

LEZIONI DI ALGEBRA 1
A.A. 2020-21
ILARIA DEL CORSO
UNIVERSITÀ DI PISA

Lezione 01

23 settembre 2020

Ricevimento Lunedì h 17 → Double lezione

$(G, \cdot)$ gruppo

G è cíclico $\Leftrightarrow \exists g \in G$ tale che $G = \langle g \rangle$

$$G \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{ord } g = n \\ \mathbb{Z} & \text{ord } g = +\infty \end{cases} \quad \text{"} \left\{ g^k \right\}_{k \in \mathbb{Z}}$$

$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non è cíclico

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

$G = H \times K \leftarrow$ prodotto diretto

$$\text{ord}(h,k) = \text{lcm}(\text{ord}_H h, \text{ord}_K k)$$

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

$$\text{ord } \bar{x} = \frac{n}{(n, \bar{x})}$$

$(1,0) \quad (0,1) \leftarrow$ generano G

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

Def $(G, \cdot)$ gruppo $S \subset G$ sottoinsieme.

G si dice generato da S $G = \langle S \rangle$

(S è un insieme di generatori per G) e

$$G = \{ \underbrace{s_1 \cdots s_n}_{\in G} \mid n \in \mathbb{N} \quad s_i \in S \cup S^{-1} \}$$

$\in G$ è ovvio perché G è chiuso per inversi e prodotti.

Se $S = \{g\}$

$$G = \{ g^{\epsilon_1} \cdots g^{\epsilon_n} \mid n \in \mathbb{N} \text{ e } \epsilon_i = \pm 1 \}$$

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (1, 0), (0, 1) \rangle$$

$$G = \{ (1, 0), (0, 1), \underbrace{(1, 0) + (0, 1)}_{(1, 1)}, (1, 0) + (1, 0) = (0, 0) \}$$

Esempio: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \langle \underbrace{s_1 \cdots s_n}_{\in \mathbb{Z}} \mid s_i \in \{2, 3, -2, -3\} \rangle$

↓

$\supseteq$ inclusione ovvia

$\subseteq$ devo mostrare che

$$\forall n \in \mathbb{Z} \exists a, b \in \mathbb{Z}$$

tale

$$n = a \cdot 2 + b \cdot 3 \quad (\otimes)$$

$\Rightarrow$ questo è vero perché $(2,3)=1$ per

$$\exists a_0, b_0 \text{ tale che } a_0 \cdot 2 + b_0 \cdot 3 = 1$$

moltiplicando per n ottengo $\otimes$

! Dovrò vedere che ottengo $1 = 3 - 2 \in \langle 2, 3 \rangle$

$\{2, 3\}$ è un insieme minimale di generatori di $\mathbb{Z}$

ma ha card=2 (non posso buttarne via nessuno)

Def G si dice finitamente generato se
ammette un insieme di generatori di
cardinalità finita

Esercizio: Se G è f.g. $\Rightarrow$ ogni insieme minimale
di generatori ha card finita.

Esempio

$$G = \mathbb{Z}/6\mathbb{Z} = \langle \bar{2}, \bar{3} \rangle$$

$\uparrow$ $\uparrow$
ord 3 ord 2

$$S_3 = \langle \overset{\sigma}{(123)}, \overset{\tau}{(12)} \rangle$$

$\searrow$ $\swarrow$
ord=3 ord=2

$$S_3 = \{id, \tau, \sigma^2, \sigma\tau, \sigma^2\tau\}$$

Hanno entrambi 2 generatori ma di ordine 3
 e uno di ordine 2 ma non sono isomorfi.

$$G = \langle x, y \mid x^3 = e, y^2 = e, xy = yx \rangle = \mathbb{Z}/6\mathbb{Z}$$

relazioni
tra i generatori

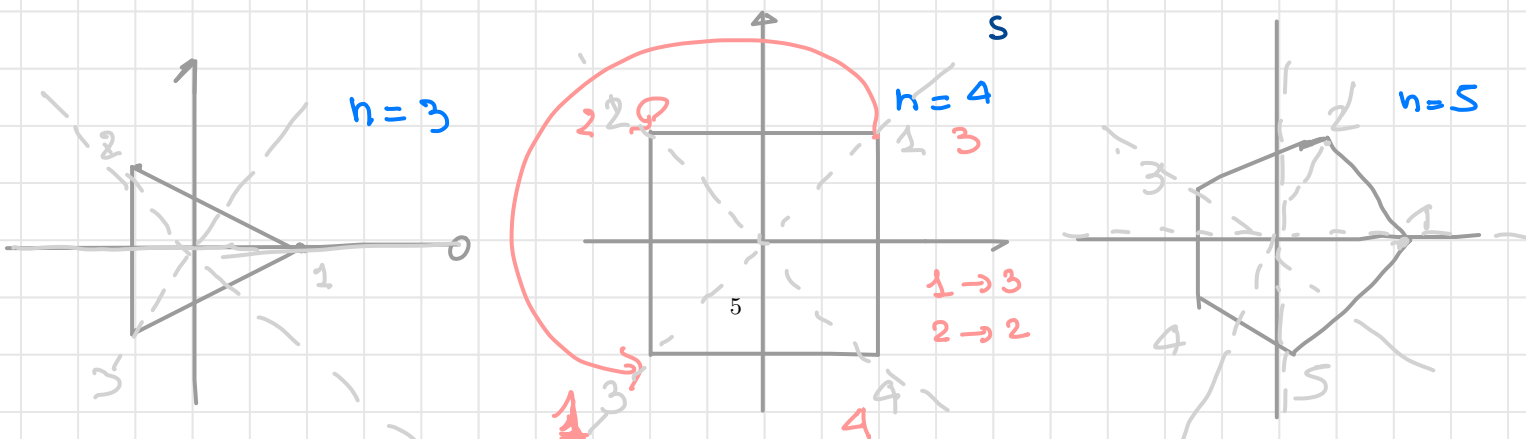
$$\langle x, y \mid x^3 = e, y^2 = e, xy = yx^2 \rangle = S_3$$

non è suff
a descrivere
il gruppo

$(S_n, \circ)$ è un gruppo non abeliano di ordine $n!$

Gruppo diedrale D_n ($n \geq 3$)

D_n è l'insieme ^{gruppo} delle isometrie del piano che manda in sé l' n -agono regolare



$$|D_n| \leq 2n$$

$x \in D_n \quad x(1) = i \quad \leftarrow n \text{ scelte}$
 $\downarrow$
 manda vertici in vertici e
 lati in lati

$\rightarrow$ il lato $1-2 \rightarrow i - \frac{i+1}{i-1}$

$$x(2) = \begin{cases} i-1 \\ i+1 \end{cases} \quad 2 \text{ scelte}$$

Dopo queste scelte le altre
 sono obbligate

Per due $|D_n| = 2n$ esistano $2n$ elementi del
 gruppo

In D_n ci sono n rotazioni attorno al centro

$$r = \text{rotazione } \frac{2\pi}{n} \quad \text{id}, r, \dots, r^{n-1}$$

Un n -agone regolare ha n assi di simmetria

e punti fissi $s_1, \dots, s_n$ simmetriche in D_n

$$D_n = \{ \text{id}, r, \dots, r^{n-1}, s_1, \dots, s_n \}$$

$\leftarrow$ sono $2n$ perche
 $r^i \neq s_j$

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

$$= \langle r, s \mid r^n = \text{id}, s^2 = \text{id} \rangle$$

$$sr^i \neq sr^j \quad \forall i \neq j$$

$$sr^i \neq r^j \quad rs = sr^{-1}$$

lo vedo usando la legge di cancellazione

$$\text{ord } r = n$$

$$\text{ord } s_n = \text{ord}(sr^{\dot{0}}) = 2 \quad \leftarrow n \text{ elementi, oh ordine } 2$$

$$sr(1) = s(2) = n$$

$$sr(2) = r^{-1}s(2)$$

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

$$\Rightarrow \boxed{sr = r^{-1}s}$$

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

Sgr di D_n $\langle sr^{\dot{0}} \rangle < D_n \leftarrow$ Es: non sono normali

$$\langle r \rangle < D_n \quad \text{ord } \langle r \rangle = n \quad [D_n : \langle r \rangle] = 2$$

$$\Rightarrow \langle r \rangle \triangleleft D_n$$

I sgr oh ordine 2
sono normali

$$\langle r^{\dot{0}} \rangle \triangleleft D_n \quad \text{PERCHÉ?}$$

$$H \triangleleft G \quad \forall g \in G$$

$$gH = Hg$$

$$\sim \forall g \in G \quad gHg^{-1} \subseteq H$$

$\langle r \rangle$ è l'unico sgr oh ordine n
oh D_n

ha un unico sgr oh ordine $d \quad \forall d|n$

$\langle r^{n/d} \rangle$ è l'unico sgr ^{ciclico} oh ordine d di D_n
se $d > 2$

Perché contiene tutti gli el oh ordine d

di D_n

Se $H \leq$ l'unico sgr oh ordine d di G

$$\Rightarrow H \triangleleft G \quad (\text{infatti } \forall g \in G$$

Inoltre se H è
ciclo gHg^{-1} è ciclo

gHg^{-1} è un sgr di G
di ordine d

$$H = \langle x \rangle \quad gHg^{-1} = \langle gxg^{-1} \rangle$$

e se H è l'unico $\Rightarrow$

quindi se H è l'unico sgr
ciclo di un certo ordine di $G \Rightarrow$

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

$$\langle r^{n/2} \rangle \triangleleft D_n \quad 2|n, \text{ infatti } H \triangleleft G$$

$$Z(D_n) = \begin{cases} \{1\} & n \text{ dispari} \\ \langle r^{n/2} \rangle & n \text{ pari} \end{cases}$$

$$Z(G) \triangleleft G$$

$$Z(G) = \{ g \in G \mid gx = xg \quad \forall x \in G \} \quad \text{CENTRO DI } G$$

$$Z(D_n) = \{ s^i r^j \in D_n \mid \begin{aligned} s^i r^j \cdot r &= r \cdot s^i r^j \\ s^i r^j \cdot s &= s \cdot s^i r^j \end{aligned} \}$$

$\downarrow$
commute con tutti

gli $x \in G (\Rightarrow)$ commute con un insieme
di generatori di G

$$x = s^\varepsilon r^j \quad x \in \langle CD_n \rangle$$

$$sr = r^{-1}s$$

$$\boxed{x \cdot s = s \cdot x}$$

$$s^\varepsilon r^j s = \underline{s^{\varepsilon+1} r^{-j}} = s s^\varepsilon r^j = \underline{s^{\varepsilon+1} r^j}$$

$$-j \equiv j \pmod{n} \quad (\Rightarrow) \quad 2j \equiv 0 \pmod{n}$$

$$n \text{ dispari} \quad j \equiv 0 \pmod{n}$$

$$x = s^\varepsilon \quad x = \begin{cases} id \\ s \end{cases}$$

$$n \text{ pari} \quad j \equiv 0 \pmod{n/2}$$

$$sr \neq rs$$

$$x = s r^{n/2}, \quad r^{n/2}$$

$$\boxed{s r^{n/2} \cdot r \neq r s r^{n/2} = s r^{-1+n/2}}$$

$$\langle CD_n \rangle = \begin{cases} \{id\} & n \text{ dispari} \\ \langle r^{n/2} \rangle & n \text{ pari} \end{cases}$$

Osservazione: $D_n < S_n \leftarrow$ identificato con le permutazioni degli n vertici dell' n -agone

Automorfismi di G

G gruppo $\text{Aut}(G) = \{ \varphi: G \rightarrow G \mid \varphi \text{ iso} \}$

$(\text{Aut}(G), \circ)$ è un gruppo

$\text{Aut}(G) < \Sigma(G) = \{ \varphi: G \rightarrow G \mid \text{bijective} \}$
permutazioni di G

($\text{id} \in \text{Aut}(G)$, $\varphi \in \text{Aut}(G) \Rightarrow \varphi^{-1} \in \text{Aut}(G)$)

Se $\varphi, \psi \in \text{Aut}(G)$ $\varphi \circ \psi \in \text{Aut}(G)$

Esempi

- $\text{Aut}(\mathbb{Z}) = \{ \pm 1 \}$

$$1 \mapsto a$$

$$\Rightarrow n \mapsto na$$

- $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$

$$\varphi \mapsto \varphi(\pm 1)$$

- $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$ pensateci!

- $\text{Aut}(S_3) \cong S_3$ lo vediamo tra poco.

- $\text{Aut}(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_n) \cong GL_n(\mathbb{F}_p)$

lo vediamo più avanti.

Automorfismi interni

G gruppo $\forall g \in G$

coniugio $\rightarrow \varphi_g \quad G \rightarrow G$
 $x \mapsto g x g^{-1}$ conjugato di x

Proposizione 1:

1) $\varphi_g \in \text{Aut}(G) \quad \forall g \in G$

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

$\uparrow$
gruppo degli automorfismi interni

Dim: $\varphi_g \quad G \rightarrow G$ è ben definita OK

φ_g è omo: $\forall x, y \in G$

$$\varphi_g(xy) = \varphi_g(x) \varphi_g(y)$$

In fatti,

$$\begin{aligned} \varphi_g(xy) &= g(xy)g^{-1} = g x (g^{-1}g) y g^{-1} = \\ &= (g x g^{-1}) (g y g^{-1}) = \\ &= \varphi_g(x) \varphi_g(y) \end{aligned}$$

φ_g è su: $\forall y \in G \quad \exists x \in G \text{ t.c.}$

$\varphi_g(x) = y$ Funzione con

$x = g^{-1} y g \in G$

φ_g is injective: $\ker \varphi_g = \{x \in G \mid \varphi_g(x) = g \cdot x \cdot g^{-1} = e\}$
 $\parallel$
 $\{e\}$ $\begin{matrix} gx = g \\ x = e \end{matrix}$

2) $\text{id} = c_g \in \text{Irr}(G)$

$$\forall g_1, g_2 \in G, \varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 g_2} \in \text{Irrn}(G)$$

Infinite, $\varphi_{g_1} \circ \varphi_{g_2}(x) = \varphi_{g_1}(g_2 \times g_2^{-1}) = g_1 g_2 \times g_2^{-1} g_1^{-1}$
 $= (g_1 g_2) \times (g_1 g_2)^{-1} = \varphi_{g_1 g_2}(x)$

$$(\varphi_g)^{-1} = \varphi_{g^{-1}} \in \text{Irr}(G)$$

$$\forall f \in \text{Aut}(G) \quad f \in \text{Inn}(G) \iff f^{-1} \in \text{Inn}(G)$$

$$\forall f \in \text{Aut}(G) \quad \forall g \in G$$

$$f \circ \varphi_g \circ f^{-1} = \varphi_{\underbrace{f(g)}} \in \text{Inn}(G)$$

$$\begin{aligned} x \in G \quad f \circ g \circ f^{-1}(x) &= f(g(f^{-1}(x))) = f(g f^{-1}(x) g^{-1}) = \\ &= f(g) f f^{-1}(x) f(g^{-1}) \stackrel{12}{=} f(g) \times f(g)^{-1} = e_{f(g)} \blacksquare \end{aligned}$$

Oss: Se G è abeliana $\Rightarrow \text{Inn}(G) = \{\text{id}\}$

$$g \times g^{-1} = x \quad \forall x, g \in G$$

Prop 2: $\text{Inn}(G) \cong G/Z(G)$

Dim: $\phi: G \longrightarrow \text{Inn}(G)$

$$g \longmapsto \varphi_g$$

È caratterizzata ben definita e surgettiva.

ϕ è omo: $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$

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

vero, già visto!

$$\ker \phi = \{g \in G \mid \varphi_g = \text{id}\} =$$

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

$$= Z(G)$$

Il teorema di isomorfismo ci dà

$$G/Z(G) \cong \text{Inn}(G)$$



$$(gZ(G) \longmapsto \varphi_g) \quad g'Z(G) = gZ(G) \quad \varphi_{g'} = \varphi_g$$

Per ripassare! $G/Z(G)$ ciclico $\Rightarrow$ Gabeliano

$\text{Inn}(G)$ ciclico $\Rightarrow G$ abeliano $\Rightarrow \text{Inn}(G) = \{1\}$

Oss: $N \trianglelefteq G \Leftrightarrow \forall \varphi_g \in \text{Inn}(G) \varphi_g(N) = N$
($\subseteq$)

Equivalentemente:

I sgr normali di G sono i sgr INVARIANTI
per automorfismi interni.

$N \trianglelefteq G$: $\text{Inn} G \longrightarrow \text{Aut} N$
 $\varphi_g \longmapsto \varphi_{g|N}$

$(\varphi_{g|N} : N \rightarrow N)$

Def: $H < G$ si dice CARATTERISTICO se

è invariante per automorfismi.

$\forall f \in \text{Aut} G$

$f(H) = H$

$\text{Aut} G \rightarrow \text{Aut}(H)$

$f \mapsto f|_H$

(anche in questo caso basterà verificare che

$f(H) \subset H \quad \forall f \in \text{Aut}(G)$

perché si ha anche $f^{-1}(H) \subset H$

che con in altre ~~parole~~ $f(H) \subset f(H)$)

H CARATTERISTICO IN $G \Rightarrow H \trianglelefteq G$

$$f(H) = H \quad \forall f \in \text{Aut}(G) \Rightarrow \varphi_g H = H \quad \forall g \in G.$$

Il viceversa è falso.

$$G = \mathbb{Z}/2 \times \mathbb{Z}/2 \quad \{(0,0), (1,0), (0,1), (1,1)\}$$

$$H_1 = \langle (1,0) \rangle \quad H_2 = \langle (0,1) \rangle \quad H_3 = \langle (1,1) \rangle$$

$H_i \trianglelefteq G$ perché è abeliano

$$\varphi \quad f \quad (1,0) \rightarrow (1,1)$$

$$(0,1) \rightarrow (0,1)$$

$$\begin{aligned} \underline{f(a,b)} &= a f(1,0) + b f(0,1) = \\ &= (a,a) + (0,b) = \underline{(a, a+b)} \end{aligned}$$

al momento devo argomentare che è un omom.

$$f(H_1) = H_3$$

$H_1 \trianglelefteq G$ ma non è CARATT.

$$\boxed{\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3}$$

scambi dei 3 elementi di ordine 2

$$(0,0) \rightarrow (0,0)$$

$$f^{15}(1,0)$$

$$f(0,1) \quad f(1,1)$$

→ ho $3!$ funzioni che fissano $(0,0)$
e scambiano i 3 el di ordine 2

Occorre verificare che Tutte le 6 funn
sono omomorfismi.

$$\text{Aut}(S_3) \cong S_3$$

$$\text{Inn}(S_3) \cong \frac{S_3}{Z(S_3)} \cong S_3$$

$$S_3 \cong \text{Inn}(S_3) \trianglelefteq \text{Aut } S_3$$

Basta vedere che $|\text{Aut } S_3| \leq 6$

$f \in \text{Aut}(S_3)$ può al più scambiare
i 3 el di ordine 2.

generano S_3

$$\left\{ \begin{array}{l} (1,2) \rightarrow \\ (1,3) \rightarrow \\ (2,3) \rightarrow \end{array} \right.$$

$$\Rightarrow (123) = (13)(12)$$

$$1 \rightarrow 2$$

$$2 \rightarrow 3$$

$$3 \rightarrow 1$$

$$(132) = (12)(13)$$

$$\Rightarrow |\text{Aut}(S_3)| \leq 6$$

Schematizziamo:

S_3 è generato dai 2-cicli

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

Al massimo posso decodificare
le loro immagini.

Gli aut conservano l'ordine

algebrici $ab \rightarrow ba$ può essere scambiati

$\rightarrow$ Al massimo ho 6 automorfismi

$$\Rightarrow |\text{Aut}(S_3)| \leq 6$$

D'altra parte $S_3 \cong \text{Inn}(S_3) \leq \text{Aut}(S_3)$

$$\Rightarrow \text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3.$$

AZIONE DI UN GRUPPO SU UN INSIEME.

G gruppo e X insieme

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

$$\varphi: G \longrightarrow \mathcal{S}(X)$$

$$g \longmapsto \varphi_g$$

$$\varphi_g$$

$$x \longmapsto g \cdot x$$

$$x^g$$

$$\varphi_g(x)$$

φ omom

$$\varphi_g: X \rightarrow X$$

bigettiva $\forall g$.

Esempio $X=G$

$$\begin{aligned} \varphi: G &\longrightarrow S(G) \\ g &\longmapsto \varphi_g = \text{conjugazione per } g \end{aligned}$$

è l'azione (abbiamo già visto nelle
prop2 che φ è omom. e φ_g è bigettivo P1)

$$\begin{aligned} \varphi_g(x) &= \int \frac{g \cdot x}{x \cdot g} \\ &\parallel \\ g \times g^{-1} &= e \end{aligned}$$

Esempio 2 V K -sp.

$$\begin{aligned} \varphi: K^* &\longrightarrow S(V) \\ \lambda &\longmapsto \varphi_\lambda: V \longrightarrow V \\ &\quad v \longmapsto \lambda \cdot v \end{aligned}$$

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

φ definisce su X una relazione di equivalenza

$$x \sim y \iff \exists g \in G \text{ tale che } \varphi_g(x) = y$$

$$\text{e' ok eq} \quad x \sim x \quad g=e \quad \varphi_e(x) = x$$

$$x \sim y \Rightarrow y \sim x$$

$$\varphi_g x = y \quad x = \varphi_{g^{-1}}(y)$$

$$x \sim y \quad y \sim z \quad y = \varphi_g(x) \quad z = \varphi_h(y)$$

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

$\sim$ è una relazione di equivalenze su X

Chiamiamo orbite le classi di equivalenze

$$\text{orbita}(x) = \{\varphi_g(x) \mid g \in G\} \subset X$$

$$X = \bigcup_{x \in R} \text{orbita}(x)$$

R = insieme di rappresentanti

Def: $\forall x \in X$ si dice STABILIZZATORE di x

$$\text{St}(x) = \{g \in G \mid \varphi_g(x) = x\}$$

Prop: $\text{St}(x) < G$

(in generale non è sgr normale)

Dim: $e \in \text{St}(x) \quad \varphi_e = \text{id}$

$g \in \text{St}(x) \quad \varphi_g(x) = x$

$$(\varphi_g)^{-1} \varphi_g(x) = (\varphi_g)^{-1}(x) \quad \text{q è om}$$

Osserviamo che $(\varphi_g)^{-1} = (\varphi(g))^{-1} = \varphi(g^{-1}) = \varphi_{g^{-1}}$

$$x = \varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(x) \Rightarrow g^{-1} \in \text{St}(x)$$

$$g, h \in \text{St}(x) \quad \varphi_g(x) = x \quad \varphi_h(x) = x$$

$$\Rightarrow \varphi_{hg}(x) \stackrel{\text{comp}}{=} (\varphi_h \circ \varphi_g)(x) = \varphi_h(\varphi_g(x))$$

$$= \varphi_h(x) = x \Rightarrow hg \in \text{St}(x) \quad \square$$

Oss: $x \in X \quad h, g \in G$

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

$$\Leftrightarrow \varphi_{h^{-1}g}(x) = x \Leftrightarrow h^{-1}g \in \text{St}(x)$$

$$\Leftrightarrow g \text{St}(x) = h \text{St}(x)$$

quindi

$$\begin{array}{ccc} \text{orb}(x) & \longleftrightarrow & \begin{array}{c} \text{clami laterali di } \text{St}(x) \\ \cdot \\ \text{in } G \end{array} \\ \varphi_g(x) & \longrightarrow & g \text{St}(x) \end{array}$$

Proposizione: G gruppo finito $\forall x \in X$

$$|G| = |\text{orb}(x)| |\text{St}(x)| \quad (\text{impedimento } |\text{orb}(x)| \mid |G|)$$

AZIONE DI CONIUGIO

$$X = G \quad \varphi \quad G \longrightarrow \text{Inn}(G) < \mathcal{S}(G) \\ g \longmapsto \varphi_g \quad x \longmapsto g x g^{-1}$$

Abbiamo già osservato che si ha azione

$$\begin{aligned} \text{orb}(x) &= \{ \varphi_g(x) \mid g \in G \} = \\ &= \{ g x g^{-1} \mid g \in G \} = \text{CLASSE DI CONIUGO DI } x \\ &= C_x \end{aligned}$$

$$\begin{aligned} \text{St}(x) &= \{ g \in G \mid \varphi_g(x) = g x g^{-1} = x \} = \\ &= Z_G(x) \quad \text{CENTRALIZZATORE DI } x. \end{aligned}$$

La prop precedente ci dice che se $|G| < +\infty$

$$\Rightarrow |G| = |C_x| |Z_G(x)|$$

$$\text{In particolare } |C_x| \mid |G|$$

$\uparrow$
è un sottoinsieme.

AZIONE DI CONIUGIO SUI SGR DI G

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

$$\varphi \quad G \longrightarrow \mathcal{S}(X)$$

$$\begin{array}{ccc} g \longmapsto \varphi_g & X \longrightarrow X \\ & H \longmapsto g H g^{-1} \end{array}$$

φ è suriezione (verifica per esercizio)
che chiamiamo ancora coniugio.

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

$$= N_G(H) \quad \text{normalizzatore di } H$$

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

$$H \trianglelefteq G \Leftrightarrow \text{orb}(H) = \{ H \} \Leftrightarrow \text{St}(H) = N_G(H) = G$$

$$\frac{\# \text{ coniugati di } H}{\# \text{ orb}(H)} = \frac{|G|}{|N_G(H)|}$$

Obs! $H < G \quad H \trianglelefteq G \Leftrightarrow$

$$H = \bigcup_{h \in H} C_h \quad \leftarrow \text{i sgr normali sono unioni di classi di coniugio dei propri elementi}$$

PENSARE

Formula delle classi

G $X = G$ azione di coniugio

$$\begin{aligned} \varphi & G \longrightarrow \Sigma(G) \\ g & \longmapsto \varphi_g \in \text{Inn}(G) \\ & \varphi_g x \longmapsto g x g^{-1} \end{aligned}$$

$$\begin{aligned} \text{orb}(x) &= \{ \varphi_g(x) \mid g \in G \} = \\ &= \{ g x g^{-1} \}_{g \in G} = C_x \leftarrow \text{classe di} \\ & \quad \text{coniugio} \end{aligned}$$

$$C_x = \{x\} \iff g x g^{-1} = x \quad \forall g \in G \iff x \in Z(G)$$

Più in generale

$$\underbrace{|C_x|}_{\text{orb}(x)} \underbrace{|Z_G(x)|}_{\text{st}(x)} = |G|$$

$$G (= X) = \bigcup_{x \in R} \text{orb}(x) = \bigcup_{x \in R} C_x$$

Se G è un gruppo finito, passando alle cardinalità otteniamo

$$|G| = \sum_{x \in R} |C_x| = \sum_{x \in Z(G)} \overset{|C_x|}{1} + \sum_{x \in R \setminus Z(G)} |C_x|$$

$$|G| = |Z(G)| + \sum_{x \in R, Z(G)} \frac{|G|}{|Z_G(x)|}$$

FORMULA
DELLE
CLASSI

Oss: $H \leq G$.

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

Se $H \trianglelefteq G$ $H = \bigcup_{x \in R \cap H} C_x$

Se $|H| < +\infty$

$$|H| = \sum_{x \in R \cap H} |C_x| =$$

$$= \sum_{x \in Z(G) \cap H} 1 + \sum_{x \in (R \setminus Z(G)) \cap H} \frac{|G|}{|Z_G(x)|} =$$

$$|H| = |Z(G) \cap H| + \sum_{x \in \dots} \frac{|G|}{|Z_G(x)|}$$

Applicazione delle formule delle classi ai p-gruppi

Un p-gruppo è un gruppo finito di ordine p^n
(p è primo)

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

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

$\uparrow$
 $p \mid |G|$

$\frac{|G|}{|Z_G(x)|} > 1$
 p^{α_x} $\alpha_x \geq 1$
 $p \mid |G/Z_G(x)| \quad \forall x$

$$\Rightarrow p \mid |Z(G)| = |G| - \sum_{x \in R \setminus Z} |G/Z_G(x)|$$

2) Un gruppo di ordine p^2 è abeliano.

$$|G| = p^2$$

$$|Z(G)| = \begin{cases} 1 \\ p \\ p^2 \end{cases}$$

← no perché il centro di un p -gr è non banale

No perché allora $|G/Z(G)| = p$

cioè $G/Z(G)$ c'è

ma questo non può essere perché G non è abeliano

$\Rightarrow G$ è abeliano.

Teorema di Cauchy

p primo, G gruppo finito.

Se $p \mid |G| \Rightarrow \exists x \in G$ ₂₅ $\text{ord}(x) = p$.

Il Teorema è già noto per gruppi abeliani

Dim: $|G| = p^n$

Per induzione su n

$n=1$ $|G|=p$ ovvio.

Supponiamo vera la Ten. per gruppi di ordine

p^m $1 \leq m < n$.

1) $\exists H \subsetneq G$ $p \mid |H|$ $\leftarrow |H| = p^m$ $m < n$ e per p
voluto $\exists x \in H \subset G$

2) $\forall H \subsetneq G$ $p \nmid |H|$ - Uso la $\neq$ delle classi
 $\text{ord}(x) = p$

$$p^n = |G| = |Z(G)| + \sum_{x \in \dots} \frac{|G|}{|Z(x)|}$$

p^n (pointing to $|G|$)
 $p \nmid |Z(x)|$ (pointing to denominator)
perché $Z(x) \subsetneq G$ (pointing to denominator)
 $p \mid \frac{|G|}{|Z(x)|} \quad \forall x$ (pointing to the fraction)

$$\Rightarrow p \mid |Z(G)| = \underbrace{|G|}_{p^n} - \sum p \ell_x$$

$\Rightarrow$ perché siamo nel caso 2 $\Rightarrow Z(G) = G$

e il Teorema vale perché G è abeliano. $\square$

Esercizio 1

Sia G un p -gruppo di ordine p^n
 $\Rightarrow G$ ammette sottogruppi normali di

ordine $p^h \quad \forall 0 \leq h \leq n$.

AGGIUNTA POST LEZIONE: La dimostrazione fatta mostra che i sgr possono
esser presi in catena - Cioè $\exists \{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_n = G$ con $|H_k| = p^k$
e $H_{k-1} \triangleleft G$

Caso G abeliano: $x \in G \quad \text{ord}(x) = p$ e consider

$G_1 = G / \langle x \rangle \leftarrow$ per ip induttiva G_1
che ha ordine p^{n-1}
ha sgr normali di ordine p^h
 $\forall 0 \leq h \leq n-1$

Uso il Teorema di corrispondenza i sgr di G e
i sgr di G_1

$$G \xrightarrow{\pi} G_1 = G / \langle x \rangle$$

$$\pi^{-1}(H) \leftarrow \dots H \triangleleft G_1$$

$$\pi^{-1}(H) \triangleleft G \quad [G_1 : H] = [G : \pi^{-1}(H)]$$

$$|H_h| = p^h \quad 0 \leq h \leq n-1$$

$$|\pi^{-1}(H_h)| = p^{h+1} \Rightarrow \text{ho trovato sgr (normali)} \\ \text{di ord } p^k \quad 1 \leq k \leq n$$

D'altra parte $\langle x \rangle$ ha ordine p (è normale)

Caso generale: per induzione su n -

$n=1$ ovvio

$$G_1 = G/Z(G) \quad |G_1| = p^m \quad m < n$$

Per ip induzione G_1 ammette sgr normali di ordine p^h $\forall 0 \leq h \leq m = n - z$ $|Z(G)| = p^z$

Come sopra uso il Teo ch' corrisponde:

$$\text{Ho in } G_1 \quad H_h \triangleleft G \quad \forall 0 \leq h \leq n - z$$

$$\pi^{-1}(H_h) = H_{h+z} \quad |H_{h+z}| = p^{h+z}$$

$$([G : \pi^{-1}(H_h)] = [G_1 : H_h] = \frac{p^{n-z}}{p^h} = p^{n-(h+z)})$$

$\Rightarrow$ ho trovato sgr normali di G di ordine p^k $z \leq k \leq n$

D'altra parte $Z(G)$ è un gruppo abeliano di ordine p^z e quindi contiene sgr normali di ordine p^e $0 \leq e \leq z$ per le

prima parte dell'esercizio - *Questi sgr sono normali anche in G perché sono contenuti nel centro*

Oss: Posso scrivere una successione esatta corta

$$0 \rightarrow Z(G) \xrightarrow{i} G \xrightarrow{\pi} G/Z(G) \rightarrow 0$$

$$(\quad 0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0 \quad) \quad \text{Im } \alpha = \text{Ker } \beta$$

iniettiva *surgettiva*

$$\dots \rightarrow A_{i-1} \xrightarrow{\alpha} A_i \xrightarrow{\beta} A_{i+1} \rightarrow \dots$$

e esatti in A_i se $\text{Im } \alpha = \ker \beta$

Teorema di Cayley

Ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni.

In particolare se $|G| = n$ G è isomorfo a un sgr di S_n .

Dim

G gruppo $S(G)$

$$\lambda : G \longrightarrow S(G)$$

$$g \longmapsto \varphi_g : G \longrightarrow G$$

$$x \longmapsto gx$$

Dico che λ è un omo iniettivo.

λ è ben definita; cioè $\varphi_g \in S(G)$

φ_g è iniettiva per l.d. cano.

