# Algebra Lezione 24/09/25 (teoria - Del Corso)

- **Definizione gruppo:** Sia $G \neq \emptyset$ insieme dotato di un'operazione $(\cdot)$. Diremo che $G$ è gruppo se (i) $\forall a,b,c \in G \quad a\cdot(b\cdot c) = (a\cdot b)\cdot c$
  (ii) $\exists e \in G \mid \forall a \in G \quad a\cdot e = e\cdot a = a$
  (iii) $\forall a \in G \ \exists b \in G \mid a\cdot b = b\cdot a = e$

- **Definizione gruppo ciclico:** Sia $G$ gruppo, diremo che $G$ è gruppo ciclico se $\exists a \in G \mid G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

- **Definizione ordine:** Sia $G$ gruppo, $x \in G$, chiameremo ordine di $x$ $\text{ord}(x) = \begin{cases} +\infty & x^n \neq e \\ \min\{n \mid x^n = e\} & \end{cases}$

- **Proposizione:** Sia $G$ gruppo ciclico, $H \leq G \Rightarrow H$ è ciclico

  → **Dim:** • Caso $H = \{e\}$ è vero • Caso $H \neq \{e\} \Rightarrow \exists x \in H - \{e\}$. Ha $x = g^n$ perché $G = \langle g \rangle$. $n_0 = \min\{n \mid g^n \in H\}$, per div. euclid $n = q n_0 + r$

- $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$ → **Dim** ($\Rightarrow$) $n \in m\mathbb{Z} \Rightarrow n = ma \Rightarrow m \mid n$
  ($\Leftarrow$) $n = ma \Rightarrow n \in m\mathbb{Z} \Rightarrow n\mathbb{Z} \subseteq m\mathbb{Z}$

**Esercizi:**

1_ $m\mathbb{Z} \cap n\mathbb{Z} = ?$ Claim $= d\mathbb{Z}$ con $d = MCD(m,n)$
→ **Dim** ($\subseteq$) sia $x \in m\mathbb{Z} \cap n\mathbb{Z} \Rightarrow x \in m\mathbb{Z} \wedge x \in n\mathbb{Z} \Rightarrow m \mid x \wedge n \mid x \Rightarrow MCD(m,n) \mid x \Rightarrow x \in d\mathbb{Z}$
($\supseteq$) sia $x \in d\mathbb{Z} \Rightarrow d \mid x \Rightarrow m \mid x \wedge n \mid x \Rightarrow x \in m\mathbb{Z} \wedge x \in n\mathbb{Z}$

2_ $m\mathbb{Z} + n\mathbb{Z} = ?$ Non è un gruppo es: $2\mathbb{Z} + 3\mathbb{Z}$, $2 \in 2\mathbb{Z}$, $3 \in 3\mathbb{Z}$ ma $2+3 = 5 \notin 2\mathbb{Z}+3\mathbb{Z}$
Dunque è gruppo $\iff m\mathbb{Z} \subseteq n\mathbb{Z}$ o $n\mathbb{Z} \subseteq m\mathbb{Z}$

- **Teorema struttura gruppi ciclici:** Sia $G$ gruppo ciclico $\Rightarrow G \cong \mathbb{Z}$ / $\mathbb{Z}/n\mathbb{Z}$

  → **Dim** Sia $\varphi: \mathbb{Z} \to G$, $1 \mapsto x$ ($\langle x \rangle = G$ perché $G$ ciclico)
  • B.d. ovvia perché mando generatore in generatore
  • È omo $\varphi(n+m) = x^{n+m} = x^n \cdot x^m = \varphi(n)\varphi(m)$
  • È surj ovvio perché prendo il generatore
  • $\ker\varphi = n\mathbb{Z}$ con $n = \text{ord}(x)$
  • 1° Th omo $\mathbb{Z}/n\mathbb{Z} \cong G$

  N.B. negli omomorfismi fra gruppi ciclici voglio mandare il generatore in un elemento che divide l'ordine del generatore

- $\text{ord}(g^n) = \frac{\text{ord}(g)}{MCD(n, \text{ord}(g))}$

- **Primo teorema di omomorfismo:** Siano $G, G'$ gruppi, $f: G \to G'$ omomorfismo, $N \trianglelefteq G$
  $N \subseteq \ker f \Rightarrow \exists!\ \varphi: G/N \to G' \mid$ (i) $f = \varphi \circ \pi_N$ (ii) $\text{Imm } f = \text{Imm } \varphi$ (iii) $\ker\varphi = \frac{\ker f}{N}$

  → **Dim** • B.d. $xN = gN$ bisogna controllare $\varphi(xN) = \varphi(gN)$
  • omo $\varphi(xgN) = f(xy) = f(x)f(y) = \varphi(xN)\varphi(gN)$
  • $\text{Imm } \varphi = \{g \in G' \mid \exists x \ \varphi(xN) = g\} = \{g \in G' \mid \exists x \ f(x) = g\} = \text{Imm } f$
  • $\ker\varphi = \{y \in G/N \mid \varphi(gN) = e\} = \{gN \mid g \in \ker f\} = \frac{\ker f}{N}$

- **Secondo teorema di omomorfismo:** Sia $G$ gruppo, $H, K \trianglelefteq G$, $H \subseteq K \Rightarrow \frac{G/H}{K/H} \cong G/K$

  → **Dim** Sia $\pi_K: G \to G/K$. Per 1° th omo $\ker\varphi = \frac{\ker\pi_K}{H} = \frac{K}{H}$

  Sia per 1° th omo la mappa $\varphi: G/H \to G/K$, $\pi: G/H \to G/H/\ker\varphi$, $\sim: G/H/\ker\varphi \to G/K$

- **Terzo teorema di omomorfismo:** Sia $G$ gruppo, $H \leq G$, $K \trianglelefteq G \Rightarrow \frac{HK}{K} \cong \frac{H}{H \cap K}$

  → **Dim** Sia $f: H \to HK/K$, $h \mapsto hK$
  • B.d. $hK = gK$ bisogna controllare $f(e) = f(g)$
  • omo $f(xy) = xyK = xKyK = f(x)f(y)$
  • 1° th omo $f: H \to HK/K$, $\pi: H \to H/\ker f$, $\varphi: H/\ker f \to HK/K$
  • $\ker f = H \cap K$

- N.B. $Z(G\times G') = Z(G)\times Z(G')$
- # sgr ciclici ord $n = \frac{\#\text{ el ord } n}{\varphi(n)}$
- $(\mathbb{Z}/p\mathbb{Z})^n$ è ssp. vett. di $\mathbb{Z}/p\mathbb{Z} \Rightarrow$ # sgr $p^r$ = # ssp. dim $r = \frac{\#\text{ r-uple le cui ind}}{\#\text{ basi stesso ssp}} = \frac{(p^n-1)(p^n-p)\dots(p^n-p^{r-1})}{(p^r-1)(p^r-p)\dots(p^r-p^{r-1})}$

# Algebra Lezione 26/09/25 (teoria - Del Corso)

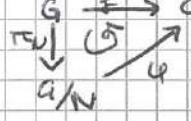
- **Teorema di corrispondenza (gruppi)**: Siano $G, G'$ gruppi, $f: G \to G'$ un omo surj, $f$ induce una corrispondenza biiettiva fra i sottogruppi di $G'$ e $H < G \mid \ker f \subseteq H$ questa corrispondenza si restringe ai sottogruppi normali e l'indice di sottogruppo.

→ **Dim**

- Dimostro per $f = \pi_N$ con $N \trianglelefteq G$ Vedi Lemma 1
- $X = \{H \leq G \mid N \subseteq H\}$ $\quad Y = \{\bar{H} \leq G/N\}$
- $\alpha: X \to Y$, $H \mapsto \pi_N(H)$ $\quad \beta: Y \to X$, $\bar{H} \mapsto \pi_N^{-1}(\bar{H})$
- $\alpha$ b. d. per Lemma 2 (ii)
- $\beta$ b. d. per Lemma 2 (i)
- $\alpha\circ\beta = id_Y$ $\quad \beta\circ\alpha = id_X$

- **Lemma 1**: Tutti gli omomorfismi surgettivi sono proiezioni al quoziente (a meno di iso).

→ **Dim**
- Sia $N \trianglelefteq G$. $\pi_N: G \to G/N$ proiezione al quoziente.
- Sia $f: G \to G'$ omo surj.
- 1th omo




ma dato che $f$ è surg $\varphi$ è biiett.

- **Lemma 2**: Siano $G, G'$ gruppi $f: G \to G'$ omo (i) $\bar{H} \leq G' \Rightarrow f^{-1}(\bar{H}) \leq G$, in part. $\bar{H} \trianglelefteq G' \Rightarrow f^{-1}(\bar{H}) \trianglelefteq G$
(ii) $H \leq G \Rightarrow f(H) \leq G'$, in parti: $H \trianglelefteq G \Rightarrow f(H) \trianglelefteq \mathrm{Imm} f$

→ **Dim** (i)
- $e \in f^{-1}(\bar{H})$ perché $e \in \ker f \subseteq f^{-1}(\bar{H})$
- $a, b \in f^{-1}(\bar{H}) \Rightarrow ab \in f^{-1}(\bar{H})$ perché $f$ omo
- $a \in f^{-1}(\bar{H}) \Rightarrow a^{-1} \in f^{-1}(\bar{H})$ perché $f$ omo
- se $\bar{H} \trianglelefteq G'$ $\quad g \in G$ $\quad h \in f^{-1}(H)$ $\quad f(ghg^{-1}) = f(g)f(h)(f(g))^{-1} \in \bar{H}$

(ii)
- $e \in f(H)$ perché $f(e) = e$
- $a, b \in f(H) \Rightarrow ab \in f(H)$ perché $f$ omo
- $a \in f(H) \Rightarrow a^{-1} \in f(H)$ perché $f$ omo
- se $H \trianglelefteq G$

- **Teorema Cauchy**: Sia $G$ gruppo, $p$ primo $\mid p \mid |G| \Rightarrow \exists x \in G : \mathrm{ord}_G(x) = p$.

→ **Dim** Sia $|G| = pn$, facciamo per induzione
- Base $n=1 \Rightarrow G$ ciclico $\Rightarrow G = \langle x\rangle \Rightarrow \mathrm{ord}_G(x) = p$
- P.I. Sia vero per $pm$ con $1 \leq m < n$.
  - Sia $H \lneq G \mid p \mid |H| \Rightarrow |H| = pa$ $\quad a \leq n \Rightarrow \exists x \mid \mathrm{ord}_H(x) = p$
  - Se $\forall H \lneq G$ $p \nmid |H| \Rightarrow pn = |G| = |Z(G)| + \sum_{x \in G\setminus Z(G)} \frac{|G|}{|C_G(x)|}$ ind

ma $p \mid \sum_{x\in G\setminus Z(G)} \frac{|G|}{|C_G(x)|} \Rightarrow p \mid |Z(G)| \Rightarrow G = Z(G)$

  - Se $G$ non è ab $\Rightarrow \exists H \mid p \mid |H|$
  - Se $G$ abeliano, prendo un $H \mid |H| = m$ $(m \mid n) \Rightarrow G/H$ allora ho $|G/H| = p\frac{n}{m}$, per hp ind $\exists \bar{x} \mid \mathrm{ord}_{G/H}(\bar{x}) = p$. Prendo un rappr. della classe $x$ ora quindi $\langle x\rangle$ è un $p$-gruppo

- **Teorema decomposizione in prodotto diretto**: Sia $G$ gruppo $H, K \leq G$
  (i) $H, K \trianglelefteq G$
  (ii) $HK = G$
  (iii) $H \cap K = \{e\}$
  $\Rightarrow G \cong H \times K$

→ **Dim** • Sia $f: H \times K \longrightarrow G$, $(h,k) \longmapsto hk$
• $f$ omo $f((h,k))f((h',k')) = hkh'k' \overset{\text{lemma } H,K \text{ coniugio}}{=} hh'kk' = f((hh', kk'))$
• $f$ inj $\ker f = \{e\}$ perché $H \cap K = \{e\}$
• $f$ surj perché $HK = G$

- **Lemma H,K coniugio**: Siano $G$ gruppo, $H, K \leq G$ (i) $H, K \trianglelefteq G$ (ii) $HK = G$ (iii) $H \cap K = \{e\}$ $\Rightarrow \forall h \in H \ \forall k \in K \ hk = kh$

→ **Dim** $hkh^{-1}k^{-1} \Rightarrow \underbrace{(hkh^{-1})}_{\in K \text{ perché } K \trianglelefteq G} k \in K$ $\quad h\underbrace{(kh^{-1}k^{-1})}_{\in H \text{ perché } H \trianglelefteq G} \in H$
$\Rightarrow hkh^{-1}k^{-1} \in H \cap K = \{e\} \Rightarrow hkh^{-1}k^{-1} = e$.

