Presentazione di un gruppo

$$D_n = \langle r, s \mid r^n = s^2 = 1, \quad srs^{-1} = r^{-1} \rangle$$

$$\mathrm{Hom}(D_n, G) = \left\{ (x,y) \in G^2 \;\middle|\; \begin{array}{l} x^n = 1 \\ y^2 = 1 \\ yxy^{-1} = 1 \end{array} \right\}$$

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

$$(\mathbb{Z}/2\mathbb{Z})^2 = \langle x, y \mid x^2 = y^2 = 1, \quad xy = yx \rangle$$

⚠ ⚠ $\langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle = \{e\}$ ? Indecidibile

# Unione coniugati

$G$ grp. finito, $H < G$. $H \neq G$

$$G \neq \bigcup_{g \in G} gHg^{-1}$$

$$hHh^{-1} = H$$

$$\# \{ gHg^{-1} \mid g \in G \} = [G : N_G(H)] = |G| / |N_G(H)|$$

$$\left| \bigcup gHg^{-1} \right| \leq \frac{|G|}{\underbrace{|N_G(H)|}_{\text{n° insiemi distinti}}} \cdot \underbrace{|H|}_{\text{card. di ogni insieme}} \leq \frac{|G|}{|H} \cdot |H| = |G|$$

non può essere $=$ perché $e = 1_G$ appartiene ad ogni $gHg^{-1}$ (a meno che $H = G$)

## $G \circlearrowleft X$ transitivamente

**Def.** Si dice che $G \circlearrowleft X$ transitivamente se

$$\forall x \in X \quad \forall y \in X \qquad \exists g \in G \quad \text{t.c.} \quad g \cdot x = y$$

**Es.** $G \circlearrowleft G$ $\qquad g \cdot h = gh \qquad$ è transitiva

$$g x = y$$

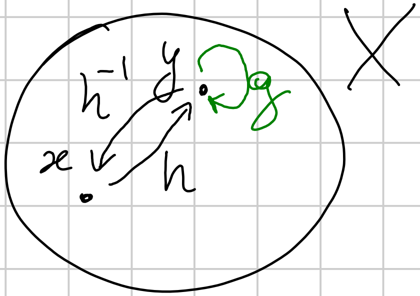
$G \circlearrowleft G \qquad g \cdot h = ghg^{-1} \qquad$ NON è transitiva (se $G \neq \{e\}$)

Equivalente: l'orbita di ogni $x \in X$ è tutto $X$.

- $\mathrm{Stab}_G(x)$ e $\mathrm{Stab}_G(y)$ sono coniugati in $G$ $\quad \forall x \ \forall y \in X$
- Se $|X| \geq 2$ $\quad \exists g \in G$ che agisce senza pti fissi, cioè

$$g \cdot x \neq x \qquad \forall x \in X$$

$h \, \mathrm{Stab}_G(x) \, h^{-1} = \mathrm{Stab}_G(y)$ $\qquad \exists h \in G \quad y = h \cdot x$



$\boxed{\subseteq}$ Se ho $g \in h \cdot \mathrm{Stab}_G(x) \cdot h^{-1}$ e lo applico ad $y = h \cdot x$ trovo (scrivendo $g = h w h^{-1}$, $w \in \mathrm{Stab}_G(x)$)

$$g \cdot y = (h w h^{-1}) \cdot (h \cdot x) = h \cdot (w \cdot x) = h \cdot x = y$$

$\boxed{\supseteq}$ Simile.

2) Vorrei $g \in \bigcap_{x \in X} \left( {}^c \mathrm{Stab}_G(x) \right) \iff g \notin \bigcup_{x \in X} \mathrm{Stab}_G(x)$

$$\Leftrightarrow \quad g \notin \underbrace{\bigcup_{h \in G} h \, \mathrm{Stab}_G(x_0) \, h^{-1}}_{\neq G}$$ , che e' vero

purché $\mathrm{Stab}_G(x_0) \neq G$: siccome l'azione e' transitiva, questo puo' succedere solo se $|X| = 1$.

$$|X| = |\mathrm{Orb}(x_0)| = |G| / |\mathrm{Stab}_G(x_0)| = |G|/|G| = 1$$

# SOTTOGRUPPO DERIVATO, AZIONI

## Sottogr. derivato

**Def.** Dato un gruppo $G$ e 2 elementi $x, y \in G$, si dice COMMUTATORE FRA $x$ E $y$ l'elemento

$$[x,y] := x y x^{-1} y^{-1}$$

**Oss** $[x,y] = e \iff x, y$ commutano

**Def.** Il SOTTOGRUPPO DERIVATO di $G$ è

$$G' := \langle [x, y] \mid x, y \in G \rangle$$

① $G'$ è caratteristico in $G$: se $\varphi \in Aut(G)$, allora

$$\varphi(G') = \langle \varphi([x,y]) \mid x,y \in G \rangle$$

$$= \langle \varphi(xyx^{-1}y^{-1}) \mid x,y \in G \rangle$$

$$= \langle [\varphi(x), \varphi(y)] \mid x,y \in G \rangle$$

$$= \langle [u,v] \mid u,v \in G \rangle = G'$$

② $G/G'$ e' abeliano:

$$xG' \cdot yG' \overset{?}{=} yG' \cdot xG'$$

$$\iff xy \cdot G' \overset{?}{=} yx \cdot G' \iff xy \cdot (yx)^{-1} \overset{?}{\in} G'$$

$$\iff xyx^{-1}y^{-1} \overset{?}{\in} G' \quad \checkmark$$

③ Sia $(A,+)$ un grp. abeliano e $\varphi : G \longrightarrow A$ un omom.

Allora $G' \subseteq \ker \varphi$: infatti ogni $[x,y]$ soddisfa

$$\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) =$$

$$= \varphi(x) + \varphi(y) + \underbrace{\varphi(x^{-1})}_{-\varphi(x)} + \underbrace{\varphi(y^{-1})}_{-\varphi(y)} = 0$$

$$\Rightarrow [x,y] \in \ker \varphi \Rightarrow \underset{\underset{G'}{\parallel}}{\langle [x,y] \rangle} \subseteq \ker \varphi$$

**Oss** $G/G'$ e

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

$G/G'$ è "il più grande quoziente abeliano di $G$"

④ $\mathrm{Hom}(G, A) \xleftrightarrow{1:1} \mathrm{Hom}(G/G', A)$

$$\overline{\varphi} \circ \pi \longleftarrow\!\shortmid \ \overline{\varphi}$$

$$\varphi \longmapsto \overline{\varphi}$$ prodotto dal 1° teo omom.

Es $(S_3)' = \langle (1,2,3) \rangle$

$$S_3/\langle (1,2,3) \rangle \simeq \mathbb{Z}/2\mathbb{Z}$$

$$\begin{tikzcd} S_3 \arrow[rr, "\varphi"] \arrow[dr] & & \mathbb{Z}/2\mathbb{Z} \\ & S_3/\langle (1,2,3) \rangle \arrow[ur] & \end{tikzcd}$$

$$\begin{array}{l} (S_3)' \subseteq \ker \varphi = \langle (1,2,3) \rangle \\ \ \ \cup\!\!\!\!/ \\ \{id\} \end{array}$$

$$\Longrightarrow \quad S_3' = \langle (1,2,3) \rangle$$

$S_n' = A_n$ $\qquad$ $S_n / A_n \simeq \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow (S_n)' \subseteq A_n$

$H < G$ , $[G:H] = p$

Sia $G$ un grp finito, $p =$ il più piccolo primo che divide $|G|$. $[G:H] = p$. Allora $H \trianglelefteq G$.

Dim. $[ G \circlearrowleft \{$ coniugati di $H \} ]$

* $G \circlearrowleft G/H$ : $g \cdot (g'H) = gg'H$

* Cioè: ho un omomorf. $\varphi : G \longrightarrow S_{G/H} \simeq S_p$

$$\begin{cases} \# \operatorname{Imm} \varphi \mid \# S_p = p! \\ \# \operatorname{Imm} \varphi = \dfrac{\# G}{\# \ker \varphi} \mid \# G \end{cases}$$
+ ipotesi p "più piccolo primo"

$$\Rightarrow \quad \# \operatorname{Imm} \varphi \mid (p!, \# G) = p$$

$$\Rightarrow \quad \# \ker \varphi = \frac{\# G}{p}, \quad \text{cioè} \quad [G : \ker \varphi] = p$$

T **Oss giusta:** $\# \operatorname{Imm} \varphi \neq 1$ perché l'azione è transitiva

$$(g_2 g_1^{-1}) \cdot g_1 H = g_2 H$$

Imm banale : $g \cdot g_1 H = g_1 H \quad \forall g, g_1$

impossibile se $g_1 = e$ e $g \notin H$

L

$$\ker \psi = \{ g \in G \mid g \cdot g_1 H = g_1 H \quad \forall g_1 \in H \}$$

$$\subseteq \{ g \in G \mid g \cdot H = H \} = H$$

$$\underbrace{\ker \psi \subseteq \overbrace{H \subseteq G}^{p}}_{p} \implies H = \ker \psi \lhd G$$

$\square$

**Oss** $h \cdot g \cdot H = gH \iff g^{-1} h g H = H$

$\iff g^{-1} h g \in H \quad \forall h \in H \quad \forall g \in G$

## Cauchy + piccolo di Fermat

$G$ grp. finito, $\quad X = \{ (g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = e \}$

$p$ n° primo

$\# X = |G|^{p-1}$

$\mathbb{Z}/p\mathbb{Z} \circlearrowright X$ come segue:

$$1 \cdot (g_1, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1)$$

$$\underbrace{(g_2 g_3 \cdots g_p)}\cdot \underbrace{g_1} \overset{?}{=} e$$

$$\Updownarrow$$

$$g_1 \cdot (g_2 \cdots g_p) = e$$

Orbite per l'azione: $\# \mathrm{Orb}(x) = \dfrac{\# \mathbb{Z}/p\mathbb{Z}}{\# \mathrm{Stab}(x)} = \dfrac{p}{\# \mathrm{Stab}(x)}$

$\in \{1, p\}$

Le orbite di lungh. 1 sono $(g, g, \dots, g)$ con $g^p = e$

$$|X| = \sum_{x \in R} |\mathrm{Orb}(x)| = 1 + \#\text{ elementi di ord } p$$

$\uparrow$ rappr. delle orbite

$+ \; p \cdot \#$ orbite non banali

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

$$n^{p-1} = 1 + 0 + p \cdot \#\text{ orb. non banali}$$

$\Rightarrow \quad n^{p-1} \equiv 1 \pmod{p}$ (piccolo teo Fermat)

- Se $G$ è t.c. $p \mid \# G$

$$(\# G)^{p-1} = 1 + \#\text{el. ord } p + p \cdot \#\text{orb. non ban.}$$

$\Rightarrow \# \text{el. ord } p \equiv -1 \pmod{p}$

$\Rightarrow \# \text{el. ord } p \neq 0$, cioè Cauchy

## Teo di Poincaré

Sia $G$ finito, $H < G$ di indice $n$. $\exists\, N \triangleleft G$ t.c.

- $N < H < G$
- $n \mid [G:N] \mid n!$

Dim. $G \circlearrowright G/H \rightsquigarrow \psi : G \longrightarrow S_{G/H} \simeq S_n$

molt. a sx
sulle classi laterali

Prendiamo $N = \ker \psi \triangleleft G$.

- $\ker \psi = \{ g \in G \mid g \cdot g' H = g' H \quad \forall g' \in G \}$

$$\subseteq \{ g \in G \mid gH = H \} = H$$

- Per il 1° teo di omomorf., $G/N = G/_{\ker \psi} \simeq \operatorname{Imm} \psi < S_n$

$$\Rightarrow \underset{[G:N]}{\overset{\shortparallel}{\# G/N}} \mid \# S_n = n!$$

$$[G:N] = [G:H] \cdot [H:N] = n \cdot [H:N] \quad \square$$

$|G| = 15$

Sia $g_5 \in G$ di ord. 5 (Cauchy)

Sia $H = \langle g_5 \rangle$. Allora $[G:H] = 15/5 = 3$ è il più piccolo primo che divide $\# G$, quindi $H \trianglelefteq G$.

Mostriamo che $H \subseteq Z(G)$.

$\iff$ $\forall g \in G$ il coniugio per $g$ è l'identità su $H$

$$\alpha : \left[ \begin{array}{l} G \longrightarrow \mathrm{Aut}(H) \\ g \longmapsto \varphi_g|_H \end{array} \right.$$

$$\varphi_g(h) = h \quad \begin{array}{l} \forall h \in H \\ \forall g \in G \end{array}$$

$$\overset{\shortparallel}{ghg^{-1}}$$

$\iff$ $gh = hg$

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(G) \quad \text{è un omomorf. gp.} \\ g &\longmapsto \varphi_g \end{aligned}$$

$\Rightarrow$ $\alpha$ è un omomorfismo di gruppi

$$\mathrm{Aut}(H) = \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) = (\mathbb{Z}/5\mathbb{Z})^{*} \simeq \mathbb{Z}/4\mathbb{Z}$$

$\alpha$ va da $G$ di ord 15 a $\mathrm{Aut}(H)$ di card. 4

$$\left.\begin{aligned} \#\,\mathrm{Imm}\,\alpha \;\Big|\; &\#\,\mathrm{Aut}(H) = 4 \\ \Big|\; &\#\,G = 15 \end{aligned}\right\} \quad \#\,\mathrm{Imm}\,\alpha \mid (4, 15) = 1$$

$\Rightarrow$ $\alpha$ è l'omomorfismo banale!

$\Rightarrow$ $H \subseteq Z(G)$.

Per finire:

(1) Lemma: se $G/Z(G)$ è ciclico, allora $G$ è abeliano.

Nel nostro caso: $5 \mid \# Z(G)$

$$\Rightarrow \quad \# G/Z(G) \in \{1, 3\}$$

$$\Rightarrow \quad G/Z(G) \text{ ciclico} \Rightarrow \text{fine.}$$

(2) Sia $h \in G$ un elemento di ord. 3

$$Z_G(h) = \{ x \in G \mid xh = hx \} < G$$

- $h \in Z_G(h)$
- $Z(G) \subseteq Z_G(h)$

$$\left.\begin{array}{l} 3 \mid \# Z_G(h) \\ 5 \mid \# Z_G(h) \end{array}\right\} \# Z_G(h) = 15$$

$$\Updownarrow$$

$$h \in Z(G)$$

$$\Downarrow$$

fine...

**Oss** Se so che $[\overset{\text{ord } 5}{g_5}, \overset{\text{ord } 3}{h}] = id$ $(g_5, h$ commutano$)$

$\operatorname{ord}(g_5 \cdot h) = \operatorname{ord}(g_5) \cdot \operatorname{ord}(h)$ [siccome sono coprimi]

$\Rightarrow G \simeq \mathbb{Z}/_{15}\mathbb{Z}$

$|G| = 2d$ con $d$ dispari

Dim. che $G$ ammette un sgp. normale di indice 2

Sia $\varphi : G \hookrightarrow S_{|G|}$ l'immersione di Cayley.

$$\begin{array}{c} S_{|G|} \\ \cup\!|\;\; 2 \\ A_{|G|} \end{array}$$

- $\varphi^{-1}(A_{|G|})$ ha indice $\leq 2$ in $G$:

$$\begin{array}{c} \varphi^{-1}(A_{|G|}) \\ \parallel \end{array}$$

$$\{ g \in G \mid \varphi(g) \in A_{|G|} \} = \ker(\pi \circ \varphi)$$

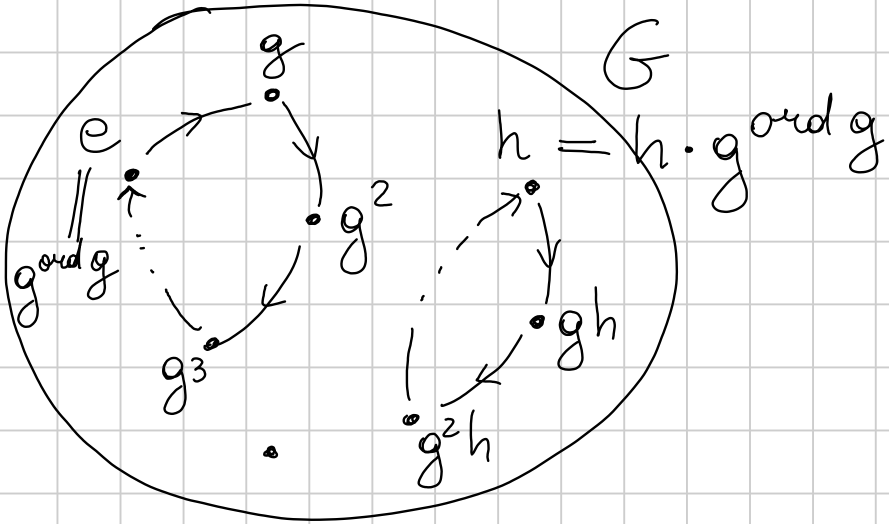
$$G \xrightarrow{\varphi} S_{|G|} \xrightarrow{\pi} S_{|G|} / A_{|G|} \simeq \mathbb{Z}/_{2}\mathbb{Z}$$

$$\frac{G}{\ker(\pi \circ \varphi)} \hookrightarrow \mathbb{Z}/_{2\mathbb{Z}} \iff [G : \ker(\pi \circ \varphi)] \leq 2$$

- $\varphi^{-1}(A_{|G|}) = G \iff \varphi(G) \subseteq A_{|G|}$
- Vorremmo quindi vedere che $\varphi(G) \not\subseteq A_{|G|}$

Cioe' vorrei $g \in G$ t.c. $\varphi(g)$ e' $\Pi$ di un numero dispari di trasp.

Oss Se $\varphi : G \longrightarrow S_{|G|}$ e' l'omom. di Cayley, qual e' la decomp. in cicli di $\varphi(g)$? Sono $\frac{\# G}{\text{ord } g}$ cicli di lungh. ord $g$.



$$\varphi(g) = (\mathrm{ord}\ g)(\mathrm{ord}\ g) \cdots (\mathrm{ord}\ g)$$

$$h \to gh \to g^2 h \to \dots \to g^m h = h$$

$\llcorner$

Sia $g \in G$ di ord 2 (c'e' per Cauchy)

$\Rightarrow$ $\varphi(g)$ e' prodotto di $\frac{\# G}{2} = d$ cicli di lungh. 2

$\Rightarrow$ $\varphi(g)$ e' dispari $\Rightarrow$ $\varphi(G) \not\subseteq A_{|G|}$

$\Rightarrow$ $\varphi^{-1}(A_{|G|})$ e' un sottogp. di G di indice 2. $\square$

Es $S_3$ $H = \langle (1,2,3) \rangle$ $\left[ \begin{array}{l} K = \langle (1,2) \rangle . \\ K' = \langle (2,3) \rangle . \end{array} \right.$

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

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

- Sia $G$ un grp, $H < G$ di indice 2, $K < G$.

Allora $H \cap K < K$ ha indice 1 o 2

$$\beta : K \longrightarrow G \longrightarrow G/H \simeq \mathbb{Z}/2\mathbb{Z} .$$

$H \cap K = \ker \beta$ ha indice 1 o 2 in $K$

$$\frac{K}{\ker \beta} \hookrightarrow \mathbb{Z}/2\mathbb{Z} \qquad \frac{\# K}{\#(K \cap H)} = 1 \text{ o } 2$$

- Se invece $H < G$ ha indice 3, $H \cap K < K$ può avere indice 1, 2, 3

## Studio di $S_5$

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

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

* $\sigma = (1,2,3,4,5)$ e $\tau = (2,5)(3,4)$

$H = \langle \sigma, \tau \rangle$

$$\sigma \underbrace{\tau \sigma^{-1} \tau^{-1}}_{} = ?$$

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

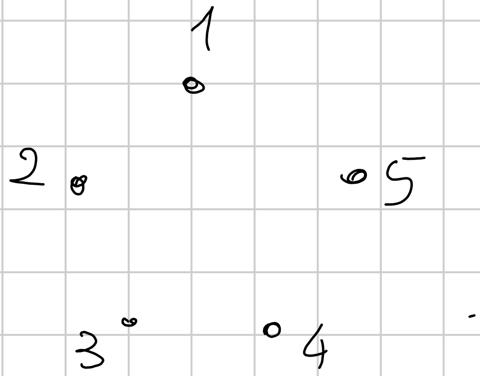
$$(\tau\sigma\tau^{-1})(\tau(i)) = \tau\sigma(i) = \tau(i+1)$$

Formula comoda Se $\sigma = (i_1, \dots, i_k)$,

$$\tau\sigma\tau^{-1} = (\tau(i_1), \dots, \tau(i_k))$$

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

$\sigma^5 = id$ $\quad$ $\tau^2 = id$ $\quad$ $\tau\sigma\tau^{-1} = \sigma^{-1}$



$$\Rightarrow \langle\sigma, \tau\rangle \underset{\uparrow}{\cong} D_5$$

$$|\langle\sigma, \tau\rangle| \equiv 0 \ (10)$$

**Oss** $H < G$ $\qquad N_G(H) = \{ g \in G \mid gHg^{-1} = H \}$

$h \in G$ $\qquad N_G(h) = N_G(\langle h \rangle)$

$= \{ g \in G \mid ghg^{-1} = h^m$ per un qualche $m \in \mathbb{Z} \}$

$\langle \sigma, \tau \rangle = \langle \sigma \rangle \langle \tau \rangle$ se $\tau \in N_G(\sigma)$

# PERMUTAZIONI

Titolo nota

## Sgp ab. di $S_n$

$G < S_n$ ab, $G$ transitivo $\quad G \circlearrowright \{1, \ldots, n\}$ transitiva

( Cioè: $\forall i, j \in \{1, \ldots, n\} \quad \exists g \in G$ t.c. $g(i) = j$ )

Tesi: $|G| = n$.

$$G_i = \mathrm{Stab}_G(i) = \{\sigma \in G \mid \sigma(i) = i\}$$

Oss. 1• $\bigcap_{i=1}^{n} G_i = \{id\}$

2• I $G_i$ sono tutti coniugati (az. transitiva)

3. Siccome $G$ è abeliano, il coniugio è banale $\Rightarrow$ tutti i $G_i$ coincidono $\left( G_i = g\, G_1\, g^{-1} = G_1 \right)$

4. 1 e 3 $\Rightarrow$ $G_i = \{id\}$ $\forall i$

5. $|G| \geq n$ ( esistono $g_1$ t.c. $g_1(1) = 1$
$g_2$ t.c. $g_2(1) = 2$
$\vdots$
$g_n$ t.c. $g_n(1) = n$ )

6. Per il lemma orbita-stab,

$$n = \# Orb(1) = \#G / \# Stab(1) = \# G$$

6' . Se $\sigma(1) = \sigma'(1) \iff \sigma(\sigma')^{-1}(1) = 1$

$\iff \sigma \cdot (\sigma')^{-1} \in \mathrm{Stab}(1) = \{id\}$

$\iff \sigma = \sigma'$

$\Rightarrow$ $\sigma$ e' det. da $\sigma(1)$ $\Rightarrow$ $|G| \leq n$.

Ora cerchiamo di capire quanto sono grandi i sgp di $S_n$ abeliani di cardinalita' massima.

Caso $\boxed{n = 3m}$. Risposta: la card. massima e' $3^m$.

① Un esempio di $G < S_n$ abeliano di ordine $3^m$

$G = \langle (1,2,3) \rangle \times \langle (4,5,6) \rangle \times \dots \times \langle (n-2, n-1, n) \rangle$

② $G < S_n$ abeliano, $\Omega_1, \dots, \Omega_K$ le sue orbite

$\varphi_i : G \longrightarrow S_{\Omega_i}$ omomorfismi di restrizione

$G_i = \text{imm } \varphi_i$ Es $g = (1,2,3)\,(4,5,6)^2$

$$\underbrace{\phantom{(1,2,3)\,(4,5,6)^2}}$$

$S_{\Omega_1} \times S_{\Omega_2} \times \dots \times S_{\Omega_K}$ $\varphi_1(g) = (1,2,3)$ $\varphi_2(g) = (4,5,6)^2$

$\varphi : G \longrightarrow G_1 \times G_2 \times \dots \times G_K$ omomorfismo INIETTIVO

$g \longmapsto (\varphi_1(g), \dots, \varphi_k(g))$

$\varphi(g) = id \iff \varphi_1(g) = id, \dots, \varphi_k(g) = id$

$\iff g|_{\Omega_1} = id_{\Omega_1}, \dots, g|_{\Omega_k} = id_{\Omega_k}$

$$\Longleftrightarrow \quad g = \mathrm{id}_{\{1,\dots,n\}}$$

Abbiamo verificato che $\ker \varphi$ è banale $\Rightarrow$ $\varphi$ iniettiva.

③ Ogni $G_i$ è abeliano (perché imm $G$ tramite un omomorf.)

e transitivo su $\Omega_i$ (per costruzione)

$$\Rightarrow \quad |G_i| = |\Omega_i|$$

④ $\varphi$ iniettivo $\Rightarrow$

$$|G| \leq |G_1| \times |G_2| \times \dots \times |G_k|$$
$$= \underbrace{|\Omega_1|}_{a_1} \times \dots \times \underbrace{|\Omega_k|}_{a_k}$$

$\sum_{i=1}^{k} a_i = n$ che massimizzano $\prod a_i$

( Nessun $a_i$ è $\geq 5$ $\rightsquigarrow$ lo sostituisco con

$3, \; a_i - 3$

Nessun $a_i$ è $= 4$ senza perdita di generalità

$(4 \longrightarrow 2+2)$

Nessun $a_i$ è $1$ )

Se $n = 3m$, il max è realizzato da $a_1 = \dots = a_m = 3$.

$$|G| \underset{(a)}{\leq} \prod |\Omega_i| \underset{(b)}{\leq} 3^m \Rightarrow \text{il max è } 3^m.$$

⑤ Quindi: se $G$ è ab. di card. $3^m$, (a) e (b) devono essere uguaglianze! Cioè: ci sono $m$ orbite, ognuna di cardinalità 3, e $\varphi: G \longrightarrow G_1 \times \dots \times G_k$ è un isomorfismo. Allora ogni $G_i$ e' un grp. ab. di cardinalita' $= |\Omega_i| = 3 \Rightarrow G \simeq G_1 \times \dots \times G_k$

$$\simeq (\mathbb{Z}/3\mathbb{Z})^k$$

Piu' in dettaglio: se le orbite sono $\{i_1, i_2, i_3\}, \dots, \{i_{n-2}, i_{n-1}, i_n\}$, allora

$$G = \langle (i_1, i_2, i_3) \rangle \times \dots \times \langle (i_{n-2}, i_{n-1}, i_n) \rangle$$

$$\updownarrow \wr$$

$$G_0 := \langle (1, 2, 3) \rangle \times \dots \times \langle (n-2, n-1, n) \rangle$$

Se prendo $\sigma$ la permutaz. che manda $j \mapsto i_j$, allora

$$\sigma G_0 \sigma^{-1} = G$$

$$\sigma G_0 \sigma^{-1} = \langle \sigma (1,2,3) \sigma^{-1} \rangle \times \dots \times \langle \sigma (n-2, n-1, n) \sigma^{-1} \rangle$$

$$= \langle (\sigma(1), \sigma(2), \sigma(3)) \rangle \times \dots \times \langle (\sigma(n-2), \sigma(n-1), \sigma(n)) \rangle$$

$$= G.$$

□

**ES** $\{ (1,2)(3,4) ; \ (1,3)(2,4) ; \ (1,4)(2,3) ; \ id \} = V_4$

( "Klein 4 - group" ) e' un sgp. ab. transitivo di $S_4$

## Proprieta' varie di $S_n$

- Quanti sono i $K$-cicli in $S_n$? $\binom{n}{K} \cdot (K-1)!$
- Dato $\sigma \in S_n$ un $K$-ciclo, qual e' la dec. in cicli di $\sigma^2$?

Risposta: se $K$ e' dispari, $\sigma^2$ e' un $K$-ciclo

se $K$ e' pari, $\sigma^2$ si decompone come 2 $\frac{K}{2}$-cicli.

Se $K$ è dispari, $\langle \sigma \rangle \simeq \mathbb{Z}/_{k\mathbb{Z}}$

$$\underset{\langle \sigma \rangle}{\langle \sigma^2 \rangle} \!\!\overset{}{\,} \simeq \mathbb{Z}/_{k\mathbb{Z}}$$

$\langle \sigma^2 \rangle = \langle \sigma \rangle$, quindi le orbite di $\sigma^2$ e $\sigma$ coincidono

$\Rightarrow$ c'è una sola orb, di lungh. $k$ $\Rightarrow$ $\sigma^2$ è un $k$-ciclo

Oss Lo stesso ragionamento dice: se $\sigma$ è un $K$-ciclo e $(n, K) = 1$, $\sigma^n$ è un $K$-ciclo.

Se invece $\sigma = (i_1 \quad i_2 \quad \dots \quad i_{2h})$, $h = k/2$

allora $\sigma^2 = (i_1, i_3, i_5, i_7, \dots, i_{2h-1})(i_2, i_4, i_6, \dots, i_{2h})$

- Centralizzatori di cicli

$$Z_{S_{10}}\left( (1,2,3) \right) \supseteq \langle (1,2,3) \rangle \times S_{\{4,5,\dots,10\}}$$

$Z_{S_n}(\sigma) = \mathrm{Stab}_{S_n}(\sigma)$ per l'azione di coniugio di $S_n$ su se stesso.

D'altra parte $\mathrm{Orb}(\sigma) = \left\{ \tau \in S_n \;\middle|\; \begin{array}{l}\text{la decomp. in cicli di} \\ \sigma \text{ e } \tau \text{ ha la stessa} \\ \text{struttura}\end{array} \right\}$

$$\sigma = (i_{1,1}, \dots, i_{1,\ell(1)}) \cdots (i_{k,1}, \dots, i_{k,\ell(k)})$$

$$\alpha \sigma \alpha^{-1} = \alpha \left( \qquad - \; - \; - \qquad \right) \alpha^{-1}$$

$$= \left(\alpha\,(i_{1,1}, \dots, i_{1,\ell(1)})\,\alpha^{-1}\right) \cdots \left(\alpha\,(i_{k,1}, \dots, i_{k,\ell(k)})\,\alpha^{-1}\right)$$

$$= \left(\alpha(i_{1,1}), \dots, \alpha(i_{1,\ell(1)})\right) \cdots \left(\alpha(i_{k,1}), \dots, \alpha(i_{k,\ell(k)})\right)$$

$$\# Z_{S_{10}}\left((1,2,3)\right) = \frac{\# S_{10}}{\#\,\text{orbita}\ (1,2,3)} = \frac{10!}{\binom{10}{3}\cdot 2} = \frac{3!\ 7!}{2}$$

$$= 3 \cdot 7!$$

$$* \ Z_{S_{10}}\left((1,2,3)\right) \supseteq \langle (1,2,3) \rangle \times S_{\{4,\dots,10\}}$$

* Uguaglianza di cardinalità

$$\Rightarrow$$

$$\Rightarrow Z_{S_{10}}\left((1,2,3)\right) = \langle (1,2,3) \rangle \times S_{\{4,\dots,10\}}$$

- $$Z_{S_9}\Big(\underbrace{(1,2,3,4)\ (5,6,7)\ (8,9)}_{\sigma}\Big) \supseteq \langle(1,2,3,4)\rangle \times \langle(5,6,7)\rangle \times \langle(8,9)\rangle$$

$$\# Z_{S_9} = \frac{\# S_9}{\# Orb(\sigma)} = \frac{9!}{\underbrace{\binom{9}{4}\cdot 3!\ \binom{5}{3}\cdot 2!\ \binom{2}{2}\cdot 1!}} = 4\cdot 3\cdot 2$$

$$3!\,2!\,1!\binom{9}{4,\,3,\,2} = \frac{9!}{\underset{4}{\cancel{4!}}\cdot\underset{3}{\cancel{3!}}\cdot\underset{2}{\cancel{2!}}}\cdot\cancel{3!}\cdot\cancel{2!}\cdot\cancel{1!}$$

$\rightsquigarrow$ come prima, $Z_{S_9}(\sigma) = \langle(1,2,3,4)\rangle \times \langle(5,6,7)\rangle \times \langle(8,9)\rangle$

$$\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

• $S_5$ in dettaglio $\qquad |S_5| = 120$

| | | | |
|---|---|---|---|
| $A_5$ | $5$ | $4! = 24$ | |
| | $4+1$ | $\binom{5}{4} \cdot 3! = 30$ | |
| | $3+2$ | $20$ | $\binom{5}{3} \cdot 2!$ |
| $A_5$ | $3+1+1$ | $20$ | |
| $A_5$ | $2+2+1$ | $\frac{1}{2}\binom{5}{2} \cdot \binom{3}{2} = 15$ | |
| | $2+1+1+1$ | $10$ | |
| $A_5$ | $1+1+1+1+1$ | $1$ | |

$$Z((1,2,3,4,5)) = \langle (1,2,3,4,5) \rangle$$

$$Z_{S_5}((1,2,3)) \ni (4,5)$$

$$Cl_{A_5}((1,2,3)) = Cl_{S_5}((1,2,3))$$

$$Z_{S_5}((1,2)(3,4)) \ni (1,2)$$

$$Cl_{A_5}((1,2)(3,4)) = Cl_{S_5}((1,2)(3,4))$$

$$Cl_{S_5}((1,2,3,4,5)) = Cl_{A_5}((1,2,3,4,5)) \sqcup Cl_{A_5}((2,1,3,4,5))$$

Classi di coniugio in $A_5$?

$$\# Cl_{A_n}(\sigma) = \frac{\# A_n}{\# Z_{A_n}(\sigma)} = \frac{\# A_n}{\#\left( Z_{S_n}(\sigma) \cap A_n \right)}$$

$$= \frac{1/2 \quad \# S_n}{\#\left( Z_{S_n}(\sigma) \cap A_n \right)} \text{, dove}$$

$$\#\left( Z_{S_n}(\sigma) \cap A_n \right) = \begin{cases} \# Z_{S_n}(\sigma) & \text{①} \\ \\ \frac{1}{2} \# Z_{S_n}(\sigma) & \text{②} \end{cases}$$

Nel caso ②, $\# Cl_{A_n}(\sigma) = \dfrac{\frac{1}{2} \# S_n}{\frac{1}{2} \# Z_{S_n}(\sigma)} = \# Cl_{S_n}(\sigma)$

$$Cl_{A_n}(\sigma) \subseteq Cl_{S_n}(\sigma) \quad \Rightarrow \quad Cl_{A_n}(\sigma) = Cl_{S_n}(\sigma)$$

Questo caso si verifica se $Z_{S_n}(\sigma)$ contiene almeno una permutazione dispari.