φ_g è su perché $g^{-1}y \longmapsto y$

λ è omo

$$\lambda(g_1 g_2) = \varphi_{g_1 g_2}$$

"

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

)) vero perché $\forall x$

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

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

$\lambda \in \text{miętwo}$ $\ker \lambda = \{ g \in G \mid \varphi_g = \text{id} \} = \{e\}$ □

Esempio

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} &\hookrightarrow S(\mathbb{Z}/6\mathbb{Z}) \cong S_6 & (a, b, c) & (d, e) \\ \bar{0} &\longmapsto \varphi_0 = \text{id} & a &\rightarrow b \\ & & b &\rightarrow c \\ & & c &\rightarrow a \\ \bar{1} &\longmapsto \varphi_{\bar{1}}(a) = \bar{1} + a & d &\rightarrow e \\ & & e &\rightarrow d \\ & & & (0, 1, 2, 3, 4, 5) \\ \bar{2} &\longrightarrow \varphi_{\bar{2}} & a &\mapsto \bar{2} + a & (0, 2, 4) & (1, 3, 5) \end{aligned}$$

In generale $G \rightarrow S(G)$

$$G = \{x_1, \dots, x_n\} \quad g \longmapsto \varphi_g \quad (x_1, gx_1, g^2x_1, \dots, g^{k-1}x_1)$$

$g \in G$ $k = \text{ord } g$

Sottogruppo derivato e abelianizzato di un gruppo

Sottogruppo derivato = sottogruppo dei commutatori

commutatore tra x e y

$$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle \text{ dove } [x, y] = xyx^{-1}y^{-1} \quad (=1 \Leftrightarrow xy = yx)$$

$$S = \{ [x, y] \mid x, y \in G \}$$

$$G' = [G : G] = \langle S \rangle$$

Proposizione

- 1) G' è un sottogruppo caratteristico (e quindi normale) di G
- 2) $G' = \{1\} \Leftrightarrow G$ è abeliano
- 3) $H \triangleleft G$ G/H è abeliano $\Leftrightarrow G' \subset H$

In particolare G/G è abeliano (è il max quoz. abeliano di G)
e si chiama abelianizzato di G

Dim: $\forall f \in \text{Aut}(G) \quad f(G') \subseteq G'$

$$f(G') = f(\langle S \rangle) = \langle f(S) \rangle \subseteq G'$$

$$\begin{aligned} f([x, y]) &= f(xy x^{-1} y^{-1}) = f(x) f(y) f(x)^{-1} f(y)^{-1} \\ &= [f(x), f(y)] \in G' \end{aligned}$$

(2) è un caso particolare di (3)

(3) G/H è abeliano $\Leftrightarrow \forall x, y \in G$

$$xH yH = yH xH \Leftrightarrow xyH = yxH$$

$$\Leftrightarrow x^{-1}y^{-1}xy \in H \Leftrightarrow S \subset H \Leftrightarrow G' \subset H$$

" $[x^{-1}, y^{-1}]$ " ▣

Permutazioni:

S_n = gruppo delle permutazioni su n elementi
di $\{1, \dots, n\}$

$\sigma \in S_3$

$\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$

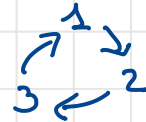
$(1\ 2\ 3)$

"

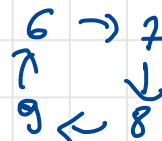
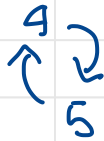
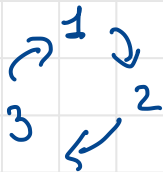
$(2\ 3\ 1)$

"

$(3\ 1\ 2)$



Esempio S_{10} $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 5 & 9 & 7 & 8 & 5 & 6 & 10 \end{pmatrix}$



$10 \rightarrow 5$

$(8\ 9\ 6\ 7)$

$\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9)(10)$

↑ in genere non si scrive

I numeri che non compaiono vengono lasciati fissi

Formalmente

$\sigma \in S_n$

descrivere σ vuol dire dare l'azione di σ su $\{1, \dots, n\} = X$

$\varphi \quad G = \langle \sigma \rangle \longrightarrow S_n$ azione di G su X

$\sigma \longmapsto \sigma \quad i \longmapsto \sigma(i)$

Considero l'azione di $\langle \sigma \rangle$ su S_n

data dall'inclusione

$$\text{orb}(x) = \{ \sigma^k(x) \mid k \geq 0 \} \quad (\text{orb}(x) = \{gx \mid g \in G\})$$
$$= \{ x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x) \}$$

$$|\text{orb}(x)| = m_x$$

L'azione $\langle \sigma \rangle$ su X divide X in orbite

e su ogni orbita σ agisce ciclicamente

$$\sigma(\text{orb}(x)) = \text{orb}(x)$$

$$m_x = \min \{ k > 0 \mid \sigma^k(x) = x \}$$

$$\text{perch\u00e9} \quad \text{se } \sigma^k(x) = x \quad \sigma^{k+1}(x) = \sigma(x)$$

$$\text{Sia } k \text{ il min tale che } \sigma^k(x) \in \{x, \dots, \sigma^{k-1}(x)\}$$

$$\Rightarrow \sigma^k(x) = \sigma^h(x) \quad 0 \leq h < k$$

$$\text{Allora vale anche } \sigma^{k-h}(x) = x \in \{x, \dots, \sigma^{k-1}(x)\}$$

e per la minimalit\u00e0 di k si ha $h=0$.

Def Sia che ciclo di $\sigma \in S_n$ l'orbita

di un elemento $x \in \{1, \dots, n\}$ vista

come insieme ordinato

Dato $\sigma \rightarrow$ ho le sue orbite $\rightarrow$ le guardo
 come insieme ordinato $(x, \sigma(x), \dots, \sigma^{m_x-1}(x))$
 ciclo di σ

Oss 1: Un ciclo di lunghezza k ha k scritture
 k -ciclo

(posso scegliere arbitrariamente il 1° el)

Oss 2: $\sigma \in S_n$ è determinato dalle immagini
 di $\{1, \dots, n\} \Rightarrow$ è determinata dai suoi
 cicli

$$\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9) \in S_{10}$$

$$\sigma_1 = (1\ 2\ 3) \quad \sigma_2 = (4\ 5) \quad \sigma_3 = (6\ 7\ 8\ 9)$$

$$\sigma_1, \sigma_2, \sigma_3 \in S_{10}$$

$$\sigma_2 \quad \begin{array}{l} 4 \rightarrow 5 \\ 5 \rightarrow 4 \\ i \rightarrow i \quad \forall i \neq 4, 5 \end{array}$$

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$$

Def: una permutazione si dice **CICLICA** se ha
 un unico ciclo non banale.

Oss: • cicli disgiunti commutano

• L'ordine di una permutazione ciclica
 è la lunghezza del suo ciclo

$$\sigma = (\underbrace{x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_k}_{\text{ciclo}}) \quad \text{ord } \sigma = k$$

$$\sigma^k = \text{id} \quad \text{e se } d < k \quad \sigma^d(x) = x_{d+1} \neq x$$

Proposizione: Ogni permutazione si scrive in modo "unico" come prodotto di cicli disgiunti
 come composizione di permutazioni cicliche che agiscono su insiemi disgiunti

"unico" = a meno dell'ordine e delle scritte dei cicli

Dim: Sostanzialmente abbiamo già detto tutto

→ i cicli sono le orbite e quindi sono univ. determinate

→ cicli disgiunti non mudano.

Corollario: S_n è generato dalle permutazioni cicliche.

Esempio

$$\begin{array}{ll}
 S_4 & \text{id} \\
 (a, b) & \leftrightarrow 2 \text{ cicli} = \text{Trasposizione} \quad \binom{4}{2} 1! = 6 \\
 (a, b, c) & \leftarrow 3\text{-cicli} \quad \binom{4}{3} 2! = 8 \\
 (a, b, c, d) & \leftarrow 4 \text{ cicli} \quad \binom{4}{4} 3! = 6 \\
 (a, b)(cd) & \leftarrow 2+2 \quad \binom{4}{2} \binom{2}{2} 1! 1! \frac{1}{2!} = 3
 \end{array}$$

$$\# \{ \sigma \in S_n \mid k\text{-cicli} \} = \binom{n}{k} \frac{k!}{k} = \binom{n}{k} (k-1)!$$

$\uparrow$
 scelgo k-elementi

$$\sigma = (12)(24) \in S_4$$

$$\sigma_2 \circ \sigma_1$$

$$\tau = (241)$$

$$2 \xrightarrow{\sigma_1} 4 \xrightarrow{\sigma_2} 4$$

$$4 \xrightarrow{\sigma_1} 2 \xrightarrow{\sigma_2} 1$$

$$1 \xrightarrow{\sigma_1} 1 \xrightarrow{\sigma_2} 2$$

Esempio: $\# \{ \sigma \in S_{20} \mid \sigma \text{ è di tipo } 2+2+2+4+5+5 \}$

$$\sigma = \underbrace{\tau_1 \tau_2 \tau_3}_{t, 2 \text{ ciclo}} \rho \xrightarrow{4 \text{ ciclo}} \underbrace{\eta_1 \eta_2}_{5 \text{ ciclo}}$$

$$= \frac{\binom{20}{2} \binom{18}{2} \binom{16}{2} 1! 1! 1!}{3!} \cdot \binom{14}{4} 3! \cdot \frac{\binom{10}{5} 4! \binom{5}{5} 4!}{2!}$$

Proposizione 2. $\sigma \in S_n \quad \sigma = \sigma_1 \dots \sigma_k \quad \sigma_i \text{ cicli}$

$$\text{disgiunti} \Rightarrow \text{ord } \sigma = \text{lcm}(\text{ord}(\sigma_i))_{i=1}^k$$

$$= \text{lcm}(\text{lunghezza}(\sigma_i))_{i=1, \dots, k}$$

Dim: σ_i è l_i -ciclo

$$\text{ord } \sigma_i = l_i$$

$$ol = [l_1, \dots, l_k]$$

$$\sigma^{ol} = (\sigma_1 \dots \sigma_k)^{ol} \underset{\substack{\uparrow \\ \sigma_i \text{ sono disgiunti} \\ \text{commutano}}}{=} \sigma_1^{ol} \dots \sigma_k^{ol} = \text{id}$$

$$l_i \mid ol \quad \forall i$$

$$m = \text{ord } \sigma \mid ol \quad \text{D'altra parte } \sigma^m = \text{id} = \sigma_1^m \dots \sigma_k^m$$

e poiché i σ_i sono disgiunti necessariamente

$$\sigma_i^m = \text{id} \quad \forall i \Rightarrow l_i = \text{ord}(\sigma_i) \mid m \quad \forall i$$

$$d = [l_1, \dots, l_k] \mid m \Rightarrow d = m \quad \square$$

Proposizione 3: Le trasposizioni (= 2 cicli) generano $S_n \quad \forall n \geq 3$.

Dim: Devo mostrare che ogni permutazione è prodotto di trasposizioni (in generale non disgiunte)

Poiché ogni permutazione è prodotto di cicli

disgiunti, basterà vedere che i cicli sono tutti

prodotto di trasposizioni

$$(1, \dots, k) = (1, k) \underbrace{(1, k-1), \dots, (1, 2)}$$

$$\begin{array}{c} i > k \\ \downarrow \\ i \rightarrow i \end{array}$$

$$i \rightarrow i$$

$$i < k \quad i \rightarrow i+1$$

$$k \rightarrow 1$$

$$i \rightarrow i \xrightarrow{(1, i)} 1 \xrightarrow{(1, i+1)} i+1 \rightarrow i+1$$

$$k \rightarrow k \dots \xrightarrow{(1, k)} 1$$

$\square$

Oss: La scrittura di una permutazione come prodotto di trans non è unica

$$S_4 \quad (12)(24) = (12)(34)(34)(24)$$

La prop seguente ci mostra però che è fissata la parità cioè se σ si scompone con prodotto di m trasposizioni ogni altra dec. come prodotto di trasposizioni ha un numero di trasposizioni con la stessa parità.

Proposizione 4: L'applicazione

$$\begin{aligned} \text{sgn} : \Sigma_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto \text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

è un omomorfismo di gruppi.

Inoltre se $\sigma = \text{trasposizione} \Rightarrow \text{sgn}(\sigma) = -1$

Oss: Questo dimostra quanto detto sopra.

$$\sigma = \tau_1 \cdots \tau_m \quad \tau_i = \text{traspos.}$$

$$\text{sgn}(\sigma) = \prod \text{sgn}(\tau_i) = (-1)^m$$

Dim: sgn è ben definita cioè

$$\text{sgn}(\sigma) = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{\pm 1\}$$

Al denominatore ho tutte le coppie $i - j$ e anche al numeratore perché σ è biettiva può

cambia però l'ordine (1-j) può comparire come i
o come i-j

sgn è omom:

$$\begin{aligned} \text{sgn}(\sigma \circ \tau) &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \frac{\tau(i) - \tau(j)}{i - j} = \\ &= \prod_{i < j} \underbrace{\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}}_{\text{sgn}(\sigma)} \underbrace{\frac{\tau(i) - \tau(j)}{i - j}}_{\text{sgn}(\tau)} \end{aligned}$$

$\sigma = (ab)$ $\text{sgn}(ab) = -1$

$\frac{\sigma(i) - \sigma(j)}{i - j}$ ← numero per le possibili coppie $i < j$

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

• $\{i, a\} \cap \{i, b\}$ $\frac{\sigma(i) - \sigma(a)}{i - a} = \frac{i - b}{i - a}$ $\frac{\sigma(b) - \sigma(i)}{b - i} = \frac{a - i}{b - i} = \frac{i - a}{i - b}$ $\left. \begin{matrix} \\ \end{matrix} \right\} +1$

• $\{i, a\} = \{a, b\}$ $\frac{\sigma(a) - \sigma(b)}{a - b} = \frac{b - a}{a - b} = -1$

$\Rightarrow \text{sgn}(ab) = -1$



Def una permutazione σ si dice PARI se $\text{sgn}(\sigma) = 1$
 DISPARI se $\text{sgn}(\sigma) = -1$

gruppo alterno

$$A_n = \ker(\text{sgn}) = \{ \sigma \in S_n \mid \sigma \text{ è pari} \}$$

$$A_n \triangleleft S_n \quad |A_n| = \frac{n!}{2}$$

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

Oss $(1, \dots, k) = \underbrace{(1, k)(1, k-1) \dots (1, 2)}_{k-1 \text{ trans}}$

$\Rightarrow$ il k -ciclo è pari se k è dispari e viceversa

Classi di coniugio in S_n

Teorema:

Due permutazioni di S_n sono coniugate $\Leftrightarrow$

hanno lo stesso tipo di decomposizione come prodotto di cicli disgiunti

Es: $S_4 \quad C_{(12)} = \{ (ab) \in S_4 \} \quad |C_{(12)}| = \binom{4}{2} 1! = 6$
 $C_{(12)} = \{ (12), (13), (14), (23), (24), (34) \}$

Dim: $\Rightarrow \sigma = (a_1 \dots a_k)$, $\tau \in S_n$ voglio vedere
 che $\tau \sigma \tau^{-1}$ è ancora un k -ciclo.

$$T(a_i) = b_i \quad \text{Allora} \quad T \sigma T^{-1} = (b_1 \dots b_k)$$

$$b_i \neq b_j \text{ se } i \neq j$$

perché T è biettiva.



$$b_i \rightarrow b_{i+1}$$

$$b_i \xrightarrow{T^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{T} b_{i+1}$$

$$x \neq b_i \forall i \text{ a s} x \text{ ho } T \sigma T^{-1}(x) = T T^{-1}(x) = x$$

$$\underbrace{\neq a_1, \dots, a_k}$$

$$a \text{ o } x$$

$$x \rightarrow x$$

$$\text{In generale } \sigma = \sigma_1 \dots \sigma_r \quad \sigma_i = k_i \text{ - ciclo}$$

$$T \sigma T^{-1} = \underbrace{T \sigma_1 T^{-1}}_{k_1 \text{ - ciclo}} \dots \underbrace{T \sigma_r T^{-1}}_{k_r \text{ - ciclo}}$$

$$\sigma \text{ di tipo } k_1 + \dots + k_r$$

$$T \sigma T^{-1} \text{ Tipo } k_1 + \dots + k_r$$

$$\Leftrightarrow \sigma = (a_1 \dots a_e) (b_1 \dots b_s) \dots (z_1 \dots z_t)$$

$$p = (a'_1 \dots a'_e) (b'_1 \dots b'_s) \dots (z'_1 \dots z'_t)$$

Sono permutazioni dello stesso tipo.

$$\text{Voglio trovare } T \text{ tale che } T \sigma T^{-1} = p$$

$$\text{Scelgo } T \text{ definita da } T(a_i) = a'_i$$

$$T(b_i) = b'_i$$

$$T(z_i) = z'_i$$

41

e eventualmente sugli altri al completo

Verifichiamo che $t\sigma t^{-1} = \rho$

$$a'_i \xrightarrow{\tau^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{\tau} a'_{i+1} \quad a'_i \xrightarrow{\rho} a'_{i+1}$$

□

Esempio S_{12} $\sigma = (123)(45678) \quad 3+5$

$$\rho = (425)(9,10,1,3,7) \quad 3+5$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 2 & 5 & 9 & 10 & 1 & 3 & 7 & 6 & 8 & 11 & 12 \end{pmatrix}$$

$t\sigma t^{-1} = \rho$ Lo so già ma lo controllo x es.

$$\tau = (\underbrace{1\ 4\ 9\ 6}_{\uparrow\ \uparrow\ \uparrow}) (\underbrace{3\ 5\ 10\ 8\ 7}_{\uparrow\ \uparrow\ \uparrow}) (\underbrace{2}_{\uparrow}) (\underbrace{11\ 12}_{\uparrow\ \uparrow})$$

$$\tau^{-1} = \begin{pmatrix} 6 & 9 & 4 & 1 \\ 1 & 6 & 9 & 4 \end{pmatrix} \begin{pmatrix} 7 & 8 & 10 & 5 & 3 \\ 3 & 7 & 8 & 10 & 5 \end{pmatrix}$$

$$\begin{aligned} t\sigma t^{-1} &= (1\ 4\ 9\ 6)(3,5,10,8,7)(123)(45678)(6\ 9\ 4\ 1)(7\ 8\ 10\ 5\ 3) \\ &= (4\ 2\ 5)(9,10,1,3,7) \end{aligned}$$

Grubano:

1) Il numero di classi di coniugio in S_n è uguale al numero di partizioni di n

2) $H < S_n$ $H \triangleleft S_n \Leftrightarrow$ contiene tutti & permuta di un certo tipo o nessuno.

Se G_1 e G_2 sono gruppi $G_1 \times G_2$ gruppo con
l'operazione fatta comp per componente $\nwarrow$ **PRODOTTO DIRETTO**

$$\mathbb{Z}/7 \times S_4 \ni \sigma = (\bar{1}, (123)), \rho = (\bar{4}, (1423))$$

$$\sigma \circ \rho = (\bar{1} + \bar{4}, (123)(1423)) =$$

$$= (\bar{5}, (1432))$$

$$\text{Es } \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Teorema 1 G gruppo $H, K \trianglelefteq G$ tali che

$$(1) \quad HK = G$$

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

$$\Rightarrow G \cong H \times K$$

Oss: • Ricordo che se $H, K \leq G$ in generale HK non è un sgr.

$$HK \leq G \Leftrightarrow HK = KH$$

$\uparrow$
se uno ha $K \leq H \trianglelefteq G$
quindi φ è sempre verificato

$$\bullet \quad H \times K < G \times G^{43}$$

- Se ho 2 gruppi G_1 e G_2 costruisco

$$G = G_1 \times G_2$$

$$H = G_1 \times \{e_2\} \triangleleft G$$

$$K = \{e_1\} \times G_2 \triangleleft G$$

$H, K \leq G$ verificano le ip del Teorema 1

$$\Rightarrow G \cong H \times K$$

Lemma

$H, K \triangleleft G, H \cap K = \{e\} \Rightarrow hk = kh \forall h \in H \forall k \in K$

Dim

$$hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})}_{\substack{\in K \\ \in K}} \underbrace{k^{-1}}_{\in K} = h \underbrace{(kh^{-1}k^{-1})}_{\in H} \in H \cap K = \{e\}$$

Dim: Sve

$$\varphi: H \times K \longrightarrow G$$

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

$$\begin{aligned} \varphi \text{ è omo: } \varphi((h_1, k_1)(h_2, k_2)) &= \varphi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \underset{\substack{\uparrow \\ \text{Lemma}}}{=} h_1 k_1 h_2 k_2 = \\ &= \varphi(h_1, k_1) \varphi(h_2, k_2) \end{aligned}$$

φ è sur: per (1)

$$\begin{aligned} \varphi \text{ è iniettiva: } \ker \varphi &= \{ (h, k) \mid \varphi(h, k) = hk = e \} = \\ &= \overset{44}{(e, e)} \end{aligned} \quad \begin{aligned} &h = k^{-1} = e \\ &\downarrow \\ &\text{per (2)} \quad \square \end{aligned}$$

Esempio $|G| = p^2$ Dalla formula delle classi avevamo ottenuto che G è necessariamente abeliano

$$\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Dico che G è isomorfo a uno dei due gruppi precedenti

$$\rightarrow G \text{ ciclico} \Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z}$$

$$\rightarrow G \text{ non ciclico} \Rightarrow \text{Tutti gli el di } G \text{ diversi da } e \text{ hanno ordine } p.$$

$$e \neq x \in G \quad H = \langle x \rangle \triangleleft G$$

$$\begin{array}{l} \uparrow \\ \text{ciclico di ordine } p \\ \cong \mathbb{Z}/p\mathbb{Z} \end{array}$$

$$y \in G \setminus \langle x \rangle \quad K = \langle y \rangle \triangleleft G$$

$$\uparrow \text{ ha ordine } p \quad \langle y \rangle \cong \mathbb{Z}/p\mathbb{Z}$$

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

$\hookrightarrow$ è un sgr di H che avendo ordine p ha solo i sgr banali e $K \neq H$

$$|HK| = \frac{|H| |K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2$$

$$HK = G \quad (1)$$

$$\Rightarrow G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

PRODOTTI SEMIDIRETTI

Def H, K gruppi e su

$$\begin{aligned} \varphi : K &\rightarrow \text{Aut}(H) && \text{omomorfismo} \\ k &\mapsto \varphi_k \end{aligned}$$

φ è azione di K su H
 (anche $\text{Aut}(H) \leq \text{Sym}(H)$)

Si dice prodotto semidiretto di H e K via φ

$$H \rtimes_{\varphi} K \quad (= K \ltimes_{\varphi} H)$$

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

$$(h, k) (h', k') = (h *_{\varphi} h', k * k')$$

Proposizione: $H \rtimes_{\varphi} K$ è un gruppo

Dim:

L'operazione è ben definita
 " " associativa (fare la verifica)

El neutro (e_H, e_K)

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

$$(e_H, e_K) (h, k) = (e_H \varphi_e(h), e_K k) = (e_H h, k) = (h, k)$$

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

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

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

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

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

$\varphi_{k^{-1}} \in \text{Aut}(H)$

Oss 1: $H \rtimes_{\varphi} K$ è un prodotto diretto $\Leftrightarrow \varphi_k = \text{id}_H \forall k$

Ho prodotto diretto $\Leftrightarrow (h, k) (h', k') = (h \varphi_k(h'), k k')$
 $(h h', k k')$

$\Leftrightarrow \forall k \in K \quad \forall h \in H \quad \cancel{h \varphi_k(h') = h h'} \Rightarrow \forall k \in K \quad \varphi_k = \text{id}_H$

Oss 2: $\overline{H} = H \times \{e_K\} \quad \overline{K} = \{e_H\} \times K$

$$\overline{H}, \overline{K} < G = H \rtimes_{\varphi} K$$

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

$$(e_H, k) (e_H, k') = (e_H \varphi_k(e_H), k k') = (e_H, k k')$$

Si vede anche che sono chiusi per inverso. (FARLO)

$\overline{H} \triangleleft G$ in quanto $H = \ker \pi$ dove

$$\pi : H \rtimes_{\varphi} K \rightarrow K \quad \text{omo}$$

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

$$\begin{aligned} \pi \text{ è omo} \quad \pi((h, k)(h', k')) &= \pi(h \varphi_k(h'), k k') \\ &= k k' = \pi(h, k) \pi(h', k') \end{aligned}$$

K in generale non è normale (lo è solo se il prodotto è diretto. In fatti in quel caso potrei applicare il Teo 1)

$$\overline{H} \overline{K} = G \quad \overline{H} \cap \overline{K} = e = (e_H, e_K)$$

Teorema 2 Sia G gruppo $H, K < G$ $H \triangleleft G$ tale che

$$(1) \quad HK = G$$

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

$$\Rightarrow G = H \rtimes_{\varphi} K \quad \text{dove } \varphi : K \rightarrow \text{Aut}(H) \\ k \mapsto \varphi_k (h \mapsto khk^{-1})$$

Oss: φ_k è la restrizione al sgr H dell'auto.

inTermo $g \mapsto kgk^{-1}$ (poiché $H \triangleleft G$)

la restrizione ^{ad H} di ogni σ in $\text{Inn}(G)$ è in $\text{Aut}(H)$)

Dim $F: H \rtimes K \rightarrow G$

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

questo è
il p.s. esterno

F è omomorfismo:

$$F((h, k)(h', k')) = F(h q_k(h'), k k') =$$

$$F(\underbrace{h k h' k^{-1}}_{q_k(h')}, k k') = h k h' \cancel{k^{-1} k} k' = h k h' k'$$

$$= F(h, k) F(h', k')$$

F è surgettiva per (1)

F è iniettiva per (2) $\ker F = \{(h, k) \mid F(h, k) = hk = e\}$

$\stackrel{= e}{\Rightarrow}$
 $H \ni h = k^{-1} \in K$

Esempio 1

$S_n \cong A_n \rtimes \langle (1, 2) \rangle$

$H = A_n \triangleleft S_n$ poiché $A_n = \ker \text{sgn}$

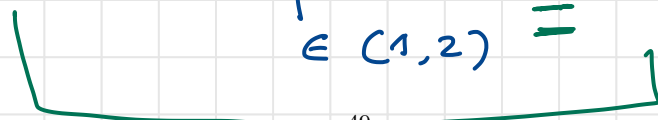
$K = \langle (1, 2) \rangle$

$H \rtimes K < S_n$ poiché $H \triangleleft S_n$ e $\cdot$

$$A_n \rtimes \langle (1, 2) \rangle \leq S_n$$

$$\uparrow$$

$$\in \langle (1, 2) \rangle =$$



40

è un sott'ordine 2 $\Rightarrow$ è un sott'ordine
 ho $S_n \cong A_n \rtimes \langle (1, 2) \rangle$

Per il Teo 2

Chi è $\varphi : \langle \mathbb{Z}, 2 \rangle \longrightarrow \text{Aut}(A_n)$

lo dice il T2

$$\begin{array}{ccc} (12) & \longmapsto & \varphi_{(12)} : p \longmapsto (12)p(12) \\ e & \longmapsto & \text{id} \end{array}$$

Esempio 2 :

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

la posso sottointendere
fuori cos'è l'op in D_n

$$D_n = \langle \{r, s \mid r^n = s^2 = \text{id}, sr = r^{-1}s\} \rangle$$

$$\langle r \rangle = H \triangleleft D_n \quad H \cong \mathbb{Z}/n\mathbb{Z}$$

$$\langle s \rangle = K$$

$$HK = D_n$$

$$H \cap K = \{\text{id}\} \Rightarrow D_n \cong H \rtimes_{\varphi} K$$

$\downarrow$
 $\{\text{id}, s\}$

$$\varphi : \langle s \rangle \longrightarrow \text{Aut}(\langle r \rangle) \cong \mathbb{Z}/n\mathbb{Z}^* \leftarrow \text{ci sono due el di ordine 2}$$

$$s \longmapsto \varphi_s \quad r \longmapsto srs^{-1} = srs = s^2 r^{-1} = r^{-1}$$

s ha ordine 2 $\Rightarrow \varphi_s$ ha ordine che divide 2

$$\Rightarrow \begin{cases} \varphi_s = \text{id} \\ \varphi_s = r \mapsto r^{-1} \end{cases} \leftarrow \text{otterrei il prodotto diretto}$$

è un prodotto semi-directo
"vero" ed è quello
che definisce D_n

Se in $\text{Aut } \mathbb{Z}/n\mathbb{Z}$ ci sono $2n-1$ elementi $\neq \text{id}$

esempio 2 (ad es se $\text{Aut}(\mathbb{Z}_{8\mathbb{Z}}) \cong \mathbb{Z}_{8\mathbb{Z}}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$)
 posso definire anche altri prodotti semi diretti

$$\mathbb{Z}_n \rtimes_q \mathbb{Z}_2$$

Rimane il problema di vedere se siamo o no gruppi isomorfi.

Esempio 3 Gruppi di ordine pq $q > p$ primi

$$|G| = pq \quad x, y \in G \quad \text{ord}(x) = q \quad \text{ord}(y) = p$$

(Cauchy)

$H = \langle x \rangle \triangleleft G$ perché ha indice p cioè p il più piccolo primo che divide $|G|$

alternativamente posso vedere che H è normale in G perché è l'unico sgr di quell'ordine

Se $H' < G$ $|H'| = q$ se fosse $H \neq H'$ $H \cap H' = \{e\}$

$$|HH'| = \frac{|H| |H'|}{|H \cap H'|} = \frac{q \cdot q}{1} = q^2 > pq$$

$$H < G$$

$$K = \langle y \rangle \quad HK = G, \quad H \cap K = \{e\}$$

$\Rightarrow$ Ogni gruppo di ordine pq è prodotto semi diretto
 $G \cong H \rtimes_q K$

Per classificarli tutti i gruppi di ordine pq

Dobbiamo classificare tutti i possibili
semi diretti $\mathbb{Z}/p\mathbb{Z} \rtimes_q \mathbb{Z}/q\mathbb{Z}$ a meno di
isomorfismo.

Considero $\varphi: \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z}^*$
 $\cong \mathbb{Z}/q-1\mathbb{Z}$

Uso la notazione moltiplicativa

$$\varphi: \langle y \rangle \xrightarrow{\mathbb{Z}/p} \text{Aut}(\langle x \rangle) \cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/q-1\mathbb{Z}$$

$$y \longmapsto \varphi_y \quad x \mapsto x^b$$

Per definire φ sul dominio (ciclico) $\langle y \rangle$ basterà
assegnare φ_y con la condizione $\text{ord } \varphi_y \mid p$

$\varphi_y \in \text{Aut}(\langle x \rangle)$ che ha ordine $q-1$

Se $p \nmid q-1$ l'unica possibilità è $\varphi_y = \text{id}$

$\Rightarrow \exists!$ gruppo di ordine pq $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Se $p \mid q-1$

$\text{ord } \varphi_y = \begin{cases} 1 & \leftarrow \text{prodotto diretto} \\ p & \leftarrow \text{ho } p-1 \text{ scelte per } \varphi_y \text{ che danno prodotti semi diretti diversi} \end{cases}$

Osservo che $\text{ord } \varphi_y = \text{ord } \bar{e}$

$$\varphi_y x \rightarrow x^e$$

$$\varphi_y^k(x) = x^{e^k}$$

$$\text{ord } \varphi_y = p \Leftrightarrow e^p \equiv 1 \pmod{q} \Leftrightarrow \text{ord } e = p$$

Le $p-1$ scelte per φ danno tutti gruppi isomorfi quindi se $p \mid q-1$ ci sono esattamente 2 gruppi di ordine pq a meno di isomorfismo. Infatti:

$$G_1 = \langle x \rangle \rtimes_{\varphi} \langle y \rangle$$

$$G_2 = \langle x \rangle \rtimes_{\psi} \langle y \rangle$$

$$\varphi_y(x) = x^e \quad \text{ord } e = p$$

$$\psi_y(x) = x^{\lambda} \quad \text{ord } \lambda = p$$

$$\langle e \rangle = \langle \lambda \rangle \quad \lambda = e^r \quad 0 < r < p$$

$$\Rightarrow \quad F \quad G_1 \longrightarrow G_2$$

$$\begin{array}{ccc} x & \longmapsto & x \\ y & \longmapsto & y^r \end{array}$$

Quella definire un isomorfismo

$$G_1 = \langle x, y \mid x^q = y^p = 1, yxy^{-1} = x^e \rangle$$

$$G_2 = \langle x, y \mid x^q = y^p = 1, yxy^{-1} = x^a \rangle$$

Bene vedere che $\begin{cases} F(x^q) = F(x)^q = 1 & \checkmark & x^q = 1 \\ F(y^p) = F(y)^p = 1 & \checkmark & y^p = 1 \\ F(yxy^{-1}) = F(x^a) \end{cases}$

$$F(yxy^{-1}) = F(y)F(x)F(y)^{-1} = \underbrace{y^r xy^{-r}}_{G_2 \ yxy^{-1} = x^a} = x^a = F(x)$$

Questo garantisce che F ottenuto è ben definito

l'assegnamento $x \mapsto x^r$ $y \mapsto y^r$ è un om.

È poi immediato vedere che è un isomorfismo.

Ricevimento Tutor (Luca Casarini) Venerdì alle 16

Prima dovete inviare gli esercizi (istruzione sul canale Tutorato su TEAMS)

Teorema di Struttura per i gruppi abeliani finiti:

Sia G un gruppo abeliano finito, allora G è prodotto diretto di gruppi ciclici, cioè

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

Inoltre questa scrittura è unica e richiediamo che

$$n_{i+1} \mid n_i \quad \forall i = 1, \dots, s-1$$

SCHEMA DELLA DIMOSTRAZIONE

Sia $G(p) = \{g \in G \mid \text{ord } g = p^k \quad k \in \mathbb{N}\}$

$G(p)$ p -sottogruppo di Sylow di G
 p -componente / componente di p -torsione

- $G(p)$ è un sgr di G perché G è abeliano

$$x, y \in G \quad \text{ord}(xy) \mid [\text{ord}(x), \text{ord}(y)]$$

- $G(p)$ è un sottogruppo caratteristico di G .

(gli automorfismi conservano l'ordine degli elementi.)

Teorema 1: G gruppo abeliano $|G| = n = p_1^{e_1} \dots p_s^{e_s}$

(p_i : primi 2 a 2 distinti) $\Rightarrow$

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

(G è prodotto diretto delle sue p -componenti)

La decomposizione di G come prodotto di p -gruppi di ordine tre loro coprimi è unica.

Teorema 2 Sia G un p -gruppo abeliano.