- **Definizione Aut(G)**: Sia $G$ gruppo, chiameremo $Aut(G) = \{f: G \longrightarrow G \mid f \text{ iso}\}$
- $Aut(G) \leq S(G)$
- $Aut(H) \times Aut(K) \hookrightarrow Aut(H \times K)$
- **Definizione coniugio**: Sia $G$ gruppo, chiameremo coniugio $\varphi_g: G \longrightarrow G$, $x \longmapsto gxg^{-1}$ con $g \in G$
  chiameremo $Inn(G) = \{\varphi_g \mid g \in G\}$
- **Proposizione proprietà Aut(G)**: (i) $\varphi_g \in Aut(G) \ \forall g \in G$
  (ii) $Inn(G) \trianglelefteq Aut(G)$

→ **Dim**: (i) • $\varphi_g$ omo per def
• $\varphi_g$ inj $\ker \varphi_g = \{e\}$ perché $\varphi_g(x) = gxg^{-1} = e \iff x = e$
• $\varphi_g$ surj perché $\forall y \in G \quad x = g^{-1}yg \Rightarrow \varphi_g(x) = y$
(ii) • $id \in Inn(G)$ con $\varphi_e$
• $\varphi_g, \varphi_h \in Inn(G) \Rightarrow \varphi_{gh} \in Inn(G)$
• $\varphi_g \in Inn(G) \Rightarrow \varphi_{g^{-1}} = \varphi_g^{-1} \in Inn(G)$
• Sia $f \in Aut(G)$ $f(\varphi_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g)ff^{-1}(x)(f(g))^{-1}$
$f(g)x(f(g))^{-1} = \varphi_{f(g)}(x)$

- $D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$ per $n$ dispari

Esercizi:

1 - Siano $H, K$ gruppi $\Rightarrow Aut(H) \times Aut(K) \hookrightarrow Aut(H \times K)$. Se $H, K \trianglelefteq H \times K$ allora è un isomorfismo.
Sia $\varphi: Aut(H) \times Aut(K) \longrightarrow Aut(H \times K)$, $(f, g) \longmapsto F: H \times K \longrightarrow H \times K$, $(h,k) \longmapsto (f(h), g(k))$

• $\varphi$ b. d. - $F$ è omo $F((h,k))F((h',k')) = [f(h), g(k)](f(h'), g(k')) = (f(h)f(h'), g(k)g(k')) = (f(hh'), g(kk')) = F((hh', kk'))$
- $F$ è bij perché $f \in Aut(H)$ e $g \in Aut(K)$ ($f, g$ omo)

• $\varphi$ inj se $(f, g) \in \ker \varphi \Rightarrow \varphi(f, g) = F(h,k) = (f(h), g(k)) = (h, k)$
ma quindi $f = id = g \rightarrow \ker \varphi = \{(id_H, id_K)\} \Rightarrow \varphi$ inj

• Se $H, K \trianglelefteq H \times K$, sia $F \in Aut(H \times K) \mid F(h,k) = (h', k')$ dato che $H, K \trianglelefteq H \times K$ posso definire $f \in Aut(H)$, $g \in Aut(K)$ $f: H \longrightarrow H$, $h \longmapsto h'$ $\quad g: K \longrightarrow K$, $k \longmapsto k'$
ma quindi $F = \varphi((f, g))$

- **Definizione caratteristico**: Sia $G$ gruppo, $H \leq G$, diremo che $H$ è caratteristico in $G$ $(H \text{ car } G)$ se $\forall f \in Aut(G)$, $f(H) = H$
- **Definizione normale**: Sia $G$ gruppo, $H \leq G$, diremo che $H$ è normale in $G$ $(H \trianglelefteq G)$ se $\forall g \in G \ \varphi_g(H) = H$

Esercizi:

1_ $Aut(\mathbb{Z}) = ?$ $Aut(\mathbb{Z}) = \{id\}$ perché $f: \mathbb{Z} \to \mathbb{Z}$ è omo $\Leftrightarrow$ mando i generatori nei generatori e gli unici generatori di $\mathbb{Z}$ sono $\pm 1$.

2_ $Aut(\mathbb{Z}/n\mathbb{Z}) = ?$ $Aut(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}^*$ perché $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ è omo bij $\Leftrightarrow$ mando il generatore in elementi di ordine $n$. Quindi $\varphi(n)$ possibilità.

3_ $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = ?$ $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = S_3$ perché in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ho 3 elementi di ordine 2 che posso mandare in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Quindi voglio permutare 3 elementi.

4_ $Aut(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ volte}}) = ?$ $Aut(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ volte}}) = GL_n(\mathbb{F}_p)$ perché voglio mandare una base in una base, le uniche che rispettano le condizioni di isomorfismo sono quelle delle matrici invertibili e dunque in $GL_n(\mathbb{F}_p)$. Viceversa, le applicazioni lineari di $GL_n(\mathbb{F}_p)$ sono isomorfismi

5_ $Aut(S_3) = ?$ $Aut(S_3) = S_3$ infatti: $|Aut(S_3)| \geq |S_3|$ perché $Z(S_3) = \{e\}$ dunque $Aut(S_3)$ contiene una copia normale di $S_3$ ($Inn(S_3) \cong S_3/Z(S_3) \trianglelefteq Aut(S_3)$). Ma $f \in Aut(S_3)$ scambia o i 2-cicli o i 3-cicli, dunque posso scambiare $3 \cdot 2 = 6$ elementi.

Algebra lezione 29/09/25 (esercitazione - Del Corso)

Esercizio 1: Siano $H \leq K \leq G$. Se $H \trianglelefteq K$ e $K \trianglelefteq G \Rightarrow H \trianglelefteq G$?

No. Troviamo un controesempio:

$G = D_4$, $K = \{e, r^2, s, sr^2\}$, $H = \langle s \rangle$.

$K \trianglelefteq G$ perché sgr di indice 2. $H \trianglelefteq K$ perché sgr di indice 2.

Ma $H \not\trianglelefteq G$, infatti $\varphi_r(s) = rsr^{-1} = r^2 s \notin H$

Esercizio 2: Siano $H \leq K \leq G$. Se $H \trianglelefteq K$ e $K \trianglelefteq G \Rightarrow H \trianglelefteq G$?

Sì. Per definizione, $K \trianglelefteq G \Rightarrow \forall f \in Aut(G)$, $f_{|K} \in Aut(K)$
Per definizione, $H \trianglelefteq K \Rightarrow \forall g \in Aut(K)$, $g_{|H} \in Aut(H)$
Ma quindi $\forall f \in Aut(G)$ $f_{|K|H} = f_{|H} \in Aut(H) \Rightarrow H \trianglelefteq G$.

Esercizio 3: Siano $H \leq K \leq G$. Se $H \trianglelefteq K$ e $K \not\trianglelefteq G \Rightarrow H \trianglelefteq G$?

No. Troviamo un controesempio:

$G = A_4$, $K = V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $H = \{e, (1,2)(3,4)\}$

$K \not\trianglelefteq G$ perché contiene tutte le permutazioni di ordine 2. $H \trianglelefteq K$ perché sgr di indice 2.

Ma $H \not\trianglelefteq G$, infatti $(1,3,4)(1,2)(3,4)(1,4,3) = (1,4,3,2) \notin H$

Esercizio 4: Siano $H \leq K \leq G$. Se $H \trianglelefteq K$ e $K \trianglelefteq G \Rightarrow H \trianglelefteq G$?

Sì. Per definizione, $K \trianglelefteq G \Rightarrow \forall g \in G$ $\varphi_{g|K} \in Aut(K)$
Per definizione, $H \trianglelefteq K \Rightarrow \forall f \in Aut(K)$ $f_{|H} \in Aut(H)$
Ma quindi: $\forall g \in G$ $\varphi_{g|K|H} = \varphi_{g|H} \in Aut(H) \Rightarrow H \trianglelefteq G$.

Lemma $|H| = 2$: Sia $G$ gruppo $H \leq G \mid |H| = 2$, $H \trianglelefteq G \Leftrightarrow H \leq Z(G)$

$\rightarrow$ Dim $\Rightarrow$ Se $|H| = 2 \Rightarrow H = \{e, h\}$. Se $H \trianglelefteq G \Rightarrow \forall g \in G$ $ghg^{-1} \in H$. Ma $ghg^{-1} \neq e$
$\Rightarrow ghg^{-1} = h$ ma quindi $gh = hg$ $\forall g \in G \Rightarrow h \in Z(G) \Rightarrow H \leq Z(G)$.

$\Leftarrow$ Se $H \leq Z(G) \Rightarrow \forall h \in H$ $gh = hg \Rightarrow ghg^{-1} = h \in H \Rightarrow H \trianglelefteq G$.

Esercizio 5: Sia $\sigma = (1,2,3,4)(5,6)(7,8) \in S_{10}$. $Z_{S_{10}}(\sigma) := \{\rho \in S_{10} \mid \rho\sigma\rho^{-1} = \sigma\} = ?$
$N_{S_{10}}(\sigma) := \{\rho \in S_{10} \mid \rho\langle\sigma\rangle\rho^{-1} = \langle\sigma\rangle\} = ?$

Per il lemma orbita-stabilizzatore sappiamo che $|Cl_{S_n}(\sigma)| \cdot |C_{S_n}(\sigma)| = |S_n|$
con $Cl_{S_n}(\sigma) = \{\rho\sigma\rho^{-1} \mid \rho \in S_n\} = \{\rho \in S_n \mid \rho$ "ha la stessa dec. in cicli di $\sigma$"$\}$

Ma $|Cl_{S_{10}}(\sigma)| = \#\rho$ fatte come $\sigma = \frac{\binom{10}{4}3!\binom{6}{2}1!\binom{4}{2}1!}{2!} = 64 = |Z_{S_{10}}(\sigma)|$

So chiaramente che: $H_1 = \langle(1\,2\,3\,4)\rangle$ $H_2 = \langle(5\,6)\rangle$ $H_3 = \langle(7\,8)\rangle$ $H_4 = \langle(9\,10)\rangle$
$H = H_1 \cup H_2 \cup H_3 \cup H_4 \subseteq Z_{S_{10}}(\sigma)$ e $|H| = 32$. Dunque voglio trovare un elemento $\tau \notin H$, così so che tutti gli el di $Z_{S_{10}}(\sigma)$ appartengono a $H$ o a $\tau H$ (perché sono classi lat quindi disgiunte e hanno entrambe cardinalità 32). Ad esempio funziona con $\tau = (5\,7)(6\,8)$.

In generale so che $\rho\sigma\rho^{-1}$ ha la stessa decomposizione in cicli di $\sigma \Rightarrow$ ha $o \cdot d = ord(\sigma)$.
In $\langle\sigma\rangle$ ci sono $\varphi(d)$ el. $o \cdot d = d$. $ord(\sigma^i) = o \cdot d(\sigma) \iff (i,d) = 1$, dunque
$\rho\sigma\rho^{-1} = \sigma^i$ con $(i,d) = 1$ quindi ho $\varphi(d)$ i.
Ma quindi $N_{S_{10}}(\sigma) = \bigcup_{\substack{1 \le i \le d \\ (i,d)=1}} \{\rho \in S_{10} \mid \rho\sigma\rho^{-1} = \sigma^i\} \Rightarrow |N_{S_{10}}(\sigma)| = \varphi(d) \cdot |Z_{S_{10}}(\sigma)|$.