Nel caso Ⓘ, $\quad \# Cl_{A_n}(\sigma) = \dfrac{1/2 \; \# S_n}{\# Z_{S_n}(\sigma)} = \dfrac{1}{2} \# Cl_{S_n}(\sigma)$

Più precisamente: $\quad Cl_{S_n}(\sigma) \underset{\supseteq}{=} Cl_{A_n}(\sigma) \amalg Cl_{A_n}(\tau\sigma\tau^{-1})$

con $\tau$ fissata permutaz. dispari.

$\alpha\sigma\alpha^{-1} \in Cl_{A_n}(\sigma)$ se $\alpha$ è pari

$\alpha\sigma\alpha^{-1} = (\alpha\tau^{-1})(\tau\sigma\tau^{-1})(\tau\alpha^{-1})$ se $\alpha$ dispari

$$\in \mathcal{C}l_{A_n}(\tau\sigma\tau^{-1})$$

D'altro canto, $\# \mathcal{C}l_{A_n}(\tau\sigma\tau^{-1}) = \begin{cases} \cancel{\# \mathcal{C}l_{S_n}(\tau\sigma\tau^{-1})} \\ \frac{1}{2} \# \mathcal{C}l_{S_n}(\tau\sigma\tau^{-1}) \end{cases}$

Se $\mathcal{C}l_{A_n}(\tau\sigma\tau^{-1}) = \mathcal{C}l_{S_n}(\tau\sigma\tau^{-1}) = \begin{array}{c} \mathcal{C}l_{S_n}(\sigma) \\ \cup\!| \\ \mathcal{C}l_{A_n}(\sigma) \end{array}$

ma questo è assurdo (altrimenti otterrei che $\sigma$ e $\tau\sigma\tau^{-1}$ sono coniugate in $A_n$, assurdo!

# Generatori di $S_n$ e $A_n$

$$S_n = \langle (i,j) \mid i,j \in \{1,\dots,n\}, \quad i<j \rangle$$

$$= \langle (1,j) \mid j \in \{2, \dots, n\} \rangle$$

$$(i,j) = (1,i) \underset{(i,\ j)}{\underset{|\quad |}{(1,j)}} \underbrace{(1,i)}^{-1}$$

$$= \langle (1,2), (2,3), (3,4), \dots, (n-1,n) \rangle$$

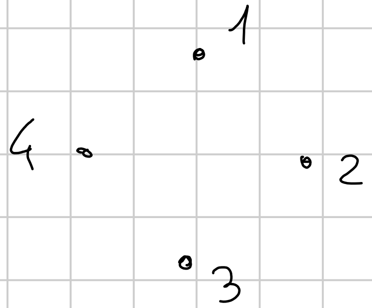
$$(1,3) = (2,3)(1,2)(2,3)$$

$$(1,4) = (3,4)(1,3)(3,4)$$

$$\vdots$$

$$= \langle \underbrace{(1,2)}_{\tau}, \underbrace{(1,2,\dots,n)}_{\sigma} \rangle \ni \begin{array}{c} \sigma^i \tau \sigma^{-i} \\ \parallel \\ (\sigma^i(1), \sigma^i(2)) \\ \parallel \\ (i+1, i+2) \end{array}$$

Es $\langle \underbrace{(1,2,3,4)}_{r}, \underbrace{(2,4)}_{s} \rangle \neq S_4$



$r^4 = s^2 = 1$, $\boxed{srs^{-1} = r^{-1}}$

Il generato è $\simeq D_4$

$$\begin{array}{c} \langle (1,2,3,4) \rangle \langle (2,4) \rangle \\ \rotatebox{90}{$\subseteq$} \\ \langle (1,2,3,4), (2,4) \rangle \end{array} \leftarrow \begin{array}{l} \leq 8 \text{ elementi} \\ (=8) \end{array}$$

# ANCORA GRUPPO SIMMETRICO E ALTERNANTE

Titolo nota

## Centralizzatori + normalizzatori in $S_n$

$\sigma = (1, 2, \dots, 7)$ in $S_7$

$$\# Z_{S_7}(\sigma) = \frac{\# S_7}{\# Orb(\sigma)} = \frac{7!}{6!} = 7 \Rightarrow Z_{S_7}(\sigma) = \langle \sigma \rangle$$

$$N_{S_7}(\sigma) = \{ g \in S_7 \mid \exists i \text{ t.c. } g \sigma g^{-1} = \sigma^i \}$$

Oss Sia $H < G$ sgp. C'è un hom. $N_G(H) \longrightarrow Aut(H)$

$$g \longmapsto \varphi_g|_H$$

$\llcorner$ coniugio per $g$

Chi e' il suo nucleo? $g$ t.c. $\varphi_g\big|_H = id_H$

$\iff \forall h \in H,\ \varphi_g(h) = h$

$\iff \forall h \in H,\ g h g^{-1} = h$

$\iff g \in Z_G(H)$

Deduciamo un omomorf. INIETTIVO

$$\begin{tikzcd}
\frac{N_G(H)}{Z_G(H)} \arrow[r, hook] & Aut(H) \\
N_G(H) \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Nel nostro caso: $\frac{N_{S_7}(\sigma)}{Z_{S_7}(\sigma)} \hookrightarrow Aut(\langle\sigma\rangle) \cong \left(\mathbb{Z}/7\mathbb{Z}\right)^{\times}$

$H = \langle\sigma\rangle \simeq \mathbb{Z}/7\mathbb{Z}$

$$\Rightarrow \quad \frac{\# N_{S_7}(\sigma)}{\# Z_{S_7}(\sigma)} \mid 6 \quad \Rightarrow \quad \# N_{S_7}(\sigma) \mid 42$$

Cerchiamo dei $g$ t.c. $g \sigma g^{-1} = \sigma^i$ $\quad i = 1, 2, \dots, 6$

$\boxed{i=2}$

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

$$\parallel$$

$$(g(1), g(2), \dots, g(7)) = (1, 3, 5, 7, 2, 4, 6)$$

Ad esempio:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 \end{pmatrix}$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 2 & 4 & 6 & 1 & 3 \end{pmatrix}$$

Ci sono 7 elementi di questo tipo

$\boxed{i=3}$ $\quad g \sigma g^{-1} = \sigma^{3} = (1, 4, 7, 3, 6, 2, 5)$

Esistono dei $g$ cosiffatti (ne esistono 7)

Conseguenza:

$$\frac{N_{S_7}(\sigma)}{Z_{S_7}(\sigma)} \xrightarrow{\sim} \mathrm{Aut}(\langle \sigma \rangle) \cong \mathbb{Z}/6\mathbb{Z}$$

$$\Big( \sigma \longmapsto \sigma^{i} \Big)$$
$$(i,7)=1$$

$$\rotatebox{90}{$\in$}$$

$$\bar{g} \longmapsto \bar{1}$$

- $|N_{S_7}(\sigma)| = 42$
- $\langle \sigma \rangle \lhd N_{S_7}(\sigma)$ $\qquad \mathrm{ord}(\bar{g}) = 6$
- C'è un elemento di ordine 6. Sia $\bar{g} \in \dfrac{N(\sigma)}{Z(\sigma)}$ di

ordine 6. Allora $\bar{g} = \pi(g)$ $\qquad \pi : N(\sigma) \to \dfrac{N(\sigma)}{Z(\sigma)}$

e $6 \mid \text{ord } g$

$\langle g \rangle \simeq \mathbb{Z}/(\text{ord } g)\mathbb{Z}$ contiene un el. ord. 6

( In effetti $\text{ord } g = 6$ )

$$\left.\begin{aligned} &\bullet\ \langle \sigma \rangle \trianglelefteq N(\sigma) \\ &\ \ \langle g \rangle \simeq \mathbb{Z}/6\mathbb{Z} \\ &\ \ \langle \sigma \rangle \cap \langle g \rangle = \{e\} \end{aligned}\right] \Longrightarrow \boxed{N(\sigma) \simeq \langle \sigma \rangle \rtimes_{\psi} \langle g \rangle}$$

$\rtimes$

——— o ———

$$\circ \quad \psi : \mathbb{Z}/6\mathbb{Z} \longrightarrow (\mathbb{Z}/7\mathbb{Z})^{\times} \simeq \mathbb{Z}/6\mathbb{Z} \qquad \mathbb{Z}/7\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/6\mathbb{Z}$$

$$1 \longmapsto 3 \text{ o } 5 \qquad \pm 1$$

$\text{ord}_7(3) = 6$

## Un central. complicato

Sia ora $\sigma = (1,2,3)(4,5,6)(7,8,9)$. $Z_{S_9}(\sigma) = ?$

$$\# Z(\sigma) = \frac{9!}{\text{orbita}(\sigma)} = \frac{9!}{\frac{1}{3!}\underbrace{\binom{9}{3}\binom{6}{3}\binom{3}{3}}_{\binom{9}{3,3,3}} 2!\,2!\,2!} = \underline{3}\cdot\underline{3}\cdot\underline{3}\cdot 3!$$

$$Z(\sigma) \supseteq \langle(1,2,3)\rangle \times \langle(4,5,6)\rangle \times \langle(7,8,9)\rangle$$

$$g\sigma g^{-1} = (4,5,6)(1,2,3)(7,8,9) = \sigma$$

$$g = (1,4)(2,5)(3,6) \in Z(\sigma)$$

$$h = (1,4,7)(2,5,8)(3,6,9)$$

$$h\sigma h^{-1} = \big(h(1), h(2), h(3)\big)\big(h(4), h(5), h(6)\big)\big(h(7), h(8), h(9)\big)$$

$$= (4,5,6)(7,8,9)(1,2,3)$$

$$H = \langle g, h \rangle \simeq S_3 = D_3 \qquad H \simeq \langle g \rangle \langle h \rangle$$

$$ghg^{-1} \overset{?}{=} h^{-1}$$

$$\| \qquad\qquad\qquad \|$$

$$(4,1,7)(5,2,8)(6,3,9)$$

$$Z(\sigma) = \big(\underbrace{\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle \times \langle(7,8,9)\rangle}_{N}\big) \rtimes H$$

① H normalizza N : basta verificarlo sui gen. di H,

$$gNg^{-1} = \langle g(1,2,3)g^{-1}, g(4,5,6)g^{-1}, g(7,8,9)g^{-1}\rangle$$

$$= \langle (4,5,6), (1,2,3), (7,8,9)\rangle = N$$

$$hNh^{-1} = \langle (4,5,6), (7,8,9), (1,2,3)\rangle = N$$

② $|N\cap H| = 1$ o 3. Se fosse 3, avremmo

$$N\cap H = \langle h\rangle \Longrightarrow h\in N$$

$$\longrightarrow (1,4,7)(2,5,8)(3,6,9) = (1,2,3)^i(4,5,6)^j(7,8,9)^k$$

che non va bene per unicità dec. cicli

③ $|NH| = \frac{|N| \cdot |H|}{|N \cap H|} = \frac{27 \cdot 6}{1} \Rightarrow NH = Z(\sigma)$

Prod. semidiretto: $Z(\sigma) \cong N \rtimes_{\varphi_1} H$

$\cong \left(\mathbb{Z}/_{3}\mathbb{Z}\right)^3 \rtimes_{\varphi_2} S_3$

$\varphi_1 : H \longrightarrow \mathrm{Aut}\left( \langle (1,2,3) \rangle \times \langle (4,5,6) \rangle \times \langle (7,8,9) \rangle \right)$

$h \longmapsto$ (l'unico aut. che manda $(1,2,3) \mapsto (4,5,6)$,

$(4,5,6) \longmapsto (7,8,9)$ e $(7,8,9) \mapsto (1,2,3)$)

$$g \longmapsto \left( \begin{array}{ll} (1,2,3) \longmapsto (4,5,6) & \\ & (7,8,9) \mapsto (7,8,9) \\ (4,5,6) \longmapsto (1,2,3) & \end{array} \right)$$

$\psi_1(h) \in Aut(N)$ e' $\varphi_h |_N$

$$\varphi_h\big((1,2,3)\big) = (4,5,6)$$

$$\varphi_h\big((4,5,6)\big) = (7,8,9)$$

Sempre piu' difficile! Dopo un isom.

$$N \longrightarrow \left(\mathbb{Z}/3\mathbb{Z}\right)^3$$

$$(1,2,3) \longmapsto (1,0,0)$$

$$(4,5,6) \longmapsto (0,1,0)$$

$$(7,8,9) \longmapsto (0,0,1)$$

$$H \xrightarrow{\sim} S_3$$

$$h \longmapsto (1,2,3)$$

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

$$\left(\mathbb{Z}/3\mathbb{Z}\right)^3 \rtimes_{\varphi_2} S_3$$

$$\varphi_2 : S_3 \longrightarrow Aut\left(\mathbb{Z}/3\mathbb{Z}\right)^3$$

$$(1,2) \mapsto \left((x,y,z) \mapsto (y,x,z)\right)$$

$$(1,2,3) \mapsto \left((x,y,z) \mapsto (z,x,y)\right)$$

# Generatori di $A_n$

$\{ (i,j)(k,\ell) \mid i \neq j,\ k \neq \ell \}$ genera

$\{ (i,j,k) \mid i,j,k \text{ distinti} \}$ genera

Voglio dire che $(i,j)(k,\ell)$ sta nel generato.

- Se $\{i,j\} = \{k,\ell\}$ ok
- Se $|\{i,j\} \cap \{k,\ell\}| = 1$, diciamo $j = k$,

$$(i,j)(j,\ell) = (\ell, i, j)$$

- Se $\{i,j\} \cap \{k,\ell\} = 0$,

$$(i,j)(k,\ell) = \underbrace{(i,j)(j,k)}_{3\text{-ciclo}} \underbrace{(j,k)(k,\ell)}_{3\text{-ciclo}}$$

$\{ (1,2,i) \mid i \in \{3,\dots,n\} \}$

$A_5$ semplice ($N \triangleleft A_5 \iff N = \{id\}$ o $A_5$)

Oss $N \triangleleft G \iff N$ unione di cl. di coniugio

In $A_5$, le cl. di coniugio sono:

| | |
|---|---|
| $(1,2,3,4,5)$ | 12 |
| $(2,1,3,4,5)$ | 12 |
| $(1,2)(3,4)$ | 15 |
| $id$ | 1 |
| $(1,2,3)$ | 20 |

Si verifica che non ci sono somme costruite con ↑ questi addendi che comprendano 1 e che dividano 60

**Lemma** Sia $N \triangleleft G$. $N$ contiene tutti gli elementi $g \in G$ con $(\operatorname{ord}(g), [G:N]) = 1$.

**Dim.** Se $g$ ha questa caratt., $\operatorname{ord}(\pi(g)) \mid \begin{matrix} \operatorname{ord} g \\ [G:N] \end{matrix}$

$\pi : G \longrightarrow G/N$

$$\Downarrow$$

$$\operatorname{ord}(\pi(g)) \mid \operatorname{mcd} = 1$$

$$g \in \ker \pi = N \Leftarrow \pi(g) = id_{G/N} \longleftarrow \Downarrow$$

$$g \in N$$

$\square$

Sia $N \triangleleft A_5$. Se $3 \nmid [A_5 : N] \Rightarrow N$ contiene tutti gli el. di ord. 3

$\Rightarrow N = A_5$

Se $2 \nmid [A_5 : N] \Rightarrow N$ contiene tutti gli el. ord 2

$\Rightarrow N$ contiene tutte le doppie trasp.

$\Rightarrow N = A_5$

$\Rightarrow$ Basta considerare i casi in cui $6 \mid [A_5 : N]$

$\Rightarrow \#N \mid 10 \Rightarrow N$ non può contenere classi di coniugio $\neq \{id\} \Rightarrow N = \{id\}$.

$A_n$ semplice $\forall n \geq 5$

Per induzione. Il caso base OK!

$N \triangleleft A_{n+1}$. Sia $H_i = \{\sigma \in A_{n+1} \mid \sigma(i) = i\} \simeq A_n$.

Gli $H_i$ sono tutti coniugati in $A_{n+1}$.

$\top$ $A_{n+1} \circlearrowleft \{1, 2, \dots, n+1\}$ in modo transitivo

$(1, i)\ (j, k)$ $j, k \neq 1, i$.

$H_i = \text{Stab}(i)$ ⌋

$N \cap H_i \triangleleft H_i$ $\qquad h_i (N \cap H_i) h_i^{-1} = N \cap H_i$

Per ip. induttiva, $N \cap H_i = \begin{cases} \{e\} \\ H_i \end{cases}$

① Se $N \cap H_i = H_i$ per almeno un $i$ $\Rightarrow$ $H_i \subseteq N$

$\Rightarrow$ $N$ contiene un 3-ciclo $(j,k,\ell)$

$\Rightarrow$ $N$ contiene $g(j,k,\ell)g^{-1}$ $\forall g \in A_{n+1}$

Voglio dire che $Cl_{A_{n+1}}(j,k,\ell) = Cl_{S_{n+1}}((j,k,\ell))$.

Per dire questo, basta (vedi es. precedente) far vedere che $\exists$ una permutaz DISPARI che commuta con $(j,k,\ell)$.

Esiste, ad es. $(a, b)$ con $\{a,b\} \cap \{j,k,\ell\} = \emptyset$.

$\Rightarrow N \supseteq Cl_{A_{n+1}}(j,k,\ell) = Cl_{S_{n+1}}(j,k,\ell) =$ tutti i 3-cicli

$\Rightarrow N = A_{n+1}$.

② Altrimenti, $N \cap H_i = \{e\}$ $\forall i$. In questo caso vogliamo dim che $N = \{id\}$.

- Se $\sigma \in N$ ha almeno 1 pto fisso, allora $\sigma = id$
  $\sigma \in H_i$

- $\sigma \in N$ $\sigma = (\ell_1)(\ell_2) \dots (\ell_k) \Rightarrow \ell_1 = \dots = \ell_k$

  Infatti: sia $r = \min \ell_i = \ell_1$ $\ell_1 \leq \ell_2 \leq \dots \leq \ell_k$

$$\sigma^{l_1} = (\ id\ )\ (l_2)^{l_1} \cdots (l_k)^{l_1} \Rightarrow \sigma^{l_1} = id$$

$$\Rightarrow \quad l_1 = \dots = l_k$$

- $\sigma \in N$, $\quad \sigma$ = $k$ cicli di lungh $l = \frac{n+1}{k}$

Se $k>1$, $Cl_{A_{n+1}}(\sigma) \subseteq N$ $\qquad = (a_1, \dots, a_l)(b_1, \dots, b_l)(\dots)$

$$\overset{?}{\|}$$

$Cl_{S_{n+1}}(\sigma)$

Devo esibire una perm. DISPARI che commuta con $\sigma$.

- Se $l$ è pari, prendo uno dei cicli di $\sigma$.
- Altrimenti $l$ è dispari e prendo

$$(a_1, b_1) \cdots (a_l, b_l)$$

- $\Rightarrow$ N contiene tutte le cose con la stessa dec. in cicli

$\Rightarrow$ trovo il prodotto di 2 che ha pti fissi ma non è l'identità:

$$\begin{array}{rccc} & (a_1, \dots, a_\ell) & (b_1, \dots, b_\ell) & \dots \\ \cdot & (a_1, \dots, a_\ell)^{-1} & (b_1, \dots, b_\ell) & \dots \\ \hline & id & (b_1, \dots, b_\ell)^2 & (\dots)^2 \end{array}$$

ha pti fissi e non è id... salvo se $\ell = 2$.

[FINITO NELLE ULTIME PAGINE DI QUESTE SLIDES]

Cor. $\langle \text{5-cicli} \rangle = A_n \qquad n \geq 5$

$$g \langle \text{5-cicli} \rangle g^{-1} = \langle g \sigma g^{-1} \mid \sigma \text{ è 5-ciclo} \rangle$$

$$= \langle 5\text{-cicli} \rangle \quad \triangleleft \; A_n$$

Per semplicità $\Rightarrow$ $\langle 5\text{-cicli} \rangle = A_n$ $\square$

## Conclusione della dim. della semplicità di $A_n$ (aggiunta dopo la lezione)

Ci eravamo ricondotti a dimostrare:

**Prop.** Sia $N \triangleleft A_{n+1}$ e sia $H_i = \{\sigma \in A_{n+1} \mid \sigma(i)=i\} \simeq A_n$.

Supponiamo che $N \cap H_i = \{id\}$ $\forall i = 1, \dots, n+1$. Allora $N = \{id\}$.

Avevamo già fatto le seguenti osservazioni:

① Se $\sigma \in N$ ha almeno un pto fisso (cioè $\exists i \in \{1, \dots, n+1\}$ t.c. $\sigma(i) = i$ ), allora $\sigma = id$.

② Sia $\sigma \in N$. La decomposizione in cicli di $\sigma$ è data da $k$ cicli, tutti della medesima lunghezza $\ell = \frac{n+1}{k}$.

③ Sia $\sigma \in N$ e siano $k$, $\ell$ come qui sopra. Se $k \geq 2$, allora $N$ contiene tutte le permutazioni in $S_n$ con la stessa decomposizione in cicli di $\sigma$.

Siamo pronti a concludere la dim. della Prop.

Dim Supponiamo per assurdo $N \neq \{id\}$ e scegliamo un qualsiasi $\sigma \in N \setminus \{id\}$. Scriviamo (osservazione ②)

$$\sigma = \underbrace{(a_{1,1}, \dots, a_{1,\ell})}_{\ell-\text{ciclo}} \underbrace{(a_{2,1}, \dots, a_{2,\ell})}_{\ell-\text{ciclo}} \cdots \underbrace{(a_{k,1}, \dots, a_{k,\ell})}_{\ell-\text{ciclo}},$$

in cui sono presenti $k$ $l$-cicli. Distinguiamo 3 casi:

(i) $k=1$, cioè $\sigma$ è un $(n+1)$ ciclo, diciamo

$$\sigma = (a_1, \dots, a_\ell). \qquad (\ell = n+1 \geq 6)$$

Siccome $N$ è normale in $A_{n+1}$, $N$ contiene $\tau\sigma\tau^{-1}$, dove $\tau = (a_1, a_2)(a_3, a_4) \in A_{n+1}$. Si noti che

$$\tau\sigma\tau^{-1} = (a_2, a_1, a_4, a_3, a_5, a_6, \dots, a_\ell)$$

Allora $N$ contiene anche il prodotto $\beta := (\tau\sigma\tau^{-1}) \cdot \sigma$.

È chiaro che $\beta \neq id$, perché $\beta(a_4) = (\tau\sigma\tau^{-1})(\sigma(a_4)) =$

$$= (\tau\sigma\tau^{-1})(a_5) = a_6 \neq a_4,$$

ma d'altra parte $\beta(a_1) = (\tau\sigma\tau^{-1})(\sigma(a_1)) =$

$$= (\tau \sigma \tau^{-1})(a_2) = a_1 .$$

Questo è assurdo: $\beta$ ha un pto fisso (cioè $a_1$), ma non è l'identità ($\beta(a_4) \neq a_4$), il che contraddice l'Osservazione ①.

(ii) $k > 1$ e $\ell > 2$. Scriviamo $\sigma$ come

$$\sigma = \underbrace{(a_{1,1}, \dots, a_{1,\ell})}_{\ell\text{-ciclo}} \cdots \underbrace{(a_{k,1}, \dots, a_{k,\ell})}_{\ell\text{-ciclo}}$$

e chiamiamo $\sigma_1, \dots, \sigma_k$ i $k$ cicli presenti in questa decomposizione. Notiamo ora che, per l'Osservazione ③, $N$ contiene anche

$$\alpha := \sigma_1^{-1} \cdot \sigma_2 \cdots \sigma_k ,$$

in quanto questa permutazione ha la stessa dec. in cicli di $\sigma$. Allora $N$ contiene anche

$$\beta = \alpha \circ \sigma = \sigma_2^2 \cdots \sigma_k^2,$$

che ha pti fissi (gli elementi coinvolti in $\sigma_1$), ma non è l'identità ($\sigma_2^2 \circ \cdots \circ \sigma_k^2$ è un prodotto di permutazioni diverse dall'identità – qui si usa che la lunghezza $\ell$, che è anche l'ordine di $\sigma_2, \dots, \sigma_k$, è $> 2$ – che agiscono su insiemi disgiunti). L'esistenza di $\beta \in N$ contraddice l'Osservazione ①, assurdo.

(iii) $k > 1$ e $\ell = 2$. Allora $\sigma$ è un prodotto di $k$ trasposiz. disgiunte; scriviamola nella forma

$$\sigma = (a_1, b_1)(a_2, b_2)(a_3, b_3) \cdots (a_k, b_k).$$

Allora $N \trianglelefteq A_{n+1}$ contiene anche $\alpha := \tau \sigma \tau^{-1}$, dove $\tau = (a_1, a_2, b_1) \in N$, e cioè $N$ contiene

$$\alpha = (a_2, a_1)(b_1, b_2)(a_3, b_3) \cdots (a_k, b_k).$$

Si noti che $k = \frac{n+1}{\ell} = \frac{n+1}{2} \geq 3$. Infine, $N$ contiene il prodotto $\beta := \alpha \circ \sigma = (a_2, a_1)(b_1, b_2)(a_1, b_1)(a_2, b_2) =$

$$= (a_1, b_2)(b_1, a_2)$$

Ancora una volta, $\beta \in N$ ha pti fissi ma $\beta \neq id$, assurdo $\square$

# PRODOTTI SEMIDIRETTI, SYLOW

## $S_4$ come prodotto semidiretto

- $V_4 = \{ id, \ (1,2)(3,4), \ (1,3)(2,4), \ (1,4)(2,3) \}$ e' normale perché unione di classi di coniugio
- $S_3 < S_4$ : consideriamo il sottogp $H = Stab(4)$

$$= \{ \sigma \in S_4 \mid \sigma(4) = 4 \} \simeq S_3$$

- $V_4 \cap H = \{id\}$
- $\underset{\overset{\|}{\langle V_4, H \rangle}}{V_4 \cdot H} \overset{?}{=} S_4$ //

Dobbiamo dim. che ogni $\sigma \in S_4$ si scrive come $\sigma = v \cdot h$ con $h \in H$, $v \in V_4$

$$|V_4 \cdot H| = \frac{|V_4| \cdot |H|}{|V_4 \cap H|} = |V_4| \cdot |H| = 24 = |S_4|$$

Guardiamo $\sigma(4) = \begin{cases} 4 \longrightarrow \sigma \in H \\ \neq 4 \longrightarrow \exists\, v \in V_4 \text{ t.c.} \end{cases}$

$$v(\sigma(4)) = 4$$

$$(v \circ \sigma)(4) = 4 \Rightarrow v \circ \sigma \in H$$

$$\Rightarrow \sigma = v^{-1} \circ h$$

Conclusione: $S_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_{\varphi} S_3$ $\quad \varphi : S_3 \longrightarrow \operatorname{Aut}(\mathbb{Z}/2\mathbb{Z})^2$

$$V_4 \rtimes_{\psi} H \qquad \psi : H \longrightarrow \operatorname{Aut}(V_4)$$

$$h \longmapsto (\text{coniugio per } h)\big|_{V_4}$$

$$V_4 \longrightarrow \left(\mathbb{Z}/2\mathbb{Z}\right)^2$$

$(1,2)(3,4) \longmapsto (1,0)$

$(1,3)(2,4) \longmapsto (0,1)$

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

$(1,2,3) \in S_3$

$\varphi((1,2,3)) \in \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z}\right)^2 :$

chi e' ?

Coniugare per $(1,2,3)$ in $S_4$ manda

$$\begin{tikzcd}
 & & (1,0) \arrow[r] \arrow[d, no head] & (1,1) \arrow[d, no head] \\
 & & (1,2)(3,4) \arrow[r, mapsto] & (2,3)(1,4) \\
(0,1) \arrow[r, mapsto] & (1,0) & (1,3)(2,4) \arrow[l] \arrow[r, mapsto] & (2,1)(3,4) \\
 & & (1,4)(2,3) \arrow[r, mapsto] & (2,4)(1,3) \arrow[d, no head] \\
 & & (1,1) & (0,1)
\end{tikzcd}$$

$$\varphi: S_3 \longrightarrow \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z}\right)^2$$

$$(1,2,3) \longmapsto \begin{pmatrix} (1,0) \longmapsto (1,1) \\ (0,1) \longmapsto (1,0) \end{pmatrix}$$

$$(1,2) \longmapsto \left( \begin{array}{l} (1,0) \longmapsto (1,0) \\ (0,1) \longmapsto (1,1) \end{array} \right)$$

**Oss.** $D_n \simeq \langle r \rangle \rtimes_\varphi \langle s \rangle \qquad \varphi : s \longmapsto (r \longmapsto r^{-1})$

$$(r^{a_1}, s^{b_1}) \circ (r^{a_2}, s^{b_2}) =$$

$$= \left(r^{a_1} \cdot \varphi(s^{b_1})(r^{a_2}), s^{b_1+b_2}\right)$$

$$r^{a_1} s^{b_1} \circ r^{a_2} s^{b_2} = r^{\circ} s^{\circ}$$

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

$$\varphi : (\mathbb{Z}/3\mathbb{Z}) \longrightarrow (\mathbb{Z}/7\mathbb{Z})^{\times}$$

$$1 \longmapsto 2$$

$\varphi(1)$ = "la molt. per 2"

$\varphi(2)$ = "la molt. per 4"

$$\overset{\varphi(2)}{\parallel}$$

$$\varphi(1+1) = \varphi(1) \circ \varphi(1)$$

somma in $\mathbb{Z}/7\mathbb{Z}$

$$(5, 2) \cdot (1, 1) = (5 + \varphi(2)(1) , 2 + 1)$$

$\in \mathbb{Z}/3\mathbb{Z}$

$$= (5 + 4 \cdot 1 , 0) = (\overset{\overset{\mathbb{Z}/7\mathbb{Z}}{\cup}}{2}, 0)$$

Elementi di ogni ordine in $G = \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ ?

- $G$ non ab $\Rightarrow$ non ciclico $\Rightarrow$ non ha elem. di ord 21
- El. di ordine 7: ogni $g$ di ord 7 genera uno

$\mathbb{Z}/7\mathbb{Z}$ , cioe' un 7- Sylow di $G$

Quanti sono i 7- Sylow di $G$? 1

Modo 1: $\left.\begin{array}{l} n_7 \equiv 1 \ (7) \\ n_7 \mid 21 \implies n_7 \mid 3 \end{array}\right\} n_7 = 1$

Modo 2: i 7- Sylow sono tutti coniugati

$$G = \underbrace{\mathbb{Z}/7\mathbb{Z}}_{\text{normale}} \rtimes \mathbb{Z}/3\mathbb{Z}$$

$$\{\text{tutti i 7-Sylow}\} = \{\text{coniugati di } \overbrace{\mathbb{Z}/7\mathbb{Z} \rtimes \{0\}}^{\text{normale in } G}\}$$

$$= \{\mathbb{Z}/7\mathbb{Z} \rtimes \{0\}\}$$

$\Rightarrow$ gli elementi di ordine 7 sono 6

Sono $(i, 0)$ con $i \not\equiv 0$ (7)

Per differenza: 14 elementi di ordine 3.