Esistono e sono univocamente determinati $r_1, \dots, r_t$

t che $r_1 \geq r_2 \geq \dots \geq r_t$ e

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

Teorema 1 + Teorema 2 $\Rightarrow$ Teorema di struttura

ESISTENZA

$$G \stackrel{T_1}{\cong} G(p_1) \times \dots \times G(p_s) \stackrel{T_2}{\cong}$$

$$\mathbb{Z}/p_1^{r_{11}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{r_{1t_1}}\mathbb{Z} \times$$

$$\dots \times \mathbb{Z}/p_s^{r_{s1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}$$

$$r_{11} \geq \dots \geq r_{1t_1}$$

$$\mathbb{Z}/p_s^{r_{s1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}$$

CRT
 $\Downarrow$
 $\cong$

$$\mathbb{Z} / \underbrace{p_1^{r_{11}} \dots p_s^{r_{s1}}}_{n_1} \mathbb{Z} \times \dots \times \mathbb{Z} / \underbrace{p_1^{r_{1t}} \dots p_s^{r_{st}}}_{n_t} \mathbb{Z}$$

ovvero $t = \max \{t_1, \dots, t_s\}$ e ponendo $r_{i,h} = 0$ e. $h > t_i$

Chiamando $n_t \mid n_{t-1} \mid \dots \mid n_1$

UNICITA' Segue dalle unicit  del T1 e del T2

(Se questi 2 decomposizioni di G diverse con
 con ordini che si dividono l'un l'altro rappresentando
 gli isomorfismi sopra al continuo avere 2 diverse
 dec per $G(p)$ e per G come prodotto
 di p componenti)

Esempio: ① $G \cong \mathbb{Z}/_{100} \times \mathbb{Z}/_8 \times \mathbb{Z}/_6 \times \mathbb{Z}/_{15} \cong$

$$\cong \mathbb{Z}/_{2^2} \times \mathbb{Z}/_{5^2} \times \mathbb{Z}/_{2^3} \times \mathbb{Z}/_2 \times \mathbb{Z}/_3 \times \mathbb{Z}/_3 \times \mathbb{Z}/_5$$

$$\cong \underbrace{(\mathbb{Z}/_{2^3} \times \mathbb{Z}/_{2^2} \times \mathbb{Z}/_2)}_{G(2)} \times \underbrace{(\mathbb{Z}/_3 \times \mathbb{Z}/_3)}_{G(3)} \times \underbrace{(\mathbb{Z}/_{5^2} \times \mathbb{Z}/_5)}_{G(5)}$$

$$\cong \mathbb{Z}/_{2^3 \cdot 3 \cdot 5^2} \times \mathbb{Z}/_{2^2 \cdot 3 \cdot 5} \times \mathbb{Z}/_2$$

② Classificare i gruppi abeliani di ordine 1000

$$1000 = 2^3 \cdot 5^3 \quad G = G(2) \times G(5)$$

$$G(2) \cong \begin{cases} \mathbb{Z}/2^3 \\ \mathbb{Z}/2^2 \times \mathbb{Z}/2 \\ \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \end{cases}$$

$$G(5) = \begin{cases} \mathbb{Z}/5^3 \\ \mathbb{Z}/5^2 \times \mathbb{Z}/5 \\ \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/5 \end{cases}$$

Quanti sono, a meno di isomorfismo, i gruppi abeliani di ordine 1000? $3 \cdot 3 = 9$

Dim Teorema 1 : $|G| = n = p_1^{e_1} \dots p_s^{e_s}$

Per l'induzione su s .

Se $s=1$ $G = G(p_1)$ ✓

Altrimenti se $s \geq 2$ $n = m m'$ con $m < n$
 $m' < n$

$$\Rightarrow \boxed{G \cong mG \times m'G} \quad \text{notazione additiva} \quad (m, m') = 1$$

Uno dei TI di cui

$$H = mG, K = m'G \triangleleft G \quad (\text{ovvia verifica})$$

$$(1) \quad mG + m'G = G \quad (H+K=G)$$

$$(2) \quad mG \cap m'G = \{0\} \quad (H \cap K = \{0\})$$

$$(m, m') = 1 \quad \exists h, h' \in \mathbb{Z} \quad \text{t.c.} \quad mh + m'h' = 1$$

$$\forall g \in G \quad mhg + m'h'g = g \Rightarrow g \in mG + m'G \quad (1)$$

$$\text{Sia } x \in mG \cap m'G$$

$$x = mg = m'g' \quad g, g' \in G$$

$$m'x = \underbrace{m'm}_n g = 0$$

$$\Rightarrow \text{ord}(x) \mid (m', m) = 1$$

$$mx = m \underbrace{m'}_n g' = 0$$

$$\Rightarrow x = 0$$

Osserviamo che $mG = G_m = \{g \in G \mid m'g = 0\}$

$$m'G = G_{m'} = \{g \in G \mid mg = 0\}$$

$$m'G \subseteq G_m$$

$$m'x \in G_m \text{ perché } \underbrace{mm'}_n g' = 0$$

$$x \in G_m \quad mx = 0$$

$$x = \cancel{mx} + m'h'x \Rightarrow x \in m'G \Rightarrow m'G = G_m$$

"0" perché $x \in G_m$

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

Applico a G_m e $G_{m'}$ l'ipotesi induttiva per

$|G_{m'}|, |G_m| < |G|$ perché G_m contiene tutti e soli gli el di G di ordine che divide m

$G_m \neq \{0\}$ per Cauchy dato che $1 < m < n$

$$\Rightarrow G_{m'} \leq G \text{ e viceversa.}$$

$$G_m = \prod_{i \in I} G(p_i) \quad G_{m'} = \prod_{j \in J} G(p_j) \quad \text{con } I \cup J = \{1, \dots, s\} \quad I \cap J = \emptyset \quad (m, m') = 1$$

$$\Rightarrow G \cong G(p_1) \times \dots \times G(p_s)$$

UNICITA': La scrittura come prodotto di p -componenti è unica anche se avessimo

$$G \cong H_1 \times \dots \times H_s \quad \text{con } H_i: p_i\text{-gruppo}$$

$$H_i \leq G$$

$H_i \subseteq G(p_i) \leftarrow$ contiene tutti gli elementi di ordine potenze di p_i .

$$\text{ma } |G| = |H_1| \dots |H_s| = |G(p_1)| \dots |G(p_s)|$$

$$\Rightarrow |H_i| = |G(p_i)| \quad \forall i \Rightarrow H_i = G(p_i) \quad \forall i.$$



Dim Teorema 2:

ESISTENZA $|G| = p^n$ Per immissione su n .

$$n=1 \quad |G|=p \quad G \cong \mathbb{Z}/p\mathbb{Z} \quad \checkmark$$

Sia $x_1 \in G$ un elemento di ordine massimo ord $x = p^{r_1}$

$$\text{Se } r_1 = n \Rightarrow G \cong \mathbb{Z}/p^n\mathbb{Z}$$

$$r_1 < n \quad G / \langle x_1 \rangle \text{ ha ordine } p^{n-r_1} < p^n$$

Per ipotesi induttiva

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

Sia ord $\bar{x}_i = p^{r_i}$

$$r_2 \geq \dots \geq r_t$$

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

$a_2 \bar{x}_2 + \dots + a_t \bar{x}_t$

Voglio ricavare informazioni da G .

Lemma: Nelle ipotesi sopra. Sia $\bar{x} \in G/\langle x_1 \rangle$

$$\Rightarrow \exists y \in \pi^{-1}(\bar{x}) \text{ t.c. } o(y) = o(\bar{x})$$

(Attenzione questo fatto in genere non vale quando si passa al quoziente qualsiasi)

$$\pi: \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} / \langle p \rangle \cong \mathbb{Z}/p\mathbb{Z}$$

$$1 \longrightarrow \bar{1} \text{ ha ordine } p$$

$$\pi^{-1}(\bar{1}) = \{1 + kp\}_{k=0, \dots, p-1} \quad 1+kp \text{ ha ordine } p^2 \quad \forall 1 \leq k \leq p$$

| Qui sto quotizzando per un elemento di ordine massimo!)

Dim Lemma : $\pi^{-1}(\bar{x}) = x + \langle x_1 \rangle \ni y$

$$\underline{y = x + ax_1}$$

$$\pi(y) = \pi(x) = \bar{x}$$

$$p^r = o(\pi(y)) = o(\bar{x}) \mid o(y) \text{ perché } \pi \text{ è om}$$

Dico che posso scegliere y (cioè a) in modo che

$$\underline{0 = p^r y = p^r x + p^r a x_1 \Leftrightarrow p^r x = -p^r a x_1}$$

$$o(\bar{x}) = p^r \Rightarrow p^r x \in \langle x_1 \rangle \Rightarrow p^r x = b x_1$$

Ora x_1 ha ordine massimo p^{r_1} $r \leq r_1$

$$\underline{0 = p^{r_1} x = p^{r_1-r} p^r x = p^{r_1-r} b x_1} \quad \text{ma } o(x_1) = p^{r_1}$$

$$\Rightarrow p^r \mid b \quad b = p^r b_1 \quad \text{Basta scegliere } a = -b_1$$

$$y = x - b_1 x_1$$

$$(p^r y = p^r x - p^r b_1 x_1 = b x_1 - \underbrace{p^r b_1 x_1}_b = 0) \quad \square$$

Per il Lemma

$$\exists x_2, \dots, x_t \in G \quad \text{Tale che} \quad o(x_i) = o(\bar{x}_i) = p^{r_i}$$

$$\text{Dico che} \quad H = \langle x_2, \dots, x_t \rangle \cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle$$

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

$$\pi|_H: H \longrightarrow \langle \bar{x}_2 \rangle \times \dots \times \langle \bar{x}_t \rangle \quad \text{è un iso}$$

La surgettività è ovvia

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

$$\Rightarrow a_i \bar{x}_i = 0 \Rightarrow p^{r_i} \mid a_i \Rightarrow a_i x_i = 0 \quad \forall i=2, \dots, t$$

$$\Rightarrow H \cong \langle \bar{x}_2 \rangle \times \dots \times \langle \bar{x}_t \rangle$$

$$\cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle$$

$$\text{Dico che} \quad G \cong \langle x_1 \rangle \times H \left(\cong \langle x_1 \rangle \times \langle x_2 \rangle \times \dots \times \langle x_t \rangle \right)$$

$$(1) \langle x_1 \rangle + H = G, \quad (2) \langle x_1 \rangle \cap H = \{0\}$$

$$(1) \quad g \in G \quad \bar{g} \in G / \langle x_1 \rangle \Rightarrow \bar{g} = a_2 \bar{x}_2 + \dots + a_t \bar{x}_t$$

$$\Rightarrow g - (a_2 x_2 + \dots + a_t x_t) \in \langle x_1 \rangle$$

$$g = a_1 x_1 + a_2 x_2 + \dots + a_t x_t$$

$$(2) \quad a_1 x_1 = a_2 x_2 + \dots + a_t x_t$$

applico π

$$0 = a_2 \bar{x}_2 + \dots + a_t \bar{x}_t \quad G/\langle x_1 \rangle \cong \prod_{i=2}^t \langle x_i \rangle$$

$$\Rightarrow a_i \equiv 0 \pmod{p^{r_i}} \quad \forall i \Rightarrow a_1 x_1 = 0$$

UNICITA': Per risoluzione su n $|G| = p^n$

$$n=1 \quad G \cong \mathbb{Z}/p\mathbb{Z} \quad \checkmark$$

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t}\mathbb{Z} \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{k_s}\mathbb{Z}$$

$$r_1 \geq \dots \geq r_t \quad k_1 \geq \dots \geq k_s$$

$$t=s$$

$$G_p = \{g \in G \mid pg = 0\} \quad \text{perché gli iso conservati}$$

gli ordini degli el

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

Consideriamo il gruppo pG

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

$$|pG| = p^{n-t}$$

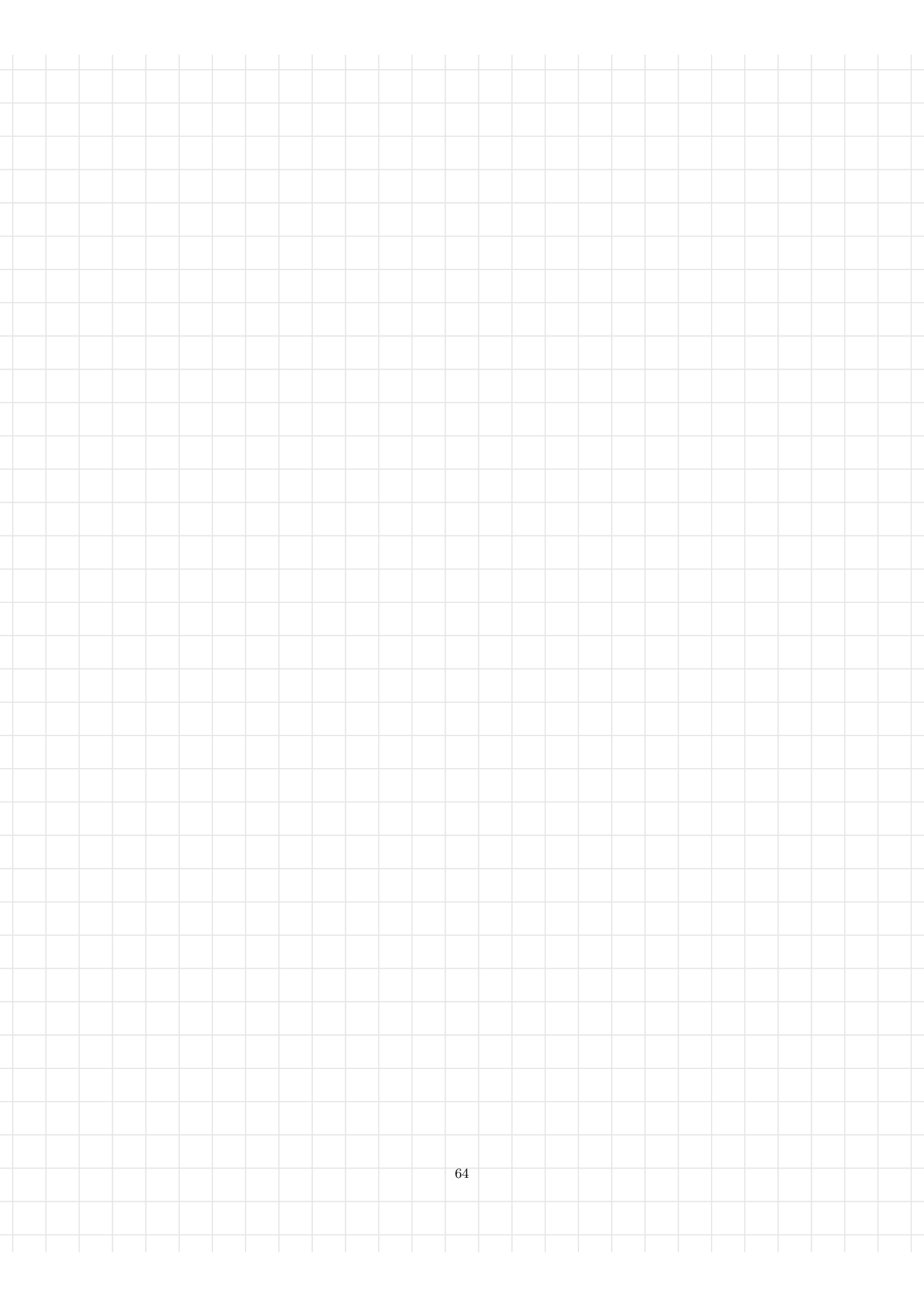
$$\cong \frac{\mathbb{Z}}{p^{k_1-1}\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p^{k_s-1}\mathbb{Z}}$$

$$r_1-1 = k_1-1, \dots, r_t-1 = k_t-1$$

$$r_1 = k_1, \dots, r_t = k_t$$



possiamo applicare
l'ipotesi di induzione
 $\Rightarrow$ Ha ordine unico



IL TEOREMA DI SYLOW

Dato G gruppo finito cosa posso dire dell'esistenza di elementi / sottogruppi di una data ordine?

- $H \leq G \Rightarrow |H| \mid |G|$ T di Lagrange
- $\forall p$ primo $p \mid |G| \Rightarrow \exists x \in G \text{ ord}(x) = p$ T di Cauchy
- G abeliano $\forall d \mid |G| \Rightarrow \exists x \in G \text{ ord}(x) = d$ (G ci aiuta)
- Il fatto sopra vale $(\Rightarrow G$ è abeliano $(d = |G|)$)
- Se G è abeliano $\forall d \mid |G| \Rightarrow \exists H \leq G \text{ } |H| = d$

$$G = G_{p_1} \times \dots \times G_{p_r} \quad |G| = p_1^{e_1} \dots p_r^{e_r} \quad p_i \neq p_j$$

$$d = p_1^{a_1} \dots p_r^{a_r}$$

$$\forall i \quad \exists H_{p_i} \leq G_{p_i} \quad |H_{p_i}| = p_i^{a_i}$$

$$G_p = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{n_s}\mathbb{Z} \quad \sum n_i = e.$$

È chiaro l'esistenza di sgr di ogni ordine

(Es: $|H_p| = p^{72}$)

posso prendere $H_p = \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{12}\mathbb{Z}$ (65)

dato che G è abeliano
 $\Rightarrow H_{p_1} \dots H_{p_r} < G$

Inoltre $H_{p_1} \dots H_{p_r} \cong H_{p_1} \times \dots \times H_{p_r}$
 perché $H_{p_i} \cap H_{p_j} = \{e\}$

$$\Rightarrow |H_{p_1} \dots H_{p_r}| = \prod |H_{p_i}| = \prod p_i^{a_i} = |G|$$

- Se G non è abeliano e $d(|G|)$ non è dato che G abbia sgr di ordine d .

Ad esempio A_4 non ha sottogruppi di ordine 6

$$|A_4| = \frac{4!}{2} = 12 \quad 6 \nmid 12$$

$$\text{Se } \exists H < A_4 \quad |H| = 6 \Rightarrow H \triangleleft A_4$$

Per Cauchy $\exists x \in H$ $\text{ord } x = 2$

$$x = (ab)(cd) \rightarrow \text{Cl}_{A_4}(x) \subset H \text{ perché } H \triangleleft A_4$$

e quindi unione di elementi di coniugio in A_4

$$\text{Cl}_{S_4}((ab)(cd)) = \{(12)(34), (13)(24), (14)(32)\}$$

(per controllo - inutile - $Z_{S_4}((12)(34))$ ha 8 elementi

TROVATELI)

$$\text{Poiché } |\text{Cl}_{S_4}((ab)(cd))| = 3 \Rightarrow \text{Cl}_{A_4}((ab)(cd)) = \text{Cl}_{S_4}((ab)(cd))$$

$$\text{Se } H \triangleleft A_4 \Rightarrow H \supset \{e, (12)(34), (13)(24), (14)(23)\} \\ = V$$

$$\Rightarrow V < H \text{ ma } 4 \nmid 6 \rightarrow \text{impossibile}$$

Def: G gruppo finito, p primo $|G| = p^n m$ $n \geq 1$
 $\gcd(m, p) = 1$
 Un sgr di G di ordine p^n si chiama
 p -sottogruppo di Sylow.

Teorema di Sylow

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

ESISTENZA: $\forall d, 1 \leq d \leq n \quad \exists H \leq G \quad |H| = p^d$

INCLUSIONE: $\forall 1 \leq d \leq n-1$ ogni sgr di ordine p^d è contenuto
 in un sgr di ordine p^{d+1} . In particolare,
 ogni p -sgr è contenuto in un p -sgr di Sylow.

CONIUGIO Due qualsiasi p -sgr di Sylow di G sono
 coniugati.

NUMERO Sia $n_p = \#$ dei p -sgr di Sylow di G
 $\Rightarrow n_p \mid |G|$ e $n_p \equiv 1 \pmod{p}$

Dim: ESISTENZA Sio $\mathcal{M} = \{ X \subset G \mid \#X = p^d \}$

Chiarimento $|\mathcal{M}| = \binom{p^h m}{p^d} = \prod_{i=0}^{p^d-1} \frac{p^h m - i}{p^d - i}$ sottoinsieme

Osservo che $p \nmid \prod_{i=1}^{p^d-1} \frac{p^h m - i}{p^d - i}$ infatti:

$\forall i=1, \dots, p^d-1$ $\text{ord}_p(p^h m - i) = \text{ord}_p(p^d - i) = \text{ord}_p i$
 (se $p \nmid i \Rightarrow p^h m - i$ e $p^d - i$ non sono divisibili per p)
 se $i = p^k j$ $(j, p) = 1 \Rightarrow k < d$ $p^d - i = p^d - p^k j = p^k (p^{d-k} - j)$
 $\underbrace{p^{d-k} - j}_{\text{non div per } p}$

$\Rightarrow p^{h-d} \parallel |\mathcal{M}|$

$M \in \mathcal{M} \Rightarrow gM \in \mathcal{M} \quad \forall g \in G$

Posso considerare l'azione di G su $\mathcal{M}$

$\phi \quad G \longrightarrow \subseteq(\mathcal{M})$
 $g \longmapsto \varphi_g \quad M \longrightarrow gM$

Individuo il sgr di ordine p^d come stabilizzatore di un M di $\mathcal{M}$.

$\mathcal{M} = \bigcup_{i=1}^s \text{orb}(M_i)$

$$p^{n-d} || |\mathcal{M}| = \sum_{i=1}^s |\text{orb}(\Pi_i)| = \sum_{i=1}^s \frac{|G|}{|\text{St}(\Pi_i)|}$$

$$\Rightarrow \exists i \text{ tale che } p^{n-d+1} \nmid |\text{orb}(\Pi_i)| = \frac{|G|}{|\text{St}(\Pi_i)|} = \frac{p^n m}{|\text{St}(\Pi_i)|}$$

$$\Rightarrow p^d \mid |\text{St}(\Pi_i)| = t \Rightarrow t \geq p^d$$

↑ voglio mostrare che $|\text{St}(\Pi_i)| = p^d$

D'altra parte $x \in \Pi_i$: la funzione

$$\begin{array}{ccc} \text{St}(\Pi_i) & \longrightarrow & \Pi_i \\ y & \longmapsto & yx \end{array} \quad \begin{array}{l} \text{è iniettiva} \\ yx = y_1 x \Leftrightarrow y = y_1 \end{array}$$

$$\Rightarrow t = |\text{St}(\Pi_i)| \leq |\Pi_i| = p^d \Rightarrow t = p^d$$

$\text{St}(\Pi_i)$ è un sottogruppo ordine p^d .

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

$$H \leq G \quad |H| = p^d. \quad X = \{ \text{classe laterali di } S \text{ in } G \}$$

$$|X| = [G : S] = p^n m / p^n = m$$

Considero l'azione di H su X data da

$$\begin{array}{ccc} \varphi & H & \longrightarrow S(X) \\ h & \longmapsto & \varphi_h \quad gS \longmapsto h\varphi_h S \end{array}$$

$$m = |X| = \sum_{i=1}^r |\text{orb}(g_i S)| \stackrel{69}{=} \sum_{i=1}^r \frac{|H|}{|\text{St}(g_i S)|} = \sum_{i=1}^r p^{a_i}$$

Perché $p \nmid m$ $\exists$ i tale $a_i = 0 \Rightarrow \text{orb}(g_i S) = \{g_i S\}$
 $\text{St}(g_i S) = H$

$\forall h \in H \quad h g_i S = g_i S \Rightarrow H \subset \underbrace{g_i S g_i^{-1}}$
 H è contenuto in un p -Sylow. è un p -Sylow perché
 $|g_i S g_i^{-1}| = |S|$

Questo dimostra la parte **CONIUGIO**. Infatti se $|H| = p^n$

$\Rightarrow H \subset g_i S g_i^{-1}$ e poiché hanno lo stesso card
 $\Rightarrow H = g_i S g_i^{-1}$

Lemma G p -gruppo $H \leq G \Rightarrow N_G(H) \geq H$

(visto a esercitazione).

$|H| = p^d \quad d \leq n-1 \quad H \leq S \Rightarrow H \leq N_S(H)$

Concluso $\frac{N_S(H)}{H}$ è un p -gruppo non banale
 per Cauchy $\exists \bar{x}$ di ordine p .

Per il Teorema di corrisp. $\overline{\pi}^{-1}(\langle \bar{x} \rangle)$ è un sgr
 di $N_S(H)$ che contiene H di ordine p^{d+1} .

NUMERO $n_p = \# \text{ } p\text{-sgr di Sylow} = [G : N_G(S)]$

Infatti $\# \text{ coniugati di } S = \frac{|G|}{|\text{St}(S)|}$ ↓ azione di
conjug
 $\# \text{ } p\text{-sgr di Sylow} \quad N_G(S)$

$$\Rightarrow n_p \mid |G|.$$

$$S \curvearrowright \phi: S \longrightarrow \mathcal{S}(X) \quad X = \{ p\text{-sgros di } G \}$$

$$s \longmapsto \varphi_s \quad H \longmapsto s H s^{-1}$$

ϕ ha un'unica orbita banale $\text{orb}(S) = \{S\}$

, $\text{orb}(S) = \{S\}$ è ovvio

$$\& \text{orb}(H) = \{ s H s^{-1} \mid s \in S \} = \{H\} \Leftrightarrow s H s^{-1} = H \quad \forall s \in S$$

$$\Rightarrow S \subset N_G(H)$$

$$S H < N_G(H) \quad (H < N_G(H) \text{ e } S H \text{ v.sgr})$$

ma questo è assurdo se $S \neq H$ giacché

$$|S H| = \frac{|S| |H|}{|S \cap H|} = \frac{p^n \cdot p^n}{p^k} = p^{2n-k} \nmid |G|$$

$k < n$

Dalla formula delle classi si ha

$$n_p = |X| = \sum_{i=1}^n \underbrace{|\text{orb}(H_i)|}_{p^{a_i} \neq 1} + \underbrace{|\text{orb}(S)|}_{=1} = p f + 1$$

$$n_p \equiv 1 \pmod{p}$$



Corollario: G abeliano finito. $\forall p \mid |G| \quad G_p = \{x \in G \mid \text{ord}(x) = p^k \text{ per qualche } k\}$

$\Rightarrow G_p$ è l'unico p -Sylow di G

$\bullet G$ è il prodotto diretto dei suoi p -Sylow

$$G \cong G_{p_1} \times \dots \times G_{p_r} \quad |G| = \prod p_i^{e_i}$$

Applicazioni

Classificazione dei gruppi di ordine 12

$$12 = 2^2 \cdot 3 \quad \text{Sylow } \exists P_2, P_3 \quad P_2 = 2\text{-Sylow } |P_2| = 4$$

$$G = P_2 P_3 \quad \left(|P_2 P_3| = \frac{|P_2| |P_3|}{|P_2 \cap P_3|} = \frac{4 \cdot 3}{1} = 12 \right) \quad P_3 = 3\text{-Sylow } |P_3| = 3$$

Almeno uno tra P_2 e P_3 è normale.

Se $P_3 \triangleleft G$ ✓

P_3 non è normale in G $n_3 \neq 1$ $n_3 \mid 2^2 \cdot 3$ $n_3 \equiv 1 \pmod{3}$

$$n_3 = \begin{matrix} 1 \\ 4 \end{matrix} \quad n_3 = 4$$

Ci sono 4 3-Sylow e quindi 8 elem di ordine 3

$\Rightarrow 4 = 12 - 8$ ed di ordine $\neq 3 \rightarrow$ costituiscono

l'unico 2 Sylow $\Rightarrow P_2 \triangleleft G$

$G = P_2 P_3$ e uno tra P_2 e P_3 è normale

$\Rightarrow G$ è prodotto semidiretto di P_2 e P_3

$$P_3 \triangleleft G \Rightarrow G \cong P_3 \rtimes P_2$$

$$P_2 \triangleleft G \Rightarrow G \cong P_2 \rtimes P_3$$

$$P_3 \cong \mathbb{Z}/3\mathbb{Z}$$

$$P_2 = \begin{cases} \mathbb{Z}/4 \\ \mathbb{Z}/2 \times \mathbb{Z}/2 \end{cases}$$

$$\underline{P_2 \triangleleft G}$$

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

$$\rightarrow q: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut } \mathbb{Z}/4 \cong \mathbb{Z}/2\mathbb{Z}$$

$$1 \mapsto \text{id}$$

$\rightarrow$ solo prodotto diretto

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

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

$$q: \mathbb{Z}/3 \rightarrow \text{Aut } (\mathbb{Z}/2 \times \mathbb{Z}/2) \cong S_3$$

$$\bar{1} \mapsto$$

$$\text{id} \rightarrow \mathbb{Z}/2 \times \mathbb{Z}/2 \rtimes \mathbb{Z}/3 \cong \mathbb{Z}/2 \times \mathbb{Z}/6$$

2 ed di ordine 3

ho 2 scelte per q con $q(\pi)$ di ordine 3

queste due scelte danno gruppi isomorfi
(si vede come per i q r di ordine pq)

ARGOMENTO BELLO: $G = \mathbb{Z}/2 \times \mathbb{Z}/2 \rtimes_q \mathbb{Z}/3$ q non banale

$$G \hookrightarrow S_4 \Rightarrow G \cong A_4$$

A_4

$\downarrow$ FACILE

G agisce su insieme su 73 4 3-Sylow. $X = \{P_3, P'_3, P''_3, P'''_3\}$

$\phi: G \rightarrow \text{SC}(X)$ $\ker \phi = \text{id}$ ESERCIZIO

$$P_3 \triangleleft G$$

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

$$q: \mathbb{Z}/4 \longrightarrow \text{Aut}(\mathbb{Z}/3) \cong \mathbb{Z}/3^* \cong \mathbb{Z}/2$$

$$\bar{1} \longrightarrow \text{id} \quad \mathbb{Z}/12$$

$$\bar{1} \longrightarrow -\text{id}$$

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

$$\mathbb{Z}/3 \rtimes_q \mathbb{Z}/2 \times \mathbb{Z}/2$$

$$q: \mathbb{Z}/2 \times \mathbb{Z}/2 \longrightarrow \text{Aut}(\mathbb{Z}/3) = \{ \pm \text{id} \}$$

$$\langle x \rangle \times \langle y \rangle \longrightarrow$$

$$\text{id}, x, y, xy \longrightarrow 2 \text{ el on ordre } 2 \quad -\text{id}$$

$$\text{id} \text{ et } -\text{id} \text{ on ordre } 2 \longrightarrow \text{id}$$

$$q_x = \text{id}$$

$$\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

$$q_y = -\text{id}$$

$$\langle z \rangle \cong \mathbb{Z}/3$$

$$q_{xy} = -\text{id}$$

$$z = q_x(z) = xzx^{-1} \Rightarrow$$

x commute avec z

$$z^{-1} = q_y(z) = yzy^{-1}$$

$$\langle y, z \mid y^2 = 1, z^3 = 1, yzy^{-1} = z^{-1} \rangle$$

$$\cong D_3$$

$$\mathbb{Z}/2 \times D_3 = D_6$$

$$\mathbb{Z}/12, \mathbb{Z}/2 \times \mathbb{Z}/6, A_4, D_6, \mathbb{Z}/3 \rtimes \mathbb{Z}/4$$

Gruppo dei quaternioni (centro dei quaternioni)

$$Q_8 = \langle i, j \mid i^4 = 1 \quad j^2 = i^2 \quad ij = j^3 i \rangle$$

$$\text{ord } i = 4 \quad \langle i \rangle \text{ ha ordine } 4$$

$$\text{ord } j = 4 \Leftrightarrow \text{ord } j^2 = \frac{\text{ord}(j)}{(2, \text{ord}(j))} = \text{ord } i^2 = 2$$

$$Q_8 = \langle i \rangle \langle j \rangle$$

$$|\langle i \rangle \langle j \rangle| = \frac{|\langle i \rangle| |\langle j \rangle|}{|\langle i \rangle \cap \langle j \rangle|} = \frac{4 \cdot 4}{2} = 8$$

$$Q_8 = \{ 1, i, i^2=j^2, i^3, j, j^3, i^2j, i^2j^3 \}$$

$$\langle i^2 \rangle = \langle j^2 \rangle \triangleleft Q_8$$

↓ ordine 2 solo è normale per verifica diretta

$$\Rightarrow \langle i^2 \rangle \subset Z(Q_8)$$

Un sottogruppo H di ordine 2 è normale $\Leftrightarrow H \subset Z(G)$

$$H = \{e, h\} \quad gHg^{-1} = H \quad \forall g \in G \quad ghg^{-1} = h \Rightarrow ghg^{-1} = h$$

Dico $\langle i^2 \rangle = Z(G)$

Infatti $|Q_8| = 2^3$ e im gruppo non abeliano
 di ordine 2^3 $|Z(G)| = \begin{cases} 1 & \leftarrow \text{No perché } p\text{-gr} \\ 2 & \leftarrow \text{no } G/Z(G) \dots \\ 4 & \leftarrow \text{No se non è } \mathbb{Z}_4 \end{cases}$

Q_8 non è ab perché $ij = j^3 i = j^{-1} i$

$Q_8 \not\cong D_4$ perché hanno un diverso numero
 di elementi di ordine 4.

$ij = k \quad i^2 = -1$

$Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \}$

$-1 = i^2$

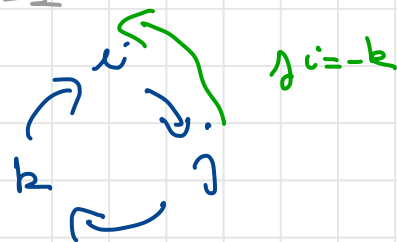
$-i = i^3$

$-j = j^3$

$k = ij$

$-k = i^3 j$

$i^4 = j^4 = k^4 = 1$
 $i^2 = j^2 = k^2 = -1$



$k^2 = (ij)^2 = ijij = j^3 i^2 j = i^2$

i^4

$j^2 = i^2$

$ij = j^3 i$

$k^2 = ijij = j^3 i^2 j = i^2$

$Q_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, xy = y^3 x \rangle$

$x \rightarrow i$

$y \rightarrow j$

$x^4 \rightarrow i^4 = 1$

$xy \rightarrow ij$

$y^3 x = j^3 i$

Ordine elementi

1 ordine

-1 ordine 2, $i, -i, j, -j, k, -k$ ordine 4

questo mostra $Q_8 \not\cong D_4$ $\leftarrow Q_8$ è un nuovo gr di ordine 8!