## Esercizi

1 - Siano $H, K$ gruppi: $(|H|, |K|) = 1 \Rightarrow H, K \trianglelefteq H \times K = \{(h,k) \mid h \in H, k \in K\}$

Sia $|H| = n$, $|K| = m \Rightarrow |H \times K| = nm$. Sia $f \in Aut(H \times K)$, dunque $f$ manda elementi di ordine $n$ in elementi di ordine $n$ e elementi di ordine $m$ in elementi di ordine $m$. Ma $(n,m) = 1 \Rightarrow f(H \times \{e\}) = H \times \{e\}$ e $f(\{e\} \times K) = \{e\} \times K$

2 - $Aut(S_3 \times \mathbb{Z}/3\mathbb{Z}) = ?$ $Aut(S_3 \times \mathbb{Z}/3\mathbb{Z}) = Aut(S_3) \times Aut(\mathbb{Z}/3\mathbb{Z}) = S_3 \times \mathbb{Z}/2\mathbb{Z}$.
Questo perché sono caratteristici.
$S_3$ è caratteristico in $S_3 \times \mathbb{Z}/3\mathbb{Z}$ perché $S_3 = \langle(1\,2),(1\,3)\rangle$ ma $f \in Aut(S_3 \times \mathbb{Z}/3\mathbb{Z})$ quindi dato che è ono devo mandare i generatori che hanno ord 2 in el di ord 2. Ma in $\mathbb{Z}/3\mathbb{Z}$ non ci sono el di ordine 2 $\Rightarrow f(S_3 \times \{e\}) = S_3 \times \{e\}$
$\mathbb{Z}/3\mathbb{Z}$ è caratteristico in $S_3 \times \mathbb{Z}/3\mathbb{Z}$ perché è il centro di $S_3 \times \mathbb{Z}/3\mathbb{Z}$ (e il centro è caratteristico.
$Z(S_3 \times \mathbb{Z}/3\mathbb{Z}) = Z(S_3) \times Z(\mathbb{Z}/3\mathbb{Z}) = \{e\} \times \mathbb{Z}/3\mathbb{Z}$.

## Algebra Lezione (01/10/25 (teoria - Del Corso)

- **Definizione azione:** Sia $G$ gruppo, $X$ insieme chiameremo azione di $G$ su $X$ l'omomorfismo $\varphi: G \longrightarrow S(X)$, $g \longmapsto \varphi_g: x \longrightarrow x$, $x \longmapsto \varphi_g(x)$ con $\varphi_g$ bij. Scriveremo $G \curvearrowright X$

- Data un'azione $\varphi: G \longrightarrow S(X)$ definiamo la relazione di equivalenza $\sim$:
$x \sim y \iff \exists g \mid \varphi_g(x) = y$.
  - riflessività $\varphi_e(x) = x$
  - simmetria $\varphi_g(x) = y \Rightarrow \varphi_{g^{-1}}(y) = x$
  - transitività $\varphi_{g_1}(\varphi_{g_2}(x)) = \varphi_{g_1}(y) = z$

- **Definizione orbita:** Sia $G$ gruppo, $X$ insieme $\sim$ una relazione di equivalenza:
$[x]_\sim = orb(x) = \{\varphi_g(x) \mid g \in G\} = \{y \in X \mid y \sim x\}$

- N.B. $X = \bigcup_{x \in R} Orb(x)$ con $R$ insieme di rappresentanti

- **Definizione stabilizzatore:** Sia $G$ gruppo, $X$ insieme, $x \in X$, chiameremo stabilizzatore di $x$ $St(x) = \{g \in G \mid \varphi_g(x) = x\}$

- **Proposizione** $St(x) \le G$: Sia $G$ gruppo, $X$ insieme $\varphi: G \longrightarrow S(X)$ azione $\Rightarrow$ $St(x) \le G$

  → **Dim:**
  - $e \in St(x)$ perché $\varphi(e) = \varphi_e = id$
  - $gh \in St(x)$ perché $\varphi_g(\varphi_h(x)) = \varphi_g(x) = x$
  - $g^{-1} \in St(x)$ perché $\varphi_g(x) = x \Rightarrow x = \varphi_g^{-1}(x) = \varphi_{g^{-1}}(x)$

- **Lemma Orbita-stabilizzatore:** Sia $G$ gruppo finito, $X$ insieme $\Rightarrow |G| = |Orb(x)| \cdot |St(x)|$

  → **Dim:** Siano $\varphi_g, \varphi_h \in Orb(x) \mid \varphi_g(x) = \varphi_h(x) \iff \varphi_{h^{-1}}(\varphi_g(x)) = x \iff$
  $\varphi_{h^{-1}g}(x) = x \iff h^{-1}g \in St(x) \iff g \in hSt(x) \iff gSt(x) = hSt(x)$.
  classi lat perché non sempre $St(x)$ è normale
  Dunque $\phi: Orb(x) \longrightarrow G/St(x)$, $\varphi_a \longmapsto aSt(x)$ è bij.

- Ma quindi se $X = \bigcup_{x \in R} Orb(x) \Rightarrow |X| = \sum_{x \in R} |Orb(x)| = \left| \sum_{x \in R} \frac{|G|}{|St(x)|} \right|$ formula di Burnside

- Questa cosa si estende ai sottogruppi; facciamo un es col coniugio: $H \leq G$
$Orb(H) = \{gHg^{-1} \mid g \in G\}$, $St(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ ovvero il normalizzatore
$\Rightarrow |Orb(H)| = [G : N_G(H)]$.
Ma quindi $H \trianglelefteq G \iff Orb(H) = \{H\} \iff N_G(H) = G \iff H = \bigcup_{x \in H} cl_x$

- Caso particolare formula di Burnside, caso in cui la relazione è il coniugio

$$|G| = \sum_{x \in R} \frac{|G|}{|St(x)|} = \sum_{x \in Z(G)} \frac{|G|}{|St(x)|} + \sum_{x \in R - Z(G)} \frac{|G|}{|St(x)|} = \sum_{x \in Z(G)} |1| + \sum_{x \in R - Z(G)} \frac{|G|}{|St(x)|} = \left| Z(G) + \sum_{x \in R - Z(G)} \frac{|G|}{|St(x)|} \right|$$

(perché $St(x) = G$ per $x \in Z(G)$)

formula delle classi

- Definizione p-gruppo: Sia $G$ gruppo, diremo che $G$ è un p-gruppo se $|G| = p^n$ ($p$ primo $n \in \mathbb{N}$)

- Se $G$ è p-gruppo $\Rightarrow Z(G) \neq \{e\}$

→ Dim $Z(G) \leq G \Rightarrow |Z(G)| \mid |G| \Rightarrow |Z(G)| = p^k$ con $k \leq n$. Ma se $k = 0$
$p \nmid |Z(G)|$ Ma $p \mid |G| \Rightarrow p \mid |Z(G)| + \sum_{x \in R - Z(G)} \frac{|G|}{|St(x)|}$ ma $p \mid |G|$ $\frac{|G|}{|St(x)|}$ ↯

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

→ Dim $|Z(G)| \mid |G|$ per Lagrange. Dunque: • $|Z(G)| = 1$, no perché è p-gruppo
• $|Z(G)| = p$, no perché $G/Z(G)$ ciclico ⇓ $G$ abel ⇓ $Z(G) = G$
• $|Z(G)| = p^2 \Rightarrow G$ abel

- $G/Z(G)$ ciclico $\Rightarrow G$ abeliano

→ Dim $G/Z(G)$ ciclico $\Rightarrow G/Z(G) = \langle gZ(G) \rangle$ per $g \in G$. Siano $x, y \in G \Rightarrow$
$\exists g_1, g_2 \mid x \in g_1 Z(G)$ $y \in g_2 Z(G)$ ma $G/Z(G)$ ciclico, dunque
$g_1 = g^k$, $g_2 = g^h \Rightarrow x = g^k z_1$ $y = g^h z_2$. Perciò
$xyx^{-1}y^{-1} = g^k z_1 g^h z_2 z_1^{-1} g^{-k} z_2^{-1} g^{-h}$ ma $z_1, z_2 \in Z(G) \Rightarrow$
$= g^k g^h g^{-k} g^{-h} z_1 z_2 z_1^{-1} z_2^{-1} = g^k g^h g^{-k} g^{-h} = g^{k+h-k-h} = e$.

## Algebra lezione 06/10/25 (esercitazione - Del Corso)

Chiameremo $D_n$ il gruppo delle isometrie del piano che mandano l'n-agono regolare in sé stesso. Sappiamo che $|D_n| = 2n$

Chi sono i sottogruppi di $D_n$?

- $R = \langle r \rangle \trianglelefteq D_n$ (perché ha indice 2)

- se $d \mid n$, $\langle r^d \rangle \leq R \trianglelefteq D_n \Rightarrow \langle r^d \rangle \trianglelefteq D_n$ (per quanto detto in 29/09)
se $d \neq \frac{n}{2}$ allora $\langle r^d \rangle \trianglelefteq D_n$

→ Dim $f \in Aut(D_n)$, $ord(f(r^d)) = ord(r^d) = \frac{n}{d} \neq 2$
$\Rightarrow f(r^d)$ è una rot. e ha ord $\frac{n}{d} \Rightarrow$
$f(r^d) \in \langle r^d \rangle$ perché unico sgr. di ord $\frac{n}{d}$.

- se $n$ pari $Z(D_n) = \{e, r^{\frac{n}{2}}\}$, se $n$ dispari $Z(D_n) = \{e\}$
$Z(D_n) \trianglelefteq D_n$, in generale $\forall G$ gruppo $Z(G) \trianglelefteq G$
→ Dim $f \in Aut(G)$ $\forall g \in G$ $\exists y \in G \mid f(y) = g$. Dunque sia $x \in Z(G)$
$gf(x)g^{-1} = f(y)f(x)f(y^{-1}) = f(yxy^{-1}) = f(x) \Rightarrow f(x) \in Z(G)$

- se $H \leq D_n$ e $H \not\leq R$ allora noto che $|H/H \cap R| = 2 \Rightarrow |H| = |H \cap R| \cdot 2$
→ Dim $H \xhookrightarrow{i} D_n \xrightarrow{\pi} D_n/R = \langle s \rangle$
(si immerge perché sottogruppo; faccio la proiezione al quoziente perché $R \trianglelefteq D_n$)
$\varphi = \pi \circ i : H \longrightarrow D_n/R$ e $\ker \varphi = H \cap R \Rightarrow$ $H/H \cap R \cong D_n/R$ 1° thm iso
$\Rightarrow |H/H \cap R| = |D_n/R| = |\langle s \rangle| = 2$

ma quindi in $H$ ho due classi laterali di $H \cap R$: $H \cap R$, $sH \cap R$, questo perché $s \notin R$. Ma questo significa che $H = \langle r^d, sr^a \rangle = D_{n/d}$ (dove $\langle r^d \rangle = H \cap R$ perché $R$ è ciclico)

Ricordiamo che dato $G$ gruppo, $H, K \leq G$; $HK \leq G \iff HK = KH$

→ Dim ⇒ ① sia $x \in HK \Rightarrow \exists h \in H \; \exists k \in K \mid x = hk$, ma $x^{-1} \in HK \Rightarrow x^{-1} = k^{-1}h^{-1} \in HK$
$\Rightarrow HK \subseteq KH$
② sia $x \in KH \Rightarrow \exists h \in H \; \exists k \in K \mid x = kh$; ma $x^{-1} \in KH \Rightarrow h^{-1}k^{-1} \in KH \Rightarrow$
$KH \subseteq HK$

($\Leftarrow$) Sia $HK = KH$, allora • $e \in HK$ perché $e = e_H e_K$
• $x, y \in HK$ $\exists h_1, h_2 \in H$ $\exists \kappa_1, \kappa_2 \in K$ | $x = h_1\kappa_1$, $y = h_2\kappa_2$
$\Rightarrow xy = h_1\kappa_1 h_2\kappa_2$ ma $HK = KH$ $\Rightarrow \exists \kappa \in K$ $\exists h \in H$ |
$\kappa_1 h_2 = h\kappa$ $\Rightarrow xy = h_1 h \kappa \kappa_2$ $\Rightarrow xy \in HK$
• $x \in HK \Rightarrow \exists h \in H$ $\exists \kappa \in K$ | $x = h\kappa$ $\Rightarrow x^{-1} = \kappa^{-1} h^{-1} \in KH = HK \Rightarrow x^{-1} \in HK$

Chi sono le classi di coniugio di $D_n$? $Cl(x) = \{gxg^{-1} \mid g \in G\}$

- $Cl(e) = \{e\}$ → ricorda che se $x \in Z(G)$ $cl(x) = \{x\}$
- $Cl(r^a) = \{r^d r^a r^{-d}, sr^d r^a r^{-d}s \mid d \in \{1, \dots, n\}\} = \{r^a, r^{-a}\}$ (per $a \neq \frac{n}{2}$ se $n$ pari)
($r^d r^{-d} r^a = r^a$; $sr^d r^a r^{-d} s = sr^{d+a-d}s$)
- $Cl(s) = \{sr^d(s)(sr^d)^{-1}, r^d sr^{-d} \mid d \in \{1, \dots, n\}\} =$ $n$ pari → $\{s, sr^2, \dots, sr^{\frac{n}{2}}\} \cup \{sr, sr^3, \dots, sr^{n-1}\}$; $n$ dispari → $\{s, sr, \dots, sr^{n-1}\}$ ← perché $2a$ è invertibile
($sr^d s (sr^d)^{-1} = sr^{2d}$; $r^d sr^{-d} = sr^{-2d}$)
- se $n$ pari $Cl(r^{\frac{n}{2}}) = \{r^{\frac{n}{2}}\}$

- **Proposizione proprietà gruppo dei commutatori:** Sia $G$ gruppo, il commutatore di $G$ è $G' = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$
(i) $G' = \{e\} \iff G$ è abel
(ii) $G' \trianglelefteq G$
(iii) $G/G'$ è il più grande sgr. abel di $G$.