A mano: $g = (x, y)$

$$g \cdot g = (x,y) \cdot (x,y) = (x + \varphi(y)(x), 2y)$$

$$= (x + \varphi(\underbrace{1+1+\dots+1}_{y})(x), 2y)$$

$$= (x + \varphi(1)^{y}(x), 2y)$$

$$= (x + 2^{y} x, 2y)$$

$$g\circ g\circ g = (x, y)\circ(x + 2^y x,\ 2y)$$

$$= \left(x + \varphi(y)\left(x + 2^y x\right),\ 3y\right)$$

$$= \left(x + 2^y x + 2^{2y} x,\ 0\right)$$

$$= \left(x\cdot\left(1 + 2^y + 2^{2y}\right),\ 0\right) = \begin{cases} (0,0) & \text{se } y\neq 0 \\ \begin{array}{c}(3x,0)\\ \shortparallel\\ (0,0)\end{array} & \text{se } y = 0\end{cases}$$

$$1 + 2^y + 2^{2y} = \begin{cases} \dfrac{(2^y)^{2+1} - 1}{2^y - 1} \\ 1 + \dots + 1 & \text{se } 2^y \equiv 1\ (7)\end{cases}$$

$$2^3 = \varphi(3) = \varphi(0) = id$$

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ con $q \mid p-1$ ha id

$i \not\equiv 0(p)$ $\quad (i, 0) \longleftarrow$ $p-1$ elem. ord $p$

$j \not\equiv 0\,(q)$ $\quad (i, j) \longleftarrow$ $pq-p$ " " $q$

## Uno strano semidiretto

$G = GL_3(\mathbb{R})$ $\qquad N = SL_3(\mathbb{R})$ = sottogp. delle matrici con $\det = 1$

$G \simeq N \times \mathbb{R}^\times$ $\qquad = \ker\left(G \xrightarrow{\det} \mathbb{R}^\times\right)$

$H < G,$ $\quad H = \left\{ \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix} : \lambda \in \mathbb{R}^\times \right\} \simeq \mathbb{R}^\times$

- $N \cap H = \{id\}$ ,
- $N$ ed $H$ commutano

- $G = N \cdot H$

$$g = s \circ (\lambda \cdot Id)$$

$$\det(g) = \det(s) \cdot \det(\lambda \cdot Id)$$

$$= \lambda^3$$

Se scelgo $\lambda = \sqrt[3]{\det g}$ , $s = \frac{1}{\sqrt[3]{\det g}} \cdot g$ ho vinto

- $N, H$ normali

$\Rightarrow \quad G \simeq N \times H = SL_3(\mathbb{R}) \times \mathbb{R}^*$

Come prodotto semidiretto

$$G \simeq N \rtimes K \qquad K = \left\{ \begin{pmatrix} x & & \\ & 1 & \\ & & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{R}^* \right\} \simeq \mathbb{R}^*$$

$$G = N \cdot K \qquad g = \left( g \circ \begin{pmatrix} \det g & & \\ & 1 & \\ & & 1 \end{pmatrix}^{-1} \right) \begin{pmatrix} \det g & & \\ & 1 & \\ & & 1 \end{pmatrix} \in N \cdot K$$

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

$\Rightarrow \quad G \simeq N \rtimes_{\varphi} K \cong N \rtimes_{\varphi} \mathbb{R}^*$ con $\varphi$ non banale

Oss Stessa costruzione funziona sostituendo $\mathbb{R}$ con $\mathbb{F}_p$,

$p \equiv 2 (3)$ $\qquad x \longmapsto x^3$ è bigettiva su $\mathbb{F}_p^\times$.

## Un criterio di isom. per prodotti semidiretti

$H, N$ due gruppi, $\varphi : H \longrightarrow Aut(N)$ un omomorfismo, $f \in Aut(H)$. Allora

$$N \rtimes_{\varphi} H \simeq N \rtimes_{\varphi \circ f} H$$

$$H \xrightarrow{f} H \xrightarrow{\varphi} Aut(N)$$

**Conseguenza** $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/q\mathbb{Z}$ con $p, q$ primi e $q \mid p-1$

ricadono in 2 classi di isomorfismo:

- quella del prod. diretto
- una che contiene tutti i semidiretti con $\varphi$ non banale.

$$\varphi_a : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^{\times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

$$1 \longmapsto a$$

con $\mathrm{ord}(a) = q$

$$a = \frac{p-1}{q}, \quad 2\frac{p-1}{q}, \quad \dots, \quad (q-1)\cdot\frac{p-1}{q}$$

$$\begin{tikzcd} \mathbb{Z}/q\mathbb{Z} \arrow[r, "f_K"] & \mathbb{Z}/q\mathbb{Z} \arrow[r, "\varphi_{\frac{p-1}{q}}"] & \mathbb{Z}/(p-1)\mathbb{Z} \end{tikzcd} = \varphi_{K\cdot\left(\frac{p-1}{q}\right)}$$

$$1 \longmapsto \frac{p-1}{q}$$

$$1 \longmapsto K \qquad\qquad (K, q) = 1$$

Allora il criterio di sopra dice:

$$\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_{\frac{p-1}{q}}} \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_{\frac{p-1}{q}} \circ f_K} \mathbb{Z}/q\mathbb{Z}$$

$$\| $$

$$\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_{K\frac{p-1}{q}}} \mathbb{Z}/q\mathbb{Z}$$

Dim criterio $\Psi : N \rtimes_{\varphi} H \xrightarrow{\sim} N \rtimes_{\varphi \circ f} H$

$$(n, h) \longmapsto (n, f^{-1}(h))$$

È chiaro che $\Psi$ è una bigezione di insiemi

$$\Psi\left( (n_1, h_1) \cdot_1 (n_2, h_2) \right) \overset{?}{=} \Psi(n_1, h_1) \cdot_2 \Psi(n_2, h_2)$$

$$\Psi\left( (n_1 \cdot \varphi(h_1)(n_2), h_1 h_2) \right) \overset{?}{=} (n_1, f^{-1}(h_1)) \cdot_2 (n_2, f^{-1}(h_2))$$

$$(n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1 h_2)) \overset{?}{=} (n_1 \cdot (\varphi \circ f)(f^{-1}(h_1))(n_2) \; , f^{-1}(h_1) f^{-1}(h_2))$$

che è vero!

# Teoremi di Sylow

$|G| = 44$ Quanti elementi di ord 11 ha?

$$\# \text{el. di ord } 11 = \varphi(11) \cdot \#\{\text{sottogp} \simeq \mathbb{Z}/_{11}\mathbb{Z}\}$$

$$= 10 \cdot \#\{11-\text{Sylow}\} = 10$$

$$\left\{ \begin{array}{l} n_{11} \equiv 1 \ (11) \\ n_{11} \mid 4 \end{array} \right\} \Rightarrow n_{11} = 1 \nearrow$$

Es $\mathbb{Z}/_{11}\mathbb{Z} \times \mathbb{Z}/_{4}\mathbb{Z}$ , $\mathbb{Z}/_{11}\mathbb{Z} \times \mathbb{Z}/_{2}\mathbb{Z} \times \mathbb{Z}/_{2}\mathbb{Z}$

$D_{22}$ ha 23 el. di ord 2 : $s \cdot r^i$ $i = 0, \dots, 21$

$r^{11}$

$|G| = 45 \Rightarrow G$ abeliano

$P_3$ un 3-Sylow. $\quad P_3 \trianglelefteq G \Leftrightarrow n_3 = 1 \Leftarrow \begin{cases} n_3 \equiv 1 \ (3) \\ n_3 \mid 5 \end{cases}$

con $P_3 \simeq \mathbb{Z}/9\mathbb{Z}$ o $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$P_5$ un 5-Sylow: $\quad \begin{cases} n_5 \equiv 1 \quad (5) \\ n_5 \mid 3 \end{cases} \Rightarrow n_5 = 1 \Rightarrow P_5 \trianglelefteq G$

$$|P_3 \cap P_5| = 1$$

$$|P_3 P_5| = \frac{|P_3| \cdot |P_5|}{|P_3 \cap P_5|} = 9 \cdot 5 = 45$$

$$\Rightarrow G \simeq P_3 \times P_5$$

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

$P_{17}$ è normale, perché $\begin{cases} n_{17} \equiv 1 \quad (17) \\ n_{17} \mid 15 \end{cases}$

Vorrei vedere che $G$ è abeliano. Sappiamo che c'è un omom.

$$\frac{N(P_{17})}{Z_G(P_{17})} \hookrightarrow \mathrm{Aut}(P_{17})$$

$$\frac{G}{Z_G(P_{17})} \hookrightarrow (\mathbb{Z}/17\mathbb{Z})^\times$$

$$\# \frac{G}{Z_G(P_{17})} \Bigg| \begin{array}{l} \# G = 3 \cdot 5 \cdot 17 \\ \# (\mathbb{Z}/17\mathbb{Z})^\times = 16 \end{array}$$

$$\Rightarrow \quad \# \frac{G}{Z_G(P_{17})} = 1 \quad \Rightarrow \quad Z_G(P_{17}) = G \Leftrightarrow P_{17} \subseteq Z(G)$$

Allora $\# \frac{G}{Z(G)} \mid 15 \Rightarrow G/Z(G)$ ciclico $\Rightarrow G$ abeliano

$$\Big\Downarrow \text{ teo strutt.}$$

$G$ ciclico

## Gruppi semplici di ordine $\leq 100$

Oss. $\mathbb{Z}/p\mathbb{Z}$ per $p$ primo e $A_5$ sono semplici.

Oss. $|G| = p^2 \Rightarrow G$ abeliano $\Rightarrow G$ non semplice

In generale: abeliano + semplice $\Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$, $p$ primo

Oss. $|G| = pq$. Supponiamo $q > p$: allora

$$\begin{cases} n_q \equiv 1 \ (q) \\ n_q \mid p \end{cases} \Rightarrow n_q = 1 \Rightarrow$$ c'è un $q$-Sylow normale.

Oss $|G| = 2 \cdot d$ con $d$ dispari $\Rightarrow \exists H < G$ di indice 2, quindi normale

$\Rightarrow G$ non semplice (o $G \simeq \mathbb{Z}/_{2}\mathbb{Z}$)

Restano fuori 56, 72, 80, 60

Idea 1: a volte "non c'è spazio"

$|G| = 7 \cdot 2^3$. Ci potrebbero essere 8 7-Sylow

7 2-Sylow

Se ci sono 8 7-Sylow, però, la loro unione ha

$\underset{\substack{\# \text{elementi di} \\ \text{ord } 7 \\ \text{in ogni Sylow}}}{6} \cdot \underset{\# \text{Sylow}}{8} + 1$ elementi (stiamo usando che $P_7 \cap P_7' = \{id\}$ se $P_7 \neq P_7'$ sono 2 7-Sylow)

Allora se $P_2$ è un 2-Sylow,

$$\underbrace{P_2 \setminus \{id\}}_{7 \text{ elementi}} \subseteq \underbrace{G \setminus \bigcup_{P_7 = 7\text{-Sylow}} P_7}_{7 \text{ elementi}}$$

$\Rightarrow$ ci può essere un solo 2-Sylow $\Rightarrow$ è normale.

$|G| = 48$ : teo Poincaré

$\exists\ P_2 < G$ 2 - Sylow $\leadsto$ $[G : P_2] = 3$

$\xRightarrow{\text{Poincaré}}$ $\exists\ H \subseteq P_2$, $H \trianglelefteq G$, $[G : H] \mid 3!$

$\Rightarrow$ $G$ non semplice.

$H < G$

$$\begin{aligned} N_G(H) &\longrightarrow \mathrm{Aut}(H) \\ g &\longmapsto \varphi_g|_H \end{aligned}$$

$$g^{-1}hg = \varphi_g(h) = h \quad \forall h$$

# SEMPRE GRUPPI

Titolo nota

## Gruppi semplici di ordine $\leq 100$

**Oss** $|G| = p^n \xrightarrow[\text{Sylow}]{} \exists H < G$ con $|H| = p^{n-1}$

$\Rightarrow [G:H] = p$ e' il piu' piccolo primo che divide $|G|$

$\Rightarrow H$ normale.

$|G| = 96 = 3 \cdot 32$ : Sia $P_2$ un 2-Sylow di $G$

$\Rightarrow [G:P_2] = 3 \xRightarrow{\text{Poincaré}} \exists N \trianglelefteq G \qquad N \subseteq P_2$

$\#N \geqslant \frac{96}{6} > 1 \quad \Leftarrow \quad \frac{\#G}{\#N} \leq 6 \qquad \Leftarrow [G:N] \mid 3!$

$|G| = 72$

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

$n_3 \mid 8 \Rightarrow n_3 \in \{1, 4\}$

Se $n_3 = 1$, $\exists$ un 3-Syl. normale e quindi $G$ non semplice

Se $n_3 = 4$, Siano $Q_1, \dots, Q_4$ i 4 3-Sylow.

Sia $X = \{Q_1, \_, Q_4\}$. C'e' un'azione $G \circlearrowright X$ per coniugio, ed e' transitiva (Sylow)

$\rightsquigarrow \exists\, \varphi : G \longrightarrow \mathrm{Sym}_X \simeq S_4$

Cosa possiamo dire di $\ker \varphi$?

* Se $|\ker \varphi| = 1$, avremmo $\varphi$ iniettivo, ma $|G| = 72 > |S_4|$

* Se $\ker \varphi = G$, l'immagine di $\varphi$ sarebbe banale, ma questo contraddice l'azione transitiva

In alternativa: se $\ker \varphi = G$, l'azione è banale, e cioè per definizione $g Q_1 g^{-1} = Q_1 \quad \forall g$

$$\Rightarrow \quad Q_1 \triangleleft G$$

Quindi $\ker \varphi \triangleleft G$ è un sottogp. normale non banale, e $G$ non è semplice.

$|G| = 80$

$n_2 \in \{1, 5\}$

$n_5 \in \{1, 16\}$

Primo modo: se $n_5 = 16$, ci sono

$$1 + 16 \cdot 4 = 65$$

elementi nell'unione dei 5-Sylow $\Rightarrow$ $P_2$ e' unico, in quanto formato da $\{id\} \cup \{$i 15 elem. che non stanno in alcun 5-Sylow$\}$

Secondo modo: sia $P_2$ un 2-Sylow, di indice 5

$\Rightarrow$ azione di $G$ su $G/P_2$

$$\Rightarrow \varphi: \underset{80}{\underset{|}{G}} \longrightarrow \mathrm{Sym}_{G/P_2} \simeq \underset{120}{\underset{|}{S_5}}$$

$\Rightarrow$ $\varphi$ ha un nucleo non banale

(ma $\ker \varphi \neq G$ perché azione transitiva)

$|G| = 60$, $G$ semplice $\Rightarrow$ $G \simeq A_5$

$n_2 \in \{\cancel{1}, \cancel{3}, 5, 15\}$ $G$ semplice $\Rightarrow n_p \neq 1$

$n_3 \in \{\cancel{1}, 4, 10\}$

$n_5 \in \{\cancel{1}, 6\}$

Escludiamo $n_2 = 3$: l'azione di coniugio di $G$ sui 3 2-Syl. dà un hom $\varphi : G \longrightarrow S_3$ non banale (az. trans.), e $\ker \varphi \neq \{id\}$ per cardinalità, assurdo ($G$ semplice)

Consideriamo il caso $n_2 = 5$. L'azione di coniugio di $G$ sull'insieme $X$ dei 2-Sylow dà un omom.

$$\varphi : G \longrightarrow \mathrm{Sym}_X \simeq S_5$$

* Se $\ker \varphi = G$, l'azione sarebbe banale, ma da Sylow sappiamo che è transitiva

* Siccome $G$ è semplice, $\ker \varphi \trianglelefteq G$ e $\ker \varphi \neq G$

$\Rightarrow \ker \varphi = \{id\} \Rightarrow \varphi$ iniettivo.

Quindi $G \simeq \underbrace{\varphi(G)}_{=:H}$ è un sottogp. di indice 2 di $S_5$

Cosa sappiamo di $H \cap A_5$? $<$

$A_5 \Rightarrow H = A_5$

sottgp di $A_5$ di indice 2

||

$$[A_5 : A_5 \cap H] = \begin{cases} 1 \\ 2 \end{cases}$$

$\Downarrow$

sarebbe un sottogp normale non banale di $A_5$, assurdo

Infine, dobbiamo escludere $n_2 = 15$.

Siano $S_1$, $S_2$ due 2-Sylow diversi. Per cardinalità,

$$S_1 \cap S_2 = \{e\} \text{ oppure un gruppo } \simeq \mathbb{Z}/2\mathbb{Z}.$$

- Se le intersezioni $S_1 \cap S_2$ fra due 2-Sylow diversi sono tutte $\{e\}$, l'unione dei 2-Sylow ha $1 + 3 \cdot 15 = 46$ elementi, che sono tutti di ordine 1, 2, 4

Poi ci sono 6 5-Sylow, che danno 24 elementi di ordine 5

- Altrimenti $\exists S_1, S_2$ 2-Sylow t.c. $|S_1 \cap S_2| = 2$.

Sia $H = S_1 \cap S_2$. Chiamiamo $N = N_G(H)$.

Cosa sappiamo di $N$?

(i) $S_1 \subseteq N$, perché $H \triangleleft S_1$ (perché di indice 2, o perché $S_1$ e' abeliano, in quanto di ord. 4)

(ii) $S_2 \subseteq N$

(iii) Quindi $S_1 < N \Rightarrow \# S_1 \mid \# N$

e $\# N > 4$ ; inoltre $\# N \mid 60$

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

(iv) Non è 60, altrimenti $H \triangleleft G$

(v) Non è 20: se fosse 20, $H$ sarebbe un sgp $< G$ di indice 3 $\underset{\text{Poincaré}}{\Longrightarrow}$ $\exists$ un sottogp normale non banale di indice $\mid 6$

Assurdo perché $G$ semplice

(vi) Non è 12: se fosse 12, l'azione di $G$ su $G/N$ per moltiplicaz. a sx darebbe un omomorfismo non banale $G \longrightarrow \mathrm{Sym}_{G/N} \simeq S_5$.

Come prima questo porta a $G \simeq A_5$, ma questo è assurdo perché $A_5$ ha 5 2-Sylow. □

Oss $A_5$ ha effettivamente 5 2-Sylow.

$A_5 \circlearrowright \{2\text{-Sylow}\}$ transitivamente

$$\# \text{orbita} = n_2 = \frac{\# A_5}{\# N_{A_5}(P)} \qquad gPg^{-1} = P$$

Ad esempio, $P = \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$

Chi c'è nel normalizzatore? Sicuramente c'è tutto

$\mathrm{Stab}_{A_5}(5) = \{\sigma \in A_5 \mid \sigma(5)\} \simeq A_4$, che ha 12 elem.

$$\Rightarrow \quad \# N_{A_5}(P) \in \{12, \cancel{60}\} \Rightarrow \quad n_2 = \frac{60}{12} = 5$$

$\llcorner N_{A_5}(P) = A_5$

# Permutazioni

## Sottogp normali di $S_n$

Per $n \geq 5$, gli unici sgp. norm. di $S_n$ sono $\{1\}$, $S_n$, $A_n$

Dim. Se $N$ è normale in $S_n$, $N \cap A_n \triangleleft A_n$

Siccome $A_n$ è semplice,

$$\begin{tikzcd} A_n \arrow[r] \arrow[rr, bend right] & S_n \arrow[r] & S_n/N \end{tikzcd}$$

$\ker = A_n \cap N$

$$N \cap A_n = \begin{cases} A_n \\ \{e\} \end{cases}$$

- Se $N \cap A_n = A_n$ : $A_n \subseteq N$, e i sgp di $S_n$ che contengono $A_n \triangleleft S_n$ sono in bigez. con i sgp di $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$

$$\begin{tikzcd} \left\{ \text{sgp. di } S_n \text{ contenenti } A_n \right\} \arrow[r, leftrightarrow] & \left\{ \text{sgp. di } S_n/A_n \right\} \\ \pi^{-1}(H) & H \arrow[l, mapsto] \end{tikzcd}$$

$$\pi : S_n \to S_n/A_n$$

$$\begin{tikzcd} A_n & \{e\} \arrow[l, mapsto] \\ S_n & S_n/A_n \arrow[l, mapsto] \end{tikzcd}$$

Oss $\frac{n!}{2} \mid \# N \mid n!$

- Se $A_n \cap N = \{e\}$ $\qquad [N : A_n \cap N] \leq 2$

$$\Downarrow$$

$$\# N \leq 2$$

Se $\#N = 1 \Rightarrow N = \{e\}$

Se $\#N = 2$ : un sgp normale con 2 elementi è contenuto nel centro [fatevelo a mano]

$$S_n \geq \frac{N_{S_n}(N)}{Z_{S_n}(N)} \hookrightarrow Aut(N) = \{id\},$$ cioè

$$Z_{S_n}(N) = S_n, \text{ ma } Z(S_n) = \{id\},$$

assurdo! $\square$

Per quali $n$ il grp $S_n$ ha sottogrp. di ordine 21?

Siccome $S_n \hookrightarrow S_{n+1}$, la risposta è "tutti gli interi $\geq n_0$", per un opportuno $n_0$

Se $S_n$ ha sgp. di ord. 21, $21 \mid n!$

$\Rightarrow 7 \mid n! \Rightarrow n \geqslant 7$

Cerchiamo di costruire un sgp. H di $S_7$ di ordine 21.

Senza perdita di generalità, $(1, 2, \dots, 7) \in H$.

$\langle (1, \dots, 7) \rangle \lhd H$ : l'indice è 3 = più piccolo primo che $\mid 21$

$$\Updownarrow$$

$$\underbrace{N_{S_7} \langle (1, \dots, 7) \rangle}_{\text{questo è un gruppo di ordine 42}} \supseteq H \qquad K := \langle (1, \dots, 7) \rangle \simeq \mathbb{Z}/7\mathbb{Z}$$

$$\underbrace{\frac{N_{S_7}(K)}{Z_{S_7}(K)}}_{K} \underset{\checkmark}{\hookrightarrow} \mathrm{Aut}(K) \simeq \underset{\underset{\{1,\,2,\,4\}}{\checkmark}}{\left(\mathbb{Z}/7\mathbb{Z}\right)^{\times}}$$

Troviamo un elem. di ord 3 nel normalizzatore

$$g\,(1,2,\ldots,7)\,g^{-1} = (1,\ldots,7)^{a}$$

$$g^{2}\,(1,\ldots,7)\,g^{-2} = g\left((1,\ldots,7)^{a}\right)g^{-1} =$$

$$= \left(g\,(1,\ldots,7)\,g^{-1}\right)^{a}$$

$$= (1,\ldots,7)^{a^{2}}$$

$$g^3 (1, \ldots, 7)\, g^{-3} = (1, \ldots, 7)^{a^3}$$

$$\|$$

$$(1, \ldots, 7)$$

$$\boxed{a^3 \equiv 1 \quad (7)}$$

Fatto $h \in G$.

$$\begin{tikzcd}
h^m = h^n \arrow[dr, Leftrightarrow] & \iff & \operatorname{ord}(h) \mid m-n \arrow[dl, Leftarrow] \\
& h^{m-n} = id &
\end{tikzcd}$$

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

$$g = (2, 3, 5)(4, 7, 6)$$

# Equazione in $S_{2p}$, $p$ primo

$\sigma^p = (1, \dots, p)(p+1, \dots, 2p)$ : ha soluzione?

Per $p = 2$ c'è la soluz. $(1, 3, 2, 4) = \sigma$

Cosa può essere $\mathrm{ord}_{S_{2p}}(\sigma)$ ?

Osservo che $\sigma^{p^2} = (\sigma^p)^p = id \Rightarrow \mathrm{ord}(\sigma) \in \{\cancel{1}, \cancel{p}, p^2\}$

$\mathrm{ord}(\sigma) = \mathrm{mcm}$ ( lunghezze dei cicli )

$\Rightarrow$ uno dei cicli ha lunghezza $p^2$

$$p^2 \leq 2p \Rightarrow p \leq 2$$

# MACEDONIA DI GRUPPI

Titolo nota

Classificazione dei grp. di ord $105 = 3 \cdot 5 \cdot 7$

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

$$\left.\begin{array}{l} n_5 \in \{1, 21\} \\ n_7 \in \{1, 15\} \end{array}\right] \quad \begin{array}{ll} n_5 = 21 & 21 \cdot 4 \text{ el. di ord } 5 \\ n_7 = 15 & 15 \cdot 6 \text{ el di ord } 7 \end{array}$$

Almeno uno fra $n_5$ ed $n_7$ e' $= 1$

Siano $P_3$, $P_5$, $P_7$ un 3-, 5- e 7-Sylow

$H := P_5 \cdot P_7$ e' un sottogp. (perché uno dei 2 e' normale)

$|H| = 35$

$$H \underset{\uparrow}{\simeq} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}$$

$|H| = p \cdot q$ con $p \nmid q-1$, $q \nmid p-1$

Inoltre $H \trianglelefteq G$ perché $[G:H] = 3 =$ più piccolo primo.

$$G = H \rtimes_{\varphi} P_3 \qquad H \cap P_3 = \{id\}$$
$$H \cdot P_3 = G$$

Si tratta allora di classificare i prodotti $\mathbb{Z}/35\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z}$,

$$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}\left(\mathbb{Z}/35\mathbb{Z}\right) = \left(\mathbb{Z}/35\mathbb{Z}\right)^{\times} \simeq \left(\mathbb{Z}/5\mathbb{Z}\right)^{\times} \times \left(\mathbb{Z}/7\mathbb{Z}\right)^{\times}$$
$$\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

Ci sono solo 3 possibilità per $\varphi$.

Chiamiamole $\varphi_0(1) = 1 \qquad \varphi_a(1) = \underset{\uparrow \text{ ord } 3}{a} \qquad \varphi_{a^{-1}}(1) = a^{-1}$

Osservo che $\varphi_{a^{-1}} = \varphi_a \circ (-id)$

$\hookrightarrow$ autom. di $\mathbb{Z}/3\mathbb{Z}$

$x \longmapsto -x$

$$a^{-1} = \varphi_{a^{-1}}(1) = \varphi_a(-1) = \varphi_a(1)^{-1} = a^{-1}$$

Criterio visto $\Rightarrow$ $\mathbb{Z}/_{35}\mathbb{Z} \rtimes_{\varphi_a} \mathbb{Z}/_{3}\mathbb{Z} \simeq \mathbb{Z}/_{35}\mathbb{Z} \rtimes_{\varphi_{a^{-1}}} \mathbb{Z}/_{3}\mathbb{Z}$

Quindi ci sono $\leq 2$ grp. di ord 105.

Due li conosciamo: $\mathbb{Z}/_{105}\mathbb{Z}$, $\mathbb{Z}/_{5}\mathbb{Z} \times \underbrace{\left(\text{l'unico grp non abeliano di ord } 21\right)}_{K}$

Vorrei convincermi che $\mathbb{Z}/_{35}\mathbb{Z} \rtimes_{\varphi_a} \mathbb{Z}/_{3}\mathbb{Z} \simeq \mathbb{Z}/_{5}\mathbb{Z} \times K$

$$\mathbb{Z}/35\mathbb{Z} \rtimes_{\varphi_a} \mathbb{Z}/3\mathbb{Z} \simeq \left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}\right) \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z}$$

$$\begin{aligned} \varphi : \mathbb{Z}/3\mathbb{Z} &\longrightarrow \mathrm{Aut}\left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}\right) \\ &\qquad\quad \| \\ \varphi(1) \in\ & \mathrm{Aut}\left(\mathbb{Z}/5\mathbb{Z}\right) \times \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right) \\ \varphi(1) :\ & (x,y) \longmapsto (x, 2y) \end{aligned}$$

$$\begin{tikzcd} \left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}\right) \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z} \arrow[r, phantom, "\overset{?}{\simeq}"] & \mathbb{Z}/5\mathbb{Z} \times \left(\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi'} \mathbb{Z}/3\mathbb{Z}\right) \\ & \text{dove } \varphi'(1) = (y \mapsto 2y) \\ ((x, y), z) \arrow[uu] \arrow[r, mapsto] & (x, (y, z)) \end{tikzcd}$$

$$((x_1, y_1), z_1) \cdot ((x_2, y_2), z_2) =$$

$$= ((x_1, y_1) + \varphi(z_1)(x_2, y_2), z_1 + z_2) =$$

$$= ((x_1, y_1) + (x_2, \varphi'(z_1) y_2), z_1 + z_2)$$

$$= ((x_1 + x_2, y_1 + \varphi'(z_1) y_2), z_1 + z_2)$$ OK

$|G| = 75 \rightsquigarrow |Z(G)| = ?$

$|Z(G)| = 75$ è possibile

$$|Z(G)| \in \{1, 3, \cancel{5}, \cancel{15}, \cancel{25}, \overset{\checkmark}{75}\}$$

$\llcorner$ $G/Z(G) \simeq \mathbb{Z}/3\mathbb{Z}$

$\Rightarrow G$ ab. $\Rightarrow$ assurdo

$n_5 = 1$ $\qquad P_5 \simeq \mathbb{Z}/25\mathbb{Z}$ o $\left(\mathbb{Z}/5\mathbb{Z}\right)^2$

$$G \simeq P_5 \rtimes_{\varphi} P_3$$

- Se $P_5 \simeq \mathbb{Z}/25\mathbb{Z}$, $\quad \varphi : P_3 \longrightarrow \mathrm{Aut}(P_5) \simeq \left(\mathbb{Z}/25\mathbb{Z}\right)^{\times}$

Siccome $\left(|P_3|, \left|\left(\mathbb{Z}/25\mathbb{Z}\right)^{\times}\right|\right) = (3,20) = 1$,

$\varphi$ è banale!

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

- Se $P_5 \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ , $\quad \varphi : P_3 \longrightarrow \mathrm{Aut}(P_5) \simeq GL_2(\mathbb{F}_5)$

$$\# GL_2(\mathbb{F}_p) = (p^2-1)(p^2-p)$$

$$\# GL_2(\mathbb{F}_5) = 24 \cdot 20$$

Prendiamo una $\varphi$ non banale. Studiamo

$$(a,b) \in Z\left( \left(\mathbb{Z}/5\mathbb{Z}\right)^2 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \right)$$

$(0,0) \in \left(\mathbb{Z}/5\mathbb{Z}\right)^2$

(1) $\quad (a,b) \cdot (\underline{0},1) = (\underline{0},1) \cdot (a,b)$

(2) $\quad (a,b) \cdot (v,0) = (v,0) \cdot (a,b) \qquad \forall v \in \left(\mathbb{Z}/5\mathbb{Z}\right)^2$

$0 \in \mathbb{Z}/3\mathbb{Z}$

Sia $M = \varphi(1) \neq id$

(1) $(a + \underline{0}, b+1) = (\underline{0} + \varphi(1) \cdot a, 1+b)$

$\iff \boxed{M \cdot a = a}$

(2) $(a + \varphi(b) v, b) = (v + a, b)$

$v + \varphi(0)(a)$

$\varphi(b) \cdot v = v \quad \forall v \iff \varphi(b) = id$

$\iff b \in \ker \varphi$

Ma $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow GL_2(\mathbb{F}_5)$ e' iniettiva $\Rightarrow \boxed{b = 0}$

Voglio dim. che in effetti anche $a = \underline{0}$

- pol. min di $M$ è un fattore di $t^3 - 1 = (t-1)(t^2+t+1)$

Inoltre $t^2+t+1$ è irrid in $\mathbb{F}_5[t]$

- grado pol min $\leq 2$
- pol min è $\underbrace{t-1}_{M = Id, \text{ non di ord } 3}$ o $\underbrace{t^2+t+1}$

└ è anche il pol. caratt
$\Rightarrow$ 1 non è autov
$\Rightarrow M \cdot a = a \Rightarrow a = 0$

$$\Rightarrow \quad Z(G) = id.$$

Secondo modo: sia $g \in Z(G)$ un elem. di ord 3.

Sia $h \in P_5$ di ord 5. $Z_G(h) \supseteq Z(G), P_5$

$$|Z_G(h)| = 75$$

$$\Rightarrow h \in Z(G) \Rightarrow |Z(G)| \geq 15 \Rightarrow |Z(G)| = 75$$

Quindi: nel grp. NON AB $P_5 \rtimes_\varphi P_3$, il centro:

- non contiene el. di ord 3
- non " " " " 5, altrimenti $G/Z(G)$ ciclico
  $\Rightarrow G$ abeliano

$$Z(G) = \{id\}$$

# Sottogp di $S_5$ isom. a $D_5$

Se $G < S_5$ e' $\simeq D_5$, contiene un 5-ciclo $\sigma$.

$G = \langle \sigma, \tau \rangle$ con $\tau \sigma \tau^{-1} = \sigma^{-1}$, con $\tau \in N_{S_5}(\sigma)$

T

$$N_{S_5}(\sigma) \simeq \mathbb{Z}/5\mathbb{Z} \rtimes_{\varphi} \left(\mathbb{Z}/5\mathbb{Z}\right)^{*}$$

$$\frac{N_{S_5}(\sigma)}{\underset{\underset{\langle\sigma\rangle}{\|}}{Z_{S_5}(\sigma)}} \longrightarrow \mathrm{Aut}\left(\langle\sigma\rangle\right) \simeq \left(\mathbb{Z}/5\mathbb{Z}\right)^{\times}$$

$$\# Z_{S_5}(\sigma) = \frac{\# S_5}{\# \mathrm{orb}(\sigma)} = \frac{5!}{4!}$$

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

$$\underset{\underset{(\rho(1), \rho(2), \dots, \rho(5))}{\|}}{\rho\sigma\rho^{-1}} = \sigma^{2} = (1, 3, 5, 2, 4)$$

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

L

Quanti sgp $\simeq D_5$ ci sono in $N_{S_5}(\langle\sigma\rangle) \simeq \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ?