$\langle -1 \rangle = Z(Q_8)$ è caratteristica

$\langle i \rangle, \langle j \rangle, \langle k \rangle$ sgr di ordine 4

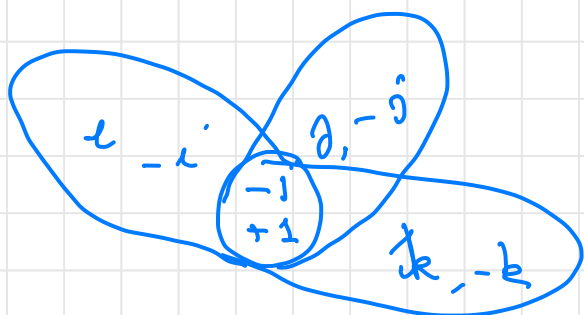
$\langle i \rangle, \langle j \rangle, \langle k \rangle \triangleleft Q_8$

$\langle i \rangle, Q_8 \triangleleft Q_8$

- Q_8 è un gruppo non abeliano che solo sottogruppi normali

- Q_8 non si spezza come prodotto semidiretto

$$\{1\} \neq H_1, H_2 \leq Q_8 \quad H_1 \cap H_2 \supset Z(Q_8)$$



Esercizio per casa
(facile)

$$Q_8 \hookrightarrow GL_2(\mathbb{C})$$

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \leftarrow \text{comp}$$

Classificazione dei gruppi di ordine 8

ABELIANI

$$\mathbb{Z}/8; \mathbb{Z}/4 \times \mathbb{Z}/2; \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$$

NON ABELIANI

• G ha un el di ordine 4

In gruppo su tutti el di ordine 2 è abeliano

$$a, b \in G \quad a^2 = b^2 = e \quad a = a^{-1} \quad b = b^{-1}$$

$$aba^{-1}b^{-1} = abab = (ab)^2 = e \Rightarrow G \text{ ab.}$$

$$a \in G \quad \text{ord } a = 4 \quad \langle a \rangle \triangleleft G \quad \text{perché ha indice 2}$$

$$G/\langle a \rangle = \{ \langle a \rangle, b\langle a \rangle \} \quad b \in G$$

$$b^2 \in \langle a \rangle \quad b^2 = \begin{cases} 1 \\ a \\ a^2 \\ a^3 \end{cases} \quad \leftarrow \text{no perché se no } \langle b \rangle = 8$$

$$b^2 = 1$$

$$b^2 = a^2$$

$$\bullet \quad a^4 = 1 \quad b^2 = 1 \quad G = \underbrace{\{1, a, a^2, a^3\}}_{\langle a \rangle} \cup \underbrace{\{b, ba, ba^2, ba^3\}}_{b\langle a \rangle}$$

$$\Rightarrow G \cong \langle a \rangle \rtimes \langle b \rangle \cong D_4$$

$$\varphi: \langle b \rangle \rightarrow \text{Aut}(\langle a \rangle) \cong \mathbb{Z}/2^* \cong \mathbb{Z}/2$$

$$b \mapsto \varphi: a \mapsto a^{-1}$$

$$\bullet \quad a^4 = 1 \quad b^2 = a^2$$

$$ba b^{-1} = \begin{cases} a \\ a^2 \\ a^3 \end{cases} \quad \text{NO perché } G \text{ non è abeliana}$$

$$\Rightarrow ba b^{-1} = a^3 \quad \begin{matrix} a \leftarrow b \\ b \leftarrow a^3 \end{matrix} \cong Q_8$$

Esercizio Determinare il minimo n tale che $Q_8 \hookrightarrow S_n$

Sicuramente $n \leq 8$ per il Teorema di Cayley.

$$S_4, S_5, S_6, S_7, S_8$$

$$|S_4| = 2^3 \cdot 3$$

Qual è la classe di iso di 2-Sylow di S_4 ? D_4

$$D_n \hookrightarrow S_n \quad \text{mandando } x \in D_4 \text{ nella corrisp. permutazione dei vertici}$$

$$|S_5| = 2^3 \cdot 3 \cdot 5 \quad D_4 \subset S_4 \subset S_5$$

I 2-Sylow di S_5 sono isomorfi a D_4

$$|S_6| = 2^4 \cdot 3 \cdot 5$$

$P_2 = 2$ -Sylow di S_6

$$Q_8 \hookrightarrow S_6 \quad ?$$

$$\begin{array}{ccc} i & \mapsto & \sigma \\ j & \mapsto & \rho \\ k & \mapsto & \sigma\rho = \eta \end{array}$$

$$\begin{aligned} \text{ord } \sigma &= \text{ord } \rho = 4 \\ \sigma^2 &= \rho^2 = \eta^2 \leftarrow \text{ordine } 2. \end{aligned}$$

ordine 2 $\Rightarrow$ prodotto di trasposizioni

$$\text{quadrato} \Rightarrow x^2 = (\eta_1 \dots \eta_k)^2 = \eta_1^2 \dots \eta_k^2$$

disgiunti

$$\eta^2 = (a_1 \dots a_{2e})^2 = (a_1 a_3 \dots a_{2e-1}) (a_2 a_4 \dots a_{2e})$$

$$\eta^2 = (a_1 \dots a_{2\frac{k+1}{2}})^2 = (a_1 a_3 \dots) \leftarrow 1 \text{ l-ado}$$

una permutazione è un $\Pi \Leftrightarrow$ i cicli di lunghezza pari compaiono in coppie.

$$(\Leftarrow) \quad \eta \text{ k-ciclo k dispari} \Rightarrow \eta \text{ è un } \Pi \text{ di cui } \eta = \eta^{k+1} = \left(\eta^{\frac{k+1}{2}}\right)^2$$

$$k \text{ pari} \quad (a_1 \dots a_k) (b_1 \dots b_k) = (a_1 b_1 a_2 \dots a_k b_k)^2$$

$$(\Rightarrow) \quad x^2 = (\eta_1 \dots \eta_s)^2 = \eta_1^2 \dots \eta_s^2 : \text{vengono fuori} \\ \text{cicli di lunghezza} \\ \text{dispari + coppie} \\ \text{di cicli}$$

$$\text{Es: } (123)(456) = (142536)^2 \quad S_6$$

$$(132)(465)^2$$

$$(12)(34) = \frac{(1324)^2}{(1432)^2} \quad S_4$$

Tornando a $Q_8 \hookrightarrow S_6$?

$\sigma^2 = \rho^2 = \eta^2$ ordine 2 + quadrato $\Rightarrow$ prodotto di un numero pari di trasposizioni

$$\sigma^2 = \rho^2 = \eta^2 = (ab)(cd) \leftarrow \text{dovrebbe avere } 6 \text{ sol}$$

Risolvo

$$X^2 = (12)(34) \quad *$$

$$\text{ord } x = 4 \quad (abc.d)^2 = (12)(34)$$

$\downarrow$

$$(ac)(bd)$$

$$a=1 \Rightarrow c=2$$

$$b=3 \quad b=4$$

$$d=4 \quad d=3$$

$$(acbd)$$

$$(acbd)(ef)$$

$$x_1 = (1 \ 3 \ 2 \ 4)$$

$$x_2 = (1 \ 4 \ 2 \ 3) = x_1^3$$

$$x_3 = (1324)(56)$$

$$x_4 = (1423)(56)$$

$\Rightarrow$ in S_8 * ha 4 soluzioni e non 6 come

sarebbero per avere $Q_8 \hookrightarrow S_8 \Rightarrow$ non si immerge.

$Q_8 \not\hookrightarrow S_7$ perché i 2-Sylow di S_7 sono isomorfi a quelli di S_6

$$Q_8 \hookrightarrow S(Q_8) \quad \text{Cayley.}$$

$$i \mapsto \varphi_i: x \mapsto ix$$

$$(1, i, -1, -i) \quad (1, i, -j, -k)$$

$$j \longmapsto (1, j, -1, -j) \left(i, \frac{-k}{ji}, -i, k \right)$$

$$S_8 \quad \begin{array}{l} 1 \longleftrightarrow 1 \\ -1 \longleftrightarrow 2 \\ i \longleftrightarrow 3 \\ -i \longleftrightarrow 4 \\ \pm j \longleftrightarrow 5, 6 \\ \pm k \longleftrightarrow 7, 8 \end{array}$$

$$i \longrightarrow (1, 3, 2, 4) (5, 7, 6, 8)$$

$$j \longrightarrow (1, 5, 2, 6) (3, 8, 4, 7)$$

— o — o —

Classificazione dei gruppi di ordine 30

$$|G| = 2 \cdot 3 \cdot 5$$

- G abeliano $\Rightarrow G \cong \mathbb{Z}/30$ perché 30 è sgr free.
- $30 = 2 \cdot 15$ 15 dispari $\Rightarrow G$ ha un sgr di ord 15
 - normale.
 - ciclico $15 = p^3 q^2$ $p \nmid q-1$
- $H = \langle x \rangle \triangleleft G$ ord $x = 15$
 $\cong \mathbb{Z}/15\mathbb{Z}$
- Per Cauchy $\exists y \in G$ ord $y = 2$ $\langle y \rangle = K$

$$\Rightarrow G \cong \langle x \rangle \rtimes_{\varphi} \langle y \rangle$$

$$\varphi \langle y \rangle \longrightarrow \text{Aut}(\langle x \rangle) \cong \mathbb{Z}/15\mathbb{Z}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

$$g \longmapsto \varphi_y(x) = x^l$$

$$\downarrow$$

$$\text{ord}(y)=2 \Rightarrow \text{ord } \varphi_y = \begin{cases} 1 & \rightarrow l=1 \\ 2 & \rightarrow \varphi_y^2 = \text{id} \end{cases}$$

$$\varphi_y^2(x) = x^{l^2} = x$$

$$l^2 \equiv 1 \pmod{15}$$

$$l^2 \equiv 1 \pmod{15} \quad \begin{cases} l^2 \equiv 1 \pmod{3} \\ l^2 \equiv 1 \pmod{5} \end{cases} \quad \begin{cases} l \equiv \pm 1 \pmod{3} \\ l \equiv \pm 1 \pmod{5} \end{cases}$$

$$l \equiv 1, -1, 4, -4$$

prodotto
diretto

$$\mathbb{Z}/30 \cong \mathbb{Z}/15 \times \mathbb{Z}_2$$

Sono tutti gruppi non iso o dei
quali iso tra questi gruppi?

Conosco

$$D_{15} \rightarrow 1$$

$$D_5 \times \mathbb{Z}_3 \rightarrow 4$$

$$D_3 \times \mathbb{Z}_5 \rightarrow 4$$

Questi gruppi non sono
isomorfi tra loro.
perché

$$Z(D_{15}) = \langle 1 \rangle$$

$$Z(D_5 \times \mathbb{Z}_3) = Z(D_5) \times Z(\mathbb{Z}_3) \cong \mathbb{Z}_3$$

$$Z(D_3 \times \mathbb{Z}_5) \cong \mathbb{Z}_5$$

$$y \longmapsto \varphi_y: x \mapsto x^l$$

$$\varphi_y(x) = x^l$$

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

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

$$yxy^{-1} = x^4$$

$$yxy^{-1} = x^{-4}$$

$$yx = x^{-1}y \quad D_{15}$$

$$l=4$$

$$l \equiv 1 (3)$$

$$l \equiv -1 (5)$$

y commute
 $x^5 \leftarrow$ el de
 ord 3

y non commute
 con l'el de
 ordre 5

$$yx^5y^{-1} = (yxy^{-1})^5 = (x^4)^5 = x^{20} = x^5$$

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

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

$$\langle y \rangle \longrightarrow \text{Aut } \mathbb{Z}/15\mathbb{Z} \cong \text{Aut}(\mathbb{Z}/3) \times \text{Aut}(\mathbb{Z}/5)$$

$$\varphi_y = l \longrightarrow \begin{pmatrix} \mathbb{Z}_3^* & \times & \mathbb{Z}_5^* \\ [l]_3 & & [l]_5 \end{pmatrix}$$

Anelli

Def Un anello è un insieme non vuoto con 2 operazioni

$(A, +, \cdot)$ Tale che

(i) $(A, +)$ gruppo abeliano

(ii) $\cdot$ è associativo

(iii) valgono le leggi distributive

$$\forall a, b, c \in A \quad a(b+c) = ab + ac$$

$$(a+b)c = ac + bc$$

Esempi:

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$

2) A anello $A[x]$ anello

3) $M_{m \times m}(K)$

4) $\text{End}(G)$ G gruppo ab $+ \circ$
" $\text{Hom}(G, G)$

Def A anello si dice COMMUTATIVO se $\cdot$ è comm.

A " " " con identità se $\exists 1 \in A$ ed
neutro per $\cdot$ proprietà: $\forall a \in A \quad a \cdot 1 = 1 \cdot a = a$

Def $(A, +, \cdot)$ si dice CAMPO

e se $(A \setminus \{0\}, \cdot)$ è un gruppo abeliano

Si dice CORPO se $(A \setminus \{0\}, \cdot)$ è un gruppo.

Def: A anello

$x \in A$ si dice DIVISORE DI ZERO se $\exists y \in A \ y \neq 0$ t.c.h. $xy = yx = 0$

$x \in A$ si dice NILPOTENTE se $\exists n \in \mathbb{N}$ t.c.h. $x^n = 0$

Se $1 \in A$, $x \in A$ si dice INVERTIBILE se $\exists y \in A$ t.c.h. $xy = yx = 1$

Def: A comm con 1 si dice DOMINIO D'INTEGRITA' se

$$D = \{x \in A \mid x \text{ è div di } 0\} = \{0\}$$

Esercizio Calcolare div di zero, nlp invertibili

$$\mathbb{Z}, \quad \mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$$A \text{ comm con } 1 \quad A^* = \{x \in A \mid x \text{ è invertibile}\}$$

$$N^p = \{x \in A \mid x \text{ è nilpotente}\} = \{x \in A \mid \exists n \in \mathbb{N} \ x^n = 0\}$$

Fatti noti: A comm con 1

1) $(A^*, \cdot)$ è un gruppo abeliano

$$2) A^* \cap D = \emptyset$$

$$3) A \text{ anello finito} \Rightarrow A = D \cup A^*$$

In particolare un dominio d'integrità finito è un campo.

$$\text{Dim (2)} \quad x \in A^* \cap D \quad \begin{array}{l} \exists y \in A \quad xy = yx = 1 \\ \exists z \in A \quad z \neq 0 \quad xz = zx = 0 \end{array}$$
$$\underline{z = 1} \quad z = (yx)z = y(xz) = y \cdot 0 = \underline{0} \Rightarrow \text{assurdo}$$

$$(3) \quad x \in A \setminus D \quad \varphi_x: A \rightarrow A \quad a \mapsto xa \quad \text{omo di gruppi}$$

$$\ker \varphi_x = \{y \in A \mid xy = 0\} = \{0\} \text{ per cui } x \in D$$

Perché $|A| < +\infty \Rightarrow \varphi_x \text{ è su} \Rightarrow \exists a \in A \varphi_x(a) = xa = 1 \Rightarrow x \in A^*$

Def. $B \subset A$ è un sottanello di A se è chiuso rispetto a $+$ e $\cdot$.

$I \subset A$ è un IDEALE di A se

• $(I, +)$ è un sgr di A

• $\forall a \in A \quad aI \subset I \quad Ia \subset I$ PROPRIETÀ DI ASSORBIMENTO

(Se A non è commutativo e $(I, +) \leq (A, +)$
 e vale $aI \subset I \quad \forall a \in A \rightarrow I$ si dice IDEALE SX)
 • $(Ia \subset I \quad \forall a \in A \rightarrow \text{" " " " } D_X)$

Esempio: 1) $\mathbb{Z}$ Gli ideali vanno marcati tra i sgr

$\{n\mathbb{Z}\}_{n \in \mathbb{N}} \quad n\mathbb{Z} \text{ è un ideale}$

$\forall x \in \mathbb{Z} \quad x \cdot n\mathbb{Z} \subset n\mathbb{Z} \quad x \cdot nz = n(xz) \in n\mathbb{Z}.$

2) $\{0\}, A$ sono ideali di A
↓ ↗
 ideale banale ideale improprio

Esercizio: $A = M_n(K)$ non ha ideali bilaterali $\neq \{0\}, A$

Def: $\emptyset \neq S \subset A \quad (S) := \left\{ \sum_{i=1}^n a_i s_i \mid n \in \mathbb{N} \quad a_i \in A, s_i \in S \right\}$

↑
 IDEALE GENERATO DA S

(S) è un ideale di A

$$x, y \in S \quad x = \sum_{i=1}^n a_i s_i \quad y = \sum_{j=1}^m d_j \tau_j \quad \begin{matrix} a_i, d_j \in A \\ s_i, \tau_j \in S \end{matrix}$$

$$\bullet x + y = \sum a_i s_i + \sum d_j \tau_j \in (S)$$

$$\bullet a \in A \quad ax = \sum_{i=1}^n \underbrace{a a_i}_{\in A} s_i \in (S)$$

$$S = \{x\} \quad C(x) = \{ax \mid a \in A\} = Ax$$

$$\text{Es: } n\mathbb{Z} = C(n)$$

$$\bullet K \subset F \quad d \in F \quad \text{alg su } K, \mu_d(\alpha) \in K[x]$$

$$\text{Sappiamo} \quad (\mu_d(x)) = \{p(x) \in K[x] \mid p(\alpha) = 0\}$$

OPERAZIONI TRA IDEALI

A anello comm

$I, J \subset A$ ideali

$$\bullet I \cup J \text{ in generale non è un ideale}$$

$$\bullet I \cap J \text{ è ideale}$$

$$\bullet I + J = (I, J) = \{i + j \mid i \in I, j \in J\} \text{ è ideale}$$

$$\bullet IJ = \langle \{xy \mid x \in I, y \in J\} \rangle$$

$$\bullet \sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\} \text{ è ideale}$$

In particolare $\sqrt{0} = \mathcal{N}$ = nilpotenti è un ideale

$$\bullet (I : J) = \{x \in A \mid xJ \subseteq I\} \text{ è ideale}$$

Verifiche:

• $I \cap J$ è sgr. e $\forall a \in A \quad \forall x \in I \cap J \quad ax \in I \Rightarrow ax \in I \cap J$
 $ax \in J$

• $I + J = \{x + y \mid x \in I \quad y \in J\}$

$x, y \in I + J \quad x = x_1 + y_1 \quad y = x_2 + y_2$

$x + y = \underbrace{(x_1 + x_2)}_{\in I} + \underbrace{(y_1 + y_2)}_{\in J} \in I + J$

$a \in A \quad ax = \underbrace{ax_1}_{\in I} + \underbrace{ay_1}_{\in J} \in I + J$

Dico che $I + J = (I, J)$
 $\subseteq \quad x + y \in (I, J)$

$\supseteq$ Basta vedere che $I \subset I + J$
 $J \subset I + J$

da queste inclusioni e dal fatto che $I + J$ è un ideale segue che $I + J \supseteq$ il più piccolo ideale di A che contiene sia I che J .

D'altro paio

$(S) = \bigcap_{\substack{S \subseteq X \subseteq A \\ X \text{ ideale}}} X$ ^{è chiaro} il più piccolo ideale di A che contiene S

è da dimostrare

($\supseteq$) (S) è uno dei termini dell'intersezione

($\subseteq$) $\forall x \in S \quad x = \sum a_i s_i \in X$ giacché X è ideale $X \supset S$

$\Rightarrow$ Per vector u $(S) \subset J$ whole A
 base vector $S \subset J$

Tornando al nostro caso

$$\begin{aligned} I &\subset I+J & 0 \in J \\ J &\subset I+J \\ j &= 0+j & 0 \in I \end{aligned} \Rightarrow (I, J) \in I+J$$

• $IJ = \{xy \mid x \in I, y \in J\}$ ← è un ideale per def.

• $\sqrt{I} = \{x \in A \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$

$$x, y \in \sqrt{I} \quad x^m \in I, y^n \in I \quad m, n \in \mathbb{N}$$

$$x+y \in \sqrt{I} \quad \exists d \in \mathbb{N} \quad (x+y)^d \in I$$

$$d = m+n \quad (x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}$$

$$\forall i \quad x^i \text{ se } i \geq n \quad \forall m+n-i \geq m$$

$$x^i \in I$$

$$y^{m+n-i} \in I$$

$$\Rightarrow \forall i \quad x^i y^{m+n-i} \in I \Rightarrow (x+y)^{m+n} \in I$$

$$\forall a \in A \quad (ax)^n = a^n \underbrace{x^n}_{\in I} \in I \Rightarrow ax \in \sqrt{I}$$

• $(I:J) = \{x \in A \mid xJ \subseteq I\}$ ⁹⁶

$$x, y \in (I : J) \quad (x+y)J = \underbrace{xJ}_{\subseteq I} + \underbrace{yJ}_{\subseteq I} \subseteq I$$

$$\Rightarrow x+y \in (I : J)$$

$$a \in A \quad x \in (I : J) \quad axJ = a(xJ) \subseteq aI \subseteq I$$

$$\Rightarrow ax \in (I : J)$$

Oss: $\bullet \quad IJ \subseteq I \cap J$

Perché $I \cap J$ è ideale basta vedere che contiene un insieme di generatori di IJ .

$$x \in I \quad y \in J \quad xy \in I \cap J \quad \text{e questo è ovvio}$$

$$\text{perché } \begin{array}{c} \nearrow \\ I \end{array} xy \in I \quad \begin{array}{c} \nearrow \\ A \end{array} xy \in J \Rightarrow xy \in I \cap J$$

$\bullet \quad I + J = A \quad \Rightarrow \quad IJ = I \cap J$

$$I + J = A \quad 1 + 0 = 1 \quad \text{Occorre dimostrare che}$$

$$\forall x \in I \cap J \quad x \in IJ$$

$$x = \underbrace{x \cdot 1}_{\in I \cdot J} + \underbrace{x \cdot 0}_{\in I \cdot J} \in IJ$$

Esempi: Operazioni tra ideali di $\mathbb{Z}$

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$$

$$m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$$

$$m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$$

$$m\mathbb{Z} + n\mathbb{Z} = \{a \cdot m + b \cdot n \mid a, b \in \mathbb{Z}\} = \{d \cdot x \mid x \in \mathbb{Z}\}$$

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

$$\sqrt{n\mathbb{Z}} = p_1 \cdots p_r \mathbb{Z}$$

$$= \{x \in \mathbb{Z} \mid x^k \in n\mathbb{Z} \quad k \in \mathbb{N}\}$$

$$= \{x \in \mathbb{Z} \mid n \mid x^k \quad k \in \mathbb{N}\}$$

$$n \mid x^k \Rightarrow p_i \mid x^k \text{ per ogni } i \Rightarrow p_i \mid x \quad \forall i$$

$$\Rightarrow p_1 \cdots p_r \mid x \Rightarrow x \in (p_1 \cdots p_r) = p_1 \cdots p_r \mathbb{Z}$$

Viceversa $x = p_1 \cdots p_r m \in \sqrt{n\mathbb{Z}}$ per cui

$$e = \max e_i: \quad x^e = p_1^e \cdots p_r^e m^e = n y \in n\mathbb{Z}$$

$$\sqrt{100\mathbb{Z}} = 10\mathbb{Z}.$$

$$(m\mathbb{Z} : n\mathbb{Z}) = \frac{m}{(m, n)} \mathbb{Z}$$

$$(75\mathbb{Z} : 18\mathbb{Z}) = \{x \in \mathbb{Z} \mid 18x\mathbb{Z} \subset 75\mathbb{Z}\} = 25\mathbb{Z}$$

$$75 \mid 18x \Leftrightarrow 25 \mid 6x \\ 25 \mid x$$

Proposizione:

1) $I \subset A$ ideale. I è ideale proprio ($I \subsetneq A$) $\Leftrightarrow I \cap A^* = \emptyset$

2) A campo ($\Leftrightarrow$ 92) gli unici ideali di A sono $\{0\}$ e A

Dim: (1) $I \cap A^* = \emptyset \quad A^* = \{1\} \Rightarrow I \subsetneq A$

$I \cap A^* \neq \emptyset \quad x \in I \cap A^* \quad \exists y \in A \quad xy = 1$

$\underset{I}{1} = \underset{A}{xy} \in I \Rightarrow a \cdot 1 \in I \quad \forall a \in A \Rightarrow A \subset I$

(2) A campo $\Leftrightarrow A^* = A - \{0\}$, l'unico idempotente
è $\{0\}$.

Anelli quoziente e omomorfismi di anelli

Def A, B anelli $f: A \rightarrow B$ omo di anelli
 $f(a_1 + a_2) = f(a_1) + f(a_2) \quad \forall a_1, a_2 \in A$
 $f(a_1 a_2) = f(a_1) f(a_2)$

Oss: Se A, B sono (comm) con 1 in genere si richiede anche

$$f(1_A) = 1_B$$

questo non è automatico

$$f(a) = f(1_A a) = f(1_A) f(a) \Rightarrow (1_B - f(1_A)) f(a) = 0$$

Se B è obnno e $f(a) \neq 0$ ($f \neq 0$) $\Rightarrow f(1_A) = 1_B$
 ma se $f(A) \subset D_B$ non è detto che $f(1_A) = 1_B$.

Def A anello $I \subseteq A$ ideale

Il gruppo quoziente $(A/I, +)$ può essere

obtenuto da una struttura di anello ponendo

$$(a+I) \cdot (b+I) \stackrel{\text{def}}{=} ab+I$$

l'op è ben definita ($a+I = a'+I$ $b+I = b'+I$
 $\Rightarrow ab+I = a'b'+I \dots$)

si verifica $(A/I, +, \cdot)$ è un anello

$$\pi_I: A \rightarrow A/I \quad \text{la proiezione}$$

$$a \mapsto a+I$$

$$\pi_I \text{ è un omomorfismo di anelli} \quad \ker \pi_I = I$$

Prop: Gli ideali sono tutti e soli i nuclei degli omomorfismi di anelli definiti su A

Dim: . $\varphi: A \rightarrow B$ omomorfismo di anelli $\Rightarrow \ker \varphi$ è ideale di A

$\ker \varphi \subseteq A$ perché φ è omomorfismo di gruppi

$$a \in A \quad x \in \ker \varphi: ax \in \ker \varphi \text{ perché } \varphi(ax) = \varphi(a)\varphi(x) = 0$$

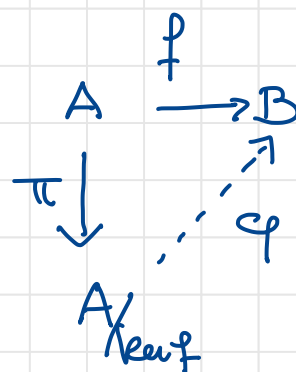
$$. I \subseteq A \text{ ideale} \Rightarrow I = \ker \pi_I.$$

□

Teorema di omomorfismo:

A, B anelli $f: A \rightarrow B$ omo.

Esiste un unico omo di anelli φ che fa commutare il diagramma,



cioè tale $f = \varphi \circ \pi$

Inoltre: φ è iniettivo.

$$\text{Im } \varphi = \text{Im } f.$$

Dim: Per il 1° di omo per gruppi dato che A, B son gruppi e f è un particolare om di gruppi.

sappiamo che posto $I = \ker f$ $\exists! \varphi: A/I \rightarrow B$

omo di gruppi tale $f = \varphi \circ \pi$ e che

val φ iniettivo e $\text{Im } \varphi = \text{Im } f$.

Resta da verificare che φ è omo di anelli:

$$\varphi(\pi(a)) = f(a) \quad \forall a \in A$$

$$\varphi(a + I) = f(a)$$

$$\varphi((a+I)(b+I)) \stackrel{95}{=} \varphi(ab+I) = f(ab)$$

$$= f(a) f(b) = \varphi(\pi(a)) \varphi(\pi(b)) = \varphi(a+I) \varphi(b+I)$$

□

Teorema di corrispondenza tra ideali

$$I \subseteq A \text{ ideale} \quad \pi: A \rightarrow A/I.$$

π induce una corrisp biunivoca tra gli ideali di A/I e gli ideali di A che contengono I (e questa corrispondenza conserva l'ordinamento)

Dim: Abbiamo la corrispondenza tra sottogruppi

Devo mostrare che se restringo la corrisp agli ideali questa associa ad un ideale di A un ideale di A/I e viceversa, cioè che

immagine e controimmagine di un ideale via π è un ideale

$$X = \{ J \subseteq A \text{ ideale} \mid I \subseteq J \} \rightarrow Y = \{ \tilde{J} \subseteq A/I \text{ ideale} \}$$

$$J \mapsto \pi(J)$$

$$\pi^{-1}(\tilde{J}) \longleftarrow \tilde{J}$$

Lemma: $f: A \rightarrow B$ omom di anelli

$$1) \quad \forall J \subseteq B \text{ ideale} \Rightarrow f^{-1}(J) \text{ è un ideale di } A$$

2) Se f è surgettiva, $\forall I \subset A$ ideale $f(I)$ ideale di B

Dim: (1) So che $f^{-1}(J)$ è un sottogruppo di A

$$a \in A \quad a \cdot f^{-1}(J) \subset f^{-1}(J)$$

$$x \in f^{-1}(J) \quad f(x) \in J \quad \Rightarrow \quad f(a) \overset{\in B}{\circ} f(x) \overset{\in J}{=} f(ax) \in J$$

$$ax \in f^{-1}(J)$$

(2) $f(I)$ è sgr di B

Sia $b \in B$; poiché f è su $\exists a \in A$ t.c.h. $b = f(a)$

$$f(x) \in f(I) \quad (x \in I)$$

$$f(I) \ni b \cdot f(x) = f(a) \cdot f(x) = f(ax) \in f(I)$$

$\downarrow$
I chiude l'ideale di A

Quanto conclude la dim del Teo di corrisp. $\square$

Esempio: Se f non è su in (2) l'immagine di un ideale non è nec. un ideale.

$$A = \mathbb{Z} \hookrightarrow \mathbb{Q} = B$$

(2) $\longrightarrow 2\mathbb{Z} \leftarrow$ non è un ideale di $\mathbb{Q}$
perché $\mathbb{Q}$ è un campo
e i suoi unici ideali son
(0) $\mathbb{Q}$.

In generale $f: A \rightarrow B \quad I \subset A$

$$(f(I)) = f(I)B = IB \quad (A \hookrightarrow B)$$

$\hookrightarrow$ ESTENSIONE DI I a B via f

$$f: A \rightarrow B \quad J \subset B \text{ ideale} \quad f^{-1}(J) \text{ è un ideale di } A$$

$f^{-1}(J)$ CONTRAZIONE di J ad A (via f)

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow q & \\ A/\ker f & & \end{array}$$

$$f = q \circ \pi$$

$\downarrow$ $\uparrow$
 imietwa, sur

Gli omi imietwa sono "sostanzialmente" inclusivi

a meno di isomorfismo

Considera la corrispondenza ideale involuta da π

quindi basta considerare le inclusioni

$$A \hookrightarrow B$$

$$I \dashrightarrow IB \leftarrow \text{estensione di } I \text{ ad } B \text{ su } B$$

$$J \cap A \dashleftarrow J$$

$\uparrow$ contrazione di J ad A su A

$$A \xrightarrow{\varphi} B \xrightarrow{\varphi} B/J$$

$$\ker \varphi = \{a \in A \mid \varphi(a) = a + J = J\} = \{a \in A \mid a \in J\} \\ = J \cap A$$

$$\Rightarrow A/J \cap A \xrightarrow{\varphi} B/J$$

Oss: Dal 1° Teo di omo per anelli si deducono il 2° e 3° Teo di omo

$$I \subset J \subset A \text{ ideali di } A \quad \left| \quad \frac{I+J}{J} \cong \frac{I}{I \cap J} \right.$$

$$A/I/J/I \cong A/J \quad \left| \quad \begin{array}{c} \uparrow \\ \text{omo di anelli} \end{array} \right.$$

Def A, B anelli $A \times B$ può essere dotato di una struttura di anello con le op comp per comp

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \forall a_1, a_2 \in A \\ (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2) \quad \forall b_1, b_2 \in B$$

$A \times B$ con queste operazioni si dice **PRODOTO DIRETTO**

TEOREMA CINESE per anelli

A anello comm con 1. I, J ideali di A

$$\nexists \quad A \longrightarrow A/I \times A/J \quad a \longmapsto (a+I, a+J)$$

f è un omomorfismo di anelli, $\ker f = I \cap J$

$I + J = A \iff f$ è surgettivo

e in tal caso si ottiene

$$A / I \cap J \cong A / I \times A / J$$

Oss: $\mathbb{Z} / mn\mathbb{Z} \cong \mathbb{Z} / m\mathbb{Z} \times \mathbb{Z} / n\mathbb{Z} \iff (m, n) = 1$

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z} / m\mathbb{Z} \times \mathbb{Z} / n\mathbb{Z}$$

$$\ker f = [m, n] \quad \mathbb{Z} / [m, n] \hookrightarrow \mathbb{Z} / m\mathbb{Z} \times \mathbb{Z} / n\mathbb{Z}$$

Sapremo che è surgettivo $\iff (m, n) = 1$

e in quel caso $[m, n] = mn$

Dim: f omomorfismo: verifica banale.

$$\begin{aligned} \ker f &= \{a \in A \mid f(a) = (a+I, a+J) = (I, J)\} = \\ &= \{a \in A \mid a \in I \wedge a \in J\} = I \cap J \end{aligned}$$

$$\Rightarrow I + J = A \quad \exists i \in I, j \in J \text{ t.c. } i + j = 1$$

Per mostrare che f è su devo far vedere che

$$\begin{aligned} \forall a, b \in A \quad \exists x \in A \text{ t.c. } f(x) &= (a+I, b+J) \\ x &= bi + aj \end{aligned}$$

$$f(x) = (\cancel{bx} + a_j + I, \quad b\cancel{x} + a_j + J)$$

$\in I$ $\in J$

$$bx + a_j \equiv a_j \pmod{I}$$

$$x + y = 1 \quad y = 1 - x$$

$$a_j + I = a(1 - x) + I = a - ax + I = a + I$$

$$y \equiv 1 \pmod{I}$$

$$x \equiv 1 \pmod{J} \quad bx \equiv b \pmod{J} \quad bx + J = b + J$$

$$f(x) = (a + I, b + J)$$

$$\iff f \text{ su } \exists x \in A \text{ tale } f(x) = (I, 1 + J)$$

" $(x + I, x + J)$

$$\Rightarrow x \in I \quad x \equiv 1 \pmod{J} \quad x = 1 + j \in J$$

$$\Rightarrow 1 \in I + J$$

$$\text{Se } I + J = A \Rightarrow f \text{ su}$$

$$A / \ker f \cong A/I \times A/J$$

$$\ker f = I \cap J \quad \text{D'altra parte } I + J = A$$

$$\Rightarrow I \cap J = IJ \quad (101 \text{ visto la volta scorsa})$$

$$I + J = A \Rightarrow A/IJ \cong A/I \times A/J$$



$(\mathcal{F}, \leq)$ insieme parzialmente ordinato

$X \subset \mathcal{F}$ $M \in \mathcal{F}$ è un maggiorante per X se
 $\forall A \in X \quad A \leq M$

$A \in \mathcal{F}$ è un massimale per $\mathcal{F}$ se
 $\forall B \in \mathcal{F}$ t.c. $A \leq B \Rightarrow A = B$

$A \in \mathcal{F}$ si dice MASSIMO per $\mathcal{F}$ se
 $\forall B \in \mathcal{F} \quad B \leq A$

Una CATENA di $\mathcal{F}$ è un sottoinsieme di $\mathcal{F}$ TOT ORDINATO
 $(\mathcal{F}, \leq)$ si dice INDUTTIVO se ogni catena di $\mathcal{F}$ ammette
un maggiorante in $\mathcal{F}$

Lemma di Zorn

$(\mathcal{F}, \leq)$ p. ordinato, $\mathcal{F} \neq \emptyset$, $\mathcal{F}$ induttivo.