→ Dim (i) $\Rightarrow$ $G' = \{e\} \Rightarrow \forall x, y \in G$ $xyx^{-1}y^{-1} = e \Rightarrow \forall x, y \in G$ $xy = yx$
$\Leftarrow$ $G$ abel $\Rightarrow \forall x, y \in G$ $xy = yx \Rightarrow \forall x, y \in G$ $xyx^{-1}y^{-1} = e \Rightarrow G' = \{e\}$

(ii) $f \in Aut(G) \iff f([x,y]) \in G$ $\forall x, y \in G \iff f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x), f(y)] \in G'$

(iii) Sia $G/N$ abel, $x, y \in G$ allora $xNyNx^{-1}Ny^{-1}N = N \iff xyx^{-1}y^{-1}N = N$
$\iff xyx^{-1}y^{-1} \in N \iff G' \leq N$

## Esercizi:

1. Dimostra che $D_{n/d} \cong \langle r^d, sr^a \rangle$

Sia $f: D_{n/d} \to \langle r^d, sr^a \rangle$, $r \mapsto r^d$, $s \mapsto sr^a$ • è omo siano $x, y \in D_{n/d} \Rightarrow x = s^i r^a$, $y = s^j r^b$

$f(x)f(y) = f(s^i r^a) f(s^j r^b) = s^i r^{aa} s^j r^{ab} = s^{i+j} r^{a(b-a)} = f(s^{i+j} r^{b-a}) = f(xy)$

• è inj $\ker f = \{x \in D_{n/d} \mid f(x) = id\} = \{x \in D_{n/d} \mid f(s^i r^a) = id\} = \{x \in D_{n/d} \mid s^i r^{ai} = id\} = \{id\}$

• è surj sia $x \in \langle r^d, sr^a \rangle \Rightarrow x = s^i r^{ab}$ ma quindi $f(s^i r^b) = x$

## Algebra lezione 08/10/25 (teoria - Del Corso)

- **Definizione prodotto semidiretto:** Siano $H, K$; $\varphi: K \to Aut(H)$ ($\leq \mathfrak{I}(H)$), $\kappa \mapsto \varphi_\kappa$; chiameremo prodotto semidiretto $H \rtimes_\varphi K$ l'insieme $H \times K$ con l'operazione $(h_1, \kappa_1)(h_2, \kappa_2) = (h_1 \cdot_H \varphi_{\kappa_1}(h_2), \kappa_1 \cdot_K \kappa_2)$

- **Proposizione prodotto semidiretto è un gruppo:** Siano $H, K$ gruppi $\Rightarrow H \rtimes_\varphi K$ è un gruppo

→ Dim • neutro $(h, \kappa)(e, e) = (h\varphi_\kappa(e), \kappa e) = (h, \kappa)$
$(e, e)(h, \kappa) = (e\varphi_e(h), e\kappa) = (h, \kappa)$

• inverso $(h, \kappa)(\varphi_{\kappa^{-1}}(h^{-1}), \kappa^{-1}) = (h\varphi_\kappa(\varphi_{\kappa^{-1}}(h^{-1})), \kappa\kappa^{-1}) = (e, e)$
$(\varphi_{\kappa^{-1}}(h^{-1}), \kappa^{-1})(h, \kappa) = (\varphi_{\kappa^{-1}}(h^{-1})h, \kappa^{-1}\kappa) = (e, e)$

• associatività $(h_1, \kappa_1)((h_2, \kappa_2)(h_3, \kappa_3)) = (h_1, \kappa_1)(h_2\varphi_{\kappa_2}(h_3), \kappa_2\kappa_3) =$
$= (h_1\varphi_{\kappa_1}(h_2\varphi_{\kappa_2}(h_3)), \kappa_1\kappa_2\kappa_3) = (h_1\varphi_{\kappa_1}(h_2)\varphi_{\kappa_1}(\varphi_{\kappa_2}(h_3)), \kappa_1\kappa_2\kappa_3)$

$((h_1, \kappa_1)(h_2, \kappa_2))(h_3, \kappa_3) = (h_1\varphi_{\kappa_1}(h_2), \kappa_1\kappa_2)(h_3, \kappa_3) =$
$= (h_1\varphi_{\kappa_1}(h_2)\varphi_{\kappa_1\kappa_2}(h_3), \kappa_1\kappa_2\kappa_3) = (h_1\varphi_{\kappa_1}(h_2)\varphi_{\kappa_1}(\varphi_{\kappa_2}(h_3)), \kappa_1\kappa_2\kappa_3)$

- Noto che $\varphi_k = id_H \ \forall k \in K \Rightarrow H \rtimes_\varphi K = H \times K$

- **Teorema decomposizione in prodotto semidiretto:** Sia $G$ gruppo, $H, K \leq G$
  (i) $H \trianglelefteq G$
  (ii) $HK = G$
  (iii) $H \cap K = \{e\}$
  $\Rightarrow G \cong H \rtimes_\varphi K \quad \varphi: K \to Aut(H)$, $k \mapsto \varphi_k : H \to H$, $h \mapsto khk^{-1}$

  → **Dim:** • $f: H \rtimes_\varphi K \to G$, $(h,k) \mapsto hk$

  • è omo $f((h_1,k_1)(h_2,k_2)) = f((h_1\varphi_{k_1}(h_2), k_1k_2)) = f((h_1k_1h_2k_1^{-1}, k_1k_2)) = h_1k_1h_2k_1^{-1}k_1k_2 = h_1k_1h_2k_2 = f((h_1,k_1))f((h_2,k_2))$

  • è surj per (ii)

  • è inj per (iii)

- Posso fare la proiezione: $\pi: H \rtimes_\varphi K \to K$, $(h,k) \mapsto k$ • è omo $\pi((h_1,k_1)(h_2,k_2)) = \pi(h_1\varphi_{k_1}(h_2), k_1k_2) = k_1k_2 = \pi(h_1,k_1)\pi(h_2,k_2)$

  ma quindi $\{e_H\} \times K \leq H \rtimes_\varphi K$. Inoltre noto che $\ker\pi = \{(h,k) \in H \rtimes_\varphi K \mid \pi((h,k)) = ke_K\} = H \times \{e_K\} \Rightarrow H \times \{e_K\} \trianglelefteq H \rtimes_\varphi K$ (perché $\ker\pi \trianglelefteq H \rtimes_\varphi K$).

  dato che $(H \times \{e_K\}) \cap (\{e_H\} \times K) = (e_H, e_K)$ allora $(H \times \{e_K\})(\{e_H\} \times K) = H \rtimes_\varphi K$

- $S_n \cong A_n \rtimes_\varphi \langle(12)\rangle$, con $\varphi: \langle(12)\rangle \to Aut(A_n)$, $(12) \mapsto \varphi_{(12)}: A_n \to A_n$, $\sigma \mapsto (12)\sigma(12)$

  noto che (i) $A_n \trianglelefteq G$
  (ii) $\langle(12)\rangle A_n = S_n$ perché $[S_n : A_n] = 2$, dunque $S_n = \{A_n, (12)A_n\}$ perché $(12) \notin A_n$
  (iii) $A_n \cap \langle(12)\rangle = \{e\}$ perché $(12) \notin A_n$

  ma quindi dal teorema segue la tesi

- $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, con $\varphi: \mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/n\mathbb{Z})$, $\bar{1} \mapsto \varphi_{\bar{1}}: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{1} \mapsto \bar{-1}$

  comincio con dire che $D_n \cong \langle r\rangle \rtimes_\varphi \langle s\rangle$ con $\varphi: \langle s\rangle \to Aut(\langle r\rangle)$, $s \mapsto \varphi_s : r \mapsto srs^{-1} = r^{-1}$

  (i) $\langle r\rangle \trianglelefteq D_n$ (Lezione 06/10)
  (ii) $\langle s\rangle\langle r\rangle = D_n$ (chiaro perché $\langle s\rangle\langle r\rangle = \langle s, r\rangle = D_n$)
  (iii) $\langle s\rangle \cap \langle r\rangle = \{e\}$

  ma $ord(r) = n$ e $\langle r\rangle$ è ciclico $\Rightarrow \langle r\rangle \cong \mathbb{Z}/n\mathbb{Z}$ e $ord(s) = 2 \Rightarrow \langle s\rangle \cong \mathbb{Z}/2\mathbb{Z}$

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

- Siano $p, q$ primi $|G| = pq$. Per Cauchy $\exists x \in G \ \exists y \in G \mid ord(x) = q, ord(y) = p$; WLOG $q > p$ e chiamiamo $H = \langle x\rangle \wedge K = \langle y\rangle$. Noto che

  (i) $H \trianglelefteq G$ perché $[G : H] = p$ e $p$ è il più piccolo primo che divide $|G|$
  (ii) $HK = G$ perché $|HK| = pq$
  (iii) $H \cap K = \{e\}$ per l'ordine degli elementi

  $\Rightarrow G \cong H \rtimes_\varphi K$

- Se $G$ ($|G| = pq$) è abeliano $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. Per quanto detto sopra $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ con $\varphi: \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/q-1\mathbb{Z}$, $y \mapsto \varphi_y : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$, $\bar{x} \mapsto \bar{x}^k$

  • se $p \nmid q-1 \Rightarrow ord\varphi_y \mid 1 \Rightarrow \varphi_y = id \Rightarrow \varphi = id$ (quindi ha il prodotto diretto)

  • se $p \mid q-1 \to ord\varphi_y \mid p \Rightarrow \varphi_y = id$
  $\Rightarrow$ ho $p-1$ scelte per il prod semid. ma quindi se $\varphi_y(x) = x^k \Rightarrow (\varphi_y(x))^k = x^{k^p}$; ovvero $\varphi_y = id \iff k^p \equiv 1 \ (q)$
  ma quindi ognuno di questi gruppi sono isomorfi

# Algebra Lezione 13/10/25 (esercitazione - Del Corso)

- **Definizione gruppo generato da insieme:** Sia $X=\{x_1,\dots,x_n\}$ insieme, definisco il gruppo generato da $X$ come $G=\langle X\rangle=\{x_i\cdots x_j \mid i,j\in\{1,\dots,n\}\ x_i\in X\cup X^{-1}\}$

- So come sono i gruppi generati da un elemento (i ciclici) ma non ho davvero info sui gruppi generati da più elementi

- Vale che $(\mathbb{Z},+)=\langle 1\rangle$ ma $(\mathbb{Z},+)=\langle 2,3\rangle$ (per Bezout $\exists\, a,b\in\mathbb{Z} \mid 1=2a+3b$ e se $1$ è comb. lin ottengo anche gli altri.

## Esercizio 1: $|\mathrm{Aut}(\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})|=?$

Voglio sapere quanti sono gli omomorfismi $f:\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\longrightarrow\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$, per farlo definisco $f$ su un insieme di generatori $\{(1,\bar0),(0,\bar1)\}$. In questo caso $(1,\bar0),(0,\bar1)$ commutano ($\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ è abeliano), voglio che $f((1,\bar0)),f((0,\bar1))$ commutino ma questo non mi dà problemi.