Sto cercando gli $H \subseteq N_{S_5}(\langle\sigma\rangle)$ che contengono $\overset{\triangledown}{\langle\sigma\rangle}$

e $|H|=10 \longleftrightarrow$ indice ✓

Ora, tali H sono in bigez. con i sgp. di $\dfrac{N(\sigma)}{\langle\sigma\rangle} \simeq \mathbb{Z}/4\mathbb{Z}$ di indice 2, e ce n'è uno solo.

Inoltre ogni H di ord 10 dentro $N(\langle\sigma\rangle)$ è $\simeq D_5$

( perché non è abeliano; oppure perché è $\mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \dfrac{2\mathbb{Z}}{4\mathbb{Z}}$

$$\rho^2\sigma\rho^{-2} = \rho(\rho\sigma\rho^{-1})\rho^{-1} = \rho(\sigma^2)\rho^{-1}$$
$$= (\rho\sigma\rho^{-1})^2 = \sigma^4 = \sigma^{-1}\Big)$$

$$\#\{\text{sgp} \simeq D_5\} = \#\{\text{sgp ciclici di ord } 5\} = \frac{1}{\varphi(5)} \cdot 24 = 6$$

$$H \simeq D_5 \longmapsto \text{sgp. di } H \text{ di ord } 5$$

$$\text{l'unico sgp. di indice } 2 \text{ di } N_{S_5}(C) \longleftarrow\!\shortmid \; C$$

$\mathrm{Aut}(A_4) \simeq S_4$

$$A_4 \overset{?}{=} \langle \underset{\sigma}{(1,2,3)}, \underset{\tau}{(1,2)(3,4)} \rangle = H \qquad \tau\sigma\tau^{-1} = (2,1,4)$$

$$\sigma\tau\sigma^{-1} = (2,3)(1,4) \in H$$

$$\left.\begin{array}{l} \Rightarrow \; V_4 \subseteq H \Rightarrow 4 \mid \# H \\ (1,2,3) \in H \rightarrow 3 \mid \# H \end{array}\right\} \# H \geqslant 12 = \# A_4$$

$$\# \mathrm{Aut}(A_4) \leq \# \{3\text{-cicli}\} \times \# \{\text{coppie di trasp}\}$$
$$= 8 \cdot 3 = 24$$

D'altra parte, $S_4 \longrightarrow \mathrm{Aut}(A_4)$. Se è iniettiva abbiamo finito

$x \longmapsto \varphi_x \big|_{A_4}$

$\varphi_x \big|_{A_4} = id \iff \varphi_x(y) = y \quad \forall y \in A_4$

$xyx^{-1} = y \quad \forall y \in A_4$

$xy = yx \rightarrow x \in Z_{S_4}(A_4) = \{id\}$

Teo $\mathrm{Aut}(S_n) \simeq S_n \quad \forall n \neq 2, 6$

$S_n \xrightarrow{\sim} \mathrm{Aut}(S_n)$

$\sigma \longmapsto \varphi_\sigma$

$H < S_n$, $\quad [S_n : H] = n \quad \Rightarrow \quad H \simeq S_{n-1}$, $\quad n \geq 5$

Consideriamo l'azione di $S_n$ su $S_n/H$ data da

$$\sigma \circ \rho H = \sigma\rho H$$

La pensiamo come un omom. $\varphi : S_n \longrightarrow \mathrm{Sym}_{S_n/H} \simeq S_n$

$\ker\varphi \triangleleft S_n \quad \Rightarrow \quad \ker\varphi = \{e\}, \cancel{A_n}, \cancel{S_n}$

└ l'azione è transitiva

└ no per lo stesso motivo

Se $\ker\varphi = A_n$, imm $\varphi$ ha 2 elem, id e $\tau$

L'orbita di un elem. $\rho H \in S_n/H$ è costituita da $\{\rho H, \ \tau(\rho H)\}$ e quindi ha card $\leq 2$

Ma azione transitiva $\Rightarrow$ c'è un'unica orbita di cardinalità $n \geq 2$

Per quest'azione, $H$ è $\mathrm{Stab}(H) = \{g \in S_n \mid g \cdot H = H\}$
$= \{g \in H\} = H$

$H \simeq \varphi(H)$ $=$ Stab di un pto per l'azione di $\mathrm{Sym}_{S_n/H}$ su $S_n/H$

$\cong$ {permutaz. in $S_n$ che fissano un elemento}

$\simeq S_{n-1}$

$\sigma^4 = (1,2,3)$ in $S_6$

$\operatorname{ord}(\sigma)$

$\sigma^{12} = (\sigma^4)^3 = (1,2,3)^3 = id \Rightarrow \operatorname{ord}(\sigma) \mid 12$

$\nmid 4$

$3 \mid \operatorname{ord}(\sigma)$

$\Rightarrow \operatorname{ord}(\sigma) = 3, \; 6, \; \cancel{12}$

$* \operatorname{ord}(\sigma) = 3 \qquad \sigma^3 = id \qquad \underset{(1,2,3)}{\underset{\parallel}{\sigma^4}} = \sigma \cdot \sigma^3 = \sigma$ ↯

$\sigma = (a,b,c) \qquad \sigma = (a,b,c)(d,e,f)$

$\sigma^4 = (a,b,c)$ $\qquad$ $\sigma^4 = (a,b,c)(d,e,f)$

* $\mathrm{ord}(\sigma) = 6$ : $\qquad$ $\sigma = (a_1, \dots, a_6) \to \sigma^4 = (3\text{-ciclo})(3\text{-ciclo})$

$\sigma = (a,b,c)(d,e) \to \sigma^4 = (a,b,c)$

$(1,2,3)\cdot(d,e)$ $\qquad$ $d,e \in \{4,5,6\}$

$G \simeq S_3 \times \left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\right)$ $\qquad$ $\mathrm{Aut}(G) = ?$

$H$ $\qquad$ $K$ : Sono caratteristici.

$K = Z(G)$, e quindi è caratteristico

Oss generale Sia $n \geq 1$ un intero. Il sottogp di $G$ generato da TUTTI gli elem. di ord $= n$ è caratteristico.

$$\varphi(\langle g \mid ord(g) = n \rangle) = \langle \varphi(g) \mid ord\, g = n \rangle$$

$$= \langle h \mid ord\, h = n \rangle$$

In questo caso: $n = 2$ → gli unici el. di ord 2 sono $(\tau, 0, 0)$ con $\tau \in S_3$ trasp $\Rightarrow$ il sgp. gen. è $S_3 \times \{0\} \times \{0\}$.

$$(S_3 \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}})' = S_3' \times \{0\} \times \{0\} = A_3 \times \{0\} \times \{0\}$$

$$Aut(G) \underset{\substack{\uparrow \\ H, K \text{ caratt}}}{\simeq} Aut(H) \times Aut(K) \simeq S_3 \times GL_2(\mathbb{F}_3)$$

Alcuni es "brevi"

- Quanti sono i grp. ab. di ordine $144 = 2^4 \cdot 3^2$ ?

$G \simeq P_2 \times P_3$

$P_3 \to \mathbb{Z}/9\mathbb{Z}$ o $(\mathbb{Z}/3\mathbb{Z})^2$

$P_2 \to \mathbb{Z}/\underset{n_1}{2^{a_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/\underset{n_r}{2^{a_r}}\mathbb{Z}$ 5 possibilità

con $n_1 \mid \dots \mid n_r$

$a_1 \leq \dots \leq a_r$ $a_1 + \dots + a_r = 4$

$4$ $3+1$ $2+2$ $2+1+1$ $1+1+1+1$

- $A_4$ è l'unico sgp di $S_4$ di indice 2.

  * È normale ⇝ OK

  * Sia $N < S_4$ di indice 2 ⇝ in partic. normale

    ⇒ N contiene tutti gli elem. di ord. coprimo con $\# S_4/N = 2$

    ⇒ N contiene tutti i 3 cicli, che generano $A_4$

**Lemma** $N \triangleleft G \Rightarrow N$ contiene tutti gli el. di $G$ di ordine coprimo con $\# G/N$

- $\{ f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \mid \exists\, a \in (\mathbb{Z}/n\mathbb{Z})^\times \quad \exists\, b \in \mathbb{Z}/n\mathbb{Z}$
  $f(x) = ax + b \}$ e'

un gruppo di ordine $n \cdot \varphi(n)$.

E' un prod. semidiretto: $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$

$$N = \overbrace{\{ f(x) = x + b \mid b \in \mathbb{Z}/n\mathbb{Z} \}} \qquad \overbrace{\{ f(x) = ax \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times \}} = H$$

$$(ax+b)^{-1} \circ (x+t) \circ (ax+b) = (ax+b)^{-1} \circ (ax+b+t) = x + a^{-1}t$$

$$(ax+b)^{-1} = a^{-1} \cdot (x-b)$$

$$N \cap H = \left\{ f(x) = ax+b \;\middle|\; \begin{matrix} b=0 \\ a=1 \end{matrix} \right\} = \{id\}$$

$NH = G$ :   (oppure $|NH| = \frac{|N| \cdot |H|}{|N \cap H|}$)

$$(x \mapsto x+b) \circ (x \mapsto ax) = (x \longmapsto ax+b)$$

$$(a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1)$$

$$\updownarrow$$

$f(x) = a_1 x + b_1$   $f(x) = a_2 x + b_2$   $a_1 a_2 x + a_1 b_2 + b_1$

Meglio: $(b_1, a_1) \cdot (b_2, a_2) = (b_1 + a_1 b_2, a_1 a_2)$

$\mathrm{Aut}(D_n)$: $\begin{cases} r \longmapsto r^a \\ s \longmapsto s \cdot r^b \end{cases}$   $(a, n) = 1$

Componiamone due:

$$r \longmapsto r^{a_2} \longmapsto r^{a_1 a_2}$$

$$s \longmapsto sr^{b_2} \longmapsto (sr^{b_1}) \cdot r^{a_1 b_2} = s \cdot r^{b_1 + a_1 b_2}$$

$$G \rtimes_{\varphi} G \simeq G \times G$$

G non abeliano. In $G \times G$ considero

$$N = G \times \{id\} \triangleleft G \times G$$

$$H = \{ (g, g) \in G \times G \mid g \in G \}$$

$$N \cap H = \{ (id, id) \}$$

$$NH = G \times G$$

$$(g_1, g_2) = \underset{\overset{\cup\!\!\!|}{N}}{(g_1 \cdot g_2^{-1}, id)} \, \underset{\overset{\cup\!\!\!|}{H}}{(g_2, g_2)}$$

$$\Rightarrow \quad G \times G \simeq N \rtimes_{\varphi} H \simeq G \rtimes_{\varphi} G$$

Quand'è che $\varphi$ è banale?

$\varphi(h) = id \iff$ il coniugio per $\overset{(g,g)}{\overset{=}{h}}$ sul gruppo $N$ è banale

$$\iff (g,g)(n, id)(g,g)^{-1} = (n, id) \quad \forall n \in G$$

$$\iff \begin{cases} gng^{-1} = n \\ g \cdot g^{-1} = id \end{cases} \iff gn = ng$$

$$\iff g \in Z(G)$$

$\varphi$ banale $\iff$ $G$ abeliano

## Un criterio di NON isomorfismo fra prodotti semidiretti

Siano $p, q$ due primi distinti, $G$ e $H$ rispett. un $p$-grp e un $q$-grp., e siano

$$X_1 = G \rtimes_{\varphi_1} H \qquad\qquad X_2 = G \rtimes_{\varphi_2} H$$

con $\varphi_1, \varphi_2 : H \longrightarrow \mathrm{Aut}(G)$.

Se $\ker \varphi_1 \not\cong \ker \varphi_2 \implies X_1 \not\cong X_2$

Dim. Sia $f : X_1 \longrightarrow X_2$ un isom. Si ha

$$f(G \rtimes_{\varphi_1} \{e\}) = G \rtimes_{\varphi_2} \{e\} :$$

infatti $G$ è l'UNICO $p$-Sylow di $X_1$ (risp. $X_2$)

Per quel che riguarda $H$, $\underbrace{f(\{e\} \rtimes_{\varphi_1} H)}_{\text{un } q\text{-Sylow di } X_2}$ è coniugato a $\{e\} \rtimes_{\varphi_2} H$. In partic, esiste un automorfismo interno $\psi$ di $X$ t.c.

$$\psi \circ f(G) = G$$
$$\psi \circ f(H) = H$$

Caratterizziamo ker $\varphi_i$ in termini di centralizzatori:

$$Z_{\{e\} \rtimes_{\varphi_1} H}(G \rtimes_{\varphi_1} \{e\}) := \{(e,h) \mid \overbrace{(e,h)(g,e)(e,h)^{-1}}^{\text{operazione in } X_1} = (g,e) \ \forall g \in G\}$$

$$= \left\{ (e,h) \;\middle|\; (\varphi_1(h)(g), h)\cdot(e,h^{-1}) = (g,e) \;\; \forall g\in G \right\}$$

$$= \left\{ (e,h) \;\middle|\; (\varphi_1(h)(g), e) = (g,e) \;\; \forall g\in G \right\}$$

$$= \left\{ (e,h) \;\middle|\; \varphi_1(h) = id \right\} = \{e\} \rtimes \ker \varphi_1$$

$G_1 = G \rtimes_{\varphi_1} \{e\}$ $\qquad$ $H_1 = \{e\} \rtimes_{\varphi_1} H$ $\qquad$ $\chi := \psi \circ f$

$G_2 = G \rtimes_{\varphi_2} \{e\}$ $\qquad$ $H_2 = \{e\} \rtimes_{\varphi_2} H$

$$\{e\} \rtimes \ker \varphi_2 = Z_{H_2}(G_2) = Z_{\chi(H_1)}\left(\chi(G_1)\right)$$

$$= \{ \chi(h_1) \mid \chi(h_1)\chi(g_1) = \chi(g_1)\chi(h_1) \quad \forall g_1 \in G_1 \}$$

$$= \{ \chi(h_1) \mid \cancel{\chi}(h_1 g_1) = \cancel{\chi}(g_1 h_1) \quad \forall g_1 \in G_1 \}$$

$$= \{ \chi(h_1) \mid h_1 \in Z_{H_1}(G_1) \}$$

$$= \chi(\{e\} \rtimes \ker \varphi_1) \qquad \square$$

$$G \rtimes_{\varphi_1} G \simeq G \rtimes_{\varphi_2} G$$

$\ker \varphi_2 \neq G$

$\varphi_1$ banale, $\ker \varphi_1 = G$

# Automorfismo esterno di $S_6$

**Oss 1** $S_5$ ha 6 5-Sylow

$$\frac{1}{\varphi(5)} \cdot \#\{\text{el. ord } 5\} = \frac{1}{4} \cdot 4! = 6$$

**Oss 2** $X = \{P_1, \dots, P_6\}$ l'insieme dei 5-Syl. di $S_5$

$S_5 \circlearrowleft X$ per coniugio in maniera transitiva (Sylow)

$$\Phi : S_5 \hookrightarrow \mathrm{Sym}_X \simeq S_6$$

**Oss 3** $\underset{\underset{H}{\shortparallel}}{\text{imm}\ \Phi} \neq \mathrm{Stab}(i) \quad \forall i = 1, \dots, 6$

**Oss. 4** D'altro canto, $S_6 \circlearrowright S_6/H$ per molt. a sx

$$\rightsquigarrow \quad \psi : S_6 \longrightarrow \mathrm{Sym}_{S_6/H} \simeq S_6$$

L'altra volta: $\psi(H) = \mathrm{Stab}($il numero che ho scelto di assegnare alla classe lat. banale$)$ $\overset{1}{/\!/}$

**Oss 5 e fine** Se $\psi$ fosse interno, $\psi^{-1}$ sarebbe interno ($\psi^{-1}$ = coniugio per $\sigma$) e si avrebbe

$$H = \psi^{-1}(\mathrm{Stab}(1)) = \sigma\, \mathrm{Stab}(1)\, \sigma^{-1} = \mathrm{Stab}(\sigma(1))$$

$\not\parallel$

$\mathrm{Stab}(i)$, assurdo! Quindi $\psi$ non è interno.

$\square$

$G = GL_2(\mathbb{F}_3)$

$\# G = (3^2-1)(3^2-3) = 48$

$\det : G \longrightarrow \mathbb{F}_3^\times$ è omom. grp

$S := SL_2(\mathbb{F}_3) = \ker \det.$

$\# SL_2(\mathbb{F}_3) = \frac{1}{2} \# GL_2(\mathbb{F}_3) = 24$

$$\frac{GL_2(\mathbb{F}_3)}{\ker \det} \simeq \mathrm{Imm} \det$$

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

$n_3(S) = ?$

$n_3(S) \in \{1, \cancel{2}, 4, \cancel{8}\}$

Troviamo dei 3-Sylow.

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

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

Ci sono almeno 2 3-Sylow $\Rightarrow$ sono 4.

⌐ Calcoliamoci il centro di $S$.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \Rightarrow \begin{matrix} c=0 \\ a=d \end{matrix}$$

Stessa cosa con $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \Rightarrow b=0$

$Z(S) = \{\pm id\}$

L

Sia $P$ un 3-Sylow di $S$. Descrivere $N_S(P)$.

$$\# N_S(P) \cdot n_3 = \# S$$

$$\# N_S(P) \cdot 4 = 24 \Rightarrow \# N_S(P) = 6$$

$$N_S(P) \supseteq P, \ Z(S) \Rightarrow N_S(P) = P \cdot Z(S) \simeq \mathbb{Z}/6\mathbb{Z}$$

$S/\{\pm id\} \simeq A_4$ : cerchiamo di costruire l'isom.

considerando un'azione su un insieme di 4 elementi, ad es. $X = \{3\text{-Sylow di } S\}$

$\Phi : S \longrightarrow \mathrm{Sym}_X$ omom. Chi è il nucleo?

$$\ker \Phi = \{ g \in S \mid gPg^{-1} = P \quad \forall \text{ 3-Sylow } P \}$$

$$= \{ g \in S \mid g \in N_S(P) \quad \forall \text{ '' } \quad \text{''} \}$$

$$= \bigcap_P N_S(P) = \bigcap_P (P \cdot Z(S)) = Z(S).$$

1° teo di omom: $S/_{\ker \Phi} \simeq \mathrm{imm}\, \Phi$

$$\overset{\shortparallel}{S/_{\{\pm id\}}}$$

└ ha 12 elem.
sta dentro $S_4$
$\Rightarrow$ è $A_4$

Cosa ci dice questo sui 2-Sylow? $\quad S/_{\{\pm id\}} \simeq A_4$

Teo corrisp: sgp. di S contenenti $\pm id$ sono in bigez. con i sgp di $A_4$

L'unico 2-Syl (normale) di $A_4$ e' il grp. Klein

La sua controimg in S e' un sgp NORMALE di indice 3 = cardinalità 8, e quindi e' un 2-Sylow, anzi l'<u>unico</u> 2-Sylow. Chiamiamolo J.

Per studiare J considero

$$i = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \in J \qquad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$ij = -ji$$

$\Rightarrow$ $J$ e' il grp dei quaternioni!

Dim. infine che $J = S'$.

- $S' \neq \{id\}$ ($S$ non e' abeliano)
- $$\begin{tikzcd} S \arrow[r] \arrow[dr] & S/\{\pm id\} \simeq A_4 \arrow[r] & A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z} \\ & S/S' \arrow[ur, two heads] & \end{tikzcd}$$

$\Rightarrow$ $3 \mid \# \overset{24}{S}/S'$ $\Leftrightarrow$ $\# S' \mid 8$ $\Leftrightarrow$ $S' \subseteq J$

- $S'$ contiene un elem. di ord $2$ (Cauchy)

L'unico è $-id$. $\{\pm id\} \subseteq S' \subseteq J$

$\Rightarrow$ $S'$ = controimg in $S$ del $\underbrace{\text{derivato di } A_4}_{V_4} = J$

$$\begin{tikzcd}
S \arrow[rr] \arrow[dr] & & A \\
& S/\{\pm id\} \simeq A_4 \arrow[ur] &
\end{tikzcd}$$

# ANELLI

Titolo nota

## Operazioni fra ideali

(a) $A = \mathbb{F}_5[x]$, $\quad I = (x^2+1)$, $\quad J = (x^3-1)$

$$I + J = \{ i+j \mid i \in I,\ j \in J \}$$

$$= \{ (x^2+1)\,a(x) + (x^3-1)\,b(x) \mid a(x), b(x) \in A \}$$

$$= \big( \underbrace{x^2+1}_{(x-2)(x+2)},\ \underbrace{x^3-1}_{(x-1)(x^2+x+1)} \big) = (1)$$

$X^3 \equiv 1 \quad (5)$

I è primo? No: il generatore è riducibile e A è a fattor. unica

$(x-2)(x+2) \in I$ ma $x-2 \notin I$, $x+2 \notin I$

(b) $A = \mathbb{Q}[x,y]$ $\quad I = (x-1, y-1)$ e $J = (1-xy)$

$J \subseteq I$ ✓, $I$ massimale, $J$ no

$$1 - xy \overset{?}{=} (x-1)\,a(x,y) + (y-1)\,b(x,y)$$

$$(x-1)\cdot(-y) + (y-1)(-1)$$

$$(-y)\cdot x + 1 = (-y)(x-1+1)+1$$

$$= (-y) \cdot (x-1) + (1-y)$$

I massimale? • Sia $p(x,y) \in A \setminus I$; dim che $(I, p(x,y)) = A$

• $A/I$ è un campo.

$$f(x,y) \equiv f(1,1) \mod I$$

$$x - 1 \equiv 0 \pmod I$$

$$x \equiv 1 \pmod I$$

$$y \equiv 1 \pmod I$$

[Questo mostra che ogni classe di resto $f(x,y) + I$ è rappresentabile con una classe $q + I$ con $q \in \mathbb{Q}$]

Se $q_1 + I = q_2 + I \iff q_1 - q_2 \in I$

$q_1, q_2 \in I$ $\iff q_1 - q_2 = 0 \iff q_1 = q_2$

Sia $q \in I$ un numero raz.; $q = (x-1)\,a(x,y) + (y-1)\,b(x,y)$

---

$\Downarrow$ sostituisco $x=y=1$

$q = 0$

Altro pto di vista:

$$\begin{tikzcd}
A \arrow[r, two heads, "\varphi"] & \mathbb{Q} \\
f(x,y) \arrow[r, mapsto] & f(1,1)
\end{tikzcd}$$

$\ker \varphi = I$

1° teo isom:

$$\begin{tikzcd}
A \arrow[rr, two heads] \arrow[dr] & & \mathbb{Q} \\
& A/I \arrow[ur, hook, "\sim"'] &
\end{tikzcd}$$

$\Rightarrow$ $A/I$ campo

$\Rightarrow$ $I$ massimale.

$\begin{array}{c} J \\ \shortparallel \\ (1-xy) \end{array}$ è primo? $\qquad$ $A/J$ è un dom. d'integrità?

Sia $S = \{ z^k \mid k \geq 0 \}$ una parte molt. di $\mathbb{Q}[z]$

$$S^{-1}\mathbb{Q}[z] \simeq A/J$$

⚠ Servirebbero verifiche

$$\begin{array}{ccc} z & \longleftarrow\!\shortmid & \bar{x} \\ 1/z & \longleftarrow\!\shortmid & \bar{y} \end{array}$$

(c) A anello qualsiasi.

$*\ \underset{\{ \sum \underbrace{\underset{\underset{I}{\cap}}{a_m} b_m}_{\in I \text{ per def. di ideale}} \mid a_m \in I, b_m \in J \} \subseteq I,\ J}{\overset{}{I \cdot J}} \subseteq I \cap J$. Possono essere $\neq$ : $(2)\cdot(2) \neq (2)\cap(2)$

$$I \cdot J = \left\{ \sum \underbrace{\underset{\underset{I}{\cap}}{a_m} b_m}_{\in I \text{ per def. di ideale}} \;\middle|\; a_m \in I, b_m \in J \right\} \subseteq I,\ J$$

$$* \quad \sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

$$\sqrt{I} = \{ a \in A \mid \exists n \in \mathbb{N} \text{ t.c. } a^n \in I \}$$

$$a \in \sqrt{I \cap J} \Rightarrow \exists n \in \mathbb{N} \text{ t.c. } a^n \in I \cap J$$

Allora $a^{2n} = \underbrace{a^n}_{\in I} \cdot \underbrace{a^n}_{\in J} \in I \cdot J$

$$\sqrt{I \cdot J} \supseteq \sqrt{I \cap J} \supseteq \sqrt{I \cdot J}$$

$a \in \sqrt{I} \cap \sqrt{J}$ $\qquad a^m \in I \qquad a^n \in J$

$$a^{m+n} = \underset{I}{\underset{\rotatebox{-90}{$\in$}}{a^m}} \cdot \underset{J}{\underset{\rotatebox{-90}{$\in$}}{a^n}} \in I \cdot J \subseteq I \cap J$$

$$\Rightarrow \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$$

TCR $\dfrac{\mathbb{Q}[x,y]}{(x-y,\ x^3+y^3-x)}$ : mostrare che è isomorfo ad un prodotto di campi

Preliminare: $\dfrac{\mathbb{Q}[x,y]}{(x-y)} \simeq \mathbb{Q}[z]$

$$\varphi : \mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[z]$$
$$f(x,y) \longmapsto f(z,z)$$

$\varphi$ surg? Sì: $g(z) = \varphi(g(x))$.

ker $\varphi$? Certamente $(x-y) \subseteq \ker \varphi$: basta osservare che $x-y \in \ker \varphi$

Ora mostriamo che sono uguali. Sia $f(x,y) \in \ker \varphi$.

Dico che $\forall f(x,y) \in \mathbb{Q}[x,y] =: A \quad \exists g(x,y) \in A,\ h(x) \in A$

$$f(x,y) = (x-y)\, g(x,y) + h(x)$$

Riformulazione: ogni classe di resto mod. $(x-y)$ è rappresentata da una classe $h(x) + (x-y)$

Ma modulo $x-y$, $\quad x \equiv y \mod (x-y)$

$$\rightsquigarrow \quad f(x,y) \equiv \underbrace{f(x,x)}_{h(x)} \mod (x-y)$$

Se $f(x,y) \in \ker \varphi$, allora

$$0 = \varphi(f) = \varphi\big((x-y)\,g(x,y)\big) + \varphi(h(x))$$

$$= 0 + h(z)$$

$$\Rightarrow \quad h(x) = 0 \quad \Rightarrow \quad f(x,y) = (x-y)\,g(x,y) \in (x-y)$$

1° teo di isom: $\dfrac{\mathbb{Q}[x,y]}{(x-y)} \simeq \mathbb{Q}[z]$

$$\frac{\mathbb{Q}[x,y]}{(x-y,\ x^3+y^3-x)} \underset{\text{isom}}{\overset{2°/3° \text{ teo}}{\simeq}} \frac{\mathbb{Q}[x,y]\,/\,(x-y)}{\underset{\sim}{(x-y, x^3+y^3-x)}/(x-y)} \simeq \frac{\mathbb{Q}[z]}{(2z^3-z)}$$

$$\begin{array}{c} (x-y)\,a(x,y) + (x^3+y^3-x)\,b(x,y) \\ \Big\downarrow \varphi \\ 0 \qquad\qquad + (z^3+z^3-z)\,b(z,z) \end{array}$$

$$\frac{A}{I} \simeq \frac{\varphi(A)}{\varphi(I)}$$

$$\frac{\mathbb{Q}[z]}{(2z^3 - z)} \simeq \frac{\mathbb{Q}[z]}{(z \cdot (2z^2-1))} \overset{\text{TCR}}{\cong} \frac{\mathbb{Q}[z]}{(z)} \times \frac{\mathbb{Q}[z]}{(2z^2-1)}$$

$$\uparrow$$

$$I = (z)$$

$$J = (2z^2-1)$$

$$\frac{\mathbb{Q}[z]}{(2z^2-1)} \cong \mathbb{Q} \times \mathbb{Q}\left(1/\sqrt{2}\right) = \mathbb{Q} \times \mathbb{Q}(\sqrt{2}) .$$

$$(1) = (z, 2z^2-1) = I + J \overset{?}{=} (1)$$

$$\uparrow \quad -(2z^2-1) + z \cdot 2z = 1$$

# Interpolazione via TCR

Dati $a_1 < \dots < a_n$ in $\mathbb{Q}$

$b_1, \dots, b_n \in \mathbb{Q}$

esiste esattamente un pol. di grado $\leq n-1$, $p(x)$, t.c.

$p(a_i) = b_i \quad \forall i = 1, \dots, n$

$$\frac{\mathbb{Q}[x]}{((x-a_1) \dots (x-a_n))} \overset{TCR}{\simeq} \frac{\mathbb{Q}[x]}{(x-a_1)} \times \dots \times \frac{\mathbb{Q}[x]}{(x-a_n)}$$

$$\overline{p(x)} \longmapsto \left(p(x) + (x-a_1), \dots, p(x) + (x-a_n)\right)$$

$I_i = (x-a_i)$

$$\underset{i \neq j}{I_i + I_j} = (x-a_i, x-a_j) \ni \underset{\overset{\#}{0}}{a_i - a_j}$$

$$a_i - a_j \in I_i + I_j$$

$$1 = \frac{1}{a_i - a_j} \cdot (a_i - a_j) \in I_i + I_j$$

$$\frac{\mathbb{Q}[x]}{(x-a_i)} \simeq \mathbb{Q} \qquad \begin{aligned} \mathbb{Q}[x] &\longrightarrow \mathbb{Q} \\ p(x) &\longmapsto p(a_i) \end{aligned}$$

$$p(x) + (x-a_i) \longmapsto p(a_i)$$

$$(b_1, \dots, b_m)$$

$$\frac{\mathbb{Q}[x]}{\prod (x-a_i)} \xrightarrow{\sim} \frac{\mathbb{Q}[x]}{(x-a_1)} \times \cdots \times \frac{\mathbb{Q}[x]}{(x-a_n)} \xrightarrow{\sim} \mathbb{Q} \times \overset{\rotatebox{90}{$\in$}}{\cdots} \times \mathbb{Q}$$

$$\overline{p(x)} \qquad \big(p(x)+(x-a_1), \dots, p(x)+(x-a_n)\big) \qquad \big(p(a_1), \dots, p(a_n)\big)$$

$$|$$

rappr. univoci:

polinomi di grado $\leq n-1$

## Una localizzazione

$S = \mathbb{Z} \setminus (2) = \{ n \text{ dispari} \}$

$S$ è parte molt. di $\mathbb{Z}$: $0 \notin S$, $1 \in S$, $\begin{matrix} x \in S \\ y \in S \end{matrix} \Rightarrow xy \in S$

Oss A anello, P ideale primo $\Rightarrow$ $A \setminus P$ è parte molt.

Consideriamo $B := S^{-1}\mathbb{Z}$: troviamone tutti gli ideali.

Sono tutti della forma $S^{-1} I$, $I \triangleleft \mathbb{Z}$

$S^{-1}(m)$

Quand'è che $S^{-1}(m) = S^{-1}(n)$ ?