$\Rightarrow \mathcal{F}$ contiene elementi massimali.

Oss: Spesso usiamo il Lemma di Zorn su famiglie
di ideali di $A \subseteq$

Def: $I \subseteq A$ ideale

I si dice ideale PRIMO se

$$\forall x, y \in A \quad xy \in I \Rightarrow x \in I \vee y \in I$$

I si dice MASSIMALE se è un el. massimo

della famiglia $\mathcal{I}$ di tutti gli ideali propri di A

Esplicitamente: $I \in \max \Leftrightarrow \forall J \subseteq A$

$$\text{t che } I \subseteq J \Rightarrow I = J$$

Esempi: • Gli ideali primi di $\mathbb{Z}$ sono (p) p primo

$$p \text{ primo } (p) \ni x, y \quad p | xy \Rightarrow p | x \vee p | y \Rightarrow$$
$$x \in p \vee y \in p$$

(m) $m = \text{non primo} \Rightarrow m$ è riducibile

$$\Rightarrow m = ab \quad 1 < a < m \quad 1 < b < m$$

$$ab \in (m) \quad a \notin (m) \quad e \quad b \notin (m) \Rightarrow (m) \text{ non primo.}$$

Proposizione:

(1) Ogni ideale proprio di A è contenuto in un ideale massimale

(2) Ogni el. non invertibile di A è contenuto in un'ideale massimale

Dim: Chianamente $(1) \Rightarrow (2)$

103

$$x \in A - A^* \Rightarrow (x) \subsetneq A$$

$$\Rightarrow \text{per (1)} \quad (x) \in \mathcal{M} \text{ di massimali} \Rightarrow x \in \mathcal{M}.$$

(1) $I \subsetneq A$ ideale

$$\mathcal{F} = \{ J \subsetneq A \mid I \subseteq J \} \quad \mathcal{F} \ni I \Rightarrow \mathcal{F} \neq \emptyset$$

$(\mathcal{F}, \subseteq)$ è induttivo

$\mathcal{C}$ catena

$$\mathcal{C} = \{ J_n \}$$

$$\bigcup J_n = J \leftarrow \begin{array}{l} \text{Dico } J \\ \text{è un} \\ \text{maggiorante} \\ \text{per } \mathcal{C}. \end{array}$$

• $\forall J_n \in \mathcal{C} \quad J_n \subseteq J$ ovvio

• $J \in \mathcal{F} \quad I \subset J_n \subset J$ e J è ideale

$$J \subsetneq A \text{ giacché se } 1 \in J = \bigcup J_n \Rightarrow$$

$$\Rightarrow \exists n \text{ t.c. } 1 \in J_n \subsetneq A \Rightarrow \text{assurdo.}$$

Per il Lemma di Zorn la famiglia $\mathcal{F}$ ammette almeno un elemento max M .

M è elemento massimale in $\mathcal{F}$. Per due che è un ideale massimale dato che è max nella famiglia di tutti gli ideali propri di A .

$$L \subsetneq A \text{ ideale} \quad M \subseteq L \Rightarrow I \subseteq M \subseteq L \Rightarrow$$

$$L \in \mathcal{F} \quad \text{Per la massimalità di } M \text{ in } \mathcal{F} \Rightarrow M = L$$

Proposizione $I \subsetneq A$ (1) I è primo $\Leftrightarrow A/I$ è un dominio

(2) I è ¹⁰⁴ massimale $\Leftrightarrow A/I$ è un campo.

Dim: $x, y \in A$

$$I \text{ è primo} \Leftrightarrow xy \in I \Rightarrow x \in I \vee y \in I$$

$$A/I \text{ dominio} \Leftrightarrow (x+I)(y+I) = I \Rightarrow x \in I \vee y \in I$$

$$\overset{''}{xy+I=I} \Rightarrow x \in I \vee y \in I$$

$$xy \in I \Rightarrow x \in I \vee y \in I$$

$$\Leftrightarrow I \text{ è ol primo}$$

$$(2) \quad I \text{ è ol max} \Leftrightarrow \text{in } A/I \text{ ho solo gli ideali}$$

$\nearrow$
TEOREMA DI CORRISP. (0) e A/I

$$\Leftrightarrow A/I \text{ è campo.}$$

Corollario : 1) A è un dominio $\Leftrightarrow (0)$ è un ideale primo

2) A è un campo $\Leftrightarrow (0)$ è un ideale max.

3) I massimale $\Rightarrow I$ primo

Dim (1) $\Leftarrow$ (2) chiara dalla prop.

$$(3) \quad I \text{ max} \Leftrightarrow A/I \text{ campo} \Rightarrow A/I \text{ dominio} \Rightarrow I \text{ primo.}$$

Esempio $\mathbb{Z}$ è un dominio ma non è un campo

(0) è un ideale primo di $\mathbb{Z}$ ma non è max.

$$(0) \subset (m) \quad \forall m \in \mathbb{Z}.$$

Corollario: La corrispondenza ha i ideali $A \rightarrow A/I$
 conserva ideali primi e ideali massimali

$$\text{Dim } I \subseteq J \subseteq A \quad A \rightarrow A/I \quad J \rightarrow \pi(J) = J/I$$

$$A/I/J/I \cong A/J \quad *$$

Devo vedere che

$$\begin{array}{ccc}
 J \text{ primo max in } A & (\Rightarrow) & J/I \text{ primo max in } A/I \\
 \Downarrow & & \Downarrow \\
 A/J \text{ dominio campo} & \Leftrightarrow & A/I/J/I \text{ dominio campo} \\
 \uparrow & & \\
 \text{dato l'isomorfismo} & & *
 \end{array}$$

Anello delle frazioni di un dominio

A anello comm con 1 DOMINIO D'INTEGRITA'.

- $S \subset A$
- $0 \notin S$
 - $1 \in S$
 - S è moltiplicativamente chiuso ($\forall x, y \in S \Rightarrow xy \in S$)

S con le 3 proprietà sopra si dice PARTE MOLTIPLICATIVA di

$$S^{-1}A =: \left\{ \frac{a}{s} \mid a \in A, s \in S \right\} / \sim \quad \frac{A \times S}{\sim}$$

$$\frac{a}{s} \sim \frac{b}{t} \Leftrightarrow at = bs$$

$$(a, s) \sim (b, t) \Leftrightarrow at = bs$$

$$\frac{a}{s}$$

$\sim$ è una rel' equivalenza

(Transitivit ) $\frac{a}{s} \sim \frac{b}{t} \quad \frac{b}{t} \sim \frac{c}{u} \Rightarrow \frac{a}{s} \sim \frac{c}{u}$

$$at = bs \quad bu = ct \quad au = cs$$

$$a u t = b u s = c t s \Rightarrow t(a u - c s) = 0 \quad t \in S$$

$$\Rightarrow t \neq 0 \quad \text{e poich  } A \text{   dominio } \Rightarrow a u = c s$$

Proposizione 1: $S^{-1}A$ con le operazioni definite

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

è un anello con inv. ($= 1/1$)

Dim: Devo verificare che le operazioni sono ben definite
e che hanno le proprietà di quello.

$$\frac{a}{s} \sim \frac{a'}{s'} \quad \frac{b}{t} \sim \frac{b'}{t'}$$

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \frac{a'}{s'} + \frac{b'}{t'} = \frac{a't' + b's'}{s't'}$$

$$as' = a's \quad bt' = b't$$

$$\text{Vale } l' = \Rightarrow \quad \underline{(at + bs)s't'} = (a't' + b's')st$$

$$\underline{a} \underline{t} \underline{t'} \underline{s'} + \underline{b} \underline{s} \underline{s'} \underline{t'} = a's \underline{t} \underline{t'} + b' \underline{t} \underline{s} \underline{s'} = (a't' + b's')st$$

Le altre verifiche per esercizio

□

Esempio: $A = \mathbb{Z}$ $S = \{10^k\}_{k \geq 0}$

$$S^{-1}A = \left\{ \frac{n}{10^k} \mid n \in \mathbb{Z}, k \geq 0 \right\}$$

$$\frac{5}{10} = \frac{1}{2} \in S^{-1}A$$

$$\underline{\text{Oss:}} \quad \frac{2}{1} \in S^{-1}A \quad \text{ed è invertibile} \quad \frac{2}{1} \frac{5}{10} = \frac{1}{1}$$

Prop 2: $f: A \longrightarrow S^{-1}A$ è un omomorfismo
 $a \longmapsto \frac{a}{1}$

(quindi $A \subset S^{-1}A$ e $S^{-1}A$ è un'estensione di A)

$$\text{Dim } f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$$

$$f(ab) = \frac{ab}{1} = \frac{a}{1} \frac{b}{1} = f(a) \cdot f(b)$$

$$\ker f = \left\{ a \in A \mid \frac{a}{1} = \frac{0}{1} \right\} = \left\{ a \in A \mid \underset{a}{a} \cdot 1 = 0 \cdot 1 = 0 \right\} = \{0\} \quad \square$$

Caso $S = A - \{0\}$ $\leftarrow$ Se A è dominio quoziente e una parte moltiplicativa
 $\forall x, y \in S (x \neq 0 \wedge y \neq 0)$
 $\Downarrow$
 $xy \in S \quad (xy \neq 0)$

$$S^{-1}A = Q(A) \quad \text{CAMPO DEI QUOZIENTI DI } A$$

Prop 3: A dominio $S = A - \{0\}$

$S^{-1}A$ è il più piccolo campo che contiene A

Dim: • $S^{-1}A$ è un campo $\forall a \in A, a \neq 0, \frac{1}{a} \in S^{-1}A$

$$\text{e } \frac{a}{1} \cdot \frac{1}{a} = \frac{1}{1}$$

• Se K campo $K \supset A \Rightarrow K \ni \frac{1}{a} \quad \forall a \in A - \{0\}$

$\Rightarrow \forall b \in A, \forall a \in A - \{0\} \quad \frac{b}{a} \in K \Rightarrow S^{-1}A \subset K \quad \square$

Esempio 1) $S_1 = \{10^k\}_{k \geq 0} \quad S_0 = A - \{0\}$

$$\mathbb{Z} \subset S_1^{-1}\mathbb{Z} \subset S_0^{-1}\mathbb{Z} = \mathbb{Q}$$

$$2) A = K[x] \quad Q(A) = \overset{109}{K(x)} = \left\{ \frac{f(x)}{g(x)} \mid f, g \in K[x], g \neq 0 \right\}$$

3) A (obiettivo) $P \subset A$ ideale primo

$S = A \setminus P$ è una parte molt.

$$0 \notin S, 1 \in S, \quad x, y \in S \Rightarrow xy \in S$$

$$\Downarrow \quad \Updownarrow$$

$$x, y \notin P \Rightarrow xy \notin P$$

$\uparrow$
 P è prim

$S^{-1}A = A_P \leftarrow$ localizzato su A a P .

$\uparrow$
 A_P è un anello locale cioè ha un unico id max

$$A = \mathbb{Z} \quad P = 2\mathbb{Z} \quad S = \mathbb{Z} \setminus 2\mathbb{Z}$$

$$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z} \ (b, 2) = 1 \right\} \leftarrow \text{Dico che } (2) \mathbb{Z}_{(2)}$$

è l'unico id max
di $\mathbb{Z}_{(2)}$

ESERCIZIO.

$$(S^{-1}A)^* = \left\{ \frac{a}{s} \mid \frac{s}{a} \in S^{-1}A \right\} = \left\{ \frac{a}{s} \mid \exists b \in A \text{ con } ab \in S \right\}$$

$\uparrow$

$$\exists b \in A \ t \in S \text{ tale che } \frac{s}{a} = \frac{b}{t} \Leftrightarrow ab = st \in S$$

$$S = \{10^k\}_{k \geq 0} \quad (S^{-1}\mathbb{Z})^* \ni 2 \quad \text{perché } \frac{1}{2} = \frac{5}{10}$$

$\frac{10}{5}$

I ideali di $S^{-1}A$

$$I \subset A \text{ ideale} \quad S^{-1}I = \left\{ \frac{x}{s} \in S^{-1}A \mid x \in I \ s \in S \right\} \simeq \frac{I \times S}{\sim}$$

Teorema: 1) $S^{-1}I$ è un ideale di $S^{-1}A$

2) $\forall J \subset S^{-1}A \exists I \subset A$ tale che $J = S^{-1}I$

3) $S^{-1}I$ è un ideale proprio $\Leftrightarrow I \cap S = \emptyset$

4) P primo $P \cap S = \emptyset \Rightarrow S^{-1}P$ è un primo

Dim: 1) $\frac{x}{s}, \frac{y}{t} \in S^{-1}I$ $\frac{x}{s} + \frac{y}{t} = \frac{x \overset{\text{di } S^{-1}A}{t} + y \overset{\text{di } S^{-1}A}{s}}{st} \in S^{-1}I$

$$\frac{a}{s} \in S^{-1}A \quad \frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st} \in S^{-1}I$$

2) $J \subset S^{-1}A$ ideale $f^{-1}(J) = I \subset A$ ideale
" $J \cap A$

Dico che

$$J = S^{-1}I$$

$$x \in I \quad \frac{x}{1} = f(x) \in J \Rightarrow \frac{1}{s} \frac{x}{1} = \frac{x}{s} \in J$$

$$\Rightarrow S^{-1}I \subset J$$

$$\frac{x}{s} \in J \Rightarrow \frac{x}{1} = \frac{x}{s} \cdot \frac{s}{1} \in J \Rightarrow x = f^{-1}\left(\frac{x}{s}\right) \in I$$

$$\frac{x}{s} \in S^{-1}I$$

3) $S^{-1}I = S^{-1}A \Leftrightarrow \frac{1}{1} \in S^{-1}I \Leftrightarrow \exists x \in I$ s.e. S tale che

$$\frac{1}{1} = \frac{x}{s} \Leftrightarrow \exists x = s \in S \Leftrightarrow I \cap S \neq \emptyset$$

$$4) \quad P \text{ primo} \quad P \cap S \begin{cases} \neq \emptyset & \Rightarrow S^{-1}P = S^{-1}A \\ = \emptyset & \Rightarrow S^{-1}P \text{ è primo} \end{cases}$$

$$\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}P \quad \exists \sigma \in S \quad p \in P \quad t \in S$$

$$\frac{ab}{st} = \frac{p}{\sigma} \quad ab\sigma = \underbrace{p}_{\in P} st \in P$$

$$\Rightarrow ab\sigma \in P \quad \sigma \in S \quad \text{e} \quad S \cap P = \emptyset \Rightarrow \sigma \notin P$$

$$\Rightarrow ab \in P \Rightarrow a \in P \vee b \in P \Rightarrow \frac{a}{s} \in S^{-1}P \vee \frac{b}{t} \in S^{-1}P$$

$$\uparrow \quad \quad \quad \Rightarrow S^{-1}P \text{ è primo}$$

$P \text{ primo}$

□

Divisibilità nei domini. Elementi primi e elem. irriducibili.
A DOMINIO

Def A dominio $a, b \in A \quad a \neq 0$ - si dice $a|b$ se

$$\exists c \in A \quad \text{t.c.} \quad b = ac.$$

$$\text{oss:} \quad a|b \Leftrightarrow (b) \subseteq (a)$$

$$a|b \Leftrightarrow \exists c \in A \quad \text{t.c.} \quad b = ac \Leftrightarrow b \in (a)$$

$$\Leftrightarrow (b) \subseteq (a)$$

Def: $a, a' \in A$ si dicono ASSOCIATI $a \sim a'$ se
vale una delle seguenti condizioni equivalenti

- (i) $a|a' \wedge a'|a$
- (ii) $\exists u \in A^* \quad \text{t.c.} \quad a = u a'$
- (iii) $(a) = (a')$

(i) $\Leftrightarrow$ (iii) segue dall'oss $a|a' \quad (a') \subseteq (a)$
 $a'|a \quad (a) \subseteq (a')$

(i) $\Rightarrow$ (ii) $a' = xa \quad a = ya' \quad a = yxa$
 $\Rightarrow a(1-xy) = 0 \quad a \neq 0 \quad A \text{ obm.} \Rightarrow$

$$xy = 1 \quad a = ya' \quad y \in A^*.$$

(ii) $\Rightarrow$ (iii) $a \in (a') \quad uv = 1 \quad v \in A$

$$a' = vua' = va \Rightarrow a' \in (a)$$

$$\Rightarrow (a) = (a') \quad \square$$

DEF a, b non entrambi 0 - $d \in A$ è un massimo com. divisore
 per a e b se

$$1) \quad d|a \wedge d|b$$

$$2) \quad \forall x \in A \text{ t.c. } x|a \wedge x|b \Rightarrow x|d$$

Proposizione: $d = (a, b) \quad d' = (a, b) \Leftrightarrow d \sim d'$

Def $x \in A \quad x \notin A^* \cup \{0\}$

x si dice PRIMO se $\forall a, b \in A \quad x|ab \Rightarrow x|a \vee x|b$

x si dice IRRIDUCIBILE se $\forall a, b \in A \quad x = ab \Rightarrow a \in A^* \vee b \in A^*$

Proposizione 1: x primo $\Rightarrow x$ irriducibile

(La dim è la stessa dello scorso anno)
 si usa A obm.

Proposizione 2: ● x è PRIMO $\Leftrightarrow (x)$ è PRIMO non nullo

● x è IRRIDUCIBILE $\Leftrightarrow (x)$ è massimale nell'unione degli ideali primari

Esempio $A = K[x, y]$ x è primo perché (x) è primo

in quanto $A/(x) \cong K[y]$ che è dominio

$\Rightarrow x$ è anche vero per la prop 1

(x) è mass tra gli id primari ma non è un id mass in A in quanto $K[y]$ non è un campo. Infatti: $(x) \subsetneq (x, y) \subsetneq A$

Dim: La prima parte è ovvia.

$(\Rightarrow)$ x irriducibile. $(x) \subsetneq (y) \subsetneq A \quad \exists z \in A \nmid x$

$x = yz$ $y \nmid A^x$ perché altrimenti sarebbe $(y) = A$

x è vero $\Downarrow$

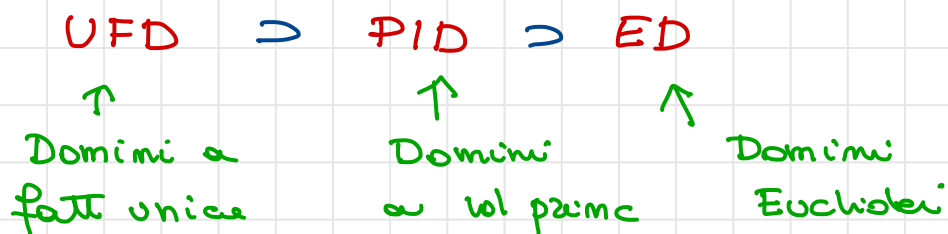
$z \in A^x \Rightarrow (x) = (y) \Rightarrow (x)$ è max tra gli id pr.

$(\Leftarrow)$ x irriducibile $\Rightarrow x = yz \quad y, z \nmid A^x$

$(x) \subsetneq (y) \subsetneq A$

$\nearrow$ $z \nmid A^x$ $\uparrow$ $y \nmid A^x$

□



Domini euclidei

Def. Un dominio d'integrità A si dice DOMINIO EUCLIDEO se

$\exists$ una funzione $d: A \setminus \{0\} \rightarrow \mathbb{N}$ detta GRADO

con le seguenti proprietà:

$$(1) d(x) \leq d(xy) \quad \forall x, y \in A \setminus \{0\}$$

$$(2) \quad \forall x \in A \quad \forall y \in A \setminus \{0\} \quad \exists q, r \in A \quad \text{t.c.}$$

$$x = yq + r \quad \text{e} \quad \begin{cases} d(r) < d(y) \\ \text{oppure} \\ r = 0 \end{cases}$$

Oss: In un dominio euclideo ogni el. si può "ben approssimare" con un multiplo di ogni altro elemento.
La funzione grado serve per due cose vuol dire approssimare bene.

Esempi 1) $(\mathbb{Z}, | \cdot |)$ è un dominio euclideo.

$$d = | \cdot | \quad |xy| = |x||y| \geq |x| \quad \forall y \neq 0$$

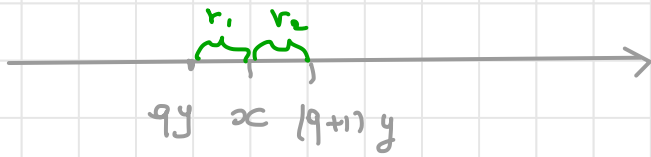
$$y \neq 0 \quad \exists q, r \quad \text{t.c.} \quad x = qy + r$$

$$|r| < |y| \quad \text{se chiesto solo punto} \quad \vee \quad r = 0 \quad \text{non ho niente}$$

Inoltre sappiamo che

$$0 < r < |y|$$

*



$$x = 18$$

$$y = 4$$

$$18 = 4 \cdot 4 + 2$$

$$18 = 5 \cdot 4 - 2$$

$$2) \quad K[x] \quad \deg \quad \text{in} \quad ED$$

$$\deg fg = \deg f + \deg g \geq \deg f$$

$$f = gq + r \quad \deg r < \deg g \quad \vee \quad r = 0$$

$$3) \quad \mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$$

$$d : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$$

$$d = a+ib \longrightarrow d(\alpha) = \alpha \bar{\alpha} = a^2 + b^2$$

" $N(\alpha)$

$\mathbb{Z}[i]$ es un dominio euclideo (Lo veremos).

Domini euclidei

Def. Un dominio d'integrità A si dice DOMINIO EUCLIDEO se

$\exists$ una funzione $d: A \setminus \{0\} \rightarrow \mathbb{N}$ detta GRADO

con le seguenti proprietà:

$$(1) d(x) \leq d(xy) \quad \forall x, y \in A \setminus \{0\}$$

$$(2) \quad \forall x \in A \quad \forall y \in A \setminus \{0\} \quad \exists q, r \in A \quad \text{t.c.}$$

$$x = yq + r \quad \text{e} \quad \begin{cases} d(r) < d(y) \\ \text{oppure} \\ r = 0 \end{cases}$$

Esempi 1) $(\mathbb{Z}, |\cdot|)$

2) $(K[x], \deg)$

ANELLO DEGLI INTERI DI GAUSS

3) $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\} \quad (\mathbb{Z}[i] \subset \mathbb{Q}(i) \subset \mathbb{C})$

$$d: \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$$

$\mathbb{Z}[i]$ dominio

$$\alpha = a+ib \longmapsto \alpha \bar{\alpha} = a^2 + b^2 = |\alpha|^2$$

$$\forall \alpha, \beta \in \mathbb{Z}[i] \setminus \{0\} \quad d(\alpha) \leq d(\alpha\beta)$$

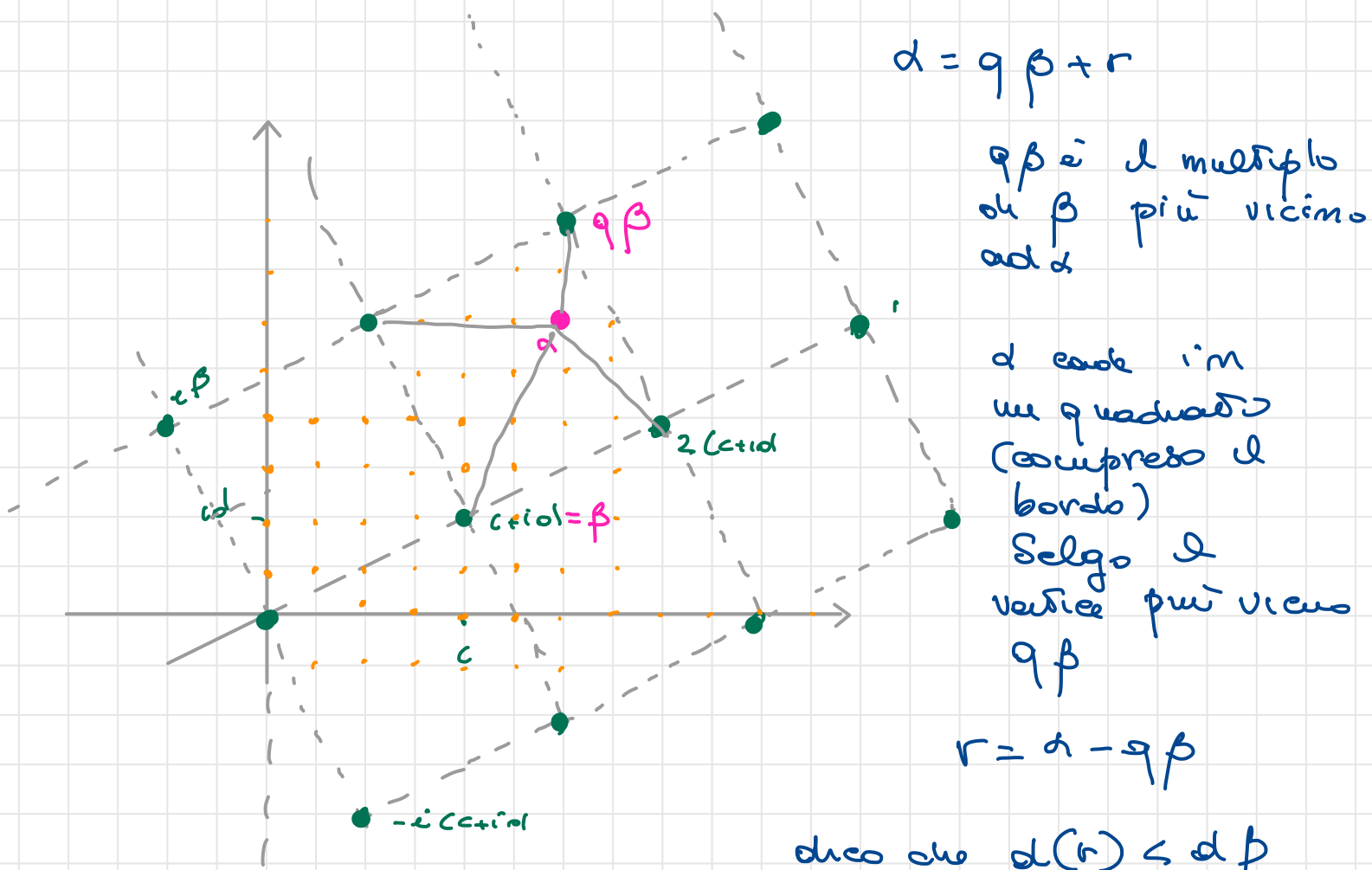
$$d(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2 |\beta|^2 \geq |\alpha|^2 = d(\alpha) \quad |\beta|^2 \geq 1$$

$$x^2 + y^2 \geq 1 \quad (\beta = x+iy)$$

(2) vuol dire che $\forall \alpha, \beta \neq 0$ si può "approssimare",
 α con un multiplo di β .

$\alpha, \beta \neq 0 \quad \frac{\alpha}{\beta} \in \mathbb{C}$ in generale $\notin \mathbb{Z}[i]$ / ecco $\frac{\alpha}{\beta}$
 $\notin \mathbb{Z}[i]$

$$\alpha = \beta q + r \quad \begin{cases} d(r) < d(\beta) \\ r=0 \end{cases}$$



$$d(r) < \frac{1}{2} \text{diag quadrato} < \text{latto} = d(\beta)$$

$r=0$

Proposizione 1: A euclideo. $\forall a, b \in A$ non entrambi nulli
 posso calcolare $\text{MCD}(a, b)$ usando
 l'algoritmo di Euclide.

Dim:
$$\begin{aligned} a &= q_0 b + r_1 \\ b &= q_1 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

(1) l'algoritmo Termina
non o' finche' le
succ dei gradi $\in \mathbb{N}$
ed e' strett decrescente

(2) $r_n = (a, b)$ stesso modulo
dei can
aritmici $\square$

Prop 2 : A ED . Gli elementi di grado minimo
di A sono gli el di A^*

Dim: $\phi \neq d(A \setminus \{0\}) \in \mathbb{N}$ ammette minimo d_0

Sia $x \in A \setminus \{0\}$ $d(x) = d_0$

$\forall y \in A \setminus \{0\} \quad y = qx + r \quad \left. \begin{array}{l} d(r) < d(x) \\ r = 0 \end{array} \right\} \leftarrow \text{NO } d(x) = d_0$

$\Rightarrow \forall y \in A \setminus \{0\} \quad y = qx \quad y \in \langle x \rangle$

In particolare $\exists q \in A$ t.c. $1 = qx \Rightarrow x \in A^*$

Viceversa, $x \in A^* \quad \langle x \rangle = A \quad (x \in A^* \quad 1 \in \langle x \rangle)$
 $\Rightarrow a \in \langle x \rangle \quad \forall a \in A$
 $\Rightarrow \langle x \rangle = A$

$d(x) \leq d(qx) \quad \forall q \in A \setminus \{0\} \quad (\text{e' la (1)})$

$d(x) \leq d(a) \quad \forall a \in A \Rightarrow d(x) \text{ e' minimo} \quad \square$

Prop 3 : A ED $\Rightarrow$ Tutti gli IDEALI di A sono PRINCIPALI
e generati da un elem di grado minimo

Dim: $I \subset A$. $I \neq \{0\}$ I e' principale

$I \neq \{0\}$ Dico che I è generato da un suo el di grado minimo

$x \in I$ di grado minimo $\Rightarrow (x) \subseteq I$

$\forall a \in I \quad a = qx + r \quad d(r) < d(x) \quad \forall r = 0$

$r = a - qx \in I \Rightarrow d(x) \leq d(r) \Rightarrow r = 0$

$\Rightarrow a = qx \in (x) \Rightarrow I \subseteq (x) \quad \square$

Domini a ideali principali (PID)

Def : Un dominio A si dice a ideali principali (PID)

se ogni ideale di A è principale

$(\forall I \subseteq A \text{ ideale } \exists x \in I \text{ tale che } I = (x))$

" Prop 3 : $A \text{ ED} \Rightarrow A \text{ PID}$ "

Prop 4 : $A \text{ PID} \Rightarrow$ Gli ideali primi di A sono $\{0\}$ e gli ideali massimali

Dim: $\{0\}$ è primo perché A è dominio
 $M \text{ max}$ è primo (è vero in ogni anello)

Viceversa, se P un ideale primo $\neq \{0\}$ - $P = (x)$

voglio vedere che P è max.

$P = (x)$ è primo $\Leftrightarrow x$ è primo $\Rightarrow x$ è irriducibile

$\begin{array}{ccc} \Downarrow & \uparrow & \Downarrow \\ ab \in (x) & & x \mid ab \Rightarrow x \mid a \vee x \mid b \\ \Rightarrow a \in (x) \vee b \in (x) & & \end{array}$

$\Rightarrow (x)$ è max tra gli ideali principali di A

Perché A è PID $\Rightarrow (x)$ è un ideale massimale $\square$

MCD nei PID

A PID $x, y \in A \dots$ $(x, y) = (d)$
d è mcd tra a e b $\nwarrow$ ideale
 $\uparrow$ è principale

$$x \in (d) \wedge y \in (d) \Rightarrow \underline{d|x \text{ e } d|y}$$

$$\underline{\text{Se } c|x \text{ e } c|y \Rightarrow x \in (c), y \in (c) \Rightarrow}$$

$$\Rightarrow (d) = (x, y) \subseteq (c) \Rightarrow d \in (c) \Rightarrow \underline{c|d}$$

Domini a fattorizzazione unica (UFD)

Def: A dominio si dice a fattorizzazione unica (UFD)

se $\forall x \in A \quad x \notin A^* \text{ si può scrivere in modo}$

"unico" come prodotto di irriducibili

"unico" = a meno dell'ordine dei fattori e dei
molti per gli invertibili

Esempi $\mathbb{Z}, K[x]$

Proposizione 5: $A \text{ UFD} \Rightarrow \forall a, b \in A$ non entrambi nulli
 $\exists \text{ MCD}(a, b)$.

$$\text{Dim: } \text{MCD}(a, b) = d$$

Definisco $d = \prod$ fattori irriducibili comuni ad a e b
con il minimo esp con cui compaiono

Per verifica delle prove che d è un mcd.