Definisco l'omomorfismo $f:\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\longrightarrow\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$, voglio capire quante

$$(1,\bar0)\longmapsto(a,\bar b)$$
$$(0,\bar1)\longmapsto(c,\bar d)$$

sono le scelte a disposizione:

- $\mathrm{ord}(1,\bar0)=+\infty \Rightarrow \mathrm{ord}(a,\bar b)=+\infty \Rightarrow a\neq0$
  $\mathrm{ord}(0,\bar1)=5 \Rightarrow \mathrm{ord}(c,\bar d)=5 \Rightarrow c=0\quad d\neq0$

- $f$ omo $f(x_1,y_1)+f(x_2,y_2)=f(\alpha_1(1,\bar0)+\beta_1(0,\bar1))+f(\alpha_2(1,\bar0)+\beta_2(0,\bar1))=(\alpha_1(a,\bar b)+\beta_1(0,\bar d)+\alpha_2(a,\bar b)+\beta_2(0,\bar d)=(\alpha_1+\alpha_2)(a,\bar b)+(\beta_1+\beta_2)(0,\bar d)=f(x_1+x_2,y_1+y_2)$

- $f$ inj $(x,y)\in\ker f \iff f(x,y)=(0,0)$ ovvero $f(\alpha(1,\bar0)+\beta(0,\bar1))=\alpha f(1,\bar0)+\beta f(0,\bar1)=\alpha(a,\bar b)+\beta(0,\bar d)=(\alpha a,\alpha\bar b+\beta\bar d)=(0,0)$
  $\iff \alpha=0\wedge\beta=0$. Dunque $\ker f=\{(0,0)\}$

- $f$ surj $\iff (1,\bar0),(0,\bar1)\in\mathrm{Imm}\,f$ dunque voglio $(x_1,y_1)\mid f((x_1,y_1))=(1,\bar0)$ e $(x_2,y_2)\mid f((x_2,y_2))=(0,\bar1)$. ovvero
  $f((x_1,y_1))=f(\alpha_1(1,\bar0)+\beta_1(0,\bar1))=(\alpha_1 a,\overline{\alpha b+\beta d})=(0,\bar1)$
  $f((x_2,y_2))=f(\alpha_2(1,\bar0)+\beta_2(0,\bar1))=(\alpha_2 a,\overline{\alpha_2 b+\beta_2 d})=(1,\bar0)$

$$\Rightarrow\begin{cases}\alpha a=0\\ \alpha b+\beta d\equiv1\ (5)\end{cases}\longrightarrow\begin{cases}\forall a\in\mathbb{Z}\\ \beta d\equiv1\ (5)\Rightarrow d\text{ invertibile}\Rightarrow d\in\mathbb{Z}/5\mathbb{Z}\setminus\{\bar0\}\end{cases}$$

$$\Rightarrow\begin{cases}\alpha a=1\\ \alpha b+\beta d\equiv0\ (5)\end{cases}\longrightarrow\begin{cases}a=1/\alpha\in\mathbb{Z}\Rightarrow a=\pm1\\ \forall b,d\in\mathbb{Z}/5\mathbb{Z}\quad d\neq\bar0\end{cases}$$

questo significa che: $a=\pm1$ (2 scelte), $b=0,1,2,3,4$ (5 scelte), $c=0$ (1 scelta), $d=1,2,3,4$ (4 scelte)

perciò ho $2\cdot5\cdot1\cdot4=40$ isomorfismi

## Esercizio 2: Definisci gli omomorfismi $f:D_n\longrightarrow G$

Sia $f:D_n\longrightarrow G$. Dato che $D_n=\langle r,s\rangle$ devo definire l'omomorfismo sui generatori dunque voglio che vengano rispettate le seguenti proprietà

(i) $f(r)=g_1 \mid g_1^n=e$
(ii) $f(s)=g_2 \mid g_2^n=e$
(iii) $g_1g_2=g_2g_1^{-1}$

## Esercizio 3: Sia $f$ come nell'es. 2. Cosa succede se $G$ è abeliano?

Per il 1th omo $\frac{D_n}{\ker f}\cong\mathrm{Imm}\,f\le G \Rightarrow \frac{D_n}{\ker f}\hookrightarrow G \Rightarrow \frac{D_n}{\ker f}$ è abeliano

ma $\frac{D_n}{\ker f}$ è abeliano $\iff D_n'=\{ghg^{-1}h^{-1}\mid g,h\in D_n\}\subseteq\ker f$ ← moralmente se $x\neq e\Rightarrow gh\neq hg$ quindi prendo gli el. di $D_n$ che non commutano e li mando a $0$

Dunque $G$ abel $\Rightarrow D_n'\le\ker f$.

Ma in $D_n$ so com'è fatto il gruppo dei commutatori: $D_n'=\{r^\alpha s r^{-\alpha}s\}$ ← noto che ho a comb. di $r^\alpha, sr^\alpha$ che portano comunque a $r^\alpha sr^{-\alpha}s$

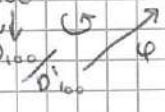
però $r^\alpha sr^{-\alpha}s=r^{2\alpha}\Rightarrow\langle r^2\rangle\le D_n'\le\langle r\rangle$

- Caso n dispari: $(n,2)=1 \Rightarrow \langle r^2\rangle$ genera $\Rightarrow \langle r^2\rangle = \langle r\rangle \Rightarrow \langle r\rangle \leq D_n' \leq \langle r\rangle$
  dunque $|D_n/D_n'| = 2$ ovvero $D_n/D_n' = \{e\langle r\rangle, s\langle r\rangle\}$

- Caso n pari: so che (lezione 06/10) che $D_n/D_n'$ è il più grande sgr. abel
  $\Rightarrow$ voglio $D_n'$ "il più piccolo possibile"
  $D_n/\langle r^2\rangle$ è abeliano perché $|D_n/\langle r\rangle| = 4$ e i gruppi di cardinalità $p^2$ sono abeliani. dunque $D_n/\langle r^2\rangle$ sarebbe un sgr abel di $D_n$ più grande di $D_n/D_n' \Rightarrow D_n' = \langle r\rangle$

**Esercizio 4:** Conta gli omomorfismi: $f: D_{100} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} =: G$

Dato che $G$ è abeliano $\Rightarrow D_{100}' \subseteq \ker f$, dunque voglio contare gli $f$ con questa proprietà.
Per 1° th omo $\forall f\ \exists!\ \varphi \mid$




dunque posso contare le $\varphi$.

Dato che n è pari, $D_{100}' \cong \langle r^2\rangle$ e $|D_{100}/\langle r^2\rangle| = 4$, dunque $D_{100}/\langle r^2\rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
ma $D_{100}/\langle r^2\rangle = \{e\langle r^2\rangle, s\langle r^2\rangle, r\langle r^2\rangle, sr\langle r^2\rangle\}$ dunque ho 3 el di ordine 2
$\Rightarrow D_{100}/\langle r^2\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Perciò posso contare $\bar\varphi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow G$.
Controllo dove posso mandare i generatori $\bar\varphi((\bar1,\bar0)) = (0,0,0,a,b)$ (non ho el di ord 2 in $\mathbb{Z}/5\mathbb{Z}$) e $\bar\varphi((\bar0,\bar1)) = (0,0,0,c,d)$.
$a, c \in \mathbb{Z}/4\mathbb{Z}$ ma voglio che $\mathrm{ord}(a) \mid 2$ e $\mathrm{ord}(c) \mid 2 \Rightarrow$ ho 2 scelte per $a, c$
$b, d \in \mathbb{Z}/2\mathbb{Z}$ dunque ho 2 scelte per $b, d$
$\Rightarrow 2\cdot2\cdot2\cdot2 = 16$ scelte. ← devo controllare che siano davvero tutti omo

**Esercizio 5:** $\mathrm{Aut}(D_n) \cong ?$

Innanzitutto $\mathrm{Aut}(D_n) = \{\varphi_{ij}: D_n \longrightarrow D_n \mid r \longmapsto r^i \text{ con } (i,n)=1 \ \wedge\ s \longmapsto sr^j \text{ con } j \in \{0,\dots,n-1\}\}$

Siano $N = \langle \varphi_{1,j}\rangle$, $H = \langle \varphi_{i,0}\rangle$. $N, H \leq \mathrm{Aut}(D_n)$

- $id \in N$, infatti: $id = \varphi_{1,0}$ ; $id \in H$, infatti: $id = \varphi_{1,0}$
- $\varphi_{1,j} \in N \Rightarrow \varphi_{1,j}^{-1} \in N$, infatti: $\varphi_{1,j}^{-1} = \varphi_{1,-j}$ ; $\varphi_{i,0} \in H \Rightarrow \varphi_{i,0}^{-1} \in H$, infatti: $\varphi_{i,0}^{-1} = \varphi_{i^{-1},0}$
- $\varphi_{1,j}, \varphi_{1,k} \in N \Rightarrow \varphi_{1,j} \circ \varphi_{1,k} \in N$, infatti: $\varphi_{1,j} \circ \varphi_{1,k} = \varphi_{1,j+k}$ ; $\varphi_{i,0}, \varphi_{k,0} \in H \Rightarrow \varphi_{i,0} \circ \varphi_{k,0} \in H$, infatti: $\varphi_{i,0} \circ \varphi_{k,0} = \varphi_{ik,0}$

Ora noto che

(ii) $NH = \mathrm{Aut}(D_n)$, infatti: $\varphi_{i,j} = \varphi_{i,0} \circ \varphi_{1,j}$
(iii) $N \cap H = \{id\} = \{\varphi_{1,0}\}$ ovvio
(i) $N \trianglelefteq \mathrm{Aut}(D_n)$
Sia $f \in \mathrm{Aut}(D_n)$, noto che $f = \varphi_{i,0} \circ \varphi_{1,j}$. Prendo un $\varphi_{1,k} \in N$
$f \circ \varphi_{1,k} \circ f^{-1} = \varphi_{i,0} \circ \varphi_{1,j} \circ \varphi_{1,k} \circ (\varphi_{i,0} \circ \varphi_{1,j})^{-1} = \varphi_{i,0} \circ \underbrace{\varphi_{1,j} \circ \varphi_{1,k} \circ \varphi_{1,j}^{-1}}_{\in N,\ \text{lo chiamiamo } \varphi_{1,a}} \circ \varphi_{i,0}^{-1} =$
$= \varphi_{i,0} \circ \varphi_{1,a} \circ \varphi_{i,0} = \varphi_{1,a}$

$\Rightarrow \mathrm{Aut}(D_n) \cong N \rtimes_\psi H$ con $\psi: H \longrightarrow \mathrm{Aut}(N)$ perché ho le hp teo dec. prod semid
$\varphi_{i,0} \longmapsto \varphi_{i,0} \circ \varphi_{1,j} \circ \varphi_{i,0}^{-1}$
$s \longmapsto sr^j$

Ma $H \cong \mathbb{Z}/n\mathbb{Z}^*$ perché ho $\varphi(n)$ scelte per $i$
$N \cong \mathbb{Z}/n\mathbb{Z}$ perché è un gruppo ciclico di ord $n$
$\Rightarrow \mathrm{Aut}(D_n) \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\gamma \mathbb{Z}/n\mathbb{Z}^*$ con $\gamma: \mathbb{Z}/n\mathbb{Z}^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$
$i \longmapsto f_i: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$
$1 \longmapsto i$

**Esercizio 6:** Sia $G$ gruppo $|G| = p^n \Rightarrow G$ ammette una serie normale, ovvero
$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$ con $G_i \trianglelefteq G$ $\forall i$ $|G_i/G_{i-1}| = p$ $\forall i > 0$

- Base $n=0 \Rightarrow |G| = 1$ $G_0 = \{e\} = G$, $G_0 \trianglelefteq G$
- PI. dato che $G$ è $p$-gruppo, $Z(G)$ è non banale, dunque per Cauchy $\exists x \in Z(G) \mid$ $\mathrm{ord}(x) = p$. Dunque $|\langle x\rangle| = p$ e $\langle x\rangle \trianglelefteq G$ perché $x \in Z(G)$
  $\Rightarrow |G/\langle x\rangle| = p^{n-1}$ e per hp ind. $\exists$ serie normale

  $G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_{n-1} = G/\langle x\rangle$ $f_i \trianglelefteq G/\langle x\rangle$ $\forall i$ $|G_i/G_{i-1}| = p$

  Noto che $\pi: G \longrightarrow G/\langle x\rangle$ è surj $\Rightarrow$ per corrispondenza ho una corrispondenza biiettiva fra i sottogruppi di $G$ e di $G/\langle x\rangle$ che mantiene normalità e indice

dunque $\{e\} = G_0 \trianglelefteq G_1 = \pi^{-1}(G_0) \trianglelefteq \dots \trianglelefteq \pi^{-1}(G_{n-2}) = G_{n-1} \trianglelefteq \pi^{-1}(G_{n-1}) = G_n = G$

# Algebra Lezione 15/10/25 (teoria - Del Corso)

- **Lemma $\forall d\ \exists H$**: Sia $G$ gruppo abeliano, $|G| = n \Rightarrow \forall d | n\ \exists H \leq G \mid |H| = d$

→ **Dim** • caso $d = p^k$ per es. 6 (lezione 13/10) $\forall i < k\ \ |H_i| = p^i$

• caso $d = p_1^{k_1} \cdots p_s^{k_s}$ $\forall i\ \ |H_i| = p_i^{k_i}$ (prendiamo il generato degli el di ord $p_i$, se non avesse ord $p_i^{k_i}$ potrei quozientare per $p_i$ e avrei un el di ord $p_i$ nel quoziente

Dunque $H_1, H_2 \leq G$ perché normali (in quanto $G$ abel, inoltre $|H_1 \cap H_2| = 1 \Rightarrow |H_1 H_2| = p_1^{k_1} p_2^{k_2}$.
Per induzione $|H_1 \dots H_2| = d$

- se $G$ non è abeliano non è detto che $\forall d | n\ \exists H \leq G \mid |H| = d$. Infatti: $A_4$ non ha sottogruppi di ord 6 e $S_5$ non ha sgr di ord 40

Per Poincaré se ho un gruppo di ord 40 $\Rightarrow$ o $H \trianglelefteq S_5$ o $K \trianglelefteq S_5$ con $K \leq H$ di ordine 20. Ma io so chi sono i gruppi normali in $S_5$ é.