$\iff$ $m$ ed $n$ sono associati in $B$

$$\begin{array}{l} S^{-1}(m) = mB \\ \parallel \\ \left\{ \frac{mk}{s} \;\middle|\; k \in \mathbb{Z},\ s \in S \right\} = \left\{ m \cdot \frac{k}{s} \;\middle|\; \frac{k}{s} \in B \right\} = mB \end{array}$$

$\iff \exists\, u \in B^\times$ t.c. $m = un$

$\iff u = m/n \in B^\times \iff \circledast$

Es $1, -1 \in B^\times$ $\qquad 2 \notin B^\times \Leftarrow \underbrace{1/2 \notin B}_{B = \left\{ \frac{m}{s} \,\middle|\, s \text{ dispari} \right\}}$

$3, \frac{1}{3} \in B^\times \Leftarrow 3,\ \frac{1}{3} = 2/6 \in B$

$$B^{\times} = \left\{ \frac{m}{n} \;\middle|\; m, n \text{ entrambi dispari} \right\}$$

⊛ : la potenza di 2 nella fattorizz. di $m$, $n$ e' la stessa.

$$\begin{array}{l} S^{-1}(1) = S^{-1}(3) = S^{-1}(5) = S^{-1}(7) = \dots \\ \neq \\ S^{-1}(2) = S^{-1}(6) = S^{-1}(10) = \dots \\ \neq \\ S^{-1}(4) = S^{-1}(12) = S^{-1}(20) = \dots \end{array}$$

Ideali di $B$ : $S^{-1}(2^k)$, $k \in \mathbb{N}$

$$\begin{aligned} f:\ &\mathbb{Z} \hookrightarrow B \\ &n \longmapsto \frac{n}{1} \end{aligned}$$

$I \triangleleft \mathbb{Z}$, $I = (m) = (2^k \cdot d)$ .
d dispari

$f(I) =$ non e' un ideale

$$f^{-1}((f(I))) = (2^k)$$

$$(f(I)) = S^{-1}(2^k d) = S^{-1}(2^k)$$

$$\left\{2^k \frac{m}{s} \,\middle|\, \frac{m}{s} \in B\right\} \cap \mathbb{Z} = (2^k) \Leftarrow \frac{m}{s} \in \mathbb{Z} \underset{s \text{ dispari}}{\Longleftrightarrow} \mathbb{Z} \ni 2^k \cdot \frac{m}{s}$$

$$\{\text{primi di } S^{-1}\mathbb{Z}\} \longleftrightarrow \left\{\begin{array}{l} \text{primi } P \text{ di } \mathbb{Z} \\ \text{t.c. } P \cap S = \emptyset \end{array}\right\}$$

$$S^{-1}(2) \qquad (2)$$

$$(0) \qquad (0)$$

# Ideali primi / massimali di $\mathbb{Z}[x]$

Esempi: $\mathfrak{M} = (2, x)$ $\qquad \mathbb{Z}[x]/\mathfrak{M} \simeq \dfrac{\mathbb{Z}[x]/(x)}{(2,x)/(x)} \simeq \dfrac{\mathbb{Z}}{(2)} \simeq \mathbb{F}_2$

$\mathfrak{P} = (x)$ $\qquad \dfrac{\mathbb{Z}[x]}{\mathfrak{P}} \simeq \mathbb{Z}$ $\qquad \mathfrak{P}$ primo ma non massimale

Sia $\mathfrak{M}$ un ideale max di $\mathbb{Z}[x]$.

$$\mathfrak{M} \cap \mathbb{Z} = \text{un ideale primo di } \mathbb{Z} = \begin{cases} (0) \\ (p) \end{cases}$$

$\rotatebox{90}{$\in$}$

$a \cdot b \implies a \in \mathfrak{M}$ o $b \in \mathfrak{M} \Rightarrow a$ o $b \in \mathfrak{M} \cap \mathbb{Z}$

$a, b \in \mathbb{Z}$ $\qquad \mathfrak{M}$ max e quindi primo

Se $\mathfrak{M} \cap \mathbb{Z} = (p)$, $\qquad \boxed{(p)\,\mathbb{Z}[x] \subseteq \mathfrak{M}}$

Gli ideali primi/max di $\mathbb{Z}[x]$ che contengono p sono in bigez. con gli ideali primi/max di

$$\frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \simeq \mathbb{F}_p[x]$$

$$\left( \begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow\!\!\!\!\rightarrow & \mathbb{F}_p[x] \\ f(x) & \longmapsto & f(x) \bmod p \end{array} \right)$$

Gli ideali max di $\mathbb{F}_p[x]$ sono quelli generati da un polinomio irrid $\overline{f(x)}$

$$\frac{\mathbb{F}_p[x]}{(\overline{f(x)})}$$

I primi sono gli stessi e $(0)$

$$\left\{ \begin{array}{l}\text{ideali primi/max di } \mathbb{Z}[x] \\ \quad\text{contenenti } p\end{array} \right\} = \left\{ (p,\ f(x)) \ \middle|\ \begin{array}{l}\overline{f(x)} \in \mathbb{F}_p[x] \\ \text{è irriduc.}\end{array} \right\}$$

$$\cup \left\{ (p)\,\mathbb{Z}[x] \right\}$$

Es. $(3,\ x^2+1)$ è un ideale max di $\mathbb{Z}[x]$.

Studiamo gli ideali primi $P$ t.c. $P \cap \mathbb{Z} = \{0\}$.

$$P \cap (\mathbb{Z} \setminus \{0\}) = \emptyset$$

$\xleftrightarrow{\text{bigez.}}$ ideali primi di $(\mathbb{Z}\setminus\{0\})^{-1}\,\mathbb{Z}[x] = \mathbb{Q}[x]$

Per finire bisogna capire "come descrivere" $(f(x))\mathbb{Q}[x] \cap \mathbb{Z}[x]$

$$\shortparallel$$

$$(d\, f(x))$$

$d$ = min. comune den.

# ANELLI, IN PARTICOLARE $\mathbb{Z}[i]$

## Massimali in $\mathbb{Z}[x]$

Primi: $(0)$, $(p)$, $\underbrace{(p, f(x))}_{\text{massimali}}$ con $f(x)$ irrid. mod p

$(f(x))$ $f(x) \in \mathbb{Z}[x]$, $c(f(x)) = 1$

$$f(x) = c \cdot g(x)$$

Dim. che $(f(x))$ non è massimale. deg $f(x) \geq 1$

Scegliamo $a \in \mathbb{Z}$ t.c. $f(a) \neq 0, 1, -1$

e scegliamo p un primo che divida $f(a)$

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, "\varphi"] & \frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \arrow[r, "\psi"] & \mathbb{F}_p \\
 & \overline{g(x)} \arrow[r, mapsto] & g(a)
\end{tikzcd}$$

$$(\psi \circ \varphi)(f(x)) = f(a) \bmod p = 0 \Rightarrow f(x) \in \ker \psi \circ \varphi$$

$$p \in \ker \psi \circ \varphi .$$

$(f(x), p) \subseteq \ker(\psi \circ \varphi) \overset{?}{\neq} \mathbb{Z}[x]$ no, perché 1 non appartiene

$$(f(x)) \subseteq (f(x), p) \subsetneq \mathbb{Z}[x]$$

Se $(f(x))$ fosse massimale si avrebbe $(f(x)) = (f(x), p)$,

ma $p \notin (f(x))$ perché i multipli di $f(x)$ sono polinomi non costanti $\square$

Altro modo: Se $(f(x))$ e' max, $A := \frac{\mathbb{Z}[x]}{(f(x))}$ e' un campo, ma

$\mathbb{Z} \hookrightarrow A$, quindi $\mathbb{Q} \hookrightarrow A$ e in partic. ogni intero $\neq 0$

e' invertibile in $A$. Sia $n \in \mathbb{Z}$.

$$(n + (f(x))) \cdot (g(x) + (f(x))) = 1 + (f(x))$$

$$\Leftrightarrow \quad n \cdot g(x) - 1 = h(x) f(x) \quad ⍟$$

Come prima: sia $a \in \mathbb{Z}$ t.c. $f(a) \neq 0, \pm 1$ e $p \mid f(a)$

e prendiamo $n = p$. Valutando ⍟ in $x = a$:

$$⍟ : \quad \underbrace{p \cdot g(a)}_{\equiv 0 (p)} - 1 = \underbrace{h(a) \cdot f(a)}_{\equiv 0 (p)} \quad , \text{ assurdo!}$$

# Eisenstein vale in ogni UFD

Sia $A$ un UFD, $\pi \in A$ un primo/irriducibile.

Sia $f(x) = a_n x^n + \dots + a_0 \in A[x]$. Se

- $\pi \nmid a_n$
- $\pi \mid a_{n-1}, a_{n-2}, \dots, a_0$
- $\pi^2 \nmid a_0$

allora $f(x)$ e' irriducibile.

# PID

- $A$ un PID. Ogni ideale primo di $A$ diverso da $(0)$ è massimale. $\Rightarrow$ UFD

Sia $\mathfrak{p} = (x)$ un primo, e supponiamo che $\mathfrak{p} \subsetneq \mathfrak{m} \neq (1)$

Anche $\mathfrak{m}$ è principale, $\mathfrak{m} = (y)$.

$$(x) \subseteq (y) \iff y \mid x$$

$$\left.\begin{array}{r} \iff x = y \cdot q \\ (x) \text{ primo} \Rightarrow x \text{ è primo} \Rightarrow x \text{ irriducibile} \end{array}\right] \Rightarrow \begin{array}{l} y \text{ unità} \\ q \text{ unità} \end{array}$$

Ma $y$ non è unità $\big( (y) \neq (1) \big)$, e se $q$ è un'unità, $(x) = (y)$

- $A$ PID, $B$ dom. integrità, $\varphi : A \longrightarrow B$ omom. surg.
Allora o $\varphi$ è un isomorfismo, o $B$ è un campo
(o entrambe)

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \\
A/\ker\varphi \arrow[ur, hook, dashed, "\sim"'] &
\end{tikzcd}$$

$\ker \varphi$ è un ideale primo, perché $A/_{\ker\varphi} \simeq B$ è dominio

Se $\ker \varphi = (0) \Rightarrow \varphi$ isom
altrimenti $\ker \varphi$ è max, e $B \simeq A/_{\ker\varphi}$ è campo.

- Sia $C$ un anello t.c. $C[x]$ è un PID. Allora $C$ è un campo.

Intanto $\mathbb{C}$ e' un dominio, perché $\mathbb{C} \subseteq \mathbb{C}[x]$ e $\mathbb{C}[x]$ e' un dominio.

1) $(x)$ e' primo, perché $\dfrac{\mathbb{C}[x]}{(x)} \underset{\uparrow}{\simeq} \mathbb{C}$ e' un dominio

$\Rightarrow$ $(x)$ e' massimale $\Rightarrow$ $\mathbb{C}$ e' un campo

2) L'omomorfismo di valutaz $\mathbb{C}[x] \longrightarrow \mathbb{C}$ e'

$p(x) \longmapsto p(0)$

surg. e non e' un isom $\Rightarrow$ $\mathbb{C}$ campo

Es. $\mathbb{Q}[x,y] = (\mathbb{Q}[y])[x]$ non e' un PID

$$\sqrt{(0)} = \bigcap_{P \text{ primo}} P$$

A anello comm. (con 1). $\sqrt{(0)} = \bigcap_{\substack{P \text{ ideale} \\ \text{primo di } A}} P$

$$\sqrt{(0)} = \{x \in A \mid \exists n \text{ t.c. } x^n = 0\}$$

$\boxed{\subseteq}$ se $x^n = 0 \Rightarrow x^n \in P \xRightarrow[P \text{ primo}]{} x \in P$

$$x \cdot x \cdots x \in P$$

$\boxed{\supseteq}$ Dobbiamo mostrare che se $x \in P$ $\forall P$ primo, allora $x$ è nilpotente. Mostriamo invece che se $x$ NON è nilpotente, $\exists P$ t.c. $x \notin P$

$$\mathcal{C} = \{ I \text{ ideale di } A, \ \forall n \ \ x^n \notin I \}$$

Applicando Zorn, otteniamo un ideale $M$ massimale ALL'INTERNO DI $\mathcal{C}$

- $\mathcal{C}$ non vuoto, perché $(0) \in \mathcal{C}$
- $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ in $\mathcal{C}$, c'e' un elem. di $\mathcal{C}$ che contiene tutti gli $I_j$ $\rightsquigarrow$ l'unione funziona

Verifichiamo che $M$ e' primo.

Siano $a, b \in A$ t.c. $ab \in M$

Supponiamo per assurdo $a \notin M$, $b \notin M$. Allora

$M \subsetneq (M, a) \rightsquigarrow \exists\, k$ t.c. $x^k \in (M, a)$.

$M \subsetneq (M, b) \rightsquigarrow \exists\, h$ t.c. $x^h \in (M, b)$.

$x^k \cdot x^h \in (\dot{M}, a)(\dot{M}, b)$

$\subseteq M$, assurdo

perché $M \in \mathcal{C}$.

**Cor** A anello comm, $I \lhd A$. $\sqrt{I} = \bigcap_{P \supseteq I} P$.

$$A \xrightarrow{\pi} A/I$$

$$\sqrt{I} = \pi^{-1}\left(\sqrt{(0)}\right) = \pi^{-1}\left(\bigcap_{\substack{P \lhd A/I \\ P \text{ primo}}} P\right)$$

$$= \bigcap_{\substack{P \supseteq I \\ P \triangleleft A}} P$$

## Polinomi invertibili

$A$ anello, $B = A[x]$.

(a) $P \triangleleft A$ primo $\Longrightarrow$ $P[x] \triangleleft A[x]$ primo

$$\frac{A[x]}{P[x]} \simeq \frac{A}{P}[x]$$

$A/P$ dominio

$\Rightarrow$ $A/P[x]$ dominio

$$\begin{tikzcd}
A[x] \arrow[rr, two heads] \arrow[dr] & & A/P[x] \\
& A[x]/P[x] \arrow[ur, "\sim"'] &
\end{tikzcd}$$

(b) $B^\times = \left\{ p(x) = a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; \begin{array}{l} a_0 \in A^\times \\ a_i \in \sqrt{0} \quad i=1,\dots,n \end{array} \right\}$

$\boxed{\supseteq}$ Dato $p(x)$ qui, $a_0^{-1} \cdot p(x) = 1 + \underbrace{\underbrace{\frac{a_1}{a_0}}_{a_1'} x + \cdots + \underbrace{\frac{a_n}{a_0}}_{a_n'} x^n}_{-t}$

$$1 - t^n = (1-t)(1+t+\cdots+t^{n-1})$$

$-t$ è nilpotente, perché $\in (a_1', \dots, a_n') \subset \sqrt{(0)}$

Se $n >> 0$, in modo che $t^n = 0$

$$1 = \underbrace{a_0^{-1} \cdot p(x)}_{(1-t)} \cdot (1+t+\cdots+t^{n-1})$$

**Oss** $$\frac{1}{p(x)} = \frac{1}{1-t} = \sum_{n\geq 0} t^n$$

$$\frac{1}{\begin{pmatrix}1&1&1\\ &1&1\\ &&1\end{pmatrix}} = \left(Id + \begin{pmatrix}0&1&1\\ &0&1\\ &&0\end{pmatrix}\right)^{-1} = Id - \begin{pmatrix}0&1&1\\ &0&1\\ &&0\end{pmatrix} + \begin{pmatrix}0&1&1\\ &0&1\\ &&0\end{pmatrix}^2$$

$\boxed{\subseteq}$ Sia $p(x) = a_0 + \dots + a_n X^n$ invertibile, con inverso $q(x)$

$(*)$ $p(x)\, q(x) = 1$

- $a_0 \in A^\times$ $\quad p(0)\, q(0) = 1 \Rightarrow a_0 \cdot q(0) = 1$
- $a_i \in \sqrt{(0)}$ $\quad i = 1, \dots, n$ : basta dim $a_i \in P$ $\forall P$ primo

Sia $P$ primo di $A$. Riduciamo $(*)$ mod $P[x]$

$$\overline{p(x)} \cdot \overline{q(x)} = \overline{1} \quad \text{in} \quad \frac{A[x]}{P[x]} \simeq A/_P [x]$$

$\overline{p(x)} \in \left(A/_P [x]\right)^*$ $\Rightarrow$ $\overline{p(x)} \in \left(A/P\right)^\times$, cioe' tutti i coeff. $a_1, \dots, a_n$ riducono a $0$ mod $P$

$\Rightarrow$ $\underset{i>0}{a_i} \in P$ $\forall P$ $\Rightarrow$ $a_i$ nilpotente

# INTERI DI GAUSS

$$\mathbb{Z}[i] = \{ a+bi \mid a,b \in \mathbb{Z} \}$$

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$$

$$a+bi \longmapsto (a+bi)(a-bi) = a^2+b^2 = \|a+bi\|^2$$

$$\| w \cdot z \| = \|w\| \cdot \|z\| \quad \forall w, z \quad \Rightarrow N(w \cdot z) = N(w) \cdot N(z)$$

**Lemma** $p \in \mathbb{Z}$ primo, $p \equiv 3 \pmod 4) \Rightarrow p$ e' $\overset{\text{primo}}{\text{irrid}}$ in $\mathbb{Z}[i]$

**Dim.** Siccome $\mathbb{Z}[i]$ e' UFD, basta dim. che e' irrid.

Se $p = (a+bi)(c+di) \Rightarrow N(p) = N(a+bi)(c+di)$

$$p^2 = \underbrace{(a^2+b^2)}_{1,\, p,\, p^2} \underbrace{(c^2+d^2)}_{1,\, p,\, p^2}$$

Se $a^2 + b^2 = 1 \rightsquigarrow (a, b) = (0, 1), (0, -1),$

$(1, 0), (-1, 0)$

cioe' $a+bi \in \{1, -1, i, -i\}$

che sono unita'
di $\mathbb{Z}[i]$

Se $a^2 + b^2 = p \rightsquigarrow a^2 + b^2 \equiv p \equiv 3 \pmod 4$

$0 + 0$
$0 + 1$
$1 + 0$
$1 + 1$

assurdo

Se $a^2 + b^2 = p^2 \Rightarrow c^2 + d^2 = 1 \Rightarrow c + di$ e' un'unita'. $\square$

**Lemma** $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

**Dim.** $1, -1, i, -i$ sono invert., con inversi $1, -1, -i, i$.

$$a+bi \in \mathbb{Z}[i]^\times \Rightarrow \exists \underset{\mathbb{Z}[i]}{\underset{\cap}{c+di}} \text{ t.c. } (a+bi)(c+di) = 1$$

$$\Big\Downarrow N$$

$$\underbrace{(a^2+b^2)}_{1}(c^2+d^2) = N(1) = 1$$

$$\Rightarrow (a,b) = (1,0), (0,1), (-1,0), (0,-1)$$

□

**Lemma** $(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = (1-i)^2\mathbb{Z}[i]$, e $1+i$ e' irrid/primo. Inoltre, $\frac{\mathbb{Z}[i]}{(1+i)} \simeq \mathbb{F}_2$.

**Oss. generale** Sia $a+bi \in \mathbb{Z}[i]$ t.c. $N(a+bi)$ e' un numero primo $p$ di $\mathbb{Z}$, allora $a+bi$ e' irrid in $\mathbb{Z}[i]$

Dim. $a+bi = (c+di)(e+fi)$

$$N(a+bi) = N(c+di)\,N(e+fi)$$

$$p = a^2+b^2 = \underbrace{(c^2+d^2)}_{p} \cdot \underbrace{(e^2+f^2)}_{1} \Rightarrow e+fi \in \mathbb{Z}[i]^\times$$

$\square$

Dim. lemma $\quad 2 = (-i)(1+i)^2 \Rightarrow (2) = ((1+i)^2)$

$$2 = i\,(1-i)^2 \qquad\qquad = ((1-i)^2)$$

$(1+i)^2 \in (2)$, ma $1+i \notin (2) = 2\mathbb{Z}[i] = \{2a+2bi \mid a,b \in \mathbb{Z}\}$

e quindi $(2)$ non e' primo.

$2 = (1+i)(1-i) \qquad\qquad (1+i) = i\,(1-i)$

$N(1+i) = 2 \xrightarrow{\text{OSS}} 1+i$ e' primo.

$$\frac{\mathbb{Z}[i]}{(1+i)} \simeq \frac{\mathbb{Z}[i]\,/(2)}{(1+i)\,/(2)} \simeq \frac{\{\overline{0},\ \overline{1},\ \overline{i},\ \overline{1+i}\}}{\{\overline{0},\ \overline{1}\}} \simeq \mathbb{F}_2$$

$$\# \frac{(1+i)}{(2)} = \begin{cases} 1 \rightsquigarrow (2) = (1+i) & \text{FALSO} \\ 2 \\ 4 \rightsquigarrow \frac{\mathbb{Z}[i]}{(1+i)} = (0) \Rightarrow (1+i) = \mathbb{Z}[i] & \text{FALSO} \end{cases}$$

$$\mathbb{Z}[i] = \frac{\mathbb{Z}[x]}{(x^2+1)}$$

$$a+bi \longmapsto \overline{a+bx}$$

$$\frac{\mathbb{Z}[i]}{(1+i)} \simeq \frac{\mathbb{Z}[x]}{(x^2+1,\ 1+x)} \simeq \frac{\mathbb{Z}[x]}{(2,\ 1+x)} \simeq \mathbb{F}_2$$

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

$\square$

**Lemma** Sia $p \in \mathbb{Z}$, $p \equiv 1 \ (4)$. Allora $p = (a+bi)(a-bi)$
$p$ primo

con $a+bi$, $a-bi$ primi
e non associati.

**Dim.** $p \equiv 1 \ (4) \implies \exists x \in \mathbb{Z}$ t.c. $x^2 \equiv -1 (p)$, ovvero

$$p \mid x^2 + 1$$

In $\mathbb{Z}[i]$ posso scrivere $p \mid (x+i)(x-i)$

Ma $p \nmid x+i$ : $x+i = p \cdot (a+bi)$

$1 = p \cdot b$ impossibile

In particolare, $p$ NON È PRIMO $\implies$ NON È IRRIDUCIBILE

$\implies p = (a+bi)(c+di)$, $a+bi, c+di \notin \mathbb{Z}[i]^\times$

$$p^2 = N(p) = N(a+bi)\,N(c+di) = \underbrace{(a^2+b^2)}_{\cancel{1},\ p,\ \cancel{p^2}}\ \underbrace{(c^2+d^2)}_{\cancel{1},\ p,\ \cancel{p^2}}$$

$$\Rightarrow \quad \underset{\displaystyle (a+bi)(a-bi)}{\underset{\parallel}{a^2+b^2}} = p$$

Con $a+bi$, $a-bi$ primi perché $N(a+bi) = N(a-bi) = p$ e' prima

$$a+bi = \underset{\underset{\displaystyle 1,\ -1,\ i,\ -i}{|}}{u} \cdot (a-bi)$$

$u=1 \Rightarrow b=0 \Rightarrow p=a^2$ NO

$u=-1 \Rightarrow a=0 \Rightarrow p=b^2$ NO

$u=i \Rightarrow a=b \Rightarrow p=2a^2$ NO

Es $5 = (2+i)(2-i)$

# ANELLI, QUESTIONI DI FATTORIZZAZIONE UNICA

Titolo nota

## Primi in $\mathbb{Z}[i]$: continua

- $1+i \sim 1-i$
- $p \equiv 3 \pmod 4$
- Se $p \equiv 1 \pmod 4$, $p = (a+bi)(a-bi)$ con $\begin{matrix} a+bi \\ a-bi \end{matrix}$ primi

sono primi in $\mathbb{Z}[i]$. Sono gli $\underbrace{\text{unici}}$! a meno di associati.

Sia $a+bi \in \mathbb{Z}[i]$ primo.

$$a+bi \mid (a+bi)(a-bi) = a^2+b^2 = \prod p_j^{e_j}.$$

Siccome $a+bi$ e' primo, $a+bi \mid p_j$ per qualche $j$.

$*$ Se $p_j \equiv 3\ (4) \implies$ e' irrid in $\mathbb{Z}[i]$

$a+bi \mid p_j \Rightarrow a+bi$ associato a $p_j$

* Se $p_j \equiv 1 \ (4)$, $p = (c+di)(c-di)$

$a+bi \mid c+di$ o $a+bi \mid c-di$

e $a+bi$ e' associato ad uno dei due

* Se $p_j = 2 \Rightarrow a+bi \mid -i(1+i)^2 \Rightarrow a+bi \mid 1+i$

$\Rightarrow a+bi$ assoc $1+i$

## Quozienti per primi

$$\frac{\mathbb{Z}[i]}{(1+i)} \simeq \mathbb{F}_2 \qquad \frac{\mathbb{Z}[i]}{(p)\mathbb{Z}[i]} \simeq ? \qquad \frac{\mathbb{Z}[i]}{(a+bi)} \simeq ?$$

$a^2+b^2 = p \equiv 1 \ (4)$

Questi quozienti sono domini; anzi campi:

① in un PID ogni primo $\neq (0)$ e' massimale

② un dominio finito e' un campo. Questi quoz. sono finiti perché rappresentano i possibili resti nella divisione per l'elemento $\alpha$ per cui si quozienta

Resti $\subseteq \{ x \mid N(x) \leq N(\alpha) \}$ e' finito.

$$\frac{\mathbb{Z}[i]}{(p)} \simeq \mathbb{F}_{p^k} = \mathbb{F}_{p^2} \qquad p \equiv 3 \ (4)$$

Classi di resto: $\left\{ a+bi \;\middle|\; \begin{array}{l} 0 \leq a \leq p-1 \\ 0 \leq b \leq p-1 \end{array} \right\}$

$$\frac{\mathbb{Z}[i]}{(a+bi)} \underset{\uparrow}{\simeq} \mathbb{F}_{p^k} = \mathbb{F}_p \qquad (a+bi)(a-bi) = a^2+b^2 = p \equiv 1 \ (4)$$

$\bar{p} = 0$ in questo quoziente

$$\frac{\mathbb{Z}[i]}{(a+bi)} \simeq \frac{\mathbb{Z}[i]\,/\,(p)}{(a+bi)\,/\,(p)} \underset{\uparrow}{\simeq} \frac{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \simeq \mathbb{Z}/p\mathbb{Z}$$

come gruppi

$$\frac{\mathbb{Z}[i]}{(5)} = \mathbb{Z}/5\mathbb{Z} \cdot \bar{1} \oplus \mathbb{Z}/5\mathbb{Z} \cdot \bar{i}$$

$\frac{(a+bi)}{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$ come gruppo : $\left|\frac{(a+bi)}{(p)}\right| \in \{\cancel{1}, p, \cancel{p^2}\}$

Se è $1$ : $(a+bi) \neq (p) = \left((a+bi)(a-bi)\right)$

Se è $p^2$ : $\dfrac{\mathbb{Z}[i]/(p)}{(a+bi)/(p)} = (0) \Rightarrow (a+bi) = \mathbb{Z}[i]$

no perché $a+bi$ non è unità

**Oss** $\dfrac{\mathbb{Z}[i]}{(p)} \simeq \dfrac{\mathbb{Z}[i]}{\underbrace{(a+bi)}_{I}\underbrace{(a-bi)}_{J}} \overset{TCR}{\simeq} \dfrac{\mathbb{Z}[i]}{(a+bi)} \times \dfrac{\mathbb{Z}[i]}{(a-bi)} \simeq \mathbb{F}_p \times \mathbb{F}_p$

$I + J = (1)$

**Es** $A$ un PID, $I = (p)$ t.c. $A/I$ sia finito.

Allora $\left|A/I^n\right| = \left|A/I\right|^n$

**Dim** Consideriamo $A \xrightarrow{\cdot p} A \xrightarrow{\pi} A/I^2$ omom DI GRUPPI

$$(a+b)\cdot p = a\cdot p + b\cdot p$$

$$\ker\left(A \xrightarrow{p} A \xrightarrow{\pi} A/I^2\right) = \{a \mid p\cdot a \in I^2 = (p^2)\}$$

$$= \{a = pb\} = I$$

$$p\cdot a = p^2\cdot b$$

$$\operatorname{Imm}\left(A \xrightarrow{p} A \xrightarrow{\pi} A/I^2\right) = \pi(pA) = \pi(I) = I/I^2$$

Conclusione: $I/I^2 \simeq A/I$

Allora $A/I \simeq \dfrac{A/I^2}{I/I^2}$ $\quad |A/I| = \dfrac{|A/I^2|}{|I/I^2|} = \dfrac{|A/I^2|}{|A/I|}$

$$\Rightarrow \left|A/I\right|^2 = \left|A/I^2\right|$$

$$\left|\frac{I^k}{I^{k+1}}\right| = \left|A/I\right|$$

$$A \xrightarrow{p^k} A \longrightarrow A/p^{k+1}$$

Imm: $I^k/I^{k+1}$, ker: $I$

$$I^k/I^{k+1} \simeq A/I$$

Mostriamo la tesi per induz. su $k \geq 1$.

$$A/I^k \simeq \frac{A/I^{k+1}}{I^k/I^{k+1}} \Rightarrow \left|A/I^k\right| = \frac{\left|A/I^{k+1}\right|}{\left|I^k/I^{k+1}\right|}$$

$$\begin{array}{ccc} \left|A/I^k\right| & = & \dfrac{\left|A/I^{k+1}\right|}{\left|I^k/I^{k+1}\right|} \\ \text{ip. ind } \| & & \| \\ \left|A/I\right|^k & & \dfrac{\left|A/I^{k+1}\right|}{\left|A/I\right|} \end{array}$$

□

## Quozienti di $\mathbb{Z}[i]$

$$I = (z) = \left( u \cdot (1+i)^{e_2} \prod (a+bi)^{e_{a+bi}} \prod p^{e_p} \right)$$

$$\frac{\mathbb{Z}[i]}{I} \overset{TCR}{\simeq} \frac{\mathbb{Z}[i]}{(1+i)^{e_2}} \times \prod \frac{\mathbb{Z}[i]}{(a+bi)^{e_{a+bi}}} \times \prod \frac{\mathbb{Z}[i]}{(p)^{e_p}}$$

Considero gli ideali $(1+i)^{e_2}$, $(a+bi)^{e_{a+bi}}$, $(p)^{e_p}$

Se ne sommo 2 viene $(1)$:

$$(\alpha) + (\beta) = (\text{mcd}(\alpha, \beta))$$

$$\left| \mathbb{Z}[i]/I \right| = \left| \frac{\mathbb{Z}[i]}{(1+i)} \right|^{e_2} \times \prod \left| \frac{\mathbb{Z}[i]}{(a+bi)} \right|^{e_{a+bi}} \times \prod \left| \frac{\mathbb{Z}[i]}{(p)} \right|^{e_p}$$

↳ esercizio precedente

$$= N(1+i)^{e_2} \cdot \prod N(a+bi)^{e_{a+bi}} \cdot \prod N(p)^{e_p}$$

$$= N\left(u(1+i)^{e_2} \prod (a+bi)^{e_{a+bi}} \prod p^{e_p}\right) = N(z)$$

Es. applicazione Contare le soluz. intere di

$$x^2+y^2 = 5\cdot 7\cdot 11\cdot 13\cdot 17$$

$$(x+iy)(x-iy) = 7\cdot 11 \cdot (2+i)(2-i)\cdot(3+2i)(3-2i)(4+i)(4-i)$$

$7 \mid x+iy$ o $7 \mid x-iy$ in $\mathbb{Z}[i]$

$$x+iy = 7\cdot(a+bi) \Rightarrow 7 \mid x,\ 7 \mid y \Rightarrow 49 \mid x^2+y^2$$

$$x-iy = 7\cdot(a+bi)$$

$\Rightarrow$ no soluz.

Oss In generale: i primi $\equiv 3\ (4)$ devono comparire con esponente PARI.

$$x^2+y^2 = 5\cdot 7^2\cdot 11^2\cdot 13\cdot 17$$

$$7^2\cdot 11^2\cdot (2+i)(2-i)\cdot(3+2i)(3-2i)(4+i)(4-i)$$

$7|x,\quad 7|y,\quad 11|x,\quad 11|y$

Studiamo $\underset{\overset{\|}{(a+bi)(a-bi)}}{a^2+b^2} = (2+i)(2-i)(3+2i)(3-2i)(4+i)(4-i)$

$3+2i \mid a+bi \iff (a+bi) = (3+2i)(c+di) \quad \exists\, c+di \in \mathbb{Z}[i]$

$3-2i \mid a-bi \iff a-bi = (3-2i)(c-di)$

$$a^2+b^2 = (2+i)(2-i)(3+2i)(3-2i)(4+i)(4-i)$$

$$\parallel$$

$$(a+bi)(a-bi)$$

$$\begin{tikzcd}
(3+2i) \arrow[d] \arrow[dr] & (3-2i) \arrow[d] \arrow[dl] \\
(a+bi) & (a-bi)
\end{tikzcd}$$

Quanti sono quindi le soluz. a+bi ?

Sono $\underset{\substack{\uparrow \\ \text{n° di modi di} \\ \text{"distribuire" le} \\ \text{coppie}}}{8} \cdot \underset{\substack{\nwarrow \\ \text{n° di unita'}}}{4}$

Es piu' semplice $x^2+y^2 = 65 = (2+i)(2-i)(3+2i)(3-2i)$

$$(x+iy) = (2+i)(3+2i) = 4+7i$$

$$(x+iy) = (2+i)(3-2i) = 8-i$$

Es

$$\underset{(4+i)^3(4-i)^3}{\underset{\shortparallel}{17^3}} = x^2+y^2 = (x+iy)(x-iy)$$

$$x+iy = u \cdot (4+i)^j \cdot (4-i)^k$$

$$x-iy = u^{-1} \cdot (4-i)^j \cdot (4+i)^k$$

$$(4+i)^{j+k} (4-i)^{j+k}$$

# Coprimalità di ideali

$I, J$ coprimi vuol dire $I + J = (1)$

Siano $I, J, K$ tre ideali di un anello $A$.

(a) Se $I + J + K = A$, allora $I^n + J^n + K^n = A$

(b) $I + J = J + K = K + I = A$, allora $IJ + JK + KI = A$

**Oss** In $\mathbb{Z}$ : $I = (m)$, $J = (h)$, $K = (k)$

(a) $(m, h, k) = (1)$

$(m^n, h^n, k^n) = (1)$

(b) $(m, h) = (h, k) = (k, m) = 1$

$(mh, hk, km) = 1$

**Oss** $(12, \quad 8) = (4)$

Dim (b) $I + J = A \iff \exists\, i_1 \in I,\ j_1 \in J$ t.c.