Oss! • A ED : Con l'algoritmo di Euclideo determino

$d = (a, b)$ e anche $x_0, y_0 \in A$ t.c.h

$$d = ax_0 + by_0$$

• A PID : $(a, b) = (d) \Rightarrow d = \text{mcd}(a, b)$

(non ho un algoritmo "facile" per determinarlo)

so però che $\exists x_0, y_0 \in A$ t.c.h

$$d = ax_0 + by_0 \quad (d \in (a, b))$$

Come li Trovo?)

• A UFD $\Rightarrow \forall a, b \dots \exists d = \text{mcd}(a, b)$

NON È DETTO CHE $(d) = (a, b)$ e quindi

neppure che $\exists x_0, y_0 \quad d = ax_0 + by_0$

(Siccome $(a, b) \subset (d)$ non è detto che
valga $\supset$ che vale solo se
 $d = ax_0 + by_0$)

$$\mathbb{Z}[x] \quad (2, x) = I \quad \text{mcd}(2, x) = 1$$

$$\text{ma } 1 \notin (2, x) \quad x=0$$

$$1 = 2a(x) + x b(x) \\ 1 = 2a(0) + 0 \Rightarrow 2 \mid 1 \text{ imp.}$$

Teorema : (Caratterizzazione degli UFD)

Adommo. Sono fatti equivalenti:

(1) A è UFD

(2) Valgono le due condizioni seguenti:

(i) Ogni residuale è primo

(ii) Ogni catena ascendente di divisibilità è stazionaria

$$\{a_i\} \subset A \quad a_{i+1} | a_i \quad \forall i \geq 0 \quad (\dots | a_3 | a_2 | a_1)$$
$$\exists n_0 \text{ tale che } a_i \sim a_{n_0} \quad \forall i \geq n_0$$

Oss: (i) $\Leftrightarrow$ unicità della fattorizzazione

(ii) $\Leftrightarrow$ esistenza della fattorizzazione.

(ii) è equivalente a

"Ogni catena ascendente di ideali principali è stazionaria"

$$\{(a_i)\}_{i \geq 0} \text{ ideali di } A \quad (a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

$$\exists n_0 \text{ tale che } (a_i) = (a_{n_0}) \quad \forall i \geq n_0$$

Corollario: $A \text{ PID} \Rightarrow A \text{ UFD}$

Dim del Corollario: Mostriamo che per un PID valgono (i) e (ii)

(i) $x \in A$ residuale $\Rightarrow (x)$ è max ~~tra gli ideali primi~~ in A

$\Rightarrow$ (2c) e^- primo $\Rightarrow x$ e primo.

(iv) $(a_1) \subseteq (a_2) \subseteq \dots$ catena ascendente di ideali (principali)

$I = \bigcup_{i=1}^n (a_i)$ è un ideale di A e quindi è primo

$$I = (a) \quad a \in (a_{n_0}) \quad I = (a) \supseteq (a_{n_0})$$
$$\Rightarrow I = (a) = (a_{n_0}) \quad (a_i) \subset (a_{n_0}) \quad \forall i$$
$$\Rightarrow (a_i) = (a_{n_0}) \quad \forall i \geq n_0 \Rightarrow \{a_i\} \text{ è stazionaria}$$

Esempi: ① $K[\{x^{\frac{1}{n}}\}_{n \geq 1}]$ non è UFD non vale (ii)

$\Rightarrow$ ~~F~~ bei falsch oder x

② $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{-5}) \subset \mathbb{C}$

NON È UFD perché non vale C_1)

In fatti, dato che 2 è irriducibile ma non primo in $\mathbb{Z}[\sqrt{-5}]$

$$2 = (a + \sqrt{-5}b)(c + \sqrt{-5}d)$$

$$4 \stackrel{||}{=} (a^2 + 5b^2)(c^2 + 5d^2) \quad \begin{matrix} a = \pm 2 & b = 0 \\ c = \pm 1 & d = 0 \end{matrix} \quad \textcircled{2}$$

$\Rightarrow 2$ è vera anche.

2 non è primo perché $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

$$\text{ma } 2 \nmid (1+\sqrt{-5}) \wedge 2 \nmid 1-\sqrt{-5}$$

$$\alpha = \frac{1 \pm \sqrt{-5}}{2} = \frac{1}{2} \pm \frac{\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$$

$$\text{In questo anello } 6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

sono due fatt. distinte di 6 (ovvero vedere che

$2, 3, 1 \pm \sqrt{-5}$ sono irriducibili)

Oss $\mathbb{Z}[\sqrt{-5}]$ non essendo UFD non è neppure PID

ad es. l'ideale $(2, 1+\sqrt{-5})$ non è principale

Se fosse principale sarebbe generato da

$$a + b\sqrt{-5} = 2\alpha + (1+\sqrt{-5})\beta \dots$$

Si fa prima a vedere che $1+\sqrt{-5}$ è irrid.

Teorema $A \text{ UFD} \Rightarrow A[x] \text{ UFD}$

Corollario $A \text{ UFD} \Rightarrow A[x_1, \dots, x_n] \text{ è UFD.}$

Schema di dim. del Teorema:

① $A[x]$ dominio

② Ogni irrid. di $A[x]$ è primo

③ Ogni catena crescente di divisibilità è staz.

$$\Rightarrow A[x] \text{ UFD,}$$

Dim:

$$\textcircled{1} \quad f, g \in A[x] \setminus \{0\} \Rightarrow \deg fg = \deg f + \deg g$$

$$f(x) = \sum_{i=0}^n a_i x^i \quad a_n \neq 0 \quad \deg f = n$$

$$g(x) = \sum_{m=0}^m b_m x^m \quad b_m \neq 0 \quad \deg g = m$$

$$fg(x) = a_n b_m x^{n+m} + \dots \neq 0 \quad \deg fg = n+m$$

$$A \text{ dominio} \Rightarrow A[x] \text{ dominio} \Rightarrow (A[x])^\times = A^\times$$

$$\left(f \in (A[x])^\times \quad \exists g \in A[x] \text{ t.c.} \quad fg = 1 \right)$$

$$\deg fg = 0 = \deg f + \deg g \Rightarrow \deg f = \deg g = 0$$

$$f, g \in A \quad f(x) = a \quad g(x) = b \quad ab = 1 \Rightarrow f \in A^\times$$

Dim (continuazione)

② Ogni irriducibile di $A[x]$ è primo.

Per prima cosa caratterizziamo gli elem. primi di $A[x]$.

Questo si può fare via Lemma di Gauss.

Def: • A : UFD $f \in A[x]$ $f(x) = \sum_{i=0}^n a_i x^i$

Si dice CONTENUTO di f $c(f) = \text{mcd} \{a_0, \dots, a_n\}$

$c(f)$ è definito a meno di associate.

• f si dice PRIMITIVO se $c(f) \sim 1$

Chiamare $f(x) = c(f) f'(x)$ $f'(x) \in A[x]$ $c(f') = 1$

$$c(f) = d \quad f'(x) = \sum_{i=0}^n \frac{a_i}{d} x^i \quad \frac{a_i}{d} \in A$$

$$\text{mcd} \left(\frac{a_0}{d}, \dots, \frac{a_n}{d} \right) = 1$$

Lemma di Gauss.

$$f, g \in A[x] \Rightarrow c(fg) = c(f)c(g)$$

Dim: CASO $c(f) = c(g) = 1$: f e g sono primitivi

e deve vedere che fg è primitivo ($c(fg) = 1$)

Se non fosse primitivo $c(fg)$ non sarebbe 1.

$\Rightarrow \exists f$ primo di A t.c.h. $p \nmid c(fg)$

$$A[x] \xrightarrow{\pi} \frac{A}{(p)}[x]$$

$$f(x) \rightarrow \overline{f}(x) \neq 0 \quad p \nmid c(f) = 1$$

$$g(x) \rightarrow \overline{g}(x) \neq 0 \quad p \nmid c(g) = 1$$

$$fg \rightarrow \overline{fg} = 0 \quad p \mid c(fg)$$

Ma questo è assurdo perché $\frac{A}{(p)}$ è un dominio

e poiché $\frac{A}{(p)}[x]$ è un dominio. $\Rightarrow c(fg) = 1$

CASO GENERALE: $f = c(f) f'$ f' primitivo

$g = c(g) g'$ g' primitivo

$\overbrace{fg}^h = c(f) c(g) \underbrace{f'g'}_{\text{è primitivo perché prodotto di polinomi primitivi}}$

$$\underbrace{c(fg)}_{h} \underbrace{(fg)'}_{h'}$$

$\uparrow$ è primitivo

$\Rightarrow$ uguagliando i contenuti dei due membri

$$c(fg) \cancel{c(fg')} = c(f) c(g) \cancel{c(f'g')}$$

$$c(fg) = c(f) c(g)$$

□

Corollario 1: $f, g \in A[x]$, $c(f) = 1$ $f \mid g$ in $K[x]$

(K = campo dei quozienti di A) $\Rightarrow f \mid g$ in $A[x]$.

Dim: $f \mid g$ in $K[x] \Rightarrow g = f h$ $h \in K[x]$

$\Rightarrow \exists d \in A$ t.c.h. $h_1 = d h(x) \in A[x]$

$$d g = f h_1 \quad \text{in } A[x]$$

$$d c(g) = c(f h_1) = \underset{\uparrow \text{LC}}{c(f)} c(h_1) = c(h_1)$$

$$\Rightarrow d \mid c(h_1) \Rightarrow \frac{h_1(x)}{d} = h(x) \in A[x]. \quad \square$$

Corollario 2: $f \in A[x]$, $f = g h$ in $K[x]$ $\deg g \geq 1$
 $\deg f \geq 1$

$\Rightarrow \exists d \in K^\times$ t.c.h. $g_1 = d g \in A[x]$
 $h_1 = d h \in A[x]$

$$f = g_1 h_1$$

(Slogan: se f è riducibile in $K[x]$ allora è riducibile anche in $A[x]$ con polinomi dello stesso grado)

$$\text{Es: } (x^2 - 2) = \left(\frac{100x + 100}{7} \right) \left(\frac{7}{100}x - \frac{7}{100} \right) \\ = (x+1)(x-1)$$

Dim: $f = g h$ in $K[x]$ $\exists d \in A$ t.c.h. $g_1 = d g \in A[x]$

$$f = (d g) (d^{-1} h) = g_1 (d^{-1} h) = c(g_1) g_1' (d^{-1} h)$$

$$g_1' \in A[x] \text{ ed } e' \text{ primitivo} \quad f = g_1' \underbrace{\left(\frac{c(g_1)}{d} h \right)}_{K[x]}$$

$$g_1' \mid f \text{ in } K[x]$$

$$\text{Per il Corollario 1} \Rightarrow g_1' \mid f \text{ in } A[x]$$

$$h_1 = \underbrace{\left(\frac{c(g_1)}{d} \right)}_{\text{"} d^{-1} \text{"}} h$$

↑ e di g_1 dall'enunciato

□

TEOREMA (Caratterizzazione degli irriducibili su $A[x]$)

A UFD. Gli elementi irriducibili di $A[x]$ sono tutti e soli quelli che soddisfanno una tra:

1) $f \in A$ irriducibili in A

2) f $\deg f \geq 1$ $c(f)=1$ f irriducibile in $K[x]$.

Dim:

• f costante $f = gh \Rightarrow \deg g + \deg h = 0 \Rightarrow g, h \in A$

f è irriducibile in $A[x] \Leftrightarrow f$ è irriducibile in A

$(A[x]^* = A^*)$

• $\deg f \geq 1$. Supponiamo f irriducibile in $A[x]$

$\Rightarrow f = c(f) f' \Rightarrow c(f)$ invertibile in $A[x]$
 $\Rightarrow c(f) \in A[x]^* = A^*$

Suo $f = gh$ in $K[x]$ per il Corollario 2

$f = g_1 h_1 \quad \deg g_1 = \deg g \quad \deg h_1 = \deg h$

Perché f è unit in $A \Rightarrow g_1$ o h_1 sono invertibili

$$\Rightarrow \deg g_1 = 0 \quad \vee \quad \deg h_1 = 0 \Rightarrow \deg g = 0 \quad \vee \quad \deg h = 0$$

$$\Rightarrow g \in K[x]^* \quad \vee \quad h \in K[x]^* \Rightarrow f \text{ è unit in } K[x].$$

Viceversa: Sia f primitivo e riducibile in $K[x]$,

$$\text{Sia } f = gh \text{ in } A[x] \text{ (e anche in } K[x])$$

Perché f è unit in $K[x]$ g o h sono invertibili

in $K[x]$ e quindi costanti, así es $g \in A$

$$1 = c(f) = c(gh) = c(g)c(h) = g c(h)$$

$$\Rightarrow g \in A^* (= A[x]^*) \Rightarrow f \text{ è riducibile in } A[x]$$

□

Proposizione: A UFD. In $A[x]$ ogni riducibile è primo

Dim: $f \in A[x]$ riducibile. Per dimostrare che è primo

devo vedere che $g, h \in A[x]$ e

$$f \mid gh \text{ in } A[x] \Rightarrow f \mid g \quad \vee \quad f \mid h \text{ in } A[x].$$

• $f \in A$ riducibile $\Rightarrow f$ è primo in A perché A è UFD

$$f \mid gh \Rightarrow f = c(f) \mid c(g)c(h)$$

$$\Rightarrow f \mid c(g) \quad \vee \quad f \mid c(h)$$

$$\Rightarrow f \mid g \quad \vee \quad f \mid h = c(h)h'$$

- f primitivo e irriducibile in $K[x]$ (ovvero $\deg f \geq 1$)

$K[x]$ è euclideo $\Rightarrow f$ è primo in $K[x]$

$$f \mid gh \text{ in } A[x] \Rightarrow \begin{cases} f \mid g & \text{in } K[x] \\ f \mid h & \text{in } K[x] \end{cases}$$

ma poiché f è primitivo per il Corollario 1

$$\Rightarrow f \mid g \vee f \mid h \text{ in } A[x]. \quad \square$$

③ Sia $\{f_n\}$ una succ di el di $A[x]$ tale che

$$\dots \quad f_3 \mid f_2 \mid f_1$$

$$f_{i+1} \mid f_i \quad \forall i \geq 1$$

Devo mostrare che $\exists n_0$ t.c.h. $f_n \sim f_{n_0} \quad \forall n \geq n_0$

Osservo che dal L.G. mi dà

$$f \mid g \Rightarrow c(f) \mid c(g) \quad f' \mid g'$$

$$(g = f h \text{ in } A[x] \quad c(g) = c(fh) = c(f)c(h)$$

$$\cancel{c(g)} g' = \cancel{c(f)c(h)} f' h' \Rightarrow f' \mid g').$$

Alle succ $\{f_i\}$ possiamo associare le succ

$$\{c(f_i)\} \quad \text{e} \quad \{f'_i\}$$

$$\Rightarrow c(f_{i+1}) \mid c(f_i) \quad \forall i \quad f'_{i+1} \mid f'_i \quad \forall i$$

La succ $\{c(f_n)\}$ è stazionaria perché è

una catena discendente di divisibilità nell'UFD A .
 $\exists m_0 \forall n \geq m_0 \quad c(f_n) \sim c(f_{m_0}) \quad \forall i \geq m_0$

Consideriamo $\{f'_n\}$ e associamo a partire
da succ $\{\deg f'_n\}$.

$$f'_{n+1} \mid f'_n \Rightarrow \deg f'_{n+1} \leq \deg f'_n$$

$\Rightarrow \{\deg f'_n\}$ è una succ decrescente su

numeri naturali $\Rightarrow$ si stabilizza $\Rightarrow \exists d_0 \forall n$

$$\deg f'_i = \deg f'_{d_0} \quad \forall i \geq d_0$$

$\Rightarrow \forall i \geq d_0 \quad f'_i$ e f'_{d_0} hanno lo stesso grado

$$f'_i \mid f'_{d_0} \Rightarrow f'_i \text{ e } f'_{d_0} \text{ differiscono}$$

per una costante ma essendo entrambi

primitivi la costante deve essere un'unità $\Rightarrow$

$$f'_i \sim f'_{d_0} \quad \forall i \geq d_0$$

$$n_0 = \max\{m_0, d_0\}$$

$$c(f_n) \sim c(f_{n_0}) \quad \forall i \geq n_0$$

$$f'_i \sim f'_{n_0} \quad \forall i \geq n_0$$

$$f_n = c(f_n) f'_n \sim c(f_{n_0}) f'_{n_0} = f_{n_0} \quad \forall i \geq n_0$$

□

Abbiamo visto che $\mathbb{Z}[x]$ non è PID

$I = (2, x)$ non è principale

Se A è ED $\Rightarrow A[x]$ è ED? anche qui

no perché $\mathbb{Z}[x]$ è anche euclideo

K campo $\Rightarrow K[x]$ EUCLIDEO $\rightarrow K[x, y]$?

$K[x, y]$ è UFD perché $K[x]$ è UFD

$\downarrow$ non è PID

ESERCIZIO.

Ad esempio $I = (x, y)$ non è principale.

$(I = (x, y) = (a(x, y)) \quad y, x \in (a(x, y))$

... $a \in K$ ma I non contiene costanti)

Criterio di irriducibilità di Eisenstein

A UFD $f(x) \in A[x]$ primitivo $f(x) = \sum_{i=0}^h a_i x^i$

$p \in A$ primo tale che 1) $p \nmid a_n$

2) $p \mid a_i \quad \forall i = 0, \dots, h-1$

3) $p^2 \nmid a_0$

134

$\Rightarrow f$ è irriducibile in $A[x]$ (e anche in $K[x]$)

Dim: Isolentice a puelle fatte per $\mathbb{Z}$

Terme pitagoriche

$$x^2 + y^2 = z^2 \quad x, y, z \in \mathbb{Z} \quad (x, y, z) = 1$$

(*) $(x + iy)(x - iy) = z^2 \quad \text{in } \mathbb{Z}[i]$

• $(x, y, z) = 1 \Rightarrow (x, y) = (x, z) = (y, z) = 1$

• $x \not\equiv y \pmod{2} : \quad x^2 + y^2 \equiv z^2 \pmod{4} \quad z^2 \equiv \begin{matrix} 1 \\ 0 \end{matrix}$

$\begin{matrix} \wedge & \wedge \\ 1 & 0 & 1 & 0 \end{matrix} \leftarrow$ non sono entrambi pari $(x, y) = 1$
ma neppure entrambi dispari
 $z^2 \equiv 2 \pmod{4}$

• $I = (x + iy, x - iy) = (1) \quad x + iy \text{ e } x - iy \text{ sono coprimi}$

$$2x = (x + iy) + (x - iy) \in I$$

$$2y \in I$$

$$x^2 + y^2 \in I$$

$2x$ e $2y$ sono pari

$$x^2 + y^2 \text{ è dispari} \Rightarrow 1 \in (2x, 2y, x^2 + y^2)$$

in $\mathbb{Z}$

In fatti altrimenti $\exists p$ T che $p \mid 2x$ $p \mid 2y$

$\Rightarrow p=2$ e $2=p \mid x^2+y^2$ che però è dispari

$$\Rightarrow I = (1)$$

$x-iy$ e $x+iy$ sono coprimi e quindi
entrambi quadratici ~~(*)~~ a meno di un'unità

$$\mathbb{Z}[i]^* \quad u \in \mathbb{Z}[i] \quad \exists v \in \mathbb{Z}[i] \quad uv=1$$

$$\Rightarrow v = \bar{u} \quad u\bar{u} = 1 \quad u = \varepsilon + i\delta \in \mathbb{Z}[i]$$

$$u\bar{u} = \varepsilon^2 + \delta^2 = 1 \quad \begin{cases} \varepsilon = \pm 1 \\ \delta = 0 \end{cases} \quad \begin{cases} \varepsilon = 0 \\ \delta = \pm 1 \end{cases}$$

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$$

$$x+iy = u d^2$$

$$(x-iy = \bar{u} \bar{d}^2)$$

$$u = \pm 1, \pm i \\ d \in \mathbb{Z}[i]$$

$$d = a+ib$$

$$x+iy = u(a^2-b^2-2iab)$$

$$u = \pm 1$$

$$x = \pm (a^2-b^2)$$

$$y = \mp 2ab$$

$$z = \pm (a^2+b^2)$$

$$u = \pm i$$

$$y = \pm (a^2-b^2)$$

$$x = \mp 2ab$$

$$z = \pm (a^2+b^2)$$

$$x^n + y^n = z^n \quad \text{FLT} \quad n \geq 3$$

$$n=p$$

$$p \nmid xyz \quad \text{CASO 1}$$

$$p \mid \text{uno tra } x, y \text{ e } z \quad \text{CASO 2}$$

$$\text{CASO 1 : } x^p + y^p = z^p$$

$$(x+y)(x+\zeta_p y) \dots (x+\zeta_p^{p-1} y) = z^p \quad \mathbb{Z}[\zeta_p]$$

Posso dimostrare che i fattori sono 2 a 2 coprimi

$\Rightarrow$ Sono tutti p -esime p -esime.

Non funziona facile $\mathbb{Z}[\zeta_p]$ in generale non è

UFD

$$p=23$$

TEORIA DEI CAMPI

$K \subset L$ campi. $\alpha \in L$ si dice algebrico su K se

$\exists f(x) \in K[x] \setminus \{0\}$ tale che $f(\alpha) = 0$

α si dice TRASCENDENTE su K se non è alg su K

cioè α $f(x) \in K[x]$ e $f(\alpha) = 0 \Rightarrow f(x) = 0$

$\alpha \in L$

$$\varphi_\alpha: K[x] \longrightarrow K[\alpha] \subset L$$

$$f(x) \longmapsto f(\alpha)$$

α è alg $\Leftrightarrow \ker \varphi_\alpha \neq \{0\}$

$$K[x] \xrightarrow{\varphi_\alpha} K[\alpha] \subset L$$

$$\downarrow \pi \quad \nearrow \bar{\varphi}_\alpha$$

$$K[x] / \ker \varphi_\alpha$$

$$K[\alpha] \cong \frac{K[x]}{\ker \varphi_\alpha}$$

è un dominio
perché è sottodomini
di un campo

$K[\alpha]$ dominio

$\Rightarrow \ker \varphi_\alpha \subseteq K[x]$ ideale primo

$K[x]$ PID e $\ker \varphi_\alpha \neq \{0\}$ perché α è algebrico

$\Rightarrow \ker \varphi_\alpha$ è max $\Rightarrow$ ¹³⁸ $K[\alpha]$ CAMPO $K[\alpha] = K(\alpha)$

$\ker \varphi_d = (\mu_d(x)) \leftarrow \text{E' MAX} \Rightarrow \mu_d(x) \text{ è irriducibile}$
 $\uparrow$
 l'unico generatore minimo

(i generatori di un ideale di $K[x]$ sono gli elementi di grado minimo - $K[x] \in D$ - e punti d'inflessione per molti per uno $\text{cost} \neq 0$)

ESTENSIONI FINITE: L/K ($K \subseteq L$) si dice GRADO di L/K

$$[L:K] = \dim_K L$$

L/K si dice di dim finita se $[L:K] < +\infty$

Prop 1: L/K d.g. L

$$[K(\alpha):K] = \begin{cases} +\infty & \alpha \text{ è trascendente su } K \\ \deg \mu_\alpha & \alpha \text{ è alg} \end{cases}$$

Dim: α è trano $(\Rightarrow) \varphi_d$ è invertibile $(\Rightarrow) K[\alpha] \cong K[x]$

$$K(\alpha) \cong K(x)$$

α è alg $K(\alpha) = K[\alpha] \cong \frac{K[x]}{(\mu_\alpha)}$ $n = \deg \mu$

$$1, \alpha, \dots, \alpha^{n-1} \leftarrow 1, x, \dots, x^{n-1}$$

$\uparrow$
 K -base di $K(\alpha)$

Prop 2: PROPRIETA' DELLE TORRI'

$K \subset L \subset F$ est di campi

F/K è finita $(\Leftrightarrow) F/L$ e L/K sono finite

Inoltre $[F:K] = [F:L][L:K]$

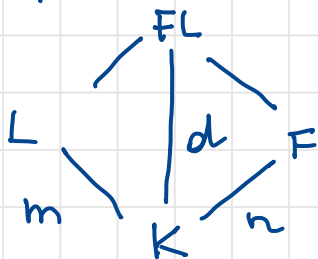
Dim $\Rightarrow$ ovvio

$\Leftarrow$ $\{v_1, \dots, v_n\}$ K -base di L

$\{w_1, \dots, w_m\}$ L -base di F

si verifica che $\{w_i v_j\}_{\substack{i=1, \dots, m \\ j=1, \dots, n}}$ K -base di F

Prop 3 (PROPRIETÀ DEL COMPOSTO)



$$[L:K] = m \quad [F:K] = n$$

$$\Rightarrow [FL:K] = dk + \dots$$

$$[m, n] \mid d$$

Def: L/K si dice ALGEBRICA se $\forall d \in L$ d è alg su K

Prop 4: L/K è finita $\Rightarrow L/K$ è algebrica

Dim: $d \in L$

$$\underbrace{K \subseteq K(d) \subseteq L}_{\text{finita}}$$

$\downarrow$
finita $\Rightarrow d$ è alg su K

$\square$

Prop 5 $L/K \quad A = \{d \in L \mid d \text{ alg su } K\}$

$\Rightarrow A$ è un campo (A/K è alg)

Dim: $\forall \alpha, \beta \in A \quad \alpha \pm \beta, \alpha\beta, \frac{1}{\alpha} \in A$

$$\alpha \in A \Rightarrow [K(\alpha) : K] < +\infty$$

$$\beta \in A \Rightarrow [K(\beta) : K] < +\infty$$

finita (x Torri)

$$K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta)$$

↓
finita

↑
finita

β alg su $K \Rightarrow \beta$ alg su $K(\alpha)$

P4
 $\Rightarrow K(\alpha, \beta) / K$ è algebrica $\Rightarrow \alpha \pm \beta, \alpha\beta, \frac{1}{\alpha}$ sono alg su K

□

Il viceversa delle prop 4 è falso

Esempio: Estensione algebrica non finita

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \quad \overline{\mathbb{Q}} = \{d \in \mathbb{C} \mid d \text{ è alg su } \mathbb{Q}\}$$

Per la Prop 5 $\Rightarrow \overline{\mathbb{Q}} / \mathbb{Q}$ è algebrica

Vediamo che $[\overline{\mathbb{Q}} : \mathbb{Q}] = +\infty$ - Infatti:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2}) \subset \overline{\mathbb{Q}} \quad \forall n \geq 2$$

↓
ha grado n

$$\mu_{\sqrt[n]{2}}(x) = x^n - 2$$

(si annulla in $\sqrt[n]{2}$, ed è verificato per Eisenstein, monico)

$$\Rightarrow \text{Per Torri} \quad [\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}} : \mathbb{Q}(\sqrt[n]{2})] [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$$

$$\geq n$$

$$\forall n \geq 2$$

Proposizione 6 L/K finitamente generata da el alg.

$\Rightarrow L/K$ è FINITA. equisoli suoi alg.

Dim: $L = K(\alpha_1, \dots, \alpha_n)$ α_i sono algebrici su K

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1)(\alpha_2) \dots (\alpha_n) \quad (c1)$$

$$= \{ p(\alpha_1, \dots, \alpha_n) \mid p(\alpha_1, \dots, \alpha_n) \in K[x_1, \dots, x_n] \} \quad (c2)$$

$$= \bigcap_{\substack{M \subset L \\ K, \alpha_i \in M}} M \quad (c3)$$

Prov in generale: $S \subset L \subset L$ sottocampi
 $\uparrow$
 sottoinsieme

$$K(S) = \bigcap_{\substack{M \subset L \\ K \subset M}} M$$

Per dimostrare che $K(\alpha_1, \dots, \alpha_n)$ è finita uso l'induzione
 e la p. delle Torri.

$n=1$ $K(\alpha)$ è finita perché α è alg. (PT)

$n-1 \Rightarrow n$ $K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$

$$K \subset K(\alpha_1, \dots, \alpha_{n-1}) \subset K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = L$$

$\uparrow$ finito x p ind $\uparrow$ finita perché semplice + α_n alg.

finita x Torri

□

Oss: Della PG vale anche il viceverso che è ovvio

$$[L : K] = n \quad v_1, \dots, v_n \text{ } K\text{-base} \Rightarrow$$

$$L = \langle v_1, \dots, v_n \rangle_K = K(v_1, \dots, v_n)$$

Proposizione 7 TORRI e COMPOSTO

1) $K \subset L \subset F$. F/K è alg $\stackrel{\text{ovvio}}{\Rightarrow} F/L$ e L/K sono algebriche

2) L/K e M/K alg $\stackrel{\text{ovvio}}{\Leftrightarrow} LM/K$ alg,

Oss: $L, M \subset \Omega$ sottocampi di uno stesso campo Ω

$$LM = L(M) = M(L) = \text{Il più piccolo sotto-campo di } \Omega \text{ che contiene sia } M \text{ che } L.$$

composto in
 L e M

$$L = K(\alpha_1, \dots, \alpha_n) \quad M = K(\beta_1, \dots, \beta_m)$$

$$LM = K(\alpha_i, \dots, \beta_j, \dots)$$

Dim: (1) $\Leftarrow$ ovvio F/K è alg $\Rightarrow \forall d \in F$ è alg su K

• $d \in L \subset F$ è alg su K

• d è alg su $L \supset K$

$(\Rightarrow)$ $d \in F$ d è ¹⁴³ alg su L $f(x) \in L[x] \setminus \{0\}$

$$f(\alpha) = 0 \quad f(x) = \sum_{i=1}^n a_i x^i$$

$$L_0 = K(a_0, \dots, a_n)$$

è finite x Torri

$$f(x) \in L_0[x] \Rightarrow \alpha \text{ è alg su } L_0$$

$$K \subset L_0 \subset L_0(\alpha)$$

$\downarrow$
*è finite
 perché è f.g
 e alg perché $\forall a_i \in L$*

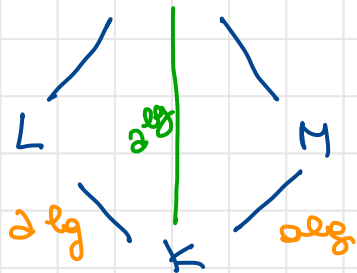
$\nwarrow$ *è finite perché
 α è alg su L_0*

a_i è alg su K

$$\Rightarrow [L_0(\alpha) : K] < \infty \Rightarrow L_0(\alpha)/K \text{ è algebrica}$$

$$\Rightarrow \alpha \text{ è alg su } K \quad \forall \alpha \in F \Rightarrow F/K \text{ è algebrica}$$

C2) ($\Leftarrow$) LM

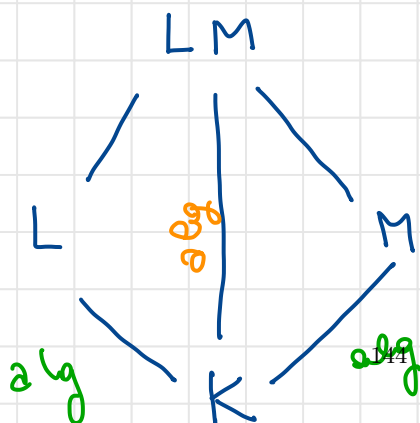


$\forall \alpha \in \Pi \subset LM$ è alg su K

$$\Rightarrow \Pi/K \text{ alg.}$$

Analogo per L

($\Rightarrow$)



$$\alpha \in LM = L(M)$$

$$\alpha = \sum_{i=1}^n \lambda_i m_i$$

$$\lambda_i \in L \quad m_i \in M$$

$\alpha \in F = K(\lambda_1, \dots, \lambda_n, m_1, \dots, m_n) \leftarrow$ E' finito per le props
 anche e' generata / K
 da un numero finito di
 el alg su K .

$\Rightarrow \alpha \in \text{alg. su } K.$

□

Chiusura alg di un campo.

Def 1 Un campo Ω si dice algebricamente chiuso se
 ogni polinomio $f(x) \in \Omega[x]$ non costante ha almeno
 una radice in Ω .

Esempi: Per il T fond dell'algebra $\mathbb{C}$ e' alg chiuso

Oss: Se Ω e' alg chiuso gli unici polinomi
 di $\Omega[x]$ sono quelli di grado 1.

Def: Ω/K Ω e' una CHIUSURA ALG di K se

- Ω e' algebricamente chiuso
- Ω/K e' algebrica

Es: $\mathbb{C}$ non e' la chiusura alg di $\mathbb{Q}$

$\mathbb{C}$ e' la chiusura alg di $\mathbb{R}$.

Teorema (Esistenza e unicità della chiusura alg)

Sia K campo, allora esiste sempre una sua chiusura algebrica. Inoltre due qualsiasi chiusure algebriche di K sono isomorfe.

Esempio

$$\overline{\mathbb{Q}} = \{d \in \mathbb{C} \mid d \text{ è alg su } \mathbb{Q}\} \text{ è una chiusura alg di } \mathbb{Q}.$$

$$\overline{\mathbb{Q}}/\mathbb{Q} \text{ è un est alg}$$

Devo dire che $\overline{\mathbb{Q}}$ è alg chiuso.

$f(x) \in \overline{\mathbb{Q}}[x]$ non costante $\Rightarrow f(x)$ ammette una radice α in $\mathbb{C}$ per cui $f(x) \in \mathbb{C}[x]$ e $\mathbb{C}$ è alg chiuso. Per mostrare che $d \in \overline{\mathbb{Q}}$ devo dire che d è alg su $\mathbb{Q}$.