Sia $H \leq A_4$ $|H| = 6 \Rightarrow H \trianglelefteq A_4$ ma per Cauchy $\exists x \mid \text{ord}(x) = 2 \Rightarrow$ $x = (a\ b)(c\ d)$. Ma dato che $H \trianglelefteq A_4$ $Cl_{A_4}(x) \subset H$. Ma $Cl_{A_4}(x) = V - \{e\}$
Noto che $Cl_{A_4}(x) = Cl_{S_4}(x)$ (per questioni di cardinalità) $\Rightarrow Cl_{A_4} \cup \{e\} \subset H$
$\Rightarrow V < H$ ma $4 \nmid 6$ ↯

- **Definizione p-Sylow**: Sia $G$ gruppo, $|G| = p^n m$ con $n \geq 1$ $p$ primo $(p, m) = 1 \Rightarrow$ $H \leq G \mid |H| = p^n$ viene detto $p$-Sylow

- **Teorema di Sylow**: Sia $G$ gruppo, $|G| = p^n m$ con $n \geq 1$ $p$ primo $(p, m) = 1 \Rightarrow$

esistenza → (i) $\forall i \leq n\ \exists H \leq G \mid |H| = p^i$
inclusione → (ii) $\forall H \leq G$ di questa forma, $\exists H' > H \mid [H' : H] = p$ (ogni $p$-sgr è contenuto in un $p$-Sylow)
coniugio → (iii) Tutti i $p$-Sylow di $G$ sono coniugati
numero → (iv) Sia $n_p$ il numero di $p$-Sylow $\Rightarrow n_p \equiv 1\ (p)$, $n_p = [G : N(S)] \Rightarrow n_p | m$ (un qualsiasi $p$-Sylow fissato $p$)

→ **Dim** Innanzitutto ricordo che:

1. $|X| = \sum_{x \in R} |\text{Orb}(x)| = \sum_{x \in R} \frac{|G|}{|\text{St}(x)|}$ (Lezione 01/10 formula Burnside)
2. Sia $X$ insieme, $G$ gruppo $G \curvearrowright X$, chiameremo $\text{Fix}_G(X) = \{x \in X \mid \forall g \in G, \phi_g(x) = x\}$
3. Sia $G$ $p$-gruppo $|X| \equiv |\text{Fix}_G(X)|\ (p)$
   • infatti per (1) $|X| = \sum_{x \in R} \frac{|G|}{|\text{St}(x)|} = |\text{Fix}_G(X)| + \sum_{x \in R, x \notin \text{Fix}_G(X)} \frac{|G|}{|\text{St}(x)|}$ (perché per la rel definita tutti gli $x \in \text{Fix}_G(X) \subset R$ e $\frac{|G|}{|\text{St}(x)|} = 1$ per quegli $x$)
   ma $\sum_{x \in R, x \notin \text{Fix}_G(X)} \frac{|G|}{|\text{St}(x)|} \equiv 0\ (p)$

(i)+(ii) Per Cauchy $\exists H < G$ $p$-gruppo. sia $X = G/H$, $H$ agisce su $X$ per moltiplicazione sx. Dunque $g \in \text{Fix}_H(X) \iff \forall h \in H$, $hgH = gH \iff \forall h \in H$, $g^{-1}hg \in H \iff g \in N_G(H)$. Ma quindi $\text{Fix}_H(X) = N_G(H)/H$.

$\varphi : H \to S(G/H)$, $h \mapsto \varphi_h$, $\varphi_h : G/H \to G/H$, $gH \mapsto hgH$

Se $|H| = p^\alpha$, $\alpha < n \Rightarrow p | [G : H] = X$ ma per (3)

$0 \equiv |X| \equiv [G : H] \equiv |\text{Fix}_H(X)| \equiv |N_G(H)/H|\ (p)$
$\Rightarrow p | |N_G(H)/H|$, chiaramente $H \trianglelefteq N_G(H)$ ma per Cauchy ho un elemento di ord $(x) = p$ in $N(H)/H$, dunque $\exists K \leq N_G(H) \mid |K/H| = p \Rightarrow |K| = p^{\alpha+1}$

(iii) Siano $P_1, P_2$ $p$-Sylow di $G$ $X = G/P_1$; allora $P_2$ agisce su $X$ per coniugio dato che $P_2$ è $p$-gruppo per (3) $|X| \equiv |\text{Fix}_{P_2}(X)|\ (p)$ ma $|X| \not\equiv 0\ (p) \Rightarrow$ $|\text{Fix}_{P_2}(X)| \not\equiv 0\ (p)$. Sia dunque $gP_1 \in \text{Fix}_{P_2}(X) \Rightarrow \forall h \in P_2$, $hgP_1 = gP_1 \iff$ $g^{-1}hg \in P_1 \iff P_2 = gP_1g^{-1}$

(iv) Sia $P$ un $p$-Sylow, $\text{Syl}_p(G)$ l'insieme dei $p$-Sylow di $G \Rightarrow$ $\text{Syl}_p(G) = \text{Orb}_{\text{per coniugio}}(P) \Rightarrow n_p = |\text{Syl}_p(G)| = |G : N_G(P)| \Rightarrow n_p | |G|$

Sia $Q$ un altro $p$-Sylow $\text{Orb}(Q) = \{gQg^{-1} \mid g \in P\} = Q \iff P \subset N_G(Q)$
$\Rightarrow PQ$ è gruppo $\Rightarrow |PQ| = \frac{|P||Q|}{|P \cap Q|} \geq p^n \Rightarrow |PQ| = p^n \Rightarrow P = Q$
ma per (1) $n_p = |\text{Syl}(G)| = \sum_{x \in P} |\text{Orb}(x)| = 1 + \sum_{x \in R, x \notin P} \frac{|P|}{|\text{St}(x)|} \equiv 1\ (p)$

- Corollario Sylow di G abeliano: Ogni gruppo abeliano è prodotto diretto dei suoi p-Sylow

→ Dim per Lemma $\forall d \mid |G| = p_1^{k_1} \cdots p_s^{k_s}$ $\exists H_1, \dots, H_s$ | $|H_i| = p_i^{k_i}$. Noto che
(i) $H_i \trianglelefteq G$ perché G abel
(ii) $H_1 \cdots H_s = G$
(iii) $H_1 \cap \dots \cap H_s = \{e\}$
Segue per teorema dec. prod dir.

## Algebra Lezione 17/10/25 (teoria/esercitazione - Del Corso)

**Esercizio 1:** Chi sono i gruppi di ordine 12?

Sia $G \mid |G| = 12$. Allora $|P_2| = 4$ e $|P_3| = 3$. Noto quindi che $P_2 \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases}$
$P_3 \cong \mathbb{Z}/3\mathbb{Z}$. (ii) $|P_2 P_3| = \frac{|P_2||P_3|}{|P_2 \cap P_3|} = \frac{4 \cdot 3}{1} = 12 = |G| \Rightarrow P_2 P_3 = G$

(iii) $P_2 \cap P_3 = \{e\}$

(i) Se $P_3 \trianglelefteq G \Rightarrow G \cong P_3 \rtimes_\varphi P_2$ } per teo dec prod semidir.
Se $P_2 \trianglelefteq G \Rightarrow G \cong P_2 \rtimes_\varphi P_3$

Questo significa che ho 2 casi: $P_3 \trianglelefteq G$ o $P_3 \not\trianglelefteq G$

→ caso $P_3 \trianglelefteq G$; dunque $P_3 \rtimes_\varphi P_2$, definiamo $\varphi: P_2 \longrightarrow Aut(P_3)$

→ caso $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ $\varphi: \mathbb{Z}/4\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z})$
ho 2 mappe a. $1 \longmapsto \varphi_0$ $1 \mapsto 1$
b. $1 \longmapsto \varphi_2$ $1 \mapsto 2$

per la mappa a $\varphi_1 = id$ ottengo $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}$
per la mappa b $\varphi_2$ ottengo $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

→ caso $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\varphi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$
a. $(1,0) \mapsto 0$ $(0,1) \mapsto 0$
b. $(1,0) \mapsto 0$ $(0,1) \mapsto 1$
c. $(1,0) \mapsto 1$ $(0,1) \mapsto 0$
d. $(1,0) \mapsto 1$ $(0,1) \mapsto 1$

per la mappa a ottengo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$
le mappe b, c, d mi portano a gruppi isomorfi
infatti preso $z \in \mathbb{Z}/3\mathbb{Z}$ $\varphi_{(1,0)}(z) = id(z)$
$\varphi_{(0,1)}(z) = -id(z)$
ottengo $D_3$ "muovendo" un generatore e "tenendo fermo" l'altro. Nel caso $(1,0) \mapsto 1$, $(0,1) \mapsto 1$ ho $(1,1) \mapsto 0$ quindi prendo come generatori $\{(1,0), (1,1)\}$
ma quindi: ottengo che $\langle (1,0), z \mid (1,0)^2 = 0, z^3 = 0, \varphi_{(1,0)}(z) = -z \rangle \cong D_3$
dunque le mappe b, c, d mi danno $\mathbb{Z}/2\mathbb{Z} \times D_3$

→ caso $P_3 \not\trianglelefteq G$ per (iv) del teorema di Sylow $n_3 = 1, 4$ ma $P_3 \not\trianglelefteq G \Rightarrow n_3 = 4$ ma quindi ci sono $2 \cdot 4 = 8$ elementi di ordine 3 in G. Dunque restano $12 - 8 = 4$ elementi e dato che $P_2 \cap P_3 = \{e\}$ appartengono tutti e 4 a $P_2 \Rightarrow P_2 \trianglelefteq G$ dunque $P_2 \rtimes_\varphi P_3$

→ caso $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ $\varphi: \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ ho solo la mappa identità con la quale ottengo nuovamente $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

→ caso $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\varphi: \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$
a. $1 \longmapsto id$
b. $1 \longmapsto (1\,2\,3)$
c. $2 \longmapsto (1\,3\,2)$

per la mappa a ottengo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ che ho già
le mappe b, c mi portano a gruppi isomorfi
per Cayley $G \longrightarrow S_4$, prendo $\phi: G \longrightarrow S_4$ che mi commuta; 4 3-Sylow e per teorema $\frac{G}{\ker\phi} \cong Imm\,\phi$; $\ker\phi = \{e\}$, dunque
$|G| = |Imm\,\phi| = 12$ e $Imm\,\phi < S_4 \Rightarrow Imm\,\phi = A_4$

dunque $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \cong A_4$

- **Teorema Cayley**: $\forall G$ gruppo, $\exists n \mid G \cong S_n$. In particolare $|G|=n \Leftrightarrow G \hookrightarrow S_n$

→ **Dim** $\lambda: G \longrightarrow \mathcal{S}(G)$ ← rappresentazione regolare a sx di $G$
$g \longmapsto \varphi_g: G \longrightarrow G$
$x \longmapsto gx$