$J + K = A$

$K + I = A$

$$\begin{cases} i_1 + j_1 = 1 & \\ j_2 + k_1 = 1 & j_2 \in J,\ k_1 \in K \\ k_2 + i_2 = 1 & k_2 \in K,\ i_2 \in I \end{cases}$$

$$(i_1 + j_1) \cdot (j_2 + k_1) \cdot (k_2 + i_2) = 1$$

$$\parallel$$

$$\underset{\substack{\cap \\ IJ,\, JK,\, KI}}{i_1 j_2 k_2} + \underset{\substack{\cap \\ JK}}{j_1 j_2 k_2} + \dots = 1$$

Ho scritto 1 come somma di el. di $IJ$, $JK$, $KI$

$\Rightarrow IJ + JK + KI = 1$

(a) $I + J + K = (1) \Rightarrow \exists\, i \in I,\ j \in J,\ k \in K$

$$i + j + k = 1$$

$$(i+j+k)^2 = 1$$

$$i^2 + j^2 + k^2 + 2ij + 2jk + 2ki$$

$$(i+j+k)^N = \sum_{x+y+z=N} \binom{N}{x,y,z} \underbrace{i^x j^y k^z}_{\in I^n \text{ o } J^n \text{ o } K^n}$$

$$\Leftarrow \max\{x, y, z\} \geq n$$

$x \geq n \qquad i^x j^y k^z = \underbrace{i^n}_{\in I^n} \cdot \left(i^{x-n} j^y k^z\right) \in I^n$

Se prendo $N \geq 3n$ $\qquad x+y+z = N \geq 3n$

$$\max\{x,y,z\} \geq \frac{x+y+z}{3} \geq n$$

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ e' PID, ma non euclideo

$$A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{ a+b\,\frac{1+\sqrt{-19}}{2} \;\middle|\; a,b\in\mathbb{Z} \right\}$$

Oss $\quad \mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right] \neq \left\{ a+b\,\frac{1+\sqrt{3}}{2} \;\middle|\; a,b\in\mathbb{Z} \right\}$

$$\left(\frac{(1+\sqrt{3})}{2}\right)^2 = \frac{1+3+2\sqrt{3}}{4}$$

$$= 1+\sqrt{3}/2 \notin \left\{a+b\,\frac{1+\sqrt{3}}{2} \middle| a,b\in\mathbb{Z}\right\}$$

$$1+\frac{\sqrt{3}}{2} = a + \frac{b+b\sqrt{3}}{2}$$

$$\Leftrightarrow \quad 2+\sqrt{3} = 2a+b+b\sqrt{3}$$

$1, \sqrt{3}$ sono $\mathbb{Q}$-lin. indip $\Leftarrow$ $\begin{cases} 2 = 2a+b \\ 1 = b \end{cases}$ $\quad 2a = 1$

$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$

Oss $\alpha := \frac{1+\sqrt{-19}}{2}$ ha pol. min.

$$\left(\alpha-\frac{1}{2}\right)^2 = -\frac{19}{4}$$

$$\alpha^2-\alpha+\frac{1}{4}+\frac{19}{4}=0$$

$$t^2-t+5=0$$

Consideriamo

$$\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{C}$$

$$p(x) \longmapsto p(\alpha)$$

$$(\ker \varphi) = \mathbb{Z}[x] \cap \{ f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0 \}$$

$$= \mathbb{Z}[x] \cap (x^2 - x + 5)\, \mathbb{Q}[x]$$

$$= (x^2 - x + 5)\, \mathbb{Z}[x]$$

$$\frac{\mathbb{Z}[x]}{(x^2 - x + 5)} \simeq \operatorname{imm} \varphi = \{ \varphi(a + bx) \} = \{ a + b\, \frac{1 + \sqrt{-19}}{2} \mid a, b \in \mathbb{Z} \}$$

└ classi di resto: $a + bx$
$a, b \in \mathbb{Z}$

Invece $\frac{1+\sqrt{3}}{2}$ ha pol. minimo $(x-1/2)^2 = 3/4$

$$x^2 - x - 1/2 = 0$$

$$2x^2 - 2x - 1$$

$\frac{\mathbb{Z}[x]}{(2x^2-2x-1)}$ contiene più classi di resto rispetto ad $\{a+bx \mid a,b \in \mathbb{Z}\}$

$x^k$

Torniamo a: $A = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$, non è dom. eucl.

$A^\times$ : consideriamo $N : A \longrightarrow \mathbb{N}$

$$a+b\omega \mapsto (a+b\omega)(a+b\overline{\omega})$$

$$= a^2 + b^2 \cdot 5 + ab$$

**Oss** Sia $u \in A^\times$. $\exists\, v \in A^\times$ t.c. $u \cdot v = 1$

$$N(u)N(v) = N(uv) = N(1) = 1$$

$$\Rightarrow N(u) = 1$$

$$a^2 + ab + 5b^2 = 1 \qquad \left(a + \tfrac{1}{2}b\right)^2 + \underbrace{\frac{19}{4}b^2}_{\leq 1} = 1 \Rightarrow b = 0$$

Uniche unità: $\pm 1$.

**Oss** Supponiamo di avere una norma euclidea

Consideriamo $\{ N(x) \mid x \in A \setminus A^\times \} \subset \mathbb{N}$

Sia $m$ il minimo di questo insieme e $x$ t.c. $N(x) = m$.

$\forall a \in A \quad \exists\, r \in \{0, \pm 1\}$ t.c. $a = x \cdot q + r$

$r = 0 \quad \vee \quad N(r) < N(x) = \min \{ N(y) : y \in A \setminus A^\times \}$

$\Rightarrow r \notin A \setminus A^\times \Rightarrow r \in A^\times$

Cioè: $0, 1, -1$ sono rappresentanti per $A/(x)$

$\{0, 1, -1\} \twoheadrightarrow A/(x) \Rightarrow A/(x) \simeq \mathbb{F}_2, \mathbb{F}_3$

$\{0, 1, 1+1\}$

In $A$, l'eqz. $t^2 - t + 5 = 0$ ha una soluz, cioè $\omega$

$$\omega^2 - \omega + 5 = 0 \text{ in } A$$

$$\Downarrow$$

$$\overline{\omega}^2 - \overline{\omega} + \overline{5} = 0 \text{ in } A/(x)$$

Dovrei avere che $t^2 - t + 5$ ha una radice in $\mathbb{F}_2$ o $\mathbb{F}_3$

Questo assurdo mostra che A non è euclideo.

Norma canonica  A dom. euclideo

$A^\times \rightsquigarrow N(a) = 0 \quad \forall a \in A^\times$

$A_1 = \{ a \in A \mid \forall b \in A \quad \exists q \in A \quad \exists r \in A^\times \cup \{0\}$ t.c.

$b = q \cdot a + r \} \rightsquigarrow N = 1$

$\{ a \in A \mid \forall b \in A \quad \exists q \in A \quad \exists r \in \{0\} \cup A^\times \cup A_1$

t.c. $b = q \cdot a + r \} \rightsquigarrow N = 2$
su $A_2 \setminus A_1$

In $\mathbb{Z}$ $\quad A^\times = \{\pm 1\} \quad A_1 = \{\pm 2, \pm 3\} \cup A^\times$

$A_2 = \{\pm 7, \pm 6, \pm 5, \pm 4\} \cup A_1$

# ESTENSIONI NORMALI

## Ripasso

$L/K$ estensione finita $\qquad K \subseteq \overline{K} \qquad K \subseteq L \subseteq \overline{K}$

$$\{ \varphi : L \longrightarrow \overline{K} \mid \varphi \text{ omom}, \ \varphi|_K = id \}$$

$L/K$ e' normale se $\varphi(L) = L$ per ogni $\varphi$

Es • $\mathbb{Q}(\sqrt[3]{2})$ non e' normale : $\{ \varphi : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \overline{\mathbb{Q}} \}$ ha $\varphi|_{\mathbb{Q}} = id$

3 elem., che mandano $\sqrt[3]{2}$ in $\underset{\varphi_1}{\sqrt[3]{2}}$, $\underset{\varphi_2}{\sqrt[3]{2} \cdot \zeta_3}$, $\underset{\varphi_3}{\sqrt[3]{2} \cdot \zeta_3^2}$

$\varphi_1(L) \subseteq \mathbb{R}$, $\varphi_2(L) \not\subseteq \mathbb{R}$, e $\underset{\mathbb{Q}(\sqrt[3]{2})}{\overset{\shortparallel}{L}}$ non e' est. normale

- $\mathbb{Q}(\sqrt{2})$ e' normale su $\mathbb{Q}$:

$$\varphi_1(a+b\sqrt{2}) = \varphi_1(a)+\varphi_1(b\sqrt{2}) = \varphi_1(a)+\varphi_1(b)\,\varphi_1(\sqrt{2}) = a+b\sqrt{2}$$

$$\varphi_2(a+b\sqrt{2}) = \quad \dots \quad = a-b\sqrt{2}$$

$$\left.\begin{aligned}\varphi_1(\mathbb{Q}(\sqrt{2})) &= \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}\\ \varphi_2(\mathbb{Q}(\sqrt{2})) &= \{a-b\sqrt{2} \mid a,b\in\mathbb{Q}\}\end{aligned}\right\} \Rightarrow$$

Se $L/K$ e' un'est. normale,

$$\varphi \in \{\varphi : L \longrightarrow \overline{K} \mid \varphi|_K = id,\ \varphi \text{ omom. anelli}\}$$

$\varphi$ iniettiva: $\ker\varphi \trianglelefteq L \Rightarrow \ker\varphi = \{0\}$

$\varphi(L) \subseteq L$ $\quad\quad \varphi : L \longrightarrow L$ e' surgettiva

(in quanto appl. lin.

iniettiva fra K-s.v. stessa dim)

$\{\varphi : L \to L\}$ si chiama il gruppo di Galois $Gal(L/K)$.

Esempi

- $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\varphi_+, \varphi_-\} \simeq \mathbb{Z}/_{2\mathbb{Z}}$

$\varphi_-(\sqrt{2}) = -\sqrt{2} \quad\quad \varphi_-(\varphi_-(\sqrt{2})) = \sqrt{2} \quad \Rightarrow \quad \varphi_- \circ \varphi_- = id = \varphi_+$

- $Gal(\underbrace{\mathbb{Q}(\sqrt{2}, \sqrt{3})}_{L}/\mathbb{Q}) \simeq ?$

$$\#\left\{\underset{\varphi|_{\mathbb{Q}} = id}{\varphi : L \longrightarrow \overline{\mathbb{Q}}}\right\} = [L : \mathbb{Q}] = 4$$

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

Base di $L$ su $\mathbb{Q}$ ? $\quad 1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

$$\varphi(1) = 1$$

$$\varphi(\sqrt{2}) = \textcircled{$\pm$}\sqrt{2}$$

($\sqrt{2}$ deve andare in una radice di $x^2 - 2$)

$$\varphi(\sqrt{3}) = \textcircled{$\pm$}\sqrt{3}$$

$$\varphi(\sqrt{6}) = \pm\sqrt{6}$$

$$\varphi(\sqrt{6}) = \varphi(\sqrt{2})\,\varphi(\sqrt{3})$$

$$\#\{\varphi : L \longrightarrow \overline{\mathbb{Q}}\} = 4$$

Siccome ho AL PIÙ 4 immersioni, tutte le $2 \times 2$ scelte di segni devono dare un omomorfismo.

Chiamiamo $\varphi_{\pm_1, \pm_2}(\sqrt{2}) = \pm_1 \cdot \sqrt{2}$ queste immersioni.

$$\varphi_{\pm_1, \pm_2}(\sqrt{3}) = \pm_2 \cdot \sqrt{3}$$

$$\{ \underset{\substack{\shortparallel \\ id}}{\varphi_{+,+}} \quad \varphi_{+,-} \quad \varphi_{-,+} \quad \varphi_{-,-} \} \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

- $K(\sqrt{a})/K$ est. quadr $\rightsquigarrow$ sempre ~~di Galois~~ normale in quanto c.d.s. di $x^2 - a$. Il grp. di Gal è $\mathbb{Z}/2\mathbb{Z}$

- $K = \text{c.d.s.}\ (x^3 - 2 \text{ su } \mathbb{Q}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

$[K : \mathbb{Q}] = 6$

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

Chi sono le immersioni di $K$ in $\overline{\mathbb{Q}}$ che fissano $\mathbb{Q}$?

$\varphi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta_3, \sqrt[3]{2} \cdot \zeta_3^{-1}\}$ $\quad x^3 - 2$

$\varphi(\zeta_3) \in \{\zeta_3, \zeta_3^{-1}\}$ $\quad x^2 + x + 1 \quad \zeta_3, \zeta_3^{-1}$

Tutte le scelte sono possibili, perché devono esistere 6 omomorfismi

Alternativa: $K = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha_1}, \underbrace{\sqrt[3]{2} \cdot \zeta_3}_{\alpha_2}, \underbrace{\sqrt[3]{2} \cdot \zeta_3^2}_{\alpha_3})$

$$\left.\begin{array}{l} \varphi(\alpha_1) \in \{\alpha_1, \alpha_2, \alpha_3\} \\ \varphi(\alpha_2) \in \{\alpha_1, \alpha_2, \alpha_3\} \\ \varphi(\alpha_3) \quad " \qquad\qquad " \end{array}\right\} \Rightarrow \begin{array}{l} \varphi \text{ e' det. da} \\ \varphi|_{\{\alpha_1, \alpha_2, \alpha_3\}} \in S_{\{\alpha_1, \alpha_2, \alpha_3\}} \end{array}$$

$$\Rightarrow \quad \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_{\{\alpha_1, \alpha_2, \alpha_3\}}$$

$$\varphi \longmapsto \varphi|_{\{\alpha_1, \alpha_2, \alpha_3\}}$$

$|\mathrm{Gal}(K/\mathbb{Q})| = 6$, si immerge in $S_3 \Rightarrow$ e' $S_3$.

Consideriamo $r(\sqrt[3]{2}) = \sqrt[3]{2} \cdot \zeta_3$

$r(\zeta_3) = \zeta_3$

$s(\sqrt[3]{2}) = \sqrt[3]{2}$

$s(\zeta_3) = \zeta_3^{-1}$

$s =$ coniugio cpx ristretto a $K$

$s^2 = id$

$$r^3(\zeta_3) = \zeta_3$$

$$r^3(\sqrt[3]{2}) = r^2(\sqrt[3]{2} \cdot \zeta_3) =$$

$$= r^2(\sqrt[3]{2}) \cdot r^2(\zeta_3)$$

$r(\zeta_3)=\zeta_3$ $\overset{\curvearrowright}{=} r(\sqrt[3]{2} \cdot \zeta_3) \cdot \zeta_3 = r(\sqrt[3]{2}) \cdot \zeta_3 \cdot \zeta_3$

$$= \sqrt[3]{2} \cdot \zeta_3^{\,3} = \sqrt[3]{2}$$

$srs^{-1} \overset{?}{=} r^{-1}$ : mostriamo che hanno lo stesso effetto sui generatori

① $srs^{-1}(\sqrt[3]{2}) \overset{?}{=} r^{-1}(\sqrt[3]{2})$

② $srs^{-1}(\zeta_3) \overset{?}{=} r^{-1}(\zeta_3) \iff sr(\zeta_3^{-1}) = \zeta_3$

$\iff s(\zeta_3^{-1}) = \zeta_3$

$\iff \zeta_3 = \zeta_3$ $\boxed{\text{OK}}$

① $srs^{-1}(\sqrt[3]{2}) = sr(\sqrt[3]{2}) = s(\sqrt[3]{2}\cdot\zeta_3) = \sqrt[3]{2}\cdot\zeta_3^{-1}$

$r^{-1}(\sqrt[3]{2}) = \sqrt[3]{2}\cdot\zeta_3^{-1}$ $\boxed{\text{OK}}$

- $f(x) = x^4 - 5x^2 + 9$. Cds e il gruppo di Gal su $\mathbb{Q}$ e su $\mathbb{F}_{11}$.

Chiamiamo $t = x^2$. $t^2 - 5t + 9 = 0$

$$t_{1,2} = \frac{5 \pm \sqrt{-11}}{2}$$

$$x_1, x_2, x_3, x_4 = \pm \sqrt{\frac{5 \pm \sqrt{-11}}{2}} \quad \text{in } \mathbb{C}$$

In $\mathbb{F}_{11}$ ho trovato $t_{1,2} = \frac{5 \pm \sqrt{-11}}{2} = 5/2 = 8$ in $\mathbb{F}_{11}$

$$t^2 - 5t + 9 = t^2 + 6t + 9 = (t+3)^2$$

Cds su $\mathbb{F}_{11}$ è $\mathbb{F}_{11}(\pm\sqrt{8}) = \mathbb{F}_{11}(\sqrt{8}) = \mathbb{F}_{11}(\sqrt{2})$

$\Gamma$ $\sqrt{2} \notin \mathbb{F}_{11}$ : $\sqrt{8} = \sqrt{-3}$ $3 = 5^2$ in $\mathbb{F}_{11}$

$-1$ non quadr. in $\mathbb{F}_{11}$

$\sqrt{2} \notin \mathbb{F}_{11}$ : $2^{\frac{11-1}{2}} \equiv 32 \equiv -1 \ (11) \Rightarrow 2$ non quadr.

↳ Il cds è $\mathbb{F}_{11^2}$ e Gal $\simeq \mathbb{Z}/2\mathbb{Z}$.

Torniamo su $\mathbb{Q}$.

$$K := \mathbb{Q}\left(\pm\sqrt{\frac{5 \pm \sqrt{-11}}{2}}\right) \qquad [K:\mathbb{Q}] = ?$$

$\boxed{\text{NO :}}$

$$\varphi\left(\sqrt{\frac{5+\sqrt{-11}}{2}}\right) \in \{x_1, \textcircled{$x_2$}, x_3, x_4\}$$

$x_3 = -x_1$

$x_4 = -x_2$

$$\varphi\left(\sqrt{\frac{5-\sqrt{-11}}{2}}\right) \in \{x_1, \cancel{x_2}, x_3, \cancel{x_4}\}$$

QUESTO NON DICE CHE CI SONO 8 SCELTE

E' vero che $f(x) = x^4 - 5x^2 + 9$ e' irriducibile? [✓ Sì]

$= f_1(x) \cdot f_3(x)$ × no

$= f_2(x) \cdot f_2'(x)$

$(x - x_1)(x - x_2) \notin \mathbb{Q}[x]$

$(x - x_1)(x - x_3) \notin \mathbb{Q}[x]$

$(x - x_1)(x - x_4) \notin \mathbb{Q}[x]$

$$\begin{tikzcd}
& K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(x_1) \arrow[dr, dash, "2"'] \arrow[ddr, dash, bend right, "4"'] & & \mathbb{Q}(x_2) \arrow[dl, dash, "2"] \\
& \mathbb{Q}(\sqrt{-11}) \arrow[d, dash, "2"'] & \\
& \mathbb{Q} &
\end{tikzcd}$$

$\mathbb{Q}(x_1) = \mathbb{Q}(x_2)$

$\iff$ $x_1^2 \cdot x_2^2$ e' un quadr.

in $\mathbb{Q}(\sqrt{-11})$

$\iff$ $9$ e' un quadr ✓

$$\sqrt{\frac{5+\sqrt{-11}}{2}} \cdot \sqrt{\frac{5-\sqrt{-11}}{2}} = \sqrt{9} = 3$$

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1, 3/x_1) = \mathbb{Q}(x_1)$$

$K = \mathbb{Q}(x_1)$ ha grado 4 su $\mathbb{Q}$

$\Rightarrow |Gal(K/\mathbb{Q})| = 4$

$\varphi \in Gal(K/\mathbb{Q}) \qquad \varphi(x_1) \in \{x_1, x_2, x_3, x_4\}$

Sia $\varphi_i$ quello che manda $x_1$ in $x_i$

$\varphi_1 = id$

$$\left[\begin{array}{l} \varphi_2(x_1) = x_2 \qquad\qquad\qquad\qquad \varphi_2^{\,2} = id \\ \varphi_2(x_2) = \varphi_2\left(\frac{3}{x_1}\right) = \varphi_2(3)/\varphi_2(x_1) = 3/x_2 = x_1 \\ \varphi_2(x_3) = \varphi_2(-x_1) = -\varphi_2(x_1) = -x_2 = x_4 \\ \varphi_2(x_4) = x_3 \end{array}\right.$$

$$\left[\begin{array}{l} \varphi_3(x_1) = x_3 = -x_1 \qquad\qquad \varphi(x_3) = x_1 \\ \varphi_3(x_2) = \varphi_3\left(\frac{3}{x_1}\right) = \frac{3}{-x_1} = -x_2 = x_4 \qquad \varphi_3(x_4) = x_2 \end{array}\right.$$

Conclusione: $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$

- $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/_{n}\mathbb{Z}$

$\mathbb{F}_{p^n}/\mathbb{F}_p$ e' normale: $\mathbb{F}_{p^n}$ = cds di $x^{p^n}-x$ su $\mathbb{F}_p$

<u>Def.</u> L' AUTOMORFISMO DI FROBENIUS e' $\varphi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$

$$x \longmapsto x^p$$

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$$
$$\varphi(x+y) = (x+y)^p = x^p + y^p = \varphi(x) + \varphi(y)$$

Che ordine ha? $\varphi^k(x) = x \iff x^{p^k} = x \quad \forall\, x \in \mathbb{F}_{p^n}$

$t^{p^k} - t$ ha $\geq p^n$ radici

$\Rightarrow \quad k \geq n \quad \Rightarrow \quad \mathrm{ord}\, \varphi \geq n$

$\varphi \in \mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$, che ha $n$ elem. $\Rightarrow \mathrm{ord}\, \varphi \mid n$

Allora $\mathrm{ord}\, \varphi = n$ e $\varphi$ e' un generatore.

Oss $\mathbb{F}_{p^2} / \mathbb{F}_p$. $\quad \varphi : x \longmapsto x^p \quad\quad p \neq 2$

$$\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{b}) \longrightarrow \overline{\mathbb{F}_p}$$

$$\sqrt{b} \longmapsto \sqrt{b}, -\sqrt{b}$$

$$(x + y\sqrt{b})^p = x^p + y^p \sqrt{b}^p = x + y \cdot b^{1/2} \cdot \underbrace{b^{\frac{p-1}{2}}}_{-1 \text{ per criterio Eulero}}$$

$$= x - y\sqrt{b}$$

# Polinomi ciclotomici $(n \geq 2)$

$X^n - 1 \in \mathbb{Q}[x]$ $\qquad$ $X^p - 1 = (x-1)\underbrace{(x^{p-1} + \dots + x + 1)}_{\text{irriducibile per Eisenstein}}$

$\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$

(a) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è normale: è il cdS $x^n - 1$

$$\mathbb{Q}(\zeta_n{}^k \mid k \geq 1) = \mathbb{Q}(\zeta_n)$$

(b) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \varphi(n)$

Sia $\psi : \mathbb{Q}(\zeta_n) \longrightarrow \overline{\mathbb{Q}}$. $\psi$ è determinata da $\psi(\zeta_n)$.

$$\psi(\zeta_n)^n = \psi(\zeta_n{}^n) = \psi(1) = 1 \Rightarrow \psi(\zeta_n) = \zeta_n^k$$

$$k \in \{\cancel{0}, \dots, n-1\}$$

Escludiamo i $k$ t.c. $(k, n) = d > 1$

$$\begin{aligned} \psi(\zeta_n)^{n/d} &= \zeta_n^{k \cdot n/d} = \zeta_n^{(k/d) \cdot n} = 1 = \psi(1) \\ &\parallel \\ \psi(\zeta_n^{n/d}) & \Rightarrow \zeta_n^{n/d} = 1 \Rightarrow d = 1 \end{aligned}$$

(c) $X^n - 1$ è SEPARABILE su un campo $K \iff \mathrm{caratt}(K) \nmid n$

$\llcorner$ tutte le radici distinte in $\overline{K}$.

In char $= 0$ è separabile, OK

Se char $K = p > 0$, radici multiple in $\overline{K} \iff$

$$(X^n - 1,\ nX^{n-1}) \neq (1)$$

Se $p \nmid n$: $(x^n - 1, nx^{n-1}) = (x^n - 1, x^{n-1}) = (1)$

Se $p \mid n$: $(x^n - 1, 0) \neq (1)$

$$(x^n - 1) = (x^{n/p} - 1)^p$$

(d) $f(x) :=$ pol. minimo di $\zeta_n$, $p \nmid n$

$g(x) :=$ pol. minimo di $\zeta_n^p$

$$f(x) \text{ divide } \underbrace{g(x^p)}_{h(x)} \qquad h(\zeta_n) = g(\zeta_n^p) = 0$$

(e) Supponiamo per assurdo $f(x) \neq g(x)$. Allora

$$f(x)\, g(x) \mid x^n - 1 \quad \text{in } \mathbb{Q}[x]$$

$$\begin{cases} f(x) \mid x^n - 1 \quad \leftarrow \quad \zeta_n \text{ radice} \\ g(x) \mid x^n - 1 \quad \leftarrow \quad \zeta_n^p \text{ radice} \end{cases}$$

$$(f(x), g(x)) = (1)$$

$$\Rightarrow \quad f(x)\, g(x) \mid x^n - 1 \quad \text{in } \mathbb{Q}[x]$$

$$\text{in } \mathbb{Z}[x] \quad (\text{Gauss})$$

$$x^n - 1 = f(x) \cdot g(x) \cdot q(x) \quad \text{in } \mathbb{Z}[x]$$

$(f)$ $$x^n - 1 = f(x) \cdot g(x) \cdot q(x) \quad \text{in } \mathbb{F}_p[x]$$

$$f(x) \mid g(x^p) \quad \text{in } \mathbb{Z}[x] \qquad g(x^p) = f(x) \cdot r(x) \text{ in } \mathbb{F}_p[x]$$

$$g(x)^p = f(x) \cdot r(x) \quad \text{in } \mathbb{F}_p[x]$$

Sia $\alpha \in \overline{\mathbb{F}_p}$ una radice di $f(x)$ $\Rightarrow$ $g(\alpha)^p = f(\alpha)\, r(\alpha) = 0$

$\Rightarrow g(\alpha)^p = 0 \Rightarrow g(\alpha) = 0$

$\alpha$ e' radice almeno doppia di $f(x) \cdot g(x) \mid x^n - 1$

$\Rightarrow \alpha$ " " " " $x^n - 1$

Ma $p \nmid n$ $\Rightarrow$ $x^n - 1$ non ha radici multiple $\Rightarrow$ assurdo.

Abbiamo dim. che: $\zeta_n$ e $\zeta_n^p$ hanno lo stesso pol. min, $\forall p$ primo, $p \nmid n$

$\zeta_n$, $\zeta_n^{p_1}$, $(\zeta_n^{p_1})^{p_2}$, $\zeta_n^{p_1 p_2 p_3}$ ... hanno tutte lo stesso pol. minimo.

$\Rightarrow$ $\zeta_n$ e $\zeta_n^k$ hanno lo stesso pol. minimo $\forall k$ coprimo con $n$.

Detto ancora $f(x)$ il pol. min $\zeta_n$:

- $\deg f(x) \geq \# \{ \zeta_n^k : (k,n)=1 \} = \varphi(n)$

$$\begin{array}{c} \deg f(x) \\ \shortparallel \\ [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \varphi(n) \end{array} \qquad \Rightarrow \deg f(x) = \varphi(n)$$

- $|Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

Gli elementi sono tutti e soli gli omom.

$$\psi_k(\zeta_n) = \zeta_n^k \qquad (k,n)=1$$

- $\psi_k \circ \psi_{k'} (\zeta_n) = \psi_k (\zeta_n^{k'}) = \psi_k (\zeta_n)^{k'} = \zeta_n^{kk'}$

$\psi_{k \cdot k'} (\zeta_n)$

**Teo** $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$

$x^{\frac{p-1}{2}} = 1$ $\qquad (\alpha^2)^{\frac{p-1}{2}} = \alpha^{p-1} = 1$

$\mathbb{F}_p^\times = Q \sqcup NQ$ $\qquad t^{\frac{p-1}{2}} \neq 1$ $\qquad (t^{\frac{p-1}{2}})^2 = 1$

$$\Phi : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$$
$$x \longmapsto x^2$$

$\mathrm{Imm}\, \Phi = Q$ $\qquad |Q| = \frac{p-1}{2}$

Titolo nota

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

$K := \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ $\qquad L = \mathbb{Q}(\sqrt[3]{2} + \zeta_3) \subseteq K$

Ricordiamoci che $\{\varphi : K \longrightarrow \overline{\mathbb{Q}} \text{ imm.}\}$ ha 6 elementi.

Mostreremo che $[L : \mathbb{Q}] = 6$.

Quante sono le immersioni $\varphi : L \longrightarrow \overline{\mathbb{Q}}$ ? $\quad [L : \mathbb{Q}]$

Oss. Sia $E$ un'est. finita di $\mathbb{Q}$, $\varphi : E \hookrightarrow \overline{\mathbb{Q}}$.

È sempre vero che $\varphi|_{\mathbb{Q}} = id$: infatti $\varphi(1) = 1$ perché $\varphi$ hom. anelli; $\varphi(n) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1) = n$

$$\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)} = a/b$$

$$\varphi(-1) = -1$$

$$\Rightarrow \quad \varphi(q) = q \quad \forall q \in \mathbb{Q}$$

L

Il n° di immersioni $L \hookrightarrow \overline{\mathbb{Q}}$ e' anche il grado del pol. minimo di $\sqrt[3]{2} + \zeta_3$ su $\mathbb{Q}$.

Sappiamo che ogni immersione $L \hookrightarrow \overline{\mathbb{Q}}$ si estende ad un'imm. $K \hookrightarrow \overline{\mathbb{Q}}$

$$\begin{tikzcd} K \arrow[rd, hook] \arrow[d, dash] & \\ L \arrow[r, hook] \arrow[d, dash] & \overline{\mathbb{Q}} \\ \mathbb{Q} & \end{tikzcd}$$

$$\{ \psi : L \hookrightarrow \overline{\mathbb{Q}} \} = \{ \varphi|_L \mid \varphi : K \hookrightarrow \overline{\mathbb{Q}} \}$$

Per mostrare che $L$ ha 6 immersioni in $\overline{\mathbb{Q}}$ basta dim. che le 6 immersioni "note" di $K$ in $\overline{\mathbb{Q}}$ restano distinte quando le restringo ad $L$.

Chiamiamo $\varphi_{i,j} : K \hookrightarrow \overline{\mathbb{Q}}$ l'imm. che manda

$$\sqrt[3]{2} \longmapsto \sqrt[3]{2} \cdot \zeta_3^{\,i}$$

$$i = 0, 1, 2$$

$$\zeta_3 \longmapsto \zeta_3^{\,j}$$

$$j = 1, -1$$

Ci chiediamo se $\varphi_{i,j}(\sqrt[3]{2} + \zeta_3) = \varphi_{m,n}(\sqrt[3]{2} + \zeta_3)$

$$\sqrt[3]{2} \cdot \zeta_3^{\,i} + \zeta_3^{\,j} = \sqrt[3]{2} \cdot \zeta_3^{\,m} + \zeta_3^{\,n}$$

$$\sqrt[3]{2} \cdot \underbrace{\left(\zeta_3^{i} - \zeta_3^{m}\right)}_{} = \zeta_3^{n} - \zeta_3^{j}$$

Se è $\neq 0$:

$$\mathbb{Q}(\sqrt[3]{2}) \ni \underset{\in \mathbb{Q}}{\sqrt[3]{2}} = \frac{\zeta_3^{n} - \zeta_3^{j}}{\zeta_3^{i} - \zeta_3^{m}} \in \mathbb{Q}(\zeta_3)$$

NO, assurdo

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}) & & \mathbb{Q}(\zeta_3) \\
& \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

[ $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$ per ragioni di grado ]

$\zeta_3^{i} - \zeta_3^{m} = 0$ e $\zeta_3^{n} = \zeta_3^{j}$ $\Rightarrow$ $i = m$, $j = n$

Cioè abbiamo dim. che la funzione

$$\{\varphi : K \hookrightarrow \overline{\mathbb{Q}}\} \longrightarrow \{\varphi|_L : L \hookrightarrow \overline{\mathbb{Q}}\}$$

è iniettiva

$$\Rightarrow \underset{\substack{\| \\ [L:\mathbb{Q}]}}{\#\{\psi : L \hookrightarrow \overline{\mathbb{Q}}\}} \geq \#\{\varphi : K \hookrightarrow \overline{\mathbb{Q}}\} = 6$$

$$[L:\mathbb{Q}] = [K:\mathbb{Q}] \Rightarrow L = K \qquad \square$$

Oss

$$\underbrace{\mathbb{Q}(\sqrt[3]{2})}_{\subseteq \mathbb{R}} \cap \underbrace{\mathbb{Q}(\zeta_3)}_{\substack{\text{grado } 2 \\ \not\subseteq \mathbb{R}}} = \mathbb{Q}$$

**Oss** Chi è il pol. min. di $\sqrt[3]{2} + \zeta_3 =: \beta$?

È quel polinomio che ha per radici $\{\psi(\beta) \mid \psi : L \hookrightarrow \overline{\mathbb{Q}}\}$

$$\rightsquigarrow \mu_\beta(x) = \prod_{i=0}^{2} \prod_{j=1}^{2} \left(x - \left(\sqrt[3]{2} \cdot \zeta_3^{\,i} + \zeta_3^{\,j}\right)\right)$$

**Fatto (vero ma non dimostrato)**

$$\begin{tikzcd}
& \mathbb{Q}(\alpha,\beta) & \\
\mathbb{Q}(\alpha) \arrow[ur, dash] & & \mathbb{Q}(\beta) \arrow[ul, dash] \\
& \mathbb{Q} \arrow[ul, dash, "m"] \arrow[ur, dash, "n"'] &
\end{tikzcd}$$

Teo: $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$

$(m, n) = 1$

## Un polinomio con Gal $\simeq \mathbb{Z}/3\mathbb{Z}$

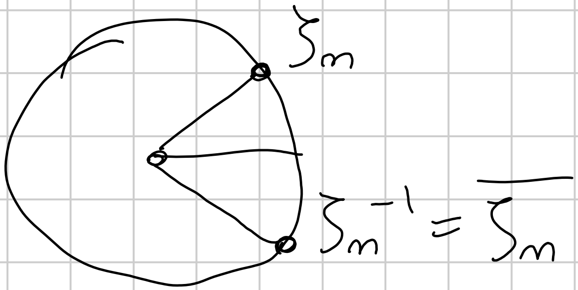
$$\begin{tikzcd}
\mathbb{Q}(\zeta_7) \arrow[d, dash, squiggly] & \\
\mathbb{Q}(\zeta_7+\zeta_7^{-1}) \arrow[d, dash, squiggly] \arrow[r, phantom, "\overset{?}{=}"] & \mathbb{Q}(\zeta_7)\cap\mathbb{R} \\
\mathbb{Q} &
\end{tikzcd}$$

$$G := \mathrm{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right) \simeq (\mathbb{Z}/7\mathbb{Z})^\times$$

$$\zeta_7 \longmapsto \zeta_7^{k} \qquad (k,7)=1$$

$\alpha := \zeta_7 + \zeta_7^{-1}$ $\qquad L := \mathbb{Q}(\alpha)$ $\qquad E = \mathbb{Q}(\zeta_7)\cap\mathbb{R}$

Oss. $L \subseteq E$ : $\quad L \subseteq \mathbb{Q}(\zeta_7)$, $\quad L \subseteq \mathbb{R}$ : $\zeta_7 + \zeta_7^{-1} = \zeta_7 + \overline{\zeta_7} \in \mathbb{R}$



Qual è il grado $[E : \mathbb{Q}]$? Divide 6

$1$
$2$
$3$
$6$

Vorremmo che fosse 3.