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}(\alpha)$$

$\uparrow$
alg

$\uparrow$

alg perché semplice e d è alg su $\overline{\mathbb{Q}}$



è alg x Torri

146

$\Rightarrow d$ è alg su $\mathbb{Q}$ $d \in \mathbb{Q}$
 $\Rightarrow d \in \overline{\mathbb{Q}}$

Posso usare lo stesso argomento per costruire

$\bar{K}$ chiusura alg di K ogni volta che

$$p_n \quad \boxed{K \subset \mathcal{Q} = \text{alg chiuso}}$$

$$\bar{K} = \{ \alpha \in \mathcal{Q} \mid \alpha \text{ è alg su } K \} \Rightarrow \bar{K} = \text{chiusura alg di } K$$

Def $f \in K[x]$ alg $f \neq 1$ $\alpha_1, \dots, \alpha_n \in \bar{K} = \text{chiusura alg di } K$

radici di $f(x)$. Si dice CAMPO DI SPEZZAMENTO

di f su K il sottocampo di $\bar{K}$

$$K(\alpha_1, \dots, \alpha_n)$$

$$J = \{ f_i \mid i \in I \} \subset K[x]$$

$\forall i \in I \quad \{ \alpha_{ij} \}_{j=1, \dots, n_i}$ radici di f_i in $\bar{K}$

Il campo di spezz di f su K

$$K(\{ \alpha_{ij} \}_{j=1, \dots, n_i} \mid i \in I)$$

Esempi $x^3 - 2 \in \mathbb{Q}[x] \quad \sqrt[3]{2}, \sqrt[3]{2} \zeta_3, \sqrt[3]{2} \zeta_3^2$

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

ζ_n radice n-esima primitiva di 1

$$\langle \zeta_n \rangle = \{ \alpha \in \mathbb{C} \mid \alpha^n = 1 \} \quad \mathbb{Q}(\zeta_n) \text{ è il c.o.d. di } x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$$

Problema 1: $K \subset \overline{K}$ $\alpha \in \overline{K}$

In quanti modi posso immergere $K(\alpha)$ in $\overline{K}$

$$\varphi: K(\alpha) \longrightarrow \overline{K}$$

$$\varphi|_K = \text{id}$$

?

$$K(\alpha) \cong K[x] / (\mu_\alpha(x)) \quad K \hookrightarrow \overline{K}$$

la estendo

$$\tilde{\varphi}: K[x] \longrightarrow \overline{K}$$

$$\begin{array}{ccc} x & \longmapsto & \beta \\ p(x) & \longmapsto & p(\beta) \end{array}$$

è un omomorfismo
se e solo se β è radice di p .

a me interessa che $\tilde{\varphi}$ induca per passaggio al quoziente un omomorfismo su $K(\alpha) \cong \frac{K[x]}{(\mu_\alpha(x))}$

Questo succede $(\Leftrightarrow) (\mu_\alpha(x)) \subset \ker \tilde{\varphi} \Leftrightarrow \mu_\alpha(x) \in \ker \tilde{\varphi}$

$$\tilde{\varphi}(\mu_\alpha(x)) = \mu_\alpha(\beta) = 0 \Rightarrow \beta \text{ deve essere radice di } \mu_\alpha$$

$$\begin{array}{ccc} K[x] & \xrightarrow{\tilde{\varphi}} & \overline{K} \\ \downarrow & \nearrow q & \\ K(\alpha) \cong K[x] / (\mu_\alpha(x)) & & \end{array}$$

φ è omomorfismo per il
teo. di omomorfismi
 φ è iniettivo perché
 $K(\alpha)$ è campo e $\varphi \neq 0$
 $1 \mapsto 1$

Proposizione: K campo $\alpha \in \overline{K}$ $k = \# \text{ radici distinte di } \mu_\alpha(x) \text{ in } \overline{K}$

$$\Rightarrow \exists q_1, \dots, q_k : K(\alpha) \longrightarrow \overline{K}$$

$$q_{i|K} = \text{id}$$

Problema 2: Quante sono le radici di $\mu_\alpha(x)$ in $\overline{K}$?

$\# \text{ radici di } \mu_\alpha \text{ con molteplicità} = \deg \mu_\alpha(x) = n$.

$\rightarrow \mu_\alpha(x)$ può avere radici multiple

CRITERIO DELLA DERIVATA

$f \in K[x]$ ha radici multiple in $\overline{K} \Leftrightarrow (f, f') \neq 1$

Se f è irriducibile in K , f ha radici multiple



$$f' = 0$$

$$(f \in K[x] \Rightarrow f' \in K[x] \quad (f, f') \in K[x])$$

e se f è irriducibile in $K[x]$

$$(f, f') \leq 1 \quad f \Rightarrow f' = 0$$

Se in K i polinomi irriducibili non hanno derivata nulla

chiamo K campo PERFETTO

$\Rightarrow \# \text{ radici distinte di un polinomio}$

1)

$\deg$ del polinomio.

Oss: • Se $\text{char } K = 0 \Rightarrow K$ è un campo PERFETTO

$$f(x) = \sum_{i=0}^n a_i x^i \quad f'(x) = \sum_{i=1}^n i a_i x^{i-1}$$

$$n \geq 1 \Rightarrow f' \neq 0$$

• $\mathbb{F}_{p^n}$ è perfetto $\forall p \forall n$.

• $K = \mathbb{F}_p(t)$ $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$

$$f'(x) = p x^{p-1} = 0$$

Dico che $f(x)$ è irriducibile in $K[x]$

$$f(x) = \underbrace{\mathbb{F}_p[t]}_A[x] = A[x]$$

A UFD (è ED) per Gauss basta

verificare che $f(x)$ è irriducibile in $A[x]$

In $A[x]$ $f(x) = x^p - t$ è irriducibile

perché da Eisenstein applicato a $P = (t)$

$P = (t)$ è primo in A giacché $A/(t) \cong \mathbb{F}_p$

$d \in \overline{K}$ radice di $f(x)$

$$f(d) = d^p - t = 0 \Rightarrow t = d^p$$

$f(x) = x^p - d^p = (x - d)^p$ in $\overline{K}$
 f ha un'unica radice in $\overline{K}$.

Ci limiteremo (e assumiamo senza dubbio)

ai campi perfetti

$\Rightarrow$ un pol ^{o di $K[x]$} ~~o di~~ grado n ha esattamente n radici
distinte in $\overline{K}$

Proposizione: $\alpha \in \overline{K} \quad n = [K(\alpha) : K] -$

Per ogni $\varphi: K \hookrightarrow \overline{K}$ immersione

Esistono esattamente n estensioni a $K(\alpha)$, cioè

$$\varphi_1, \dots, \varphi_n: K(\alpha) \rightarrow \overline{K} \quad \text{t.c. } \varphi_i|_K = \varphi$$

Oss: Abbiamo già visto che punto è vero $\varphi = \text{id}$

$$K = \mathbb{Q}(\sqrt[3]{2}) \quad \varphi: K \hookrightarrow \overline{K}$$

$$\sqrt[3]{2} \mapsto \sqrt[3]{2} \zeta_3$$

Dim:

$$\varphi: K \hookrightarrow \overline{K}$$

$$\tilde{\varphi}: K[x] \rightarrow \overline{K} \quad \tilde{\varphi}|_K = \varphi$$

$$x \mapsto \beta$$

$$p(x) \mapsto (p\tilde{\varphi})(\beta)$$

Come devo scegliere β affinché $\ker \tilde{\varphi} \supseteq (p_2(x))$?

$$\tilde{\varphi}(p_2(x)) = 0$$

$$(p_2\tilde{\varphi})(\beta) = 0 \Rightarrow \beta \text{ deve essere radice di}$$

$\varphi|_{\mu_d} \Rightarrow$ le estensioni di φ a $K(\alpha)$
 sono tutte le radici distinte di $\varphi|_{\mu_d}$
 in $\overline{K}$

μ_d irriducibile $\Rightarrow \varphi|_{\mu_d}$ è irriducibile

$\deg \mu_d = \deg(\varphi|_{\mu_d})$ perché φ è unitario

Poiché K è perfetto

radici distinte $\varphi|_{\mu_d} = \deg \varphi|_{\mu_d} = \deg \mu_d$ $\square$

Corollario: E/K $[E:K]=n$

$\forall \varphi \in K \hookrightarrow \overline{K}$ immersione $\exists$ esattamente n immersioni

$\varphi_1, \dots, \varphi_n: E \rightarrow \overline{K}$ tale $\varphi_n|_K = \varphi$

Dim:

Per induzione su $n = [E:K]$

$n=1$ ovvio

$n>1$ $\alpha \in E \setminus K$ $K \subset K(\alpha) \subset E$
 m n

$m=n \Rightarrow E=K(\alpha)$ e vale la prop precedente

$1 < m < n \Rightarrow 0 < n$

φ si estende $\varphi_1, \dots, \varphi_m: K(\alpha) \rightarrow \overline{K}$ per la prop
 di primo

Ogni $\varphi_i: K(\alpha) \rightarrow \overline{K}$ si estende

$\varphi_{i1} \mapsto \varphi_{i\alpha} \quad E \rightarrow \overline{K}$ per i' invol.

$\Rightarrow \{ \varphi_{i\alpha} \}_{i=1, \dots, n} \quad E \rightarrow \overline{K}$

$$\varphi_{i\alpha}|_{K(\alpha)} = \varphi_i$$

$$\varphi_{i\alpha}|_K = \varphi_i|_K = \varphi$$

□

Esempio 1: $f(x) = x^3 - 2 \leftarrow \mu_{\sqrt[3]{2}} \text{ su } \mathbb{Q} \quad \alpha = \sqrt[3]{2}$

$$\varphi: \mathbb{Q}(\alpha) \longrightarrow \overline{\mathbb{Q}} \quad \varphi|_{\mathbb{Q}} = \text{id.}$$

$$\varphi(\alpha) = \begin{cases} \alpha \\ \alpha \zeta_3 \\ \alpha \zeta_3^2 \end{cases}$$

$$\alpha, \alpha \zeta_3, \alpha \zeta_3^2$$

radici di μ_2
= coniugati di α

$$\varphi(\mathbb{Q}(\alpha)) = \mathbb{Q}(\varphi(\alpha)) = \begin{cases} \mathbb{Q}(\alpha) \\ \mathbb{Q}(\alpha \zeta_3) \\ \mathbb{Q}(\alpha \zeta_3^2) \end{cases}$$

I coniugati di $\alpha \in \mathbb{K}$
sono le radici del
pol. min. di α su $\mathbb{K}$

Esempio 2 p primo $\mathbb{Q}(\zeta_p)$

Sappiamo $\mu_{\zeta_p}(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1$

È un pol.
lineare Trasforma
di Estensione

i coniugati di ζ_p sono $\sum_{i=1}^{p-1} \zeta_p^i$

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p) = p-1$$

Immersioni di $\mathbb{Q}(\zeta_p)/\mathbb{Q}$

$$\begin{aligned} \varphi_i: \mathbb{Q}(\zeta_p) &\longrightarrow \overline{\mathbb{Q}} \\ \zeta_p &\longmapsto \zeta_p^i \end{aligned}$$

$$\forall i \quad \varphi_i(\mathbb{Q}(\zeta_p)) = \mathbb{Q}(\varphi_i(\zeta_p)) = \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta_p)$$

$$\mu_{\zeta_p^i} = \mu_{\zeta_p} \Rightarrow \text{stesso grado}$$

Def F/K estensione algebrica, si dice NORMALE se

$$\forall \varphi : F \longrightarrow \overline{K} \quad \varphi|_K = \text{id} \quad \text{si ha}$$

$$\varphi(F) = F$$

Es: $\mathbb{Q}(\zeta_p)$ è normale su $\mathbb{Q}$

F: $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) / \mathbb{Q}$ è normale

$$\varphi : F \longrightarrow \overline{\mathbb{Q}} \quad \varphi|_{\mathbb{Q}} = \text{id}$$

$$\begin{aligned} \varphi(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) &= \mathbb{Q}(\varphi(\sqrt[3]{2}), \varphi(\zeta_3)) = \\ &= \mathbb{Q}(\sqrt[3]{2} \zeta_3^i, \zeta_3^j) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \end{aligned}$$

$$i=0,1,2 \quad , \quad j=1,2$$

↑
CONTROCCARCO

Proposizione:

Sia F/K algebrica (finita). Sono fatti equivalenti:

1) F/K è normale

2) Ogni polinomio IRRIDUCIBILE $f(x) \in K[x]$ che ha una radice in F ha tutte le sue radici in F

3) F è il c.o.s. su K di una famiglia di pol. di $K[x]$.

Dim: Per estensioni finite

1) $\Rightarrow$ 2)

$f(x) \in K[x]$ $\alpha_1, \dots, \alpha_n \in \overline{K}$ radici di f .

$$\alpha_1 \in F \Rightarrow K(\alpha_1) \subseteq F$$

$$\forall i = 1, \dots, n \text{ su } \varphi_i: K(\alpha_1) \longrightarrow K(\alpha_i) \subseteq \overline{K}$$

$$\alpha_1 \longmapsto \alpha_i$$

$$\varphi_i = \text{id}$$

$\forall i$ su $\tilde{\varphi}_i$ un'estensione di φ_i a $\overline{F}$ $\leftarrow$ È vero in gen
ma lo abbiamo
dimostrato fu
estensione
finite

$$\tilde{\varphi}_i: F \longrightarrow \overline{K}$$

$$\tilde{\varphi}_i|_{K(\alpha_1)} = \varphi_i$$

$$\tilde{\varphi}_i|_K = \text{id}$$

$$\tilde{\varphi}_i F = F \text{ perché } F/K \text{ è normale}$$

$$\Rightarrow \tilde{\varphi}_i(\alpha_1) = \varphi_i(\alpha_1) = \alpha_i \in F \quad \forall i = 1, \dots, n$$

$\Rightarrow$ tutte le radici di f sono in F .

2) $\Rightarrow$ 3) Contradico

$$F_0 = \text{comp su } K \left\{ \mu_\alpha \mid \alpha \in F, \mu_\alpha = \text{polinomio di } \alpha \text{ su } K \right\}$$

$F \subseteq F_0$. D'altra parte su

$$F_0 = K(\beta \mid \beta \text{ radice di } \mu_\alpha \in \mathcal{F})$$

β radice di μ_α e μ_α è separabile su K e ha una radice

$$(2) \quad \dim F \Rightarrow \beta \in F \Rightarrow F_0 \subseteq F.$$

(3) $\Rightarrow$ (1)

$$\varphi: F \longrightarrow \overline{K}$$

156

$\varphi|_K = \text{id}$. Devo mostrare $\varphi F = F$

$F = \text{c.d.s.p. } K \text{ di } \mathcal{F}$

$$\mathcal{F} = \{f_1, \dots, f_k\} \quad \{ \alpha_{ij} \}_{j=1}^{n_i} = \text{radici di } f_i$$

$$F = K(\{ \alpha_{ij} \} \mid i=1, \dots, k, j=1, \dots, n_i) \quad \left(f = \prod_{i=1}^k f_i \right)$$

Sappiamo che $\forall i, j \quad \varphi(\alpha_{ij}) = \alpha_{ij}$ per un auto j'
 $\uparrow$
 radice di $f_i \in K[x]$
 $\mu_{\alpha_{ij}} \mid f_i$

$$\Rightarrow \varphi F = \varphi K(\alpha_{ij} \mid i=1, \dots, j=1, \dots) = K(\varphi(\alpha_{ij}) \mid \dots) \subset F$$

$\Rightarrow K \subset \varphi F \subseteq F$ - Poiché F e φF hanno lo

stesso grado FINITO su $K \Rightarrow \varphi(F) = F \quad \square$

Esempio: • Ogni estensione di grado 2 è normale

$$F/K \quad [F:K] = 2 \quad \alpha \in F \setminus K \Rightarrow F = K(\alpha)$$

$$M_\alpha = \text{pol. min. di } \alpha / K \quad \mu_\alpha(x) = x^2 + bx + c \in K[x]$$

$$\alpha_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2}$$

$$\alpha = \frac{-b + \sqrt{\Delta}}{2} \quad F = K(\alpha) = K(\sqrt{\Delta})$$

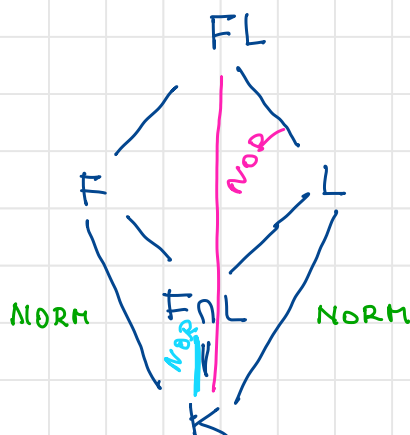
$$\alpha_1, \alpha_2 \in K(\sqrt{\Delta}) = F \leftarrow F \text{ è c.d.s.p. di } \mu_\alpha / K$$

• $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è normale - $x^3 - 2$ è irriducibile su $\mathbb{Q}$
 ha una radice in $\mathbb{Q}(\sqrt[3]{2})$ ma non tutte

PROPRIETA' DELLE ESTENSIONI NORMALI

COMPOSTO E INTERSEZIONE

$$F, L \subset \Omega$$



F/K e L/K normali $\Rightarrow FL/K$ e $F \cap L/K$ sono normali

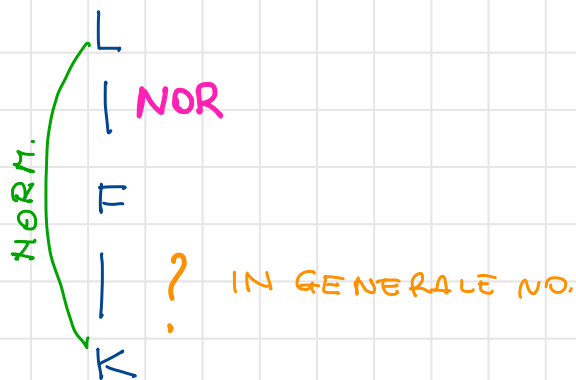
$$\forall \varphi: FL \rightarrow \overline{K} \quad \varphi|_K = id$$

$$\varphi(FL) = \varphi(F) \varphi(L) = FL \quad \checkmark$$

$$\varphi: F \cap L \rightarrow \overline{F} \quad \varphi|_K = id$$

$$\varphi(F \cap L) = \varphi(F) \cap \varphi(L) = F \cap L$$

TORRI



L/K normale $\Rightarrow L/F$ e normale

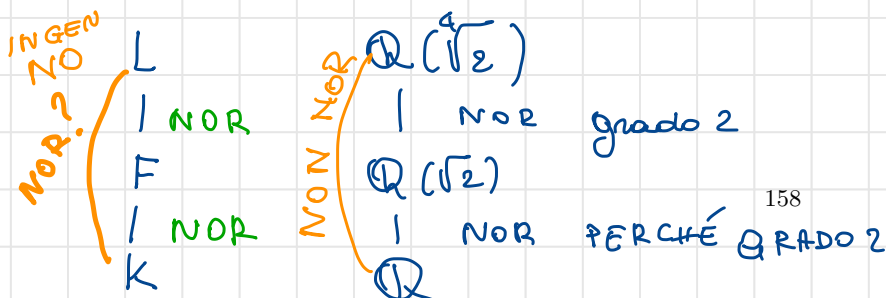
$$\forall \varphi: L \rightarrow \overline{K} \quad \varphi|_F = id \Rightarrow \varphi|_K = id$$

$$\varphi(L) = L$$

perché L è normale su K

$$K = \mathbb{Q} \quad F = \mathbb{Q}(\sqrt[3]{2}) \quad L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \quad L/K \text{ è normale}$$

ma F/K no



$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ non è normale perché contiene $\sqrt[4]{2}$ radice di $x^4 - 2 = 0$ ma non le altre radici.

Gruppo di Galois

Sia E/k un'estensione di Galois, cioè normale e

LO ASSUMIAMO SEMPRE
separabile ($\forall \alpha \in E \quad m_{\alpha/k}$ ha radici distinte in E)

FINITA $[E:k] = n$ - Perché E/k è normale

$$\{ \varphi: E \rightarrow \overline{k} \mid \varphi|_k = \text{id} \} = \text{Aut}_k E = \{ \varphi: E \rightarrow E \mid \varphi|_k = \text{id} \}$$

piccolo abuso di
notazione

Potremo

$$\text{Gal}(E/k) \doteq \text{Aut}_k(E) \leftarrow \begin{array}{l} \text{GRUPPO DI} \\ \text{GALOIS di } E/k \end{array}$$

Sappiamo che

$$|\text{Gal}(E/k)| = [E:k]$$

Proposizione:

$\text{Gal}(E/k)$ è un gruppo.

Dim: $\varphi, \psi \in \text{Gal}(E/k) \Rightarrow \varphi \circ \psi \in \text{Gal}(E/k)$

$\varphi \in \text{Gal}(E/k) \Rightarrow \varphi^{-1} \in \text{Gal}(E/k)$

□

Proposizione: $f \in k[x]$ irriducibile di grado n

F = c.d.s.p di f/k ,

si immerge in S_n

Allora $n \mid [F:k] \mid n!$ $\text{Gal}(F/k) \hookrightarrow S_n$

159

Dim:

$\alpha_1, \dots, \alpha_n$ radici di f in $\overline{k} \Rightarrow F = k(\alpha_1, \dots, \alpha_n)$

$$K \subseteq K(\alpha_1) \subseteq F \Rightarrow n \mid [F:K] = |\text{Gal}(F/K)|$$

$\downarrow$
 n

$$\Phi: \text{Gal}(F/K) \longrightarrow S\{a_1, \dots, a_n\}$$

$$\sigma \longmapsto \sigma|_{\{a_1, \dots, a_n\}}$$

Φ è ben definita perché $\forall \sigma \in \text{Gal}(F/K)$

σ permuta le radici di $f(x)$

Φ è omomorfismo di gruppo: $\Phi(\sigma \circ \tau) = (\sigma \circ \tau)|_{\{a_i\}} =$
 $= \sigma(\tau|_{\{a_i\}}) = \sigma|_{\{a_i\}} \circ \tau|_{\{a_i\}}$

Φ è iniettivo:

$$\ker \Phi = \{ \sigma \in \text{Gal}(F/K) \mid \sigma(a_i) = a_i \forall i \}$$

$$= \{id\}$$

$\text{Gal}(F/K)$ agisce fedelmente su $\{a_1, \dots, a_n\}$

$\downarrow$
(Φ è iniettivo)

L'azione di $\text{Gal}(F/K)$ su $\{a_1, \dots, a_n\}$ è TRANSITIVA
 perché ha un'unica orbita

$$\text{orb}(a_1) = \{ \sigma(a_1) \mid \sigma \in \text{Gal}(F/K) \} = \{a_1, \dots, a_n\}$$

$\downarrow$
*

n immersioni

$$\textcircled{*} \quad K \subseteq K(\alpha_1) \subseteq F \quad \forall i \exists \varphi_i: K(\alpha_1) \longrightarrow \overline{K(\alpha_i)} \subseteq \overline{F}$$

$\alpha_1 \longmapsto \alpha_i$

Ogni φ_i si estende ad F

Esempi

K campo $f \in K[x]$ unidivisa $F = \text{c.d.s.p. di } f/K$.

- $\deg f = 2$ $[F:K] = 2$ ($2=2!$) $\text{Gal}(F/K) \cong \mathbb{Z}/2\mathbb{Z}$
"cioè C_2 "

$$F = K(\sqrt{\Delta}) \quad a + b\sqrt{\Delta} \rightarrow a \pm b\sqrt{\Delta}$$

Quelloggi $f(x) = (x - \alpha_1)(x - \alpha_2)$ $\alpha_1 \rightarrow \alpha_1$
 $\alpha_1 \rightarrow \alpha_2$

- $\deg f = 3 \Rightarrow 3 \mid [F:K] \nmid 6$ $\text{Gal}(F/K) < S_3$
 $\Rightarrow \text{Gal}(F/K) \cong \begin{cases} A_3 \cong \mathbb{Z}/3\mathbb{Z} \\ S_3 \end{cases}$

Si presentano entrambi i casi.

$$f(x) = x^3 - 2 \quad K = \mathbb{Q} \quad F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \Rightarrow [F:\mathbb{Q}] = 6$$

$$\Rightarrow \text{Gal}(F/\mathbb{Q}) \cong S_3$$

$$\varphi \in \text{Gal}(F/\mathbb{Q}) \quad \varphi(\sqrt[3]{2}) = \sqrt[3]{2} \zeta_3^i \quad i = 0, 1, 2$$

$$\varphi(\zeta_3) = \zeta_3^j \quad j = 1, 2$$

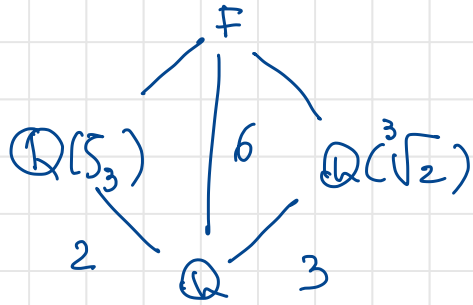
Neessanamente φ deve verificare le relazioni sopra

che danno AL PIÙ 6 possibili φ . Perché φ

grado è 6 tutte le 6 funzionano

Si intende sul F . ¹⁶¹ Funzionano tutte perché

$$[F:\mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] [\mathbb{Q}(\zeta_3):\mathbb{Q}]$$



$f(x) = x^3 + x^2 - 2x - 1$ è il pol. minimo di $\zeta_7 + \zeta_7^{-1}$ su $\mathbb{Q}$.

e $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ è normale $\Rightarrow \text{Gal}(F/\mathbb{Q}) \cong A_3$
 $\zeta = \zeta_7$

$$[\mathbb{Q}(\zeta):\mathbb{Q}] = \phi(7) = 6 \quad \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{ \sigma \mid \sigma(\zeta) = \zeta^i \text{ (i, 7)} \}$$

$\alpha = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta) \Rightarrow$ Tutte le radici di $M_{\zeta + \zeta^{-1}}$ $\in \mathbb{Q}(\zeta)$

Le radici di $M_{\zeta + \zeta^{-1}}$ sono $\{ \sigma(\alpha) \mid \sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$$

Le immersioni ψ mandano α in una qualsiasi radice di μ_α $\{ \psi(\alpha) \}$ $\leftarrow$ è l'insieme delle radici di μ_α

$$\Rightarrow \mu_\alpha(x) = \prod_{\psi} (x - \psi(\alpha))$$

D'altra parte ogni ψ si estende ad un

$$\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \quad \text{e} \quad \forall \sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

$\sigma(\alpha)$ sarà ancora una radice di μ_α

$$\text{radici di } \mu_\alpha = \{ \psi(\alpha) \}_{\psi: \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}} = \{ \sigma(\alpha) \}_{\sigma \in \text{Gal}}$$

Dim:

Per prima cosa vediamo che $\phi \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$

$$\begin{aligned}\phi: \mathbb{F}_{q^d} &\rightarrow \mathbb{F}_{q^d} \\ x &\mapsto x^q\end{aligned}$$

$q=p^r$ e siamo in
caso di P

- è un omo di anelli: giacché $\phi(\alpha+\beta) = (\alpha+\beta)^q = \alpha^q + \beta^q$
- è iniettivo e suriettivo

Inoltre $\forall \alpha \in \mathbb{F}_q \quad \phi(\alpha) = \alpha^q = \alpha \leftarrow$ vero per def di $\mathbb{F}_q$

$$\Rightarrow \phi \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q).$$

$\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ è un gruppo di ordine $d \Rightarrow \text{ord } \phi = k | d$

D'altra parte se $\phi^k = \text{id} \quad \forall \alpha \in \mathbb{F}_{q^d}$ si ha

$$\phi^k(\alpha) = \alpha^{q^k} = \alpha \quad \text{cioè il polinomio}$$

$f(X) = X^{q^k} - X$ ha come radici tutti i q^d elementi

di $\mathbb{F}_{q^d}$ e poiché $\mathbb{F}_{q^d}$ è un campo finito

simplex che $\deg f(X) = q^k \geq q^d \Rightarrow k \geq d$

da cui $k=d \Rightarrow \text{ord } \phi = d = |\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)|$

$$\Rightarrow \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \phi \rangle$$

□

Esempio: $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$

$$E \longrightarrow \overline{\mathbb{Q}}$$

$$\sqrt{2} \longmapsto \pm \sqrt{2}$$

$$\sqrt{3} \longmapsto \pm \sqrt{3}$$

$$\varphi_1: \begin{matrix} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{matrix}$$

$$\varphi_2: \begin{matrix} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{matrix}$$

$$\varphi_3: \begin{matrix} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{matrix}$$

$$\varphi_4: \begin{matrix} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{matrix}$$

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ $\mathbb{Q}$ -base di E

$$\varphi_i E = E \quad \forall i$$

$$\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

$$\varphi_i^2 = \text{id} \quad \forall i$$

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$\supset$ ovvio
 $\subset$...

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq E$$

4
4 =

$$\varphi_1(\sqrt{2} + \sqrt{3}) = \sqrt{2} + \sqrt{3}$$

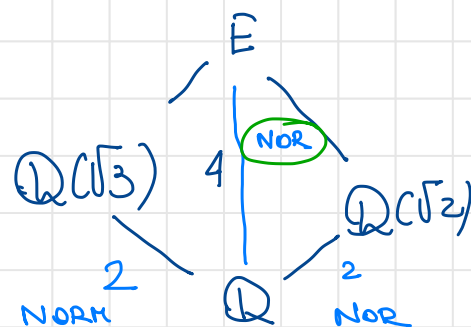
$$\varphi_2(\sqrt{2} + \sqrt{3}) = -\sqrt{2} + \sqrt{3}$$

$$\varphi_3(\sqrt{2} + \sqrt{3}) = \sqrt{2} - \sqrt{3}$$

$$\varphi_4(\sqrt{2} + \sqrt{3}) = -\sqrt{2} - \sqrt{3}$$

sono
distinti

$\gamma = \sqrt{2} + \sqrt{3}$ ha 4 immagini distinte mediante le
immersioni di E in $\overline{\mathbb{Q}}$ $\Rightarrow \gamma$ ha almeno
4 coniugati su $\mathbb{Q} \Rightarrow$ ha $\mathbb{Q}$ -grado 4 $\Rightarrow \mathbb{Q}(\gamma) = E$



Oss: $\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset E \quad \# \{ \varphi: \mathbb{Q}(\gamma) \rightarrow \overline{\mathbb{Q}} \}$
 $= \deg \mu_\gamma$

Ogni φ si estende ad E $\varphi|_E: E \rightarrow \overline{\mathbb{Q}}$

$\Rightarrow \{ \varphi_i(\gamma) \}$ è l'insieme dei coniugati di γ su $\mathbb{Q}$

TEOREMA DELL'ELEMENTO PRIMITIVO

Sia K campo e sia E/K finita (e separabile)

$\Rightarrow E/K$ è semplice cioè $\exists \gamma \in E$ t.c. $E = K(\gamma)$

Dim

K campo infinito: E/K finita $\Rightarrow E = K(\alpha_1, \dots, \alpha_n)$

Provo che E/K è semplice per induzione su n .

$n=2 \quad E = K(\alpha, \beta) \quad [E:K] = n$

$\varphi_1, \dots, \varphi_n: E \rightarrow \overline{K} \quad \varphi_i|_K = \text{id}$

α indeterminata $d + \alpha \beta$

$$F(x) = \prod_{1 \leq i < j} (\varphi_i(\alpha) + x \varphi_j(\beta) - \varphi_j(\alpha) - x \varphi_i(\beta)) \in \overline{K}[x]$$

$F(x) \neq 0, \quad \deg F(x) \leq \binom{n}{2}$

$\hookrightarrow$ se fosse $\varphi_n(\alpha) + x \varphi_n(\beta) = \varphi_0(\alpha) + x \varphi_0(\beta)$

$x(\varphi_n(\beta) - \varphi_0(\beta)) + \varphi_n(\alpha) - \varphi_0(\alpha) = 0 \quad \begin{matrix} \varphi_n(\alpha) = \varphi_0(\alpha) \\ \varphi_n(\beta) = \varphi_0(\beta) \end{matrix}$

$\Rightarrow \varphi_i \equiv \varphi_j$ perche $E = K(\alpha, \beta)$ e punto è assunto.

F ha al più $\deg F(x)$ radici in K e perche

K è un campo infinito $\Rightarrow \exists t \in K$ t.c.h. $F(t) \neq 0$

$$F(t) = \prod_{i < j} \left(\underbrace{\varphi_i(\alpha) + t\varphi_i(\beta)}_{\varphi_i(\alpha + t\beta)} - \underbrace{\varphi_j(\alpha) + t\varphi_j(\beta)}_{\varphi_j(\alpha + t\beta)} \right) \neq 0$$

$$\forall i \neq j \quad \varphi_i(\alpha + t\beta) \neq \varphi_j(\alpha + t\beta)$$

$\gamma = \alpha + t\beta$ ha n coniugati $\Rightarrow [K(\gamma) : K] = n$

$$\Rightarrow E = K(\gamma)$$

K campo finito : E/K è finito $\Rightarrow E$ è finito

$\Rightarrow E^*$ è un sgr. mult. finito di $E \Rightarrow E^* = \langle \gamma \rangle$

$$E = K(\gamma)$$

□



L/K estensione finita e di Galois

$$\begin{array}{l} \text{Gal} \left(\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array} \right) \\ \sum_{L/K} = \{ F \mid K \subseteq F \subseteq L \} \longrightarrow \mathcal{G} = \{ H < \text{Gal}(L/K) \} \\ F \xrightarrow{\alpha} \text{Gal}(L/F) \\ L^H \xleftarrow{\beta} H \end{array}$$

$$L^H = \text{Fix}(H) = \{ \alpha \in L \mid \varphi \alpha = \alpha \quad \forall \varphi \in H \} \leftarrow \text{CAMPO (FATE LA VERIFICA)}$$

167
 Tutti gli α di $\text{Gal}(L/K)$ fissano K e punti
 $\downarrow$
 $K \subseteq L^H \subseteq L$
 $\Rightarrow \beta$ è ben definito

È chiaro

α è ben definita: $\text{Gal}(L/F) < \text{Gal}(L/K)$
 ovvero un automorfismo di L che fissa
 F puntualmente fissa anche K ($K \subseteq F$)

Lemma 1: L/M un'estensione di Galois - $H < \text{Gal}(L/M)$

$$L^H = M \iff H = \text{Gal}(L/M)$$

Dim: $\Leftarrow$ $G = \text{Gal}(L/M)$ Tesi: $L^G = M$

$$\text{Se } M \subsetneq L^G \quad [L^G : M] > 1 \Rightarrow \exists \varphi: L^G \rightarrow \overline{M} \quad \varphi|_M = \text{id}$$

$$\varphi \neq \text{id} \Rightarrow \text{Sce } \tilde{\varphi}: L \rightarrow \overline{M} \quad \tilde{\varphi}|_{L^G} = \varphi$$

(tutte le immersioni si estendono ad una est del campo)

$$\tilde{\varphi}|_M = \varphi|_M = \text{id} \quad L/M \text{ è normale } \tilde{\varphi} L = L$$

$$\Rightarrow \tilde{\varphi} \in \text{Gal}(L/M) = G \Rightarrow \tilde{\varphi} \text{ fissa puntualmente } L^G$$

$\Rightarrow$ assurdo.