- $\lambda$ ben def: $\varphi_g$ inj perché $\ker \varphi_g = \{g^{-1}\}$; $\varphi_g$ surj perché $\forall y \in G \ \exists x := g^{-1}y \mid \varphi_g(x) = y$ $\Rightarrow \varphi_g \in \mathcal{S}(G)$
- $\lambda$ omo: $\lambda(g_1 g_2) = \varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2} = \lambda(g_1)\lambda(g_2)$
  ↳ $\varphi_{g_1 g_2}(x) = g_1 g_2 x = \varphi_{g_1} \circ \varphi_{g_2}(x)$
- $\lambda$ inj: $\ker \lambda = \{g \in G \mid \lambda(g) = \varphi_g = id\} = \{e\}$
- $|G|=n$ per Fth omo $G/\ker\lambda \cong \operatorname{Imm}\lambda \leq S_n$

**Esercizio 2**: $H < S_n \Rightarrow [H : H \cap A_n] = \leq 2$

Dato che $H \leq S_n$ $\exists f: H \longrightarrow S_n$ e $\pi: S_n \longrightarrow S_n/A_n$; dunque
$\varphi = \pi \circ f: H \longrightarrow S_n/A_n$.
Per 1° Fth omo $H/\ker\varphi \cong \operatorname{Imm}\varphi < S_n/A_n$. Chiaramente $\ker\varphi = H \cap A_n$
e $|S_n/A_n| = 2$. Dunque $|H/H\cap A_n| = |\operatorname{Imm}\varphi| = \leq 2$ (i divisori di 2)

**Esercizio 3**: Sia $G$ gruppo $|G| = 2d$ con $d \geq 1$ $(2) \Rightarrow \exists H \trianglelefteq G \mid |H| = d$

Per Cayley $\lambda: G \longrightarrow S_{2d}$ inj poi ho la proiezione $\pi: S_{2d} \longrightarrow S_{2d}/A_{2d}$ surj
$\Rightarrow \varphi: G \longrightarrow S_{2d}/A_{2d}$ per quanto detto nell'esercizio 2 $|G/G\cap A_n| = 1, 2$

ma $G \leq S_{2d}$, $H = G \cap A_{2d} \subsetneq G$, dunque ho un $x \in G - A_{2d} \mid ord(x) = 2$ per Cauchy che è dispari, dunque $|H| = d$
Infine $H \trianglelefteq G$ perché ha indice 2 per Gemma $|H| = 2$ (lezione 29/09)

**Esercizio 4**: Chi sono i gruppi di ordine 30?

Sia $G \mid |G| = 30$. per es 3 $\exists N \trianglelefteq G \mid |N| = 15$, per Cauchy $\exists x \in G - N \mid ord(x) = 2$
A questo punto noto che $N \cong \mathbb{Z}/15\mathbb{Z}$ per il teorema dei gruppi di ordine pq (se $p \nmid q-1 \Rightarrow G$ ciclico)
e $P_2 = \langle x \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Dunque (i) $N \trianglelefteq G$
(ii) $NP_2 = G$ $\Rightarrow$ per th dec prod semidir $G \cong N \rtimes_\varphi P_2$
(iii) $N \cap P_2 = \{e\}$

definisco $\varphi: \mathbb{Z}/2\mathbb{Z} \longrightarrow \operatorname{Aut}(\mathbb{Z}/15\mathbb{Z})$
$1 \longmapsto \varphi_k: \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$
$x \longmapsto x^k$

ma $ord(1) = 2 \Rightarrow ord(\varphi_k) \mid 2 \Rightarrow \varphi_k^2(x) = x$ ovvero $\varphi_k(\varphi_k(x)) = \varphi_k(x^k) = (x^k)^k = x^{k^2} = x$
dunque voglio: $k \mid k^2 \equiv 1 \ (15)$ (piccolo teorema di Fermat)
perciò ottengo $k \equiv \pm 1, \pm 4 \ (15)$. Dunque ho i seguenti possibili isomorfismi

$\varphi(1) = \varphi_1: x \longmapsto x' \Rightarrow \varphi = id$ perciò ho $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z}$
$\varphi(-1) = \varphi_{-1}: x \longmapsto x^{-1} \Rightarrow k x k^{-1} = x^{-1}$ ovvero sto descrivendo $D_{15}$
$\varphi(4) = \varphi_4: x \longmapsto x^4 \Rightarrow k x k^{-1} = x^4$ ovvero sto descrivendo $D_5 \times \mathbb{Z}/3\mathbb{Z}$
$\varphi(-4) = \varphi_{-4}: x \longmapsto x^{-4} \Rightarrow k x k^{-1} = x^{-4}$ ovvero sto descrivendo $D_3 \times \mathbb{Z}/5\mathbb{Z}$

non sono isomorfi perché hanno centri diversi

## Algebra Lezione 20/10/25 (esercitazione - Del Corso)

**Esercizio 1**: Sia $G$ gruppo, $H < G$, $[G:H] = p$ con $p = \min\{q \text{ primo} \mid q \mid |G|\} \Rightarrow H \trianglelefteq G$

Prendiamo $X = \{g_1 H, \dots, g_p H, H\}$ (insieme degli H-laterali). Facciamo agire $G$ su $X$ per moltiplicazione a sx:
$G \circlearrowright X$ ovvero $\varphi: G \longrightarrow \mathcal{S}(X) \cong S_p$ perché ho $p$ elementi
$g \longmapsto \varphi_g: X \longrightarrow X$
$g_i H \longmapsto g g_i H$

Nel compito devo verificare
- $\varphi$ b.d. ovvero verifico $\varphi_g$ bij
- $\varphi$ inj

Sia $\psi: H \longrightarrow \mathcal{S}(X) \cong S_{p-1}$ perché fisso $H \mapsto H$ la restrizione di $\varphi$. $\ker\psi \trianglelefteq H$ e per Fthomo
$h \longmapsto \varphi_h: X \longrightarrow X$
$g_i H \longmapsto h g_i H$

$H/\ker\psi \cong \operatorname{Imm}\psi < S_{p-1} \Rightarrow [H : \ker\psi] \mid (p-1)!$ Ma $H/\ker\psi < G \Rightarrow |H/\ker\psi| \mid |G|$.
Ma $p = \min\{\dots\} \Rightarrow 1, \dots, p-1 \nmid |G| \Rightarrow MCD((p-1)!, |G|) = 1$ dunque $[H : \ker\psi] = 1$

Dunque $\varphi_h(gH) = hgH = gH$ perciò $hgeg^{-1}H \Rightarrow \forall h \in H \quad hgHg^{-1} \Rightarrow Hg \subseteq gHg^{-1}$
$\Rightarrow H \trianglelefteq G$. Noto che $\ker\varphi = \{g \in G \mid gg_iH = g_iH, \forall H \in H\}$

- **Teorema di Poincaré**: Sia $G$ gruppo, $H < G$ $[G:H] = n \Rightarrow \exists N \trianglelefteq G \quad N \subseteq H \mid [G:N] \mid n!$

→ **Dim** Sia $X = \{x_1H, \dots, x_{n-1}H, H\}$ $\varphi: G \longrightarrow S(X) \cong S_n$
$g \longmapsto \varphi_g : X \longrightarrow X$
$xH \longmapsto gxH$

Scelgo $N = \ker\varphi$. Dunque per 1° th omo $G/\ker\varphi \hookrightarrow S_n$

Noto che $\ker\varphi = \{g \in G \mid gxH = xH\} \Rightarrow g \in \ker\varphi \quad gH = H \Rightarrow g \in H$
Dunque $N \trianglelefteq G$, $N \subseteq H$ e per def $[G:N] \mid |S_n| = n!$
(↑ perché $\ker\varphi$)

- **Definizione semplice**: Sia $G$ gruppo, diremo che $G$ è semplice se i suoi unici sottogruppi normali sono $\{e\}$ e $G$

**Esercizio 2**: Sia $G$ gruppo semplice, $H < G \mid [G:H] = n \geq 3 \Rightarrow \varphi: G \hookrightarrow A_n$

Costruisco $G \xhookrightarrow{\varphi} S_n \xrightarrow{\pi} S_n/A_n$, $\bar{\varphi}$

Noto che $\ker\bar{\varphi} = G \cap A_n \trianglelefteq G$. Dunque $\begin{cases} G \cap A_n = G \Rightarrow G \subseteq A_n \\ G \cap A_n = \{e\} \Rightarrow 1° \text{ th omo } G/\ker\bar{\varphi} \cong \operatorname{Imm}\bar{\varphi} = S_n/A_n \\ \Rightarrow |G| = 2 \not\geq \end{cases}$

**Esercizio 3**: Sia $G$ gruppo, $|G| = 112 \Rightarrow G$ non è semplice

Noto che $112 = 2^4 \cdot 7$ Se $G$ è semplice per es 2 $\Rightarrow G \hookrightarrow A_7$. Prendo $p_2$ (so che esiste e ho $[G:p_2] = 7$, dunque $G \hookrightarrow A_7 \Rightarrow |G| \mid \frac{7!}{2}$ ↯ (in $G$ ho un el $2^4$ ma in $A_7$ il max è $2^3$)

**Esercizio 4**: $(\mathbb{Z}/n\mathbb{Z})^*$ è ciclico $\Leftrightarrow n = 2, 4, p^n, 2p^n$ ($p$ primo dispari)

Ho due casi $n = \underbrace{ab}_{\text{(iii)}}, \underbrace{a,b>2}_{\text{(i)}} \underbrace{(a,b)=1}_{\text{(ii)}}$ $\underbrace{2^k, p^n, 2p^n}_{\text{(iv)}}$ (ho solo questi perché i primi 3 non hanno 2 fattori diversi e $2p^n$ ha 2 e $a,b>2$)

(i) Se $n = ab$ $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ e so che $|(\mathbb{Z}/a\mathbb{Z})^*| = \phi(a)$ e $|(\mathbb{Z}/b\mathbb{Z})^*| = \phi(b)$. Dunque
$x^2 \equiv 1 \ (n) \xRightarrow[\text{↑TCR}]{} \begin{cases} x^2 \equiv 1 \ (a) \\ x^2 \equiv 1 \ (b) \end{cases} \Rightarrow \begin{cases} x \equiv \pm 1 \ (a) \\ x \equiv \pm 1 \ (b) \end{cases}$ ho almeno 3 el di ordine 2 ma in un gruppo ciclico ce ne sono $\phi(2) = 1 \Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ non è ciclico

(ii) Se $n = 2^k$ con $k \geq 3$

$\pi: \mathbb{Z}/2^k\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z}$ è surj perché proiezione al quoziente
($\mathbb{Z}/2^k\mathbb{Z} = \mathbb{Z}/2^n\mathbb{Z}$ $n = k+3$)

noto che questa funzione "manda i pari nei pari" e "i dispari nei dispari"
ma quindi $\pi' = \pi_{|(\mathbb{Z}/2^k\mathbb{Z})^*} : (\mathbb{Z}/2^k\mathbb{Z})^* \longrightarrow (\mathbb{Z}/8\mathbb{Z})^*$ ha la stessa definizione
(↑ sto togliendo i pari e mandoli dispari dove li mandava prima)

Ma quindi per 1° th omo $(\mathbb{Z}/2^k\mathbb{Z})^*/\ker\pi' \cong \operatorname{Imm}\pi' = (\mathbb{Z}/8\mathbb{Z})^*$ (↑ perché surj)
ma $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow (\mathbb{Z}/8\mathbb{Z})^*$ non è ciclico $\Rightarrow \frac{(\mathbb{Z}/2^k\mathbb{Z})^*}{\ker\pi'}$ non è ciclico $\Rightarrow (\mathbb{Z}/2^k\mathbb{Z})^*$ non è ciclico

(iii) $(\mathbb{Z}/2\mathbb{Z})^* = \{e\}$ che è ciclico $(\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ che è ciclico

(iv) Se $n = p^n$

Allora $|(\mathbb{Z}/p^n\mathbb{Z})^*| = \phi(p^n) = (p^n - p^{n-1}) = p^{n-1}(p-1)$