Dico che $[\mathbb{Q}(\zeta_7) : E] \leq 2$:

$$\zeta_7 + \zeta_7^{-1} = \alpha \in E$$

$$\zeta_7^2 + 1 - \alpha \cdot \zeta_7 = 0$$

$$X^2 - \alpha X + 1 \in E[x]$$

↳ ha $\zeta_7$ come radice

$\Rightarrow$ pol. min. di $\zeta_7$ su $E$ ha grado $\leq 2$

$\Rightarrow [\mathbb{Q}(\zeta_7) : E] \leq 2$

Se $[\mathbb{Q}(\zeta_7) : E] = 1 \Rightarrow \underset{\mathbb{R}}{\underset{\cap}{E}} = \underset{\mathbb{R}}{\underset{\not\subset}{\mathbb{Q}(\zeta_7)}} \Rightarrow$ assurdo.

$$\begin{tikzcd} \mathbb{Q}(\zeta_7) \arrow[d, dash, "2"] \arrow[dd, bend right=60, dash, "6"'] \\ E \arrow[d, dash, "3"] \\ \mathbb{Q} \end{tikzcd}$$

**Oss** $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2 \quad \forall n \geq 3$

Dim. Osservo che $\zeta_n + \zeta_n^{-1} \in \mathbb{Q}(\zeta_n) \cap \mathbb{R}$, lo chiamo $\alpha$.

Il pol. $x^2 + 1 - \alpha x$ ha radici $\zeta_n, \zeta_n^{-1}$

$\Rightarrow$ $\zeta_n$ soddisfa eqz. su $\mathbb{Q}(\zeta_n) \cap \mathbb{R}$ di grado 2

$\Rightarrow$ $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] \leq 2$.

Se il grado fosse 1, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n) \cap \mathbb{R} \Rightarrow \zeta_n \in \mathbb{R}$

$\Rightarrow n \leq 2$ □

$$\begin{tikzcd}
\mathbb{Q}(\zeta_7) \arrow[d, dash, "\le 2"'] \arrow[dd, dash, bend left=60, "\le 2"] & \\
\mathbb{Q}(\zeta_7)^+ := \mathbb{Q}(\zeta_7) \cap \mathbb{R} \arrow[d, equal] & \\
\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \arrow[d, dash] & \\
\mathbb{Q} &
\end{tikzcd}$$

$\alpha := \zeta_7 + \zeta_7^{-1}$

Chi è il pol. min di $\zeta_7 + \zeta_7^{-1}$? È il pol che ha come radici $\varphi(\zeta_7 + \zeta_7^{-1})$ al variare di $\varphi$ fra le imm. $\varphi : \mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$

Ogni $\varphi$ è della forma $\psi|_{\mathbb{Q}(\alpha)}$, dove $\psi : \mathbb{Q}(\zeta_7) \hookrightarrow \overline{\mathbb{Q}}$

Quindi: le radici $\mu_\alpha(x) \in \mathbb{Q}[x]$ sono $\psi_k(\zeta_7 + \zeta_7^{-1})$

al variare di $\psi_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$

$$\overset{\shortparallel}{(\zeta_7 \longmapsto \zeta_7^{k})}$$

$$\left\{ \underset{k=1,\dots,6}{\psi_k(\zeta_7 + \zeta_7^{-1})} \right\} = \left\{ \zeta_7^{k} + \zeta_7^{-k} \;\middle|\; k=1,\dots,6 \right\}$$

$$= \left\{ \begin{array}{ll} \zeta_7 + \zeta_7^{-1} & k=1,6 \\ \zeta_7^{2} + \zeta_7^{-2} & k=2,5 \\ \zeta_7^{3} + \zeta_7^{-3} & k=3,4 \end{array} \right\}$$

Siccome $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$, $\mu_\alpha(x)$ deve avere 3 radici → deve essere

$$\mathbb{Q}[x] \ni (x-(\zeta_7+\zeta_7^{-1}))(x-(\zeta_7^{2}+\zeta_7^{-2}))(x-(\zeta_7^{3}+\zeta_7^{-3}))$$

Coeff. grado 2: $-(\zeta_7+\zeta_7^{-1}+\zeta_7^{2}+\zeta_7^{-2}+\zeta_7^{3}+\zeta_7^{-3})$

$$= -\zeta_7^{-3}\big(\underbrace{\zeta_7^{4}+\zeta_7^{2}+\zeta_7^{5}+\zeta_7+\zeta_7^{6}+1}_{-\zeta_7^{3}}\big)=1$$

Pol. min $\zeta_7$: $1+x+x^2+\dots+x^6$

$$x^3+x^2-2x-1=0$$

$$\zeta_7^6+\zeta_7^5+\zeta_7^4+\zeta_7^3+\zeta_7^2+\zeta_7+1=0$$

$$\underbrace{\zeta_7^3 + \frac{1}{\zeta_7^3}}_{\alpha^3 - 3\alpha} + \underbrace{\zeta_7^2 + \frac{1}{\zeta_7^2}}_{(\alpha^2 - 2)} + \underbrace{\zeta_7 + \frac{1}{\zeta_7}}_{\alpha} + \underbrace{1}_{1} = 0 \qquad \alpha^3 + \alpha^2 - 2\alpha - 1 = 0$$

$$\alpha^3 = \zeta_7^3 + 3\zeta_7^2\zeta_7^{-1} + 3\zeta_7\zeta_7^{-2} + \zeta_7^{-3} = \zeta_7^3 + \zeta_7^{-3} + 3\alpha$$

**Oss** $p(x) := x^3 + x^2 - 2x - 1$ ha grp. di Galois $\simeq \mathbb{Z}/3\mathbb{Z}$

Basta dim. che il suo campo di spezz. è $\mathbb{Q}(\alpha)$

⌜ Se sappiamo questo: $|\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ ⌟

Sotto-oss: $\zeta_7^{k} + \zeta_7^{-k} \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$

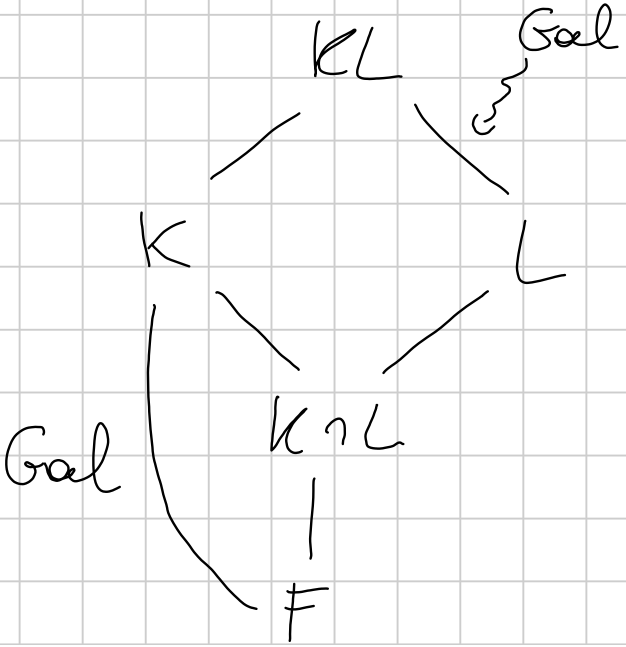
(perché $x^k + 1/x^k$ e' un pol. in $x + 1/x$)

## Gruppo di Galois del traslato

$K/F$ est di Galois (finita), $L/F$ est. finita

(1) $KL/L$ e' di Galois

(2) $\mathrm{Gal}(KL/L) \simeq \mathrm{Gal}(K/L \cap K)$



(1) $K/F$ Gal $\rightsquigarrow$ $K = F(\alpha_1, \dots, \alpha_n)$

dove $\alpha_1, \dots, \alpha_n$ sono tutte le radici di un certo $p(x) \in F[x]$

$KL = L(\alpha_1, \dots, \alpha_n)$ è il c.d.s. di $p(x)$ su $L$

(2) $R : Gal(KL/L) \longrightarrow Gal(K/L \cap K)$

$\quad\; \rotatebox{90}{$\in$}\; \varphi \qquad\qquad\qquad \varphi|_K : K \hookrightarrow \overline{F}$ $\quad\left(\begin{array}{l}\text{Oss:}\\ \varphi|_K(K) = K\end{array}\right)$

un elem. qui è un'immersione $KL \hookrightarrow \overline{F}$ che fissa $L$

L'omomorfismo $R$ è iniettivo?

Se $R(\varphi) = id \iff \begin{cases} \varphi|_K = id \\ \varphi|_L = id \end{cases} \iff \varphi = id$ perché $\varphi \in Gal(KL/L)$

L'omomorfismo $R$ è surgettivo? Lo vedremo quando avremo maggiori strumenti

**Cor.** $K/F$ di Galois e $L/F$ qualsiasi (finite)

Se $L \cap K = F$, allora $[KL : F] = [K : F]\,[L : F]$

$$\underset{\substack{\parallel \\ [KL : L]}}{\mathrm{Gal}\left(KL/L\right)} \simeq \mathrm{Gal}\left(K/L\cap K\right) = \underset{\substack{\parallel \\ [K : F]}}{\mathrm{Gal}\left(K/F\right)}$$

$$\begin{tikzcd}
 & KL \arrow[dl, dash] \arrow[dr, dash, "\mathrm{Gal}"] & \\
K \arrow[dr, dash, "\mathrm{Gal}"'] & & L \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

$$[KL : F] = [KL : L]\,[L : F] = [K : F] \cdot [L : F]$$

**Oss**

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

$$\begin{tikzcd}
K \arrow[dr, dash, "\mathrm{Gal}"'] & & F \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

# Gruppo di Galois del composto

$K_1, K_2$ due est. di Gal di $F$

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash, "\mathrm{Gal}"'] \arrow[dr, dash, "\mathrm{Gal}"] \arrow[dd, dash, "\mathrm{Gal}"] & \\
K_1 \arrow[dr, dash, "\mathrm{Gal}"'] & & K_2 \arrow[dl, dash, "\mathrm{Gal}"] \\
 & F &
\end{tikzcd}$$

$K_1K_2/F$ è di Gal: cds di $p_1(x)\,p_2(x)$

$K_1$ = cds di $p_1(x)$

$K_2$ = " " $p_2(x)$

(1) $\mathrm{Gal}(K_1K_2/F) \hookrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$

(2) Questo omom. è surg $\iff K_1 \cap K_2 = F$

$$(1) \qquad \begin{array}{ccc} \mathrm{Gal}(K_1K_2/F) & \hookrightarrow & \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \\ \varphi & \longmapsto & \varphi|_{K_1} \qquad \varphi|_{K_2} \end{array}$$

Se $\varphi|_{K_1} = id$ e $\varphi|_{K_2} = id \rightsquigarrow \varphi|_{K_1K_2} = id$

$K_1, K_2 \subseteq \{x \in K_1K_2 \mid \varphi(x) = x\}$ e' un campo

$x, y \in \nearrow \longrightarrow \varphi(x+y) = \varphi(x) + \varphi(y) = x+y$

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

(2) Surgettivo $\iff |Gal(K_1K_2/F)| = |Gal(K_1/F)| \cdot |Gal(K_2/F)|$

$\iff [K_1K_2 : F] = [K_1 : F][K_2 : F]$ ⊛

$Gal(K_1K_2/K_1) \simeq Gal(K_2/K_1 \cap K_2)$

$$[K_1K_2 : F] = [K_1K_2 : K_1]\cdot[K_1 : F]$$

$$= [K_2 : K_1\cap K_2]\,[K_1 : F]$$

$\textcircled{\star\star}$

Swg $\Longleftrightarrow$ $\textcircled{\star}$ $\Longleftrightarrow$ $[K_2 : K_1\cap K_2]\cancel{[K_1 : F]} = \cancel{[K_1 : F]}[K_2 : F]$

$\Longleftrightarrow$ $K_1\cap K_2 = F.$

$$\begin{tikzcd}
K_2 \arrow[d, dash] \\
K_1\cap K_2 \arrow[d, dash] \\
F
\end{tikzcd}$$

Esempio: $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$

Calcolare $\mathrm{Gal}(K/\mathbb{Q})$

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

$K/\mathbb{Q}$ e' Galois in quanto composto di est. di Galois

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash, "\mathrm{Gal}"] \arrow[dr, bend right, "\mathbb{Z}/2\mathbb{Z}"'] & & \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \arrow[dl, dash, "\mathrm{Gal}"'] \arrow[dl, bend left, "S_3"] \\
 & \mathbb{Q} & \\
 & & \text{cds } x^3-3 \arrow[uu]
\end{tikzcd}$$

$$\mathrm{Gal}(K/\mathbb{Q}) \overset{?}{\simeq} S_3 \times \mathbb{Z}/2\mathbb{Z}$$

Per avere l'isom basta dim che $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[3]{3}, \zeta_3) = \mathbb{Q}$.

L'intersez. e' $\mathbb{Q}$ o $\mathbb{Q}(i)$. Se fosse $\mathbb{Q}(i)$:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_3, \sqrt[3]{3}) \arrow[ddl, dash] \arrow[ddr, dash] & \\
 & \mathbb{Q}(i,\zeta_3) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "4"] & \\
\mathbb{Q}(i) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$4 \nmid 6 \Rightarrow \mathbb{Q}(i) \not\subseteq \mathbb{Q}(\zeta_3, \sqrt[3]{3})$

$f(x) \in \mathbb{Q}[x]$ con 2 radici $\notin \mathbb{R}$

$p$ un primo, $f(x) \in \mathbb{Q}[x]$ irrid. grado $p$. Supponiamo che $f(x)$ abbia $p-2$ radici reali e 2 in $\mathbb{C} \setminus \mathbb{R}$.

Dim. che $\mathrm{Gal}(f(x)) \simeq S_p$

$K =$ c.d.s. di $p(x)$ su $\mathbb{Q}$ e $G = \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_p$

$|G| = [K : \mathbb{Q}]$

$$\begin{tikzcd}
K = \mathbb{Q}(\alpha_1, \dots, \alpha_p) \arrow[d, dash] \\
\mathbb{Q}(\alpha_1) \arrow[d, dash, "p"] \\
\mathbb{Q}
\end{tikzcd}$$

$\Rightarrow p \mid \# G \Rightarrow G$ contiene un $p$-ciclo

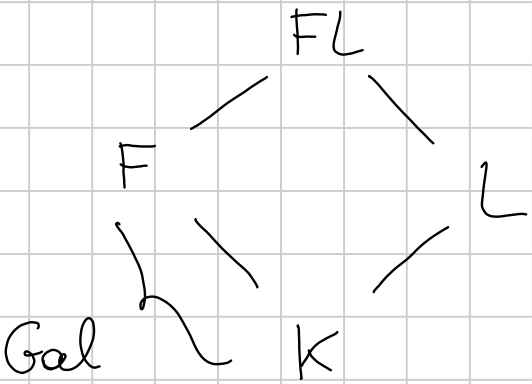
G contiene una trasposizione:

$$\begin{tikzcd}
K \arrow[rrd, bend right] & \subseteq \overline{\mathbb{Q}} \subseteq & \mathbb{C} \arrow[d, "\text{coniugio}"] \\
 & & \mathbb{C}
\end{tikzcd}$$

il coniugio cpx, ristretto a $K$, dà una permutaz. delle radici che e' una trasp $\Rightarrow$ $G$ contiene un $p$-ciclo e una trasp.

$$\Rightarrow G \simeq S_p.$$

## Gruppo di Gal del traslato



1. $FL/L$ è di Galois
2. $\mathrm{Gal}(FL/L) \hookrightarrow \mathrm{Gal}(F/K)$
3. L'immagine di questa immersione è $\mathrm{Gal}(F/L \cap F)$

$i : \mathrm{Gal}(FL/L) \hookrightarrow \mathrm{Gal}(F/k)$. Sia $H = \mathrm{imm}(i)$

$\varphi \longmapsto \varphi|_F$

Chi è $F^H$? Per def. è $\{x \in F \mid \varphi(x) = x \ \ \forall \varphi \in H\}$

$$= \left\{ x \in F \;\middle|\; \psi(x) = x \quad \forall \psi \in Gal(FL/L) \right\}$$

$$= F \cap \left\{ x \in FL \;\middle|\; \psi(x) = x \quad \forall \psi \in Gal(FL/L) \right\}$$

$$= F \cap (FL)^{Gal(FL/L)} = F \cap L$$

Per il teo di corrisp., $H = Gal\left(F/F\cap L\right)$

$$F^H = F \cap L = F^{Gal(F/F\cap L)} \iff H = Gal\left(F/F \cap L\right)$$

Ripasso

$$\begin{tikzcd} E \arrow[d, dash, "\text{Galois}\ G"] \\ F \end{tikzcd}$$

C'è una <u>bigezione</u>

$$\{ H \leq G \} \longleftrightarrow \{ \text{sottocampi } F \subseteq K \subseteq E \}$$

$$H \longmapsto E^H$$

$$\{ \varphi : \varphi|_K = id \} \longmapsfrom K$$

# Problema inverso di Galois

Sia $G$ un gruppo finito.

**Lemma (Artin)** Sia $G \subseteq \mathrm{Aut}(K)$. Allora $K$ e' di Galois
$G$ finito $\quad \begin{array}{c} K \\ | \\ K^G \end{array}$
con gruppo $G$

**Dim.** Sia $K = K^G(\alpha)$ (Teo. elemento primitivo)

Sia $\mu(x) \in K^G[x]$ il pol. minimo di $\alpha$.

Voglio mostrare che $K$ e' il c.d.s. $L$ di $\mu(x)$.

Certamente $K = K^G(\alpha) \subseteq L$

Considero $p(x) := \prod_{g \in G} (x - g(\alpha)) \in K[x]$

In realtà: $\prod_{g \in G} (x - g(\alpha)) \in K^G[x]$, perché $\forall g' \in G$

$$g'\left(\prod_{g \in G} (x - g(\alpha))\right) = \prod_{g \in G} (x - g'(g(\alpha)))$$
$$= \prod_{h \in G} (x - h(\alpha))$$

Allora $\mu(x) \mid p(x)$ : sono entrambi in $K^G[x]$ e $p(\alpha) = 0$.

$\Rightarrow$ le radici di $\mu(x)$ sono tutte della forma $g(\alpha)$,

per certi $g \in G$ $\Rightarrow$ stanno tutte in $K$

$\Rightarrow$ c.d.s. $L$ di $\mu(x) \subseteq K \subseteq L$

Quindi $K/K^G$ è di Galois perché c.d.s.

Sia $H$ il grp. di Gal. di questa estensione.

$$K^H = K^{Gal(K/K^G)} = K^G \xrightarrow[\text{corrisp}]{\text{teo}} G = H. \qquad \square$$

Oss

$$\begin{tikzcd} L \arrow[d, dash, "\text{Galois con grp } G" right] \\ F \end{tikzcd} \quad H \leq G$$

$$\begin{tikzcd} L \arrow[dr, dash, "\text{Gal con grp } H"] & \\ & L^H \arrow[dl, dash] \\ F & \end{tikzcd}$$

Ricordiamoci: se $f(x) \in \mathbb{Q}[x]$ ha grado $p$, è irrid, e ha esattamente 2 radici non reali, allora (detto $K=$ cds $f(x)$) si ha $Gal(K/\mathbb{Q}) = S_p$

<u>Es</u> Si costruiscono tali polinomi $\forall p$

Sia $G$ grp. finito qualsiasi. $G \hookrightarrow S_{|G|} \hookrightarrow S_p$

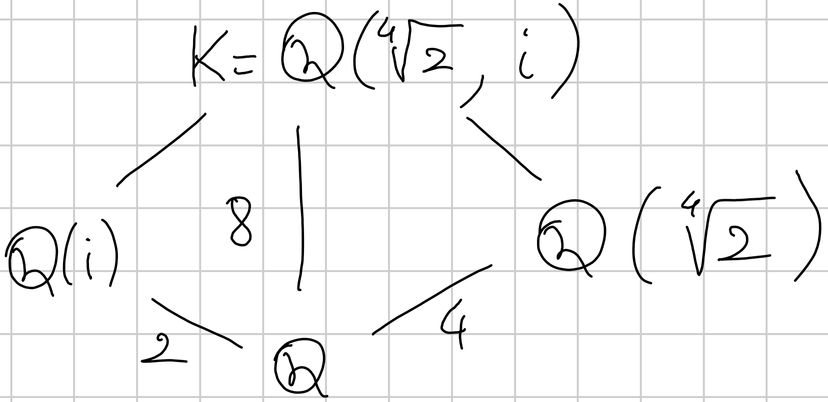
con $p$ primo abbastanza grande.

Es $\rightsquigarrow$ c'è un polinomio $f(x) \in \mathbb{Q}[x]$ il cui cds $K$ ha grp. di Galois $Gal(K/\mathbb{Q}) \simeq S_p$

$$\begin{tikzcd}
K \arrow[dd, dash, "S_p"'] \arrow[dr, dash] & \\
 & K^G \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

di Galois con gruppo $G$

# Sottocampi del c.d.s. di $x^4-2$



$K = \text{cds}(x^4-2)$ su $\mathbb{Q}$

$$\left.\begin{matrix} \mathbb{Z}/8\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{matrix}\right\} \text{no}$$

$G = \text{Gal}(K/\mathbb{Q}) \simeq \, ?$

**Oss** $K/\mathbb{Q}$ ha est. intermedie NON di Galois $/\mathbb{Q}$

$\iff G$ ha sgp NON NORMALI $\Rightarrow G$ non abeliano

(e dev'essere $D_4$)

$|G| = [K:\mathbb{Q}] = 8$

$$\varphi : \left| \begin{array}{lll} \sqrt[4]{2} & \longmapsto & \sqrt[4]{2} \cdot i^h \qquad h = 0,1,2,3 \\ i & \longmapsto & \{\pm i\} \end{array} \right.$$

Chiamiamo $r : \left| \begin{array}{lll} \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}\, i \\ i & \longmapsto & i \end{array} \right.$ $\quad s : \left| \begin{array}{lll} \sqrt[4]{2} & \longmapsto & \sqrt[4]{2} \\ i & \longmapsto & -i \end{array} \right.$

$s r s^{-1} = r^{-1} \qquad r^4 = id \qquad s^2 = id$

Sottogruppi di $D_4$ ?

- $\{e\}$
- $D_4$
- $\langle r \rangle$

  $\langle r^2, s \rangle$

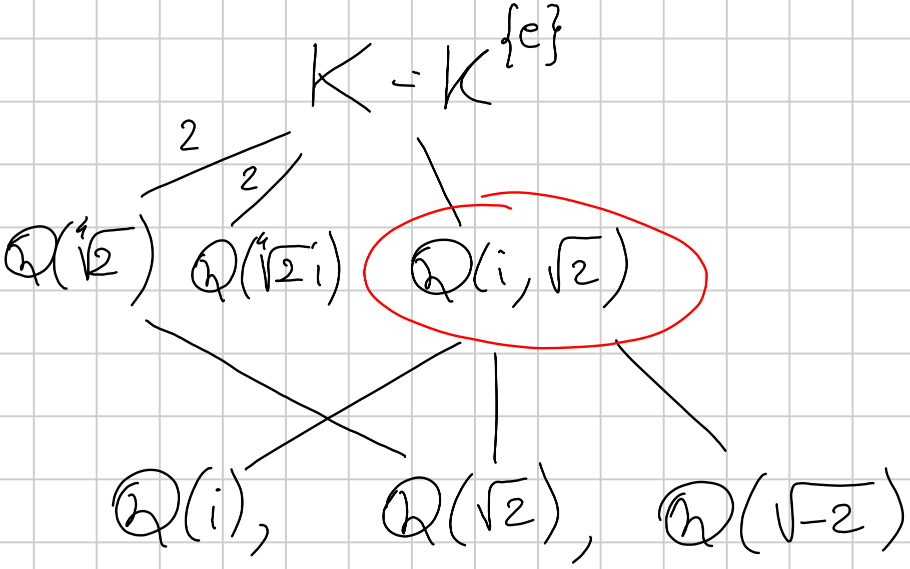
  $\langle r^2, sr \rangle$

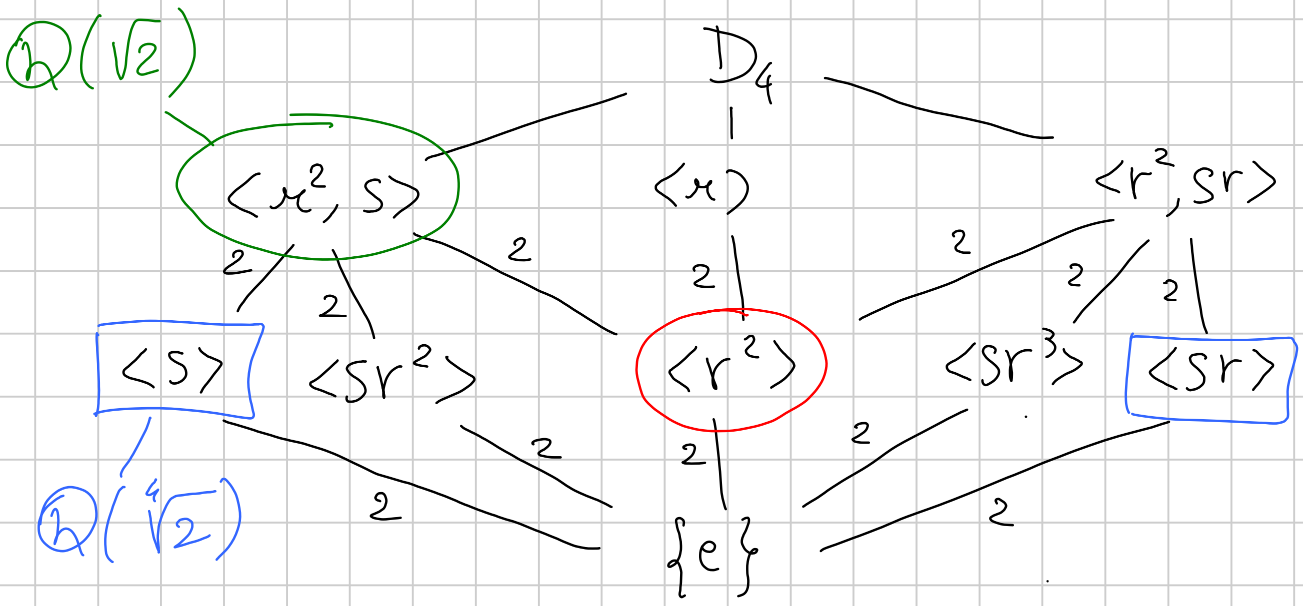
  ordine 4
- $\langle s \rangle, \langle sr \rangle, \langle sr^2 \rangle, \langle sr^3 \rangle$

  $\langle r^2 \rangle$

  ordine 2

Sottocampi di $K$?





$K^{\langle r\rangle} = \{x \in K \mid r(x) = x\} = \mathbb{Q}(i)$ ha grado $\underset{\underset{2}{\|}}{[D_4 : \langle r\rangle]}$ su $\mathbb{Q}$

$K^{\langle s\rangle} = \{x \in K \mid s(x) = x\} = \mathbb{Q}(\sqrt[4]{2})$ ha grado $[D_4 : \langle s\rangle] = 4$ su $\mathbb{Q}$

$K^{\langle r^2 \rangle} \supseteq \mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ ha grado 4

$$r^2(\sqrt{2}) = r^2\left(\left(\sqrt[4]{2}\right)^2\right) = \left(r^2\left(\sqrt[4]{2}\right)\right)^2 = \left(-\sqrt[4]{2}\right)^2 = \sqrt{2}$$

Facciamo $K^{\langle sr \rangle}$.

$$sr : \left| \begin{array}{l} \sqrt[4]{2} \longmapsto \sqrt[4]{2}\, i \longmapsto -\sqrt[4]{2}\, i \\ i \longmapsto i \longmapsto -i \end{array} \right.$$

Base di $K/\mathbb{Q}$: $1, \sqrt[4]{2}, \left(\sqrt[4]{2}\right)^2, \left(\sqrt[4]{2}\right)^3$

$i, \sqrt[4]{2}\, i, \left(\sqrt[4]{2}\right)^2 i, \left(\sqrt[4]{2}\right)^3 i$

Oss * Se $g$ e' un el. di ordine 2 e $\alpha \in K$ e' qualsiasi,

$$\alpha + g\alpha \in K^{\langle g \rangle}$$

$$g(\alpha + g\alpha) = g(\alpha) + g^2(\alpha) = g(\alpha) + \alpha$$

* Se $g$ è di ord $n$, stessa cosa con $\alpha + g\alpha + \dots + g^{n-1}(\alpha)$

Per noi: $\sqrt[4]{2} + sr(\sqrt[4]{2}) = \sqrt[4]{2} - \sqrt[4]{2}\, i \in K^{\langle sr \rangle}$

$$= \sqrt[4]{2}\,(1-i) =: \beta$$

$$\beta^2 = \sqrt{2} \cdot (-2i)$$

$$\beta^4 = 2 \cdot (-2)^2 \cdot i^2 = -8$$

Se $t^4 + 8 \in \mathbb{Q}[t]$ è irrid $\Rightarrow [\mathbb{Q}(\beta) : \mathbb{Q}] = 4$

Oss. Pol. annullato da $\beta/2$ è $(2t)^4 + 8$, e quindi anche

$t^4 + 1/2$

$$\mathbb{Q}(\beta) = \mathbb{Q}(\beta/2) = \mathbb{Q}\left(\sqrt[4]{-1/2}\right) = \mathbb{Q}\left(\sqrt[4]{-2}\right)$$

$$\Rightarrow \quad [\mathbb{Q}(\beta) : \mathbb{Q}] = 4$$

Alternativa: prendiamo $\beta = \sqrt[4]{2}\,(1-i)$ e applichiamo tutti gli el. del grp. di Gal ⇝ così troviamo radici pol. min.

| | |
|---|---|
| $1$ | $sr$ |
| $r$ | $sr^2$ |
| $r^2$ | $sr^3$ |
| $r^3$ | $s$ |

$g(\beta) \qquad g \in G$

$(g \cdot sr)(\beta) = g(\beta)$

Le 4 img che trovo sono

$\sqrt[4]{2} \cdot i^h \cdot (1-i) \qquad h = 0, 1, 2, 3$

$\Rightarrow$ il pol. min. ha 4 radici

$$\Rightarrow \quad [\mathbb{Q}(\beta) : \mathbb{Q}] = 4 = [K^{\langle sr \rangle} : \mathbb{Q}]$$

$$\Rightarrow \quad K^{\langle sr \rangle} = \mathbb{Q}(\beta)$$

$$K^{\langle r^2, s \rangle} = K^{\langle r^2 \rangle} \cap K^{\langle s \rangle} = \mathbb{Q}(\sqrt{2}, i) \cap \mathbb{Q}(\sqrt[4]{2})$$

$$= \mathbb{Q}(\sqrt{2})$$

Chi sono i campi $\subseteq \mathbb{Q}(\sqrt[4]{2})$? Corrisponde ad un sgp di $D_4$ che contiene $\langle s \rangle$ $\rightsquigarrow$ c'e' solo $D_4 \longleftrightarrow \mathbb{Q}$

$\langle s, r^2 \rangle \leftrightarrow \mathbb{Q}(\sqrt{2})$

## Fattorizzazione di $x^n - 1$ in $\mathbb{Q}[x]$

$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ : questo dice che

$$\begin{array}{c} [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n) \\ \| \\ \text{grado pol. min } \zeta_n \text{ su } \mathbb{Q} \end{array}$$

Sia $\Phi_n(x) =$ pol. min $\zeta_n$ su $\mathbb{Q}$

$= \prod_{(k,n)=1} (x - \zeta_n^k) =$ polinomio che ha come radici tutte e sole le radici n-esime PRIMITIVE di 1

⊛ $$x^n - 1 = \prod_{d|n} \Phi_d(x), \quad \text{dove} \quad \deg \Phi_d(x) = \varphi(d)$$

$$n = \sum_{d|n} \varphi(d)$$

⊛ vale perché:

- sono due polinomi senza radici multiple
- ogni radice di $x^n - 1$ è una radice prim. $d$-esima per un qualche $d|n$ $\Rightarrow$ è radice di $\Phi_d(x)$
- viceversa, una radice $\alpha$ di $\prod \Phi_d(x)$ è radice di uno dei $\Phi_d$ $\Rightarrow$ è radice prim. $d$-esima $\Rightarrow \alpha^d = 1 \Rightarrow \alpha^n = 1$

- Sono entrambi monici

**Es** $x^{10}-1 = (x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$

## Teo fond. dell'algebra

Sia $p(x) \in \mathbb{C}[x]$. Vogliamo dim che $\exists\, \alpha \in \mathbb{C}$ t.c. $p(\alpha)=0$

① $p(x) \cdot \overline{p(x)} =: q(x) \in \mathbb{R}[x]$

$$\overline{q(x)} = \overline{p(x)} \cdot \overline{\overline{p(x)}} = \overline{p(x)} \cdot p(x) = q(x)$$

Se $q(\alpha)=0$

- o $p(\alpha)=0$ e fine
- o $\overline{p}(\alpha)=0 \iff \underset{\substack{\| \\ p(\overline{\alpha})}}{\overline{\overline{p}(\alpha)}} = 0$

② Sia $q(x) \in R[x]$ e sia $K =$ cds di $q(x)$ su $\mathbb{R}$.