$(\Rightarrow)$ $L = M(\alpha)$ per α l'elemento primitivo.

$$H \leq G \quad \text{e considero } f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \quad \deg f = |H|$$

$$\text{Si ha } f(x) \in L^H[x]$$

$$\rho \in H \quad \rho f(x) = \prod_{\sigma \in H} (x - \rho \sigma(\alpha)) = \prod_{\sigma \in H} (x - \sigma(\alpha)) = f(x)$$

$$f \in K[x] \text{ e } f(\alpha) = 0 \Rightarrow \mu_{\alpha} | f(x)$$

$$|G| = [L^H : M] = \deg \mu_{\alpha/M} \stackrel{168}{\leq} \deg f = |H| \Rightarrow H = G$$

□

Teorema di corrispondenza di Galois

L/K di Galois finite. C'è una corrisp. biunivoca

$$\begin{array}{ccc} \mathcal{C}_{L/K} & \xleftrightarrow{\sim} & G_{L/K} \\ F & \xrightarrow{\alpha} & \text{Gal}(L/F) \\ L^\# & \xleftarrow{\beta} & H \end{array}$$

$$(\alpha = \beta^{-1})$$

Inoltre $H \triangleleft G \iff L^\# / K$ è normale

$$\text{e in tal caso } \text{Gal}(L^\# / K) \cong \frac{\text{Gal}(L/K)}{\text{Gal}(L/L^\#)} = \frac{G}{H}$$

Dim: Mostriamo che $\alpha \circ \beta = \text{id}$ $\beta \circ \alpha = \text{id}$

$$\beta \circ \alpha (F) = \beta (\text{Gal}(L/F)) = L^{\text{Gal}(L/F)} = F$$

per il L1

$$\alpha \circ \beta (H) = \alpha (L^\#) = \text{Gal}(L/L^\#) = H$$

$$H \subseteq \text{Gal}(L/L^\#)$$

$$H \triangleleft G = \text{Gal}(L/K)$$

$\hookrightarrow$ automorfismi di L

Tutti gli el di $L^\#$ sono fissati dagli el di H per def.

$$\Rightarrow H \subseteq \text{Gal}(L/L^\#)$$

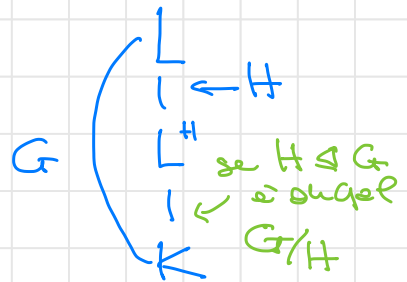
$$\text{Gal}(L/L^\#) \subseteq H$$

$\stackrel{H}{=}$

$$H \subseteq \text{Gal}(L/H) \text{ e } L^\# = H$$

$$\Downarrow \text{L1}$$

$$H = \text{Gal}(L/H)$$



Lemma 2: L/K di Galois $H < \text{Gal}(L/K)$ $\sigma \in \text{Gal}(L/K)$

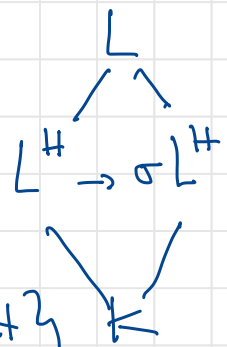
$$\Rightarrow L^{\sigma H \sigma^{-1}} = \sigma(L^H)$$

Dim:

$$L^H = \{a \in L \mid \varphi a = a \quad \forall \varphi \in H\}$$

$$\sigma L^H = \{ \sigma(a) \mid a \in L^H \} = \{ \sigma(a) \mid \varphi a = a \quad \forall \varphi \in H \}$$

$$= \{ \beta \in L \mid \sigma \varphi \sigma^{-1}(\beta) = \sigma(a) \quad \forall \varphi \in H \} = L^{\sigma H \sigma^{-1}} \quad \square$$



$$H \triangleleft G \Leftrightarrow \forall \sigma \in G \quad \sigma H \sigma^{-1} = H \stackrel{L^2}{\Leftrightarrow} \sigma L^H = L^{\sigma H \sigma^{-1}} = L^H \quad \forall \sigma \in G$$

$$\Leftrightarrow L^H/K \text{ \u00e9 normale.}$$



$$\begin{array}{ccc} L & \xrightarrow{\psi} & \overline{K} \\ \psi|_{L^H} & = & \text{id} \end{array} \quad \psi|_K = \text{id}$$

Perch\u00e9 ogni ψ si estende

$$\text{a } L \Rightarrow \forall \varphi \exists \sigma \in G \text{ tale } \sigma|_{L^H} = \varphi$$

Resta da vedere che $\text{Gal}(L^H/K) \cong G/H$

$$\begin{array}{ccc} \text{res}: G & \longrightarrow & \text{Gal}(L^H/K) \\ \varphi & \longmapsto & \varphi|_{L^H} \end{array} \quad \begin{array}{l} \text{omomorfismo di} \\ \text{restrictione} \end{array}$$

- \u2022 \u00e9 surgettivo perch\u00e9 ogni $\varphi \in \text{Gal}(L^H/K)$ si estende ad L

$$\begin{aligned} \text{Ker}(\text{res}) &= \{ \varphi \in G \mid \varphi|_{L^H} = \text{id} \} = \{ \varphi \in G \mid \varphi(a) = a \quad \forall a \in L^H \} \\ &= \text{Gal}(L/L^H) \cong H \quad \square \end{aligned}$$

Proposizione:

1

$$H, S \leq \text{Gal}(L/K)$$

$$(1) H \leq S \Leftrightarrow L^H \supset L^S$$

$$(2) L^{H \cap S} = L^H L^S$$

$$(3) L^{\langle S, H \rangle} = L^H \cap L^S$$

Dim: (1) ovvio (scrivete i diagrammi)

$$(2) H \cap S \leq H, S \quad L^{H \cap S} \supset L^H, L^S \text{ per (1)} \Rightarrow L^{H \cap S} \supseteq L^H L^S$$

$$L^H L^S \subset L \Rightarrow \exists N \leq \text{Gal}(L/K) \quad L^H L^S = L^N$$

$$\text{Gal}\left(\underbrace{L}_{L^S L^H}\right) = N \subset \text{Gal}\left(\underbrace{L}_{L^H}\right) \cap \text{Gal}\left(\underbrace{L}_{L^S}\right)$$

$$H \cap S \Rightarrow N \subset H \cap S$$

$$L^N \supseteq L^{H \cap S}$$

$$(3) \begin{matrix} H \leq \langle S, H \rangle \\ S \leq \langle S, H \rangle \end{matrix} \quad L^S, L^H \supseteq L^{\langle H, S \rangle} \Rightarrow L^{\langle H, S \rangle} \subseteq L^H \cap L^S$$

Viceversa $d \in L^H \cap L^S \quad \varphi(d) = d \quad \forall \varphi \in H$
 $\forall \varphi \in S$

$\Rightarrow d$ è fissato dai generatori del gruppo $\langle H, S \rangle$

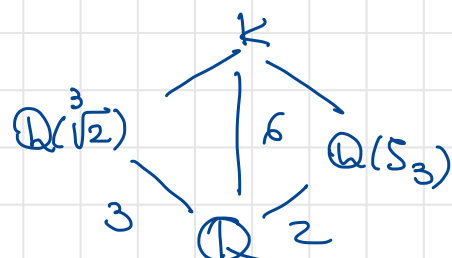
$\Rightarrow d$ è fissato da tutti gli el di $\langle H, S \rangle$

$$\Rightarrow L^H \cap L^S \subseteq L^{\langle H, S \rangle} \Rightarrow (3) \quad \square$$

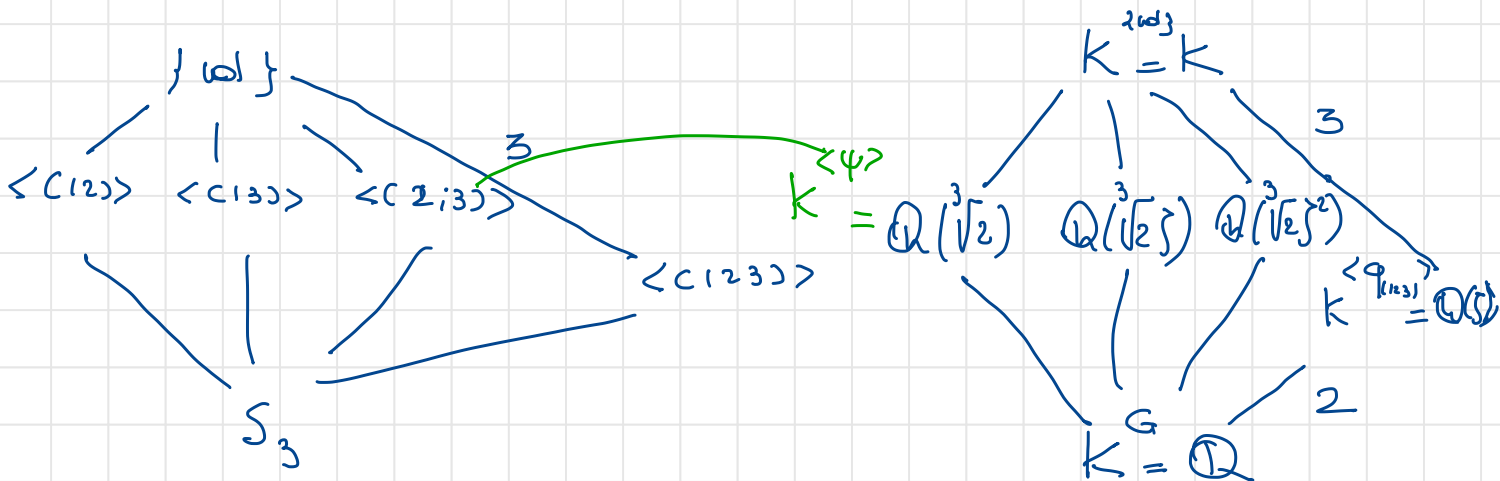
Esempio $x^3 - 2$ irrip in $\mathbb{Q}$ $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K$

$$[K:\mathbb{Q}] = 6 \quad \text{Gal}(K/\mathbb{Q}) \cong S_3$$

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \sqrt[3]{2} \zeta, \quad \alpha_3 = \sqrt[3]{2} \zeta^2$$



S_3 $\{101\}$, $\langle C(12) \rangle$, $\langle C(13) \rangle$, $\langle C(23) \rangle$, $\langle C(1,2,3) \rangle$, S_3



$$q \quad K \rightarrow \mathbb{Q}$$

$$\alpha_1 = \sqrt[3]{2} \rightarrow \sqrt[3]{2} \zeta^i \quad i=0,1,2$$

$$\zeta \rightarrow \zeta^j \quad j=0,1$$

$$q_{(123)} \quad \alpha_1 \rightarrow \alpha_2 \quad \sqrt[3]{2} \rightarrow \sqrt[3]{2} \zeta \quad i=1$$

$$\zeta \rightarrow \zeta \quad j=0$$

$$q(\sqrt[3]{2} \zeta) = q(\sqrt[3]{2}) q(\zeta) = \sqrt[3]{2} \zeta^2$$

$$q_{(123)} \quad \psi$$

$$\sqrt[3]{2} \rightarrow \sqrt[3]{2}$$

$$\zeta \mapsto \zeta^2$$

$$q_{(132)} \quad \left(\begin{array}{l} \sqrt[3]{2} \zeta \mapsto \sqrt[3]{2} \zeta \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \zeta^2 \\ \zeta \mapsto \zeta^j \end{array} \right)$$

$$q(\sqrt[3]{2} \zeta) = q(\sqrt[3]{2}) q(\zeta) = \sqrt[3]{2} \zeta^{2+j} = \sqrt[3]{2} \zeta$$

$$2+j=1 \quad (3) \quad \Rightarrow j=2$$

COMPLEMENTI

Estensione degli omomorfismi

Teorema: F/K un'estensione ALGEBRICA, $\varphi: K \rightarrow \overline{K}$

immersione $\Rightarrow \exists \tilde{\varphi}: F \rightarrow \overline{K} \quad \tilde{\varphi}|_K = \varphi$

Dim: Il risultato è già noto per le estensioni

finite (L/K finito $L = K(\alpha)$ $[L:K] = \deg \mu_{\alpha/K}$

e le immersioni $L \rightarrow \overline{K}$ $\tilde{\varphi}|_K = \varphi$
sono tante quante il numero di
radici DISTINTE di μ_{α} in $\overline{K}$

Se abbiamo l'ipotesi di separabilità
 $\Rightarrow \# \text{radici distinte di } \mu_{\alpha} \text{ in } \overline{K} = \deg \mu_{\alpha}$)

Per dimostrare uso il Lemma di Zorn

$$X = \{ (E, \psi) \mid K \subseteq E \subseteq F \quad \psi: E \rightarrow \overline{K}, \quad \psi|_K = \varphi \}$$

idea: Mostro che X è iniettivo $\rightarrow \exists$ el max $(\mathcal{F}, \leq)$
e dico che $\mathcal{F} = F$

$$X \neq \emptyset \quad (K, \varphi) \in X$$

$$\leq \text{ who definirlo } (E_1, \psi_1) \leq (E_2, \psi_2) \Leftrightarrow$$

$$E_1 \subseteq E_2 \text{ e } \psi_2|_{E_1} = \psi_1$$

$\leq$ È un ordinamento parziale su X

$(X, \leq)$ dico che è involutivo (ogni catena ha un maggiorante in X)

$\mathcal{C} = \{E_i, \psi_i\}_{i \in I}$ ← catene, sottoinsiemi TOT ordinati

$E = \bigcup_{i \in I} E_i$ ← campo padre: gli E_i sono incatenati

$$K \subseteq E \subseteq F$$

$$\psi(x) = \psi_i(x) \Big|_{x \in E_i}$$

$$\forall x \in E$$

$$\psi: E \rightarrow K$$

$$x \mapsto \psi_i(x)$$

è ben definito?

$$x \in E_i, x \in E_j$$

$$\psi_i(x) = \psi_j(x)? \text{ si fa bene?}$$

$$E_i \subseteq E_j \text{ (o viceversa)}$$

$$\psi_j|_{E_i} = \psi_i \Rightarrow \psi_j(x) = \psi_i(x)$$

$\Rightarrow (X, \leq)$ è involutivo

⇓ Zorn

$f \in X$ elemento massimale

Dico che $f = F$ - Chiamo $f \subseteq F$

Se fosse $f \subsetneq F \Rightarrow f \in F \setminus f \Rightarrow f(\alpha) \subseteq F$

$f \subseteq f(\alpha)$
è padre,
perché
α è seq.

e per il Teo di estensione nel caso di eri finite

$$\Rightarrow \tilde{q} \text{ si estende } \tilde{q}|_{f(\alpha)} \rightarrow K \quad \tilde{q}|_f = \tilde{q}$$

$$\Rightarrow \tilde{q}|_K = \tilde{q}|_K = q \Rightarrow \text{assue per } q$$

$$(f, \tilde{q}) \text{ è un max mo } (f, \tilde{q}) \subsetneq (f(\alpha), \tilde{q})$$

Corollario: Due chiusure algebriche di un campo K sono sempre isomorfe.

Dim $\Omega, \bar{K}$ chiusure alg di K . Devo mostrare $\Omega \cong \bar{K}$

$i: K \hookrightarrow \bar{K}$. Poiché Ω/K è algebrica, per il T

esiste estensione $\varphi: \Omega \rightarrow \bar{K}$ $\varphi|_K = i$

φ è chiamata immagine iniziale (Ω è campo) Devo anche che

è surgettiva: $\varphi(\Omega) = \bar{K}$

• $\varphi(\Omega)$ è alg chiuso: $p(x) \in \varphi(\Omega)[x]$ $\deg p \geq 1$

$$p(x) = \varphi(q(x)) \quad q(x) \in \Omega[x]$$

Ω alg chiuso $\Rightarrow \exists \alpha \in \Omega$ tale $q(\alpha) = 0$

$$\Rightarrow \varphi(\alpha) = \beta \in \varphi(\Omega) \quad \text{e} \quad p(\beta) = 0$$

$$\varphi(0) = \varphi(q(\alpha)) = \varphi(q)(\varphi(\alpha)) =$$

• $\varphi(\Omega) \subset \bar{K}$

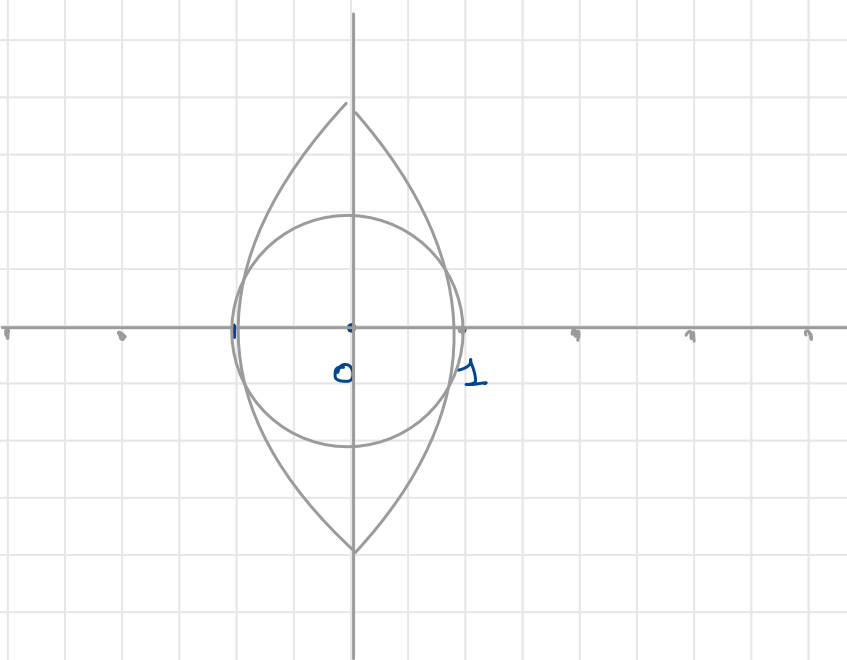
$\gamma \in \bar{K}$ γ è alg su $K \Rightarrow \gamma$ è alg su $\varphi(\Omega) \supset K$

$\Rightarrow \varphi(\Omega)$ alg chiuso $\Rightarrow \gamma \in \varphi(\Omega) \Rightarrow \varphi(\Omega) = \bar{K}$

$\Rightarrow \Omega \cong \bar{K}$

□

COSTRUZIONI CON RIGHE E COMPASSO



Si parte da 2 punti
 $0, 1$

e poi Traccio retta
per 2 punti costruiti
e cerchi di centro
in punto costruito
e raggio tanto
quanto la distanza
tra i 2 punti costruiti

Si Traccio perpendicolare ad una retta data per
un punto assegnato e anche //

Def: Un punto si dice COSTRUIBILE se fa parte
di una succ. finite di punti $\Gamma_1, \dots, \Gamma_n$

Torero

(1) $\Gamma_1 = 0, 1$ ed sono stati costruiti con
intersezione di rette e circonferenze
che costruisce

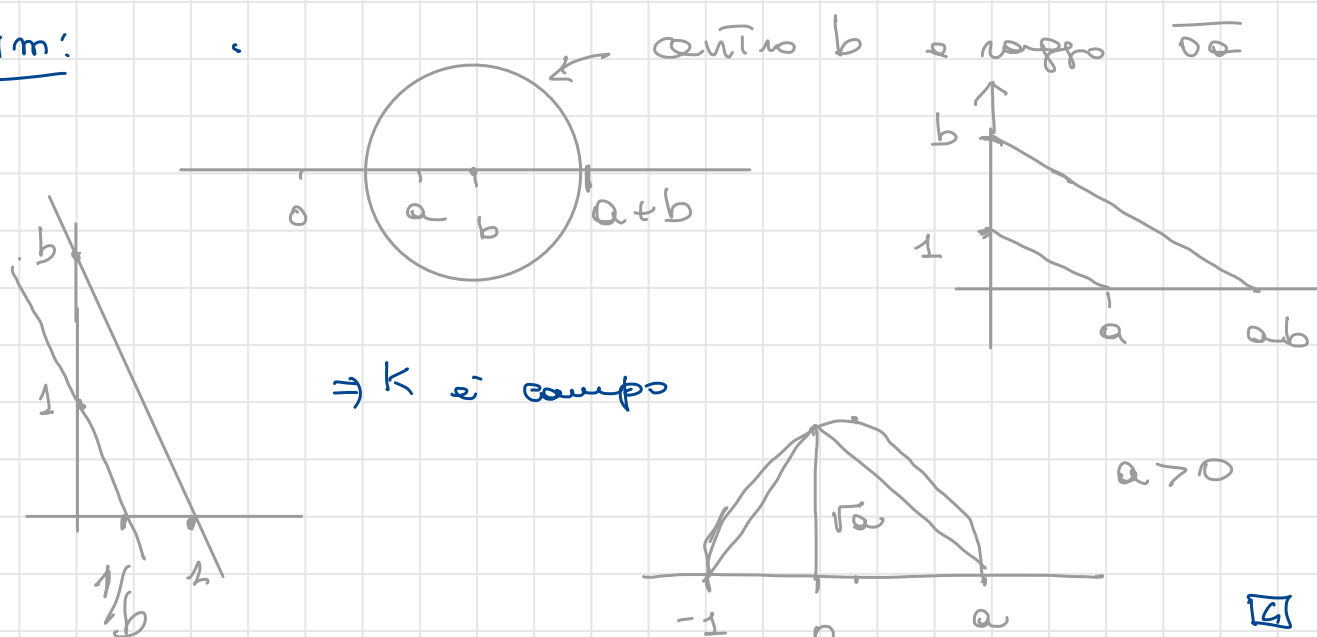
(2) Γ_1 è una retta per punto già costruito

(3) Γ_1 è una circonferenza con centro punto
già costruito e raggio di lunghezza
 $\overline{\Gamma_1 \Gamma_k}$ dove $0, k < n$ e Γ_2, Γ_k punti

Teorema: $K = \{x \in \mathbb{R} \mid x \text{ è costruibile}\} \Rightarrow \mathbb{Q} \subset K$

e K è un campo chiuso rispetto alle $\sqrt[n]{a}$
di cui per ogni $a \in K$ $a > 0$

Dim:



Teorema

$L = \{d \in \mathbb{C} \mid d \text{ è costruibile}\}$ è un campo chiuso rispetto allo $\sqrt{}$.

Dim

$x+iy$ è costruibile $\Leftrightarrow (x, y)$ è costruibile

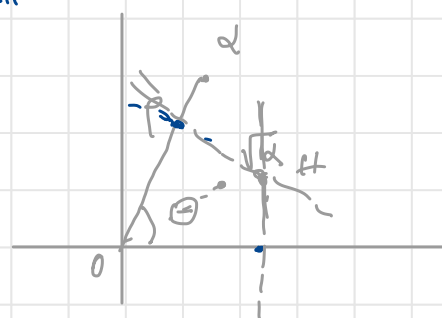
$\Rightarrow (x, 0)$ e $(0, y)$ sono costruibili

$\Rightarrow L$ è campo

$d \in L$

$$d = \rho e^{i\theta}$$

$$\sqrt{d} = \sqrt{\rho} e^{i\frac{\theta}{2} + k\pi}$$



$\sqrt{\rho}$ è la radice di un reale > 0

$\frac{\theta}{2} \leftarrow$ Tracciando la bisettrice dell'angolo

Oss: Le equazioni di rette e cerchi costruibili hanno coeff costruibili

Teorema:

$\alpha \in L \Leftrightarrow \exists$ una succ di campi: $\mathbb{Q} \subset L_0 \subset L_1 \subset \dots \subset L_n$

con $\alpha \in L_n$ e $[L_{i+1} : L_i] = 2 \quad \forall i = 0, \dots, n-1$

Dim:

($\Rightarrow$) α è costruibile $\Rightarrow \exists z_0, \dots, z_n = \alpha$ Tche
 $\forall i \quad z_i$ si ottiene $\cap$ rette costruibili
 $\cap$ cerchi
 $\cap$ cerchi

$$L_0 = \mathbb{Q}$$

$$L_i = \mathbb{Q}(z_0, \dots, z_i)$$

z_{i+1} è intersezione di rette e/o cerchi
 con eq che appartiene a L_i

$$\Rightarrow \begin{cases} \text{rette} \\ \text{rette} \end{cases} \begin{cases} \text{rette} \\ \text{cerchi} \end{cases} \begin{cases} \text{cerchi} \\ \text{cerchi} \end{cases}$$

eq uscente ha grado $\leq 2 = L_{i+1} = L_i(z_{i+1})$

$$[L_{i+1} : L_i] \leq 2$$

$$(\Leftarrow) \text{ Sia } \alpha \in L_n \supset L_{n-1} \supset \dots \supset \mathbb{Q}$$

$$\downarrow \quad \downarrow \quad \downarrow$$

$$2 \quad 2 \quad 2$$

Devo dire che α è costruibile - Procedo per induzione su

$n=0 \quad L_0 = \mathbb{Q} \Rightarrow \alpha$ è costruibile perché tutti i punti di $\mathbb{Q}$ lo sono

$\alpha \in L_n \Rightarrow$ tutti i punti di L_{n-1} sono costruibili per ip induzione

$$L_n = L_{n-1}(z) \quad z \text{ ha grado } 2 \quad \begin{cases} \text{se } \Delta \in L_{n-1} \\ \text{se } \Delta \in L_{n-1} \end{cases} \Rightarrow z \text{ è costruibile}$$

$$z = \frac{-a \pm \sqrt{\Delta}}{2}$$

Corollario: α è costruibile $\Rightarrow \alpha$ è algebrico su $\mathbb{Q}$
di grado 2^k $d \in \mathbb{N}$

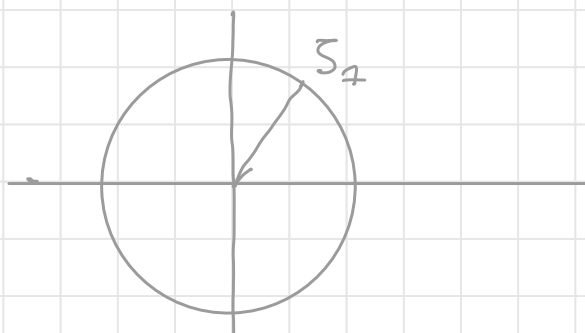
- $\Rightarrow$
- π non è costruibile perché non è algebrico
 - non si possono tracciare gli angoli ^{generici} con riga e compasso $\sqrt[3]{\alpha}$
 $X^3 - \alpha$ se è irriducibile $\sqrt[3]{\alpha}$ ha grado 3
 - non si può duplicare il cubo con riga e compasso

ho un cubo di volume 1 voglio costruire NO
un cubo di volume 2

$$l^3 = 2$$

$x^3 - 2$ ha radici di grado 3.

- Non si può costruire con riga e compasso un poligono regolare con 7 lati



$\rightarrow$ costruirlo vorrebbe
dire costruire S_4
che non è costruibile
perché

$$[\mathbb{Q}(S_4) : \mathbb{Q}] = 6$$
 che non è potenza
di 2.

- I poligoni regolari con n lati costruibili con riga e compasso devono avere $\phi(n) = 2^k$

Vale anche

$\Leftarrow$ perché

in questo caso

la Torre di

Assise l'ontano

della Torre di

1800 anni

in questo caso

n -agono è costruibile $\Leftrightarrow S_n$ è costruibile

179

$$\Leftrightarrow [\mathbb{Q}(S_n) : \mathbb{Q}] = \phi(n) = 2^k$$

$$n = 2^a p_1^{e_1} \dots p_r^{e_r} \quad p_i: \text{primi dispari}$$

$$\phi(n) = 2^{a-1} p_1^{e_1-1} (p_1-1) \dots p_r^{e_r-1} (p_r-1) \quad p_i \neq p_j$$

$$\Rightarrow e_i = 1$$

$$p_1 - 1 = 2^{k_1} \quad p_1 = 2^{k_1} + 1 \quad k_1 = 2^{d_1}$$

$$p_i = 2^{2^{d_i}} + 1 \quad \leftarrow \text{primi di Fermat}$$

(Attenzione: non tutti i numeri di questa forma sono primi $2^{2^5} + 1, \dots$)

Oss: Non è detto che se $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^n$

allora α sia costruibile.

Vale però se $\mathbb{Q}(\alpha)$ è di Galois perché in questo caso la T di Galois + risultati sui sottogruppi garantiscono l'esistenza della succ di sottocampi. In fatti:

Teorema: α è costruibile $\Leftrightarrow$ $\mathbb{Q}(\alpha)$ è contenuto in un'ext di Galois di grado 2^d per qualche d .

$$(\Leftarrow) \quad L \ni \alpha \quad L/\mathbb{Q} \text{ di Galois} \quad G = \text{Gal}(L/\mathbb{Q})$$

$$|G| = 2^d \Rightarrow \exists \{e\} = G_d \leq G_{d-1} \leq \dots \leq G_0 = G$$

$\downarrow \quad \quad \downarrow \quad \quad \downarrow$
 $2 \quad \quad 2 \quad \quad 2$

Via Teoria di Galois

$$L \supset L^{G_{d-1}} \supset \dots \supset L^{G_0} = \mathbb{Q}$$

$\downarrow \quad \quad \downarrow \quad \quad \downarrow$
 $2 \quad \quad 2 \quad \quad 2$

Risolubilità per radicali

$f(x) \in \mathbb{Q}[x]$ $\deg f(x) = n$ $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$ radici di f

È una formula che mi permette di esprimere le radici di f in termini dei coeff con espressioni di campo e radicali?

$$x^7 - 5 = 0 \quad \alpha_i = \sqrt[7]{5} \zeta_7^i$$

In qualche caso specifico si può fare

È una formula generale per tutti i polinomi di grado n fissato?

$n=2, 3, 4$ sì

$n \geq 5$ NO $\leftarrow$ si dimostra che non può esistere!

f si può risolvere per radicali se il suo campo di spezzamento $K/\mathbb{Q}$ ammette una catena del tipo

$$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_n = K$$

$$K_{i+1} = K_i \left(\sqrt[n_i]{\gamma_i} \right) \quad \gamma_i \in K_i$$

Esempio $x^7 - 5$ $K = (\sqrt[7]{5}, \zeta_7)$

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(\zeta_7, \sqrt[7]{5})$$

$\mathbb{Z}/7\mathbb{Z}^* \quad \hookrightarrow \mathbb{Z}/7\mathbb{Z}$

$\rightarrow$ Le estensioni per radicali quando sono normali hanno gruppo di Galois abeliano

$K(\sqrt[n]{\gamma})$ $x^n - \gamma$ ← in "genere" di polinomio
 $K(\sqrt[n]{\gamma})/K$ è normale se K contiene ζ_n
 In tal caso il gruppo di Galois è $\mathbb{Z}/n\mathbb{Z}$

→ L/K ha gruppo di Galois abeliano

$$\begin{array}{ccc}
 K = L_0 & \subset L_1 & \subset \dots \subset L_n = L \\
 \downarrow & & \downarrow \\
 \text{ciclici} & & \text{ciclici}
 \end{array}$$

$(G = \mathbb{Z}/2 \times \mathbb{Z}/2) \quad \mathbb{Q} \subseteq L^{\mathbb{Z}_2 \times \{0\}} \subset L$

→ Un polinomio si risolve per radicali se il suo campo di spezzamento simmetrico è una catena

$$L_0 = \mathbb{Q} \subset L_1 \subset \dots \subset L_n = L \quad (*)$$

L_{i+1}/L_i ciclici.

Vale anche il viceversa. Se le radici di f appartengono ad un campo L per cui ho una catena $(*)$ allora $\Rightarrow f$ è risolvibile per radicali.

Hilbert 90 $\Rightarrow$ Se L/K è ciclico e $\zeta_n \in K$ di grado n
 $\Rightarrow L = K(\sqrt[n]{\gamma}) \quad \gamma \in K$.

Formula per radicali: stelle eq generate di grado n -

→ Il polinomio generico univ. di grado n ha come gruppo di Galois S_n

$$L = \text{c.d.s.p. di } f \quad \text{Gal}(L/\mathbb{Q}) = S_n$$

f è risolubile per radicali $\Leftrightarrow$

$$\mathbb{Q} = L_0 \subset L_1 \subset \dots \subset L_n$$

$\downarrow$ $\downarrow$ $\downarrow$
 cicliche

$$S_n = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{n-1} \triangleright \{e\}$$

$$G_i / G_{i+1} \text{ ciclico.}$$

$$S_2 \triangleright \{e\}$$

$$S_3 \triangleright A_3 \triangleright \{e\}$$

$$S_4 \triangleright A_4 \triangleright \{\text{id}, (12)(34), (13)(24), (14)(23)\} \triangleright \{\text{id}\}$$

$\downarrow$ $\downarrow$ $\downarrow$
 2 3

$\uparrow$
 $\text{id}, (12)(34)$

$$S_5 \triangleright A_5 \dots$$

S_n non ammette la catena normale con quozienti ciclici

non è RISOLUBILE per $n \geq 5$.