Sia $P_2 < G$ un 2-Sylow di $G$

$$\begin{tikzcd}
K \arrow[dd, dash, "G"'] \arrow[dr, dash, "|P_2|"] & \\
& K^{P_2} = \mathbb{R}(\beta) \arrow[dl, dash, "d"] \\
\mathbb{R} &
\end{tikzcd}$$

$d \rightsquigarrow \ = |G| / |P_2| =$ dispari

Il pol. min. di $\beta$ su $\mathbb{R}$, $\mu(x)$, ha grado $d$ dispari

③ $\mu(x)$ ha una radice in $\mathbb{R}$, ma e' irrid $\Rightarrow \deg \underset{\substack{\| \\ d}}{\mu(x)} = 1$

④
$$\begin{tikzcd}
K \arrow[d, dash, "2^n"'] \\
\mathbb{R}
\end{tikzcd}$$

$\{e\} = G_n \lhd \dots \underset{2}{\lhd} G_2 \underset{2}{\lhd} G_1 \underset{2}{\lhd} G$

$$\begin{tikzcd}
K = K^{G_n} \arrow[d, dash, "2"'] & \\
K^{G_{n-1}} \arrow[d, dash, "2"'] & \\
\vdots & \\
K^{G_2} = \mathbb{C}(\sqrt{\gamma_2}) \arrow[d, dash, "2"'] & \cancel{\mathbb{R}} \\
K^{G_1} = \mathbb{R}(\sqrt{\gamma_1}) = \arrow[d, dash, "2"'] \arrow[ru, dash] \arrow[rd, dash] & \\
\mathbb{R} & \mathbb{C}
\end{tikzcd}$$

Ma in $\mathbb{C}$ ogni elemento è un quadrato! Quindi non posso fare ulteriori est. quadr $\Rightarrow K = \mathbb{R}$

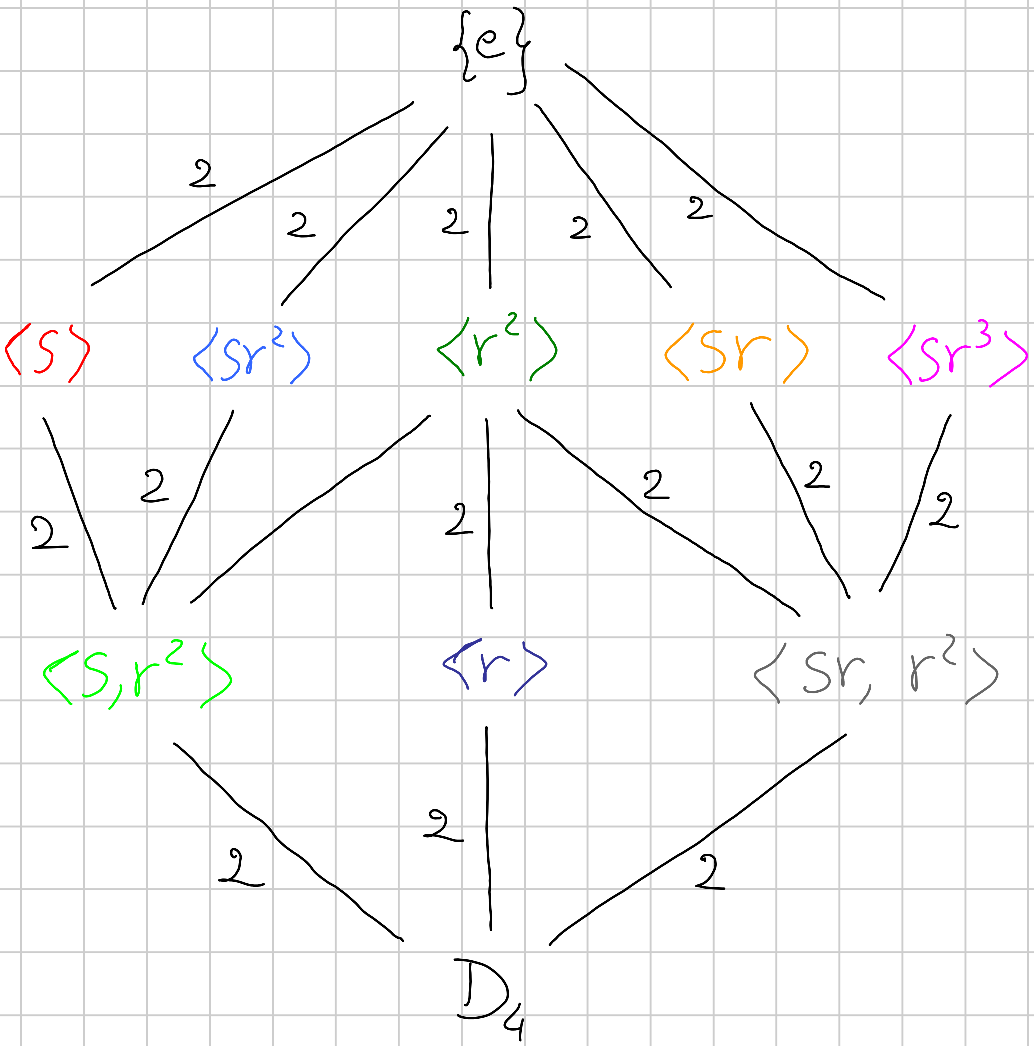
$= \mathbb{C}$

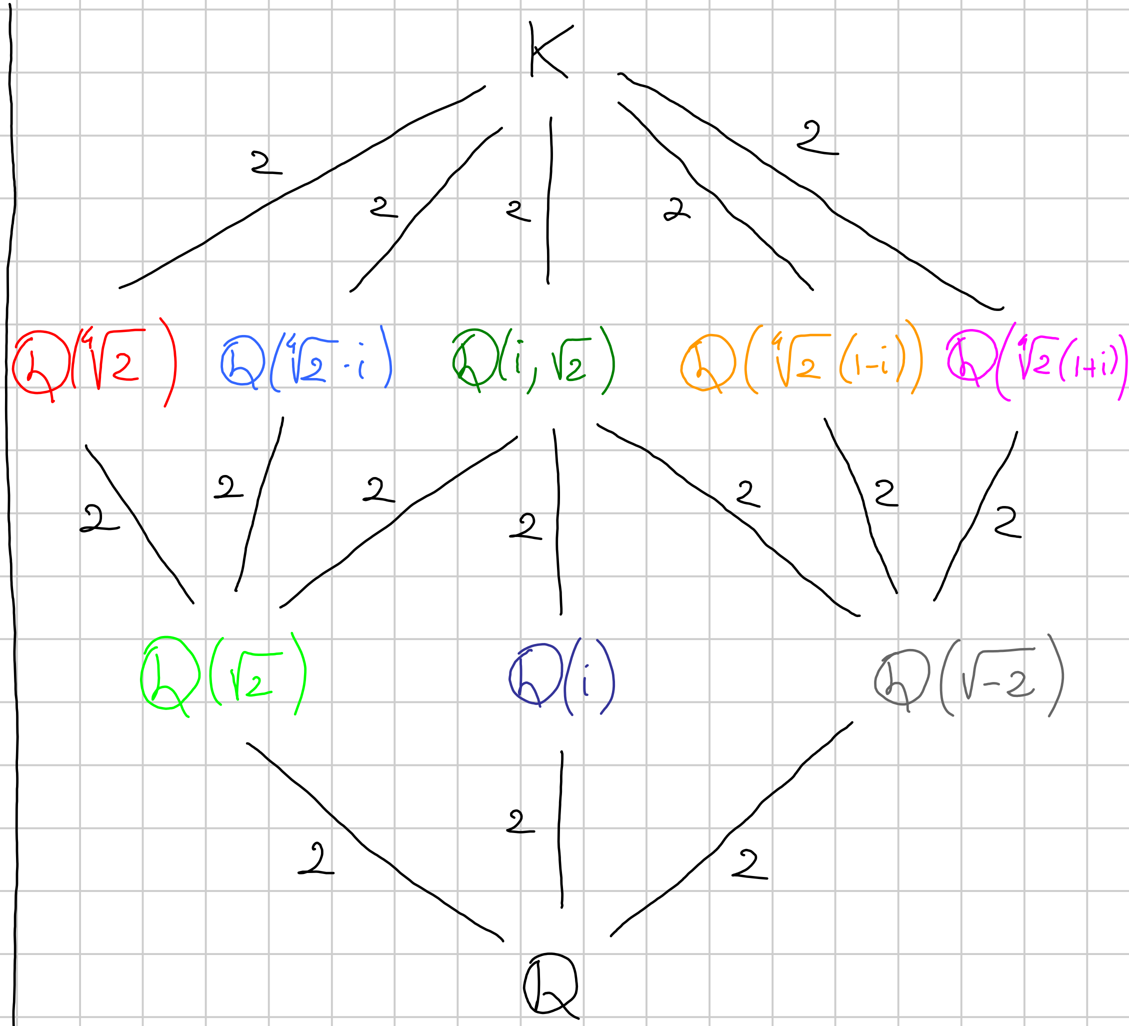
$$\mathbb{R}(\sqrt{\gamma}) = \mathbb{R}(\sqrt{-1})$$

$$\Leftrightarrow \gamma < 0$$

□

# Diagramma completo dei sottocampi del cds $(x^4-2) =: K$





Il campo $K^{\langle sr \rangle}$ contiene $\sqrt[4]{2} + sr(\sqrt[4]{2}) = \sqrt[4]{2}(1-i)$, che come abbiamo visto ha pol. min. $x^4+8$

$$\Rightarrow \left[\mathbb{Q}\left(\sqrt[4]{2}\cdot(1-i)\right):\mathbb{Q}\right] = 4 = [D_4 : \langle sr \rangle] = [K^{\langle sr \rangle} : \mathbb{Q}]$$

$$\Rightarrow K^{\langle sr \rangle} = \mathbb{Q}\left(\sqrt[4]{2}\cdot(1-i)\right)$$

Il campo $K^{\langle sr^2 \rangle}$ contiene $\sqrt[4]{2}i + sr^2(\sqrt[4]{2}\,i) =$

$$= \sqrt[4]{2}\cdot i + s(\sqrt[4]{2}\cdot i^3) = 2\sqrt[4]{2}\,i \Rightarrow K^{\langle sr^2 \rangle} = \mathbb{Q}(\sqrt[4]{2}\cdot i)$$

Il campo $K^{\langle sr^3 \rangle}$ contiene $\sqrt[4]{2} + sr^3(\sqrt[4]{2}) = \sqrt[4]{2} + s(\sqrt[4]{2}\cdot i^3)$

$$= \sqrt[4]{2} + \sqrt[4]{2}\cdot i = \sqrt[4]{2}(1+i),$$

che e' un'altra radice di $x^4+8$ ⇝ ha grado 4, quindi

$$K^{\langle sr^3 \rangle} = \mathbb{Q}\left(\sqrt[4]{2}(1+i)\right)$$

# TEO DI GALOIS

$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$

$p_1, \dots, p_n$ primi distinti

Per induzione, vogliamo dim.

$$\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$$

Caso base: $n=1$ $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$ quadr $\Rightarrow$ normale

$$\text{Gal}(\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$$

Passo induttivo: vogliamo più precisamente capire chi sono tutte le sotto-est quadratiche di $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$

$K_n := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$

$$\begin{tikzcd}
 & K_{n+1} & \\
K_n \arrow[ur, dash, "1 \text{ o } 2"] & & \mathbb{Q}(\sqrt{p_{n+1}}) \arrow[ul, dash] \\
 & \mathbb{Q} \arrow[ul, dash, "2^n"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

Quante sono le sotto-est. quadr. di $K_n$?

$$\begin{tikzcd}
K_n \arrow[d, dash] & & \{e\} \arrow[d, dash] \\
F \arrow[d, dash, "2"] & \arrow[leftrightsquigarrow]{r} & H \arrow[d, dash, "2"] \\
\mathbb{Q} & & (\mathbb{Z}/2\mathbb{Z})^n
\end{tikzcd}$$

$\#$ Sgp di indice 2

$\parallel$

$\#$ iperpiani in $\mathbb{F}_2^n$

$\parallel$

$2^n - 1$

Cerchiamo $2^n - 1$ sottocampi quadratici

$$\mathbb{Q}\left(\sqrt{p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_n^{\varepsilon_n}}\right) \qquad \varepsilon_i \in \{0, 1\}$$

Ci sono $2^n - 1$ scelte per gli $\varepsilon_i$ che danno un'est. quadratica. Sono tutte diverse?

$$\left(p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}\right) \cdot \left(p_1^{\delta_1} \cdots p_n^{\delta_n}\right) \in \mathbb{Q}^{\times 2}$$

$$\iff \quad \varepsilon_i + \delta_i \equiv 0 \ (2) \qquad \forall i = 1, \dots, n$$

$$\iff \quad \varepsilon_i \equiv \delta_i \ (2)$$

$$\begin{tikzcd}
& K_{n+1} \arrow[dl, dash] \arrow[dr, dash] & \\
K_n \arrow[dr, dash] & & \mathbb{Q}(\sqrt{p_{n+1}}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Se so che $K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$

$$\Rightarrow \mathrm{Gal}(K_{n+1}/\mathbb{Q}) = \mathrm{Gal}(K_n/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_{n+1}})/\mathbb{Q})$$

Questo fallisce solo se $\mathbb{Q}(\sqrt{p_{n+1}}) \subseteq K_n$,

cioè se è una delle est. $\mathbb{Q}(\sqrt{p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}})$

$\Leftrightarrow p_{n+1} \cdot \prod_{i=1}^{n} p_i^{\varepsilon_i} \in \mathbb{Q}^{\times 2}$

$\Leftrightarrow$ è un quadrato in $\mathbb{Z}$, ma non è così, perché $p_{n+1}$ compare con esponente dispari.

**Oss.** $\alpha := \sqrt{p_1} + \sqrt{p_2} + \dots + \sqrt{p_n}$. Che grado ha il suo pol. minimo?

Consideriamo le immersioni di $\mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$.

Siccome $\mathbb{Q}(\alpha) \subseteq K_n$, ogni immersione si estende a $K_n \hookrightarrow \overline{\mathbb{Q}}$, e queste le conosciamo.

$$\sigma(\alpha) = \pm\sqrt{p_1} \pm \sqrt{p_2} \pm \dots \pm \sqrt{p_n}$$

Sono tutti diversi: $\sqrt{p_1}, \dots, \sqrt{p_n}$ fanno parte di una base di $K_n / \mathbb{Q}$.

Per l'induz precedente:

$1, \sqrt{p_1}$ base di $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$

$1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1 p_2}$ base di $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})/\mathbb{Q}$

$\vdots$

$1, \sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{p_i p_j}, \sqrt{p_i p_j p_k}, \ldots$ base di $K_n/\mathbb{Q}$

$\Rightarrow$ $\alpha$ ha $2^n$ possibili img tramite immersioni $\mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$

$\Rightarrow$ $\mu_\alpha(x)$ ha grado $2^n$ $\Rightarrow$ $\mathbb{Q}(\alpha) = K_n$

Alternativa: mostriamo che $\sqrt{p_1}, \ldots, \sqrt{p_n}$ sono lin. indip.

Per induz su $n$; $n=1$ banale.

$$a_1 \sqrt{p_1} + \dots + a_n \sqrt{p_n} = 0 \qquad a_i \in \mathbb{Q}$$

$\forall \sigma \in Gal(K_n/\mathbb{Q})$, $\quad \sigma(a_1\sqrt{p_1} + \dots + a_n\sqrt{p_n}) = 0 \quad ✪$

Scelgo $\sigma$ t.c. $\sigma(\sqrt{p_1}) = -\sqrt{p_1}$

$\sigma(\sqrt{p_i}) = \sqrt{p_i}$ per $i > 1$

$✪ \implies -a_1\sqrt{p_1} + a_2\sqrt{p_2} + \dots + a_n\sqrt{p_n} = 0$

Per differenza, $a_1 = 0$; per hp indutt., $a_2 = \dots = a_n = 0$

# Biquadratiche

$f(x) = x^4 + a x^2 + b \in \mathbb{Q}[x]$, irriducibile

$K$ = c.d.s. $f(x)$, $\quad Gal(K/\mathbb{Q}) = ?$

$t = x^2 \qquad t^2 + at + b = 0 \qquad t_{1,2} = \dfrac{-a \pm \sqrt{a^2-4b}}{2}$

$$K = \mathbb{Q}\left( \underbrace{\pm \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}}}_{x_1,\, x_2},\ \underbrace{\pm \sqrt{\frac{-a-\sqrt{a^2-4b}}{2}}}_{x_3,\, x_4} \right); \quad \Delta := a^2-4b$$

$2x_1^2 + a = \sqrt{\Delta}$

$$\begin{tikzcd}
 & K \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(x_1) \arrow[dr, no head, "2"] \arrow[ddr, no head, bend right, "4"'] & & \mathbb{Q}(x_3) \arrow[dl, no head, "2"] \\
 & \mathbb{Q}(\sqrt{\Delta}) \arrow[d, no head, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$[\mathbb{Q}(x_1) : \mathbb{Q}] = \deg f(x) = 4$$

$[K : \mathbb{Q}] = 4$ o $8$

$$\mathbb{Q}(x_1) = \mathbb{Q}(x_3) \iff \left(\frac{-a+\sqrt{\Delta}}{2}\right) \cdot \left(\frac{-a-\sqrt{\Delta}}{2}\right) \text{ e'}$$

un $\square$ in $\mathbb{Q}(\sqrt{\Delta})$

$\iff \quad a^2 - \Delta = \square$ in $\mathbb{Q}(\sqrt{\Delta})$

$\iff \quad 4b = \square$

$\iff \quad b = \square$ in $\mathbb{Q}(\sqrt{\Delta})$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{\Delta}) \arrow[dr, dash] & \supseteq & \mathbb{Q}(\sqrt{b}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

$\iff$ o $b = \square$ in $\mathbb{Q}$, oppure $b \cdot \Delta$ è un $\square$ in $\mathbb{Q}$

Finora: • se né $b$, né $b(a^2 - 4b) = \square$ in $\mathbb{Q}$

$\implies [K : \mathbb{Q}] = 8$

- altrimenti $[K : \mathbb{Q}] = 4$

Nel primo caso, $Gal(K/\mathbb{Q})$ è un grp. ordine 8 che si immerge in $S_4$

$\Rightarrow Gal(K/\mathbb{Q})$ è un 2-Sylow di $S_4$, cioè è $D_4$.

Considieriamo il 2° caso, in cui $K = \mathbb{Q}(x_1)$

$\exists$ 4 elementi di $Gal(K/\mathbb{Q})$ sono univocamente det. da

$$\varphi(x_1) = \left| \begin{array}{l} x_1 \\ x_2 = -x_1 \\ x_3 \\ x_4 = -x_3 \end{array} \right.$$

$\varphi_2$ e' di ordine 2 : $\varphi_2^2(x_1) = \varphi_2(-X_1)$

$= -\varphi_2(x_1) = X_1$

Consideriamo $\varphi_3 : X_1 \longrightarrow X_3$

$$X_1 = \sqrt{\frac{-a+\sqrt{\Delta}}{2}} \qquad x_3 = \sqrt{\frac{-a-\sqrt{\Delta}}{2}}$$

Siccome $\sqrt{\Delta} = 2X_1^2 + a$

$$\varphi_3(\sqrt{\Delta}) = 2X_3^2 + a = -\sqrt{\Delta}$$

$$X_1 \cdot X_3 = \sqrt{\frac{a^2 - \Delta}{4}} = \sqrt{b}$$

* Se $b$ è un quadrato in $\mathbb{Q}$:

$$X_3 = \sqrt{b}/x_1 \qquad \varphi_3(X_3) = \varphi_3^{\,2}(x_1)$$

$$\begin{array}{c} \| \\ \sqrt{b}/\varphi_3(x_1) = \sqrt{b}/X_3 = x_1 \end{array} \Bigg] \left(\mathbb{Z}/2\mathbb{Z}\right)^2$$

* Se $b$ NON è quadr. in $\mathbb{Q}$, ma è $\square$ in $\mathbb{Q}(\sqrt{\Delta})$,

$$b = \Delta \cdot q^2 \quad \text{con } q \in \mathbb{Q}$$

$$X_3 = \sqrt{\Delta} \cdot q/x_1 \qquad \varphi_3^{\,2}(x_1) = \varphi_3(X_3) =$$

$$x_1 = \sqrt{\Delta} \cdot q/X_3 \qquad = q \cdot \frac{-\sqrt{\Delta}}{X_3} = -x_1$$

$$\rightsquigarrow \mathbb{Z}/4\mathbb{Z}$$

**Prop** $x^4+ax^2+b$ irrid., $K$ = cds. $\mathrm{Gal}(K/\mathbb{Q})$ è:

- $D_4$, se né $b$ né $b(a^2-4b)$ è $\square$
- $(\mathbb{Z}/_2\mathbb{Z})^2$ se $b=\square$
- $\mathbb{Z}/_4\mathbb{Z}$ se $b\neq\square$ ma $b(a^2-4b)=\square$

### Sottoest. quadratiche

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

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash, "\mathbb{Z}/_2\mathbb{Z}"'] & & \mathbb{Q}(\sqrt[3]{3},\zeta_3) \arrow[dl, dash, "S_3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Se $\mathbb{Q}(i)\subset\mathbb{Q}(\sqrt[3]{3},\zeta_3)$ : assurdo

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "6"] & \\
\mathbb{Q}(i) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/_2\mathbb{Z} \times S_3 =: G$

Sgp di $G$ di indice 2 contengono $\langle g^2 \mid g \in G \rangle =: G^{\square}$

$H < G$ con $[G : H] = 2$

$$gH \begin{cases} \mathrm{id}: & g \in H \Rightarrow g^2 \in H \\ \neq \mathrm{id} & (gH)^2 = H \Rightarrow g^2 \in H \end{cases}$$

$G^{\square} \triangleleft G \qquad x G^{\square} x^{-1} = \langle x g^2 x^{-1} \mid g \in G \rangle$

$$= \langle (xgx^{-1})^2 \mid g \in G \rangle = G^{\square}$$

Dal teo di corrisp:

$$\left\{ \begin{matrix} H < G \text{ di indice } 2 \\ (G^{\square} \subseteq H) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{sgp. di } G/G^{\square} \\ \text{di indice } 2 \end{matrix} \right\}$$

Inoltre, il grp. $G/G^{\square}$ e' della forma $(\mathbb{Z}/2\mathbb{Z})^k$

Infatti:

- in $G/G^{\square}$, $x^2 = id$ $\forall x$ $\qquad (gG^{\square})^2 = g^2 \cdot G^{\square}$
  $= G^{\square}$
- $x^2 = 1$ $\forall x$ $\Rightarrow$ grp. abeliano
- teo struttura $\Rightarrow$ $G/G^{\square} \simeq (\mathbb{Z}/2\mathbb{Z})^h$

Quindi: il n° di sottoest. quadr. di $K$ è

$$= \# \{ \text{sgp } H < G \text{ di indice } 2 \}$$

$$= \# \{ \text{sgp di } G/G^{\square} \text{ di indice } 2 \} = 2^h - 1$$

Nel caso particolare $G = \mathbb{Z}/_2\mathbb{Z} \times S_3$

$G^{\square} = \{0\} \times \langle (1,2,3) \rangle$

$G/G^{\square} = \mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_2\mathbb{Z}$

$\rightsquigarrow$ 3 sottoext. quadr $\rightsquigarrow$ $\mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\sqrt{3})$

# Radici dell'unità in un campo

$$\begin{tikzcd}
K \arrow[dd, dash, "G"'] \arrow[dr, dash] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\
 & \boxed{K \cap \mathbb{Q}(\zeta_n)} & \\
\mathbb{Q} \arrow[ur, dash] & &
\end{tikzcd}$$

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$$

$$\Downarrow$$

ogni sotto-est. di $\mathbb{Q}(\zeta_n)$ è normale su $\mathbb{Q}$, con gruppo di Gal. abeliano

In $K$ c'è solo un n° finito di radici di 1:

se $\zeta_n \in K$

$\Rightarrow \mathbb{Q}(\zeta_n) \subseteq K$

$\Rightarrow \varphi(n) \leq [K : \mathbb{Q}]$

$\Rightarrow n$ limitato

$$\begin{tikzcd} K \cap \mathbb{Q}(\zeta_n) \arrow[d, dash, "\text{normale}"] \\ \mathbb{Q} \end{tikzcd} \qquad \longleftrightarrow \qquad H < G = Gal(K/\mathbb{Q})$$

$$H \lhd G$$

$$Gal\left(K \cap \mathbb{Q}(\zeta_n)/\mathbb{Q}\right) = G/H$$

abeliano

$$\Leftrightarrow \quad H \geq G'$$

Es $f(x) \in \mathbb{Q}[x]$ pol. irrid. di grado $n$ con grup $S_n$

$K =$ c.d.s. Che radici di 1 ci possono essere in $K$?

$$S_n \left\{ \begin{tikzcd} K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd} \right.$$

$H \leq S_n$ con $S_n' = A_n \leq H \leq S_n$

$\mathbb{Q}(\zeta_n) \cap K \longleftrightarrow H \in S_n, A_n$

Se $H = S_n$, $\mathbb{Q}(\zeta_n) \cap K = \mathbb{Q}$

$H = A_n$, $[\mathbb{Q}(\zeta_n) \cap K : \mathbb{Q}] = 2$

$\Rightarrow$ se $\zeta_n \in K$

$n \in \{3, 4, 6\} \Leftarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2$

$\mathbb{Q}(\zeta_p)$ : sottoest. quadr?

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_p) / \mathbb{Q}\right) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[d, dash] \\
F \arrow[d, dash, "d"] \\
\mathbb{Q}
\end{tikzcd}$$

Per ogni $d \mid p-1$ c'è una e una sola sottoest. di quel grado.

Studiamo il caso $d = 2$. Sottogp.

$F_2$ := l'unica sottoest. quadr. $\longleftrightarrow$ $(\mathbb{Z}/p\mathbb{Z})^{\times 2}$

$K := \mathbb{Q}(\zeta_p) \cap \mathbb{R}$ $\longleftrightarrow$ $\langle -1 \rangle$

Domanda: $F_2 \subseteq K$?

$$\begin{aligned} \varphi : \mathbb{F}_p^\times &\longrightarrow \mathbb{F}_p^\times \\ x &\longmapsto x^2 \end{aligned}$$

$$|\text{Quadr}| = |\text{imm } \varphi| = \frac{p-1}{2}$$

$$\begin{tikzcd} \mathbb{Q}(\zeta_p) \arrow[d, dash, "2"'] \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \end{tikzcd}$$

$F_2 \subseteq K \iff$ sottogp. corrisp ad $F_2$ $\supseteq$ sottogp corrisp a $K$

$$\underset{\frac{p-1}{2}}{\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times 2}} \supseteq \underset{2}{\langle -1 \rangle}$$

$\iff p \equiv 1 \ (4)$

$$F_2 = \begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \ (4) \\ \mathbb{Q}(\sqrt{-p}) & p \equiv 3 \ (4) \end{cases}$$

Es $p = 5$ $\mathbb{Q}(\zeta_5) \cap \mathbb{R} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$

$p = 7$ $\qquad$ $F_2$ = campo fissato dal sgp $H$

$$\left(\mathbb{Z}/7\mathbb{Z}\right)^\times = \{1, 2, 4\}$$

$$\zeta_7 \longmapsto \zeta_7$$

$$\zeta_7 \longmapsto \zeta_7^2$$

$$\zeta_7 \longmapsto \zeta_7^4$$

$$\alpha := \zeta_7 + \zeta_7^2 + \zeta_7^4 \in \mathbb{Q}(\zeta_7)^H \overset{?}{=} F_2$$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2$ : $\qquad$ $\mathbb{Q}(\alpha)$ e' fissato da $H$

$\mathbb{Q}(\alpha) \neq \mathbb{Q}$ : $\qquad$ sia $\sigma \longleftrightarrow -1 \in \left(\mathbb{Z}/7\mathbb{Z}\right)^\times$

$$\sigma(\alpha) = \zeta_7^{-1} + \zeta_7^{-2} + \zeta_7^{-4}$$

$$= \zeta_7^6 + \zeta_7^5 + \zeta_7^3 \neq \alpha$$

## Discriminante di $f(x) \in K[x]$

Vorrei sapere se $\mathrm{Gal}(f(x))$ è $\subseteq A_n$ oppure no.

Introduciamo

$$\mathrm{disc}(f(x)) := \prod_{i<j} (\alpha_i - \alpha_j)^2$$

dove le $\alpha_i$ sono le radici di $f(x)$ in una chiusura algebrica. Supporremo $f(x)$ senza radici multiple.

**Fatto:** $\mathrm{disc}\, f(x) \in K$

Es $\quad \alpha_{1,2} = \dfrac{-a \pm \sqrt{\Delta}}{2} \qquad (\alpha_1 - \alpha_2)^2 = \Delta \in K$

Sia $G := \mathrm{Gal}(f(x))$. Si ha $G \subseteq A_n \iff \sqrt{\mathrm{disc}\, f(x)} \in K$

Dim

$$\sqrt{\mathrm{disc}\, f(x)} = \prod_{i<j} (\alpha_i - \alpha_j)$$

Sia $\sigma$ una permutaz di $\{\alpha_1, \dots, \alpha_n\}$.

$$\prod_{i<j} \left(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}\right) = \mathrm{sgn}(\sigma) \prod_{i<j} (\alpha_i - \alpha_j)$$

In particolare: $G$ si identifica ad un sgp. di $S_n$.

Agisce su $\sqrt{\mathrm{disc}\, f(x)}$ come qui sopra; in particolare

$\sqrt{\text{disc } f(x)} \in K \iff G$ fissa $\sqrt{\text{disc } f(x)} \iff G \subseteq A_n$

## Teo fondam. funzioni simmetriche

$$(t-x_1)(t-x_2)\;\dots\;(t-x_n) = t^n - (x_1+\dots+x_n)\,t^{n-1}$$
$$+ \Big(\sum_{i<j} x_i x_j\Big)\,t^{n-2} - \;\dots\; + (-1)^n x_1 \dots x_n$$

$$e_i := \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I| = i}} \; \prod_{i \in I} x_i$$

$$\begin{tikzcd}
\mathbb{Q}(x_1,\dots,x_n) \arrow[d, dash, "n!"] \arrow[d, dash, bend right=60, "S_n"'] \arrow[dd, dash, bend left=60, "\leq n!"] \\
\mathbb{Q}(x_1,\dots,x_n)^{S_n} \arrow[d, equal] \\
\mathbb{Q}(e_1,\dots,e_n)
\end{tikzcd}$$

$\mathbb{Q}(x_1,\_,x_n)$ = c.d.s. su $\mathbb{Q}(e_1,\_,e_n)$

di $t^n - e_1 t^{n-1} + e_2 t^{n-2} + \dots \pm e_n$