$\pi: \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p^n\mathbb{Z}/\mathbb{Z}/p^{n-1}\mathbb{Z}$ come prima $\pi' = \pi_{|(\mathbb{Z}/p^n\mathbb{Z})^*} : (\mathbb{Z}/p^n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$
$[a]_{p^n} \longmapsto [a]_p$

questo perché se $[a]_{p^n} \in (\mathbb{Z}/p^n\mathbb{Z})^* \Rightarrow (a,p) = 1$ dunque ho $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^*$
$(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/p-1\mathbb{Z}$ che è ciclico ma quindi: $\langle a \rangle = \mathbb{Z}/p-1\mathbb{Z}$

sia $[a]_{p^n} \in (\mathbb{Z}/p^n\mathbb{Z})^* \mid \pi([a]_{p^n}) = a$. Ma quindi $(p-1) \mid ord([a]_{p^n})$
ma $ord([a]_{p^n}) \mid p^{n-1}(p-1) \Rightarrow ord([a]_{p^n}) = p-1$

Noto che $1+p$ ha ordine $p^{n-1}$. Infatti: $(1+p)^{p^{n-1}} \equiv 1 + p^n \ (p^{n+1})$

- Base $k=1$ $(1+p)^{p^0} \equiv 1+p \ (p^2)$
- P. I. $(1+p)^{p^k} \equiv ((1+p)^{p^{k-1}})^p \overset{hp\ ind}{\equiv} (1+p^k+ap^{k+1})^p = (1+p^k(1+ap))^p = \sum_{i=0}^{k} \binom{p}{i} p^{ik}(1+ap)^i$
$\equiv 1 + p^{k+1}(1+ap) + \dots + p^{2k}(1+ap)^k \equiv 1 + p^{k+1} \ (p^{k+2})$
($p^{k+2}(\dots) \equiv 0$)

Ma quindi dato che ho $x \mid ord(x) = p-1$ e $y \mid ord(y) = p^{n-1}$ allora $ord(xy) = p^{n-1}(p-1) \Rightarrow (\mathbb{Z}/p^n\mathbb{Z})^*$ è ciclico

(v) Se $n = 2p^n$ $(\mathbb{Z}/2p^n\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^n\mathbb{Z})^* \cong \{e\} \times (\mathbb{Z}/p^n\mathbb{Z})^* \cong (\mathbb{Z}/p^n\mathbb{Z})^*$
che è ciclico per (iv)

## Algebra Lezione 22/10/25 (teoria - Del Corso)

- **Teorema**: gruppi abeliani sono prodotto delle loro p-componenti:
Sia $G$ gruppo abeliano, $|G| = n = p_1^{e_1} \cdot \dots \cdot p_s^{e_s}$ con $p_i^{e_i} \neq p_j$ primi $\forall i \neq j$
$\Rightarrow G \cong G(p_1) \times \dots \times G(p_s)$ con $G(p_i) = \{g \in G \mid ord(g) = p_i^k, k \in \mathbb{N}\}$
Inoltre la decomposizione di $G$ come prodotto di p-gruppi di ordine tra loro coprimi è unica.

→ **Dim** Dato che $G$ è abeliano e che i p-Sylow sono tutti coniugati tra loro, $G(p_i)$ è il p-Sylow di $G$.
Procediamo per induzione su $s$:

- Base: $s=1$ $G = G(p_1^{e_1})$
- P. I.: sia $n = mm'$ $|(m,m') = 1$.
  - $mG, m'G < G$, infatti: $ma + mb = m(a+b)$ e $m'a + m'b = m'(a+b)$
  - $mG, m'G \lhd G$, perché $G$ abeliano
  - $mG + m'G \subseteq G$ ovvio
  - $G \subseteq mG + m'G$, perché per Bezout $\exists h,k \mid hm + nm' = 1$ } $G = mG + m'G$
  - $mG \cap m'G = \{e\}$, infatti: $x \in mG \cap m'G \Rightarrow x = ma = m'b \Rightarrow$
$ord(x) \mid m \wedge ord(x) \mid m'$ ovvero $ord(x) \mid (m,m') = 1$

$\Rightarrow$ per il teorema di decomposizione del prodotto diretto
$G \cong mG \times m'G$
Ci manca mostrare che $mG = G(m')$ e $m'G = G(m)$
Sia $\varphi_k : G \to G$, $g \mapsto kg$ è omo. Noto che
$mG = Im\, m\varphi_m \overset{*}{=} \ker \varphi_{m'} = G(m')$ $\quad m'G = Im\, m\varphi_{m'} \overset{*}{=} \ker \varphi_m = G(m)$

* c $\varphi_{m'}(m) = m'mg = 0$
$\supset g \in mag + \cancel{mbg}$

A questo punto dato che $m = p_1^{e_1} \cdot \dots \cdot p_i^{e_i}$ $m' = p_{i+1}^{e_{i+1}} \cdot \dots \cdot p_s^{e_s}$
per hp ind
$G(m) = G(p_1) \times \dots \times G(p_i)$ $\quad G(m') = G(p_{i+1}) \times \dots \times G(p_s)$
dunque $G = G(p_1) \times \dots \times G(p_s)$

Per l'unicità se $G \cong H_1 \times \dots \times H_s$ ma questo significherebbe che
$H_i \subseteq G(p_i)$ ma $|G| = |H_1| \dots |H_s| = |G(p_1)| \dots |G(p_s)| \Rightarrow H_i = G(p_i)$

- **Teorema**: p-gruppi si spezzano come prodotto di p-gruppi ciclici
Sia $G$ un gruppo abeliano. Esistono e sono univocamente determinati $r_1, \dots, r_t \mid r_1 \geq \dots \geq r_t \mid G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$

- con questa decomposizione so subito l'ordine degli elementi. Gli elementi di ordine p sono quelli nel sottogruppo $H \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_{t \text{ volte}}$ e sono $p^t - 1$ (l'unico elemento che non ti va bene è $(0,0,\dots,0)$)

- **Teorema di struttura dei gruppi abeliani finiti**:
Sia $G$ un gruppo abeliano finito $\Rightarrow G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_s\mathbb{Z}$.
Tale scrittura è unica se $n_{i+1} \mid n_i \ \forall i \in \{1, \dots, s-1\}$

→ **Dim** solo l'idea
- $G(p) = \{g \in G \mid ord(g) = p^k, k \in \mathbb{N}\}$
- $G(p) \lhd G$ perché $G$ abeliano
(* $x, y \in G(p) \Rightarrow p \mid ord(x)$ e $p \mid ord(y)$ ma $ord(xy) = [ord(x), ord(y)]$

$\Rightarrow p \mid ord(xy) \Rightarrow xy \in G(p)$

- $G(p) \trianglelefteq G$ tante ragioni $\longrightarrow$ gli automorfismi conservano l'ordine
  $\longrightarrow$ p-Sylow normale $\Rightarrow$ p-Sylow abeliano

**Esercizio 1:** Chi sono i gruppi di ordine 8? $\longrightarrow$ scegliamo 8 perché:

Sia $G \mid |G| = 8$

- caso $G$ abeliano: per il teorema di struttura dei gruppi abeliani finiti
  $G \cong G(2) \Rightarrow$
  $\mathbb{Z}/8\mathbb{Z}$
  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

- caso $G$ non abeliano:
  se $\forall x \in G \ ord(x) = 2 \Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ↯
  quindi $\exists a \in G \mid ord(a) = 4$.
  Noto che $\langle a \rangle \trianglelefteq G$ perché $[G : \langle a \rangle] = 2$
  Sia $b \in G - \langle a \rangle \Rightarrow G/\langle a \rangle = \{\langle a \rangle, b\langle a \rangle\}$
  ma questo significa che $b\langle a \rangle$ ha ordine 2
  $\Rightarrow b^2\langle a \rangle = \langle a \rangle \Rightarrow b^2 \in \{e, a, a^2, a^3\}$
  - $b^2 = a \Rightarrow ord(b) = 8 \Rightarrow G$ ciclico ↯ assurdo perché abbiamo assunto $G$ non abel
  - $b^2 = a^3 \Rightarrow ord(b) = 8 \Rightarrow G$ ciclico ↯
  - $b^2 = e$ (i) $\langle a \rangle \trianglelefteq G$
    (ii) $\langle b \rangle \langle a \rangle = G$
    (iv) $\langle b \rangle \cap \langle a \rangle = \{e\}$ perché $b \in G - \langle a \rangle$

    teorema di decomposizione in prodotto semidiretto
    $\Rightarrow \langle a \rangle \rtimes_\varphi \langle b \rangle \cong D_4$

    $\varphi : D_4 \longrightarrow G$
    $a \longmapsto a$
    $b \longmapsto b$
  - $b = a^2$ dato che $\langle a \rangle \trianglelefteq G \Rightarrow bab^{-1} \in \{e, a, a^2, a^3\}$
    - $bab^{-1} = e \Rightarrow a = e$ ↯ a ha ordine 4
    - $bab^{-1} = a \Rightarrow G$ abel ↯
    - $bab^{-1} = a^2$ ↯ perché $ord(bab^{-1}) = 4$ e $ord(a^2) = 2$

    $\Rightarrow bab^{-1} = a^3 \Rightarrow ba = a^3 b$ ma quindi ottengo $Q_8$

    $\varphi : Q_8 \longrightarrow G$
    $i \longmapsto a$
    $j \longmapsto b$

- **Definizione gruppo dei quaternioni:** Si definisce il gruppo dei quaternioni il gruppo
  $Q_8 = \langle i, j \mid i^4 = 1, \ i^2 = j^2, \ ij = j^3 i \rangle$

- Alcune osservazioni su $Q_8$: $\langle i \rangle, \langle j \rangle \trianglelefteq Q_8$ e $\langle i^2 \rangle, \langle j^2 \rangle \trianglelefteq Q_8$
  - $|Z(Q_8)| = \begin{cases} 1 \longrightarrow \text{no perché } p\text{-gruppo} \\ p^2 \longrightarrow \text{no perché altrimenti: } Q_8/Z(Q_8) \text{ ciclico} \\ p^3 \longrightarrow \text{no perché altrimenti: } Z(Q_8) = Q_8 \\ p \longrightarrow \text{per forza lui} \end{cases}$
  - $Z(Q_8) = \langle i^2 \rangle$ perché ha cardinalità 2 e $\langle i^2 \rangle \leq Z(Q_8)$

## Algebra lezione 24/10/25 (esercitazione + Del Corso)

**Esercizio 1:** Sia $G$, $|G| = p^n$, $H \lneq G \Rightarrow H \lneq N_G(H)$

- caso $Z(G) \nsubseteq H$ ma $H \subseteq N_G(H)$ e $Z(G) \subseteq N_G(H)$ ma quindi $H \subsetneq N_G(H)$
- caso $Z(G) \subseteq H$ studiamo $\pi : G \longrightarrow G/Z(G)$
  $H \longmapsto \pi(H) = H/Z(G) = \overline{H}$

  ma quindi $yZ(G) \in N(\overline{H}) \cdot \overline{H} \Rightarrow yZ(G)hZ(G)y^{-1}Z(G) \in \overline{H}$ perché
  $yhy^{-1}Z(G) = \overline{H}$ perché $h \in H$ ed ho un rappresentante e y commuta con h
  ma quindi $y \in \pi^{-1}(yZ(G)) \Rightarrow y^{-1}hy \in H$ ma $y \notin H \Rightarrow y \in N_G(H)$

**Esercizio 2:** Sia $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, determina il minimo $n \mid Q_8 \hookrightarrow S_8$

Innanzitutto noto che per Cayley $n \leq 8$ (perché $G \hookrightarrow S_{|G|}$) e per Lagrange $n \geq 4$ (perché $|Q_8| \mid |S_n|$)

Se $Q_8 \hookrightarrow S_4$, dato che $|Q_8| = 8 \Rightarrow Q_8$ è uno dei 2-Sylow di $S_4$. Ma $D_4 \hookrightarrow S_4$ e $|D_4| = 8 \Rightarrow D_4$ è un 2-Sylow di $S_4$. Però $Q_8$ non è coniugato con $D_4$. Quindi: $Q_8 \not\hookrightarrow S_4$.
Ma quindi $Q_8 \hookrightarrow S_5$ perché $|S_5| = 2^3 \cdot 3 \cdot 5$, dato che $S_4 \subset S_5$ i 2-Sylow di $S_4$ sono quelli di $S_5$.

Se $Q_8 \hookrightarrow S_6$ allora avrò $\begin{matrix} i \longmapsto \sigma \\ j \longmapsto \rho \\ k \longmapsto \sigma\rho = \eta \end{matrix}$ con $\text{ord}(\sigma) = \text{ord}(\rho) = 4$ e $\text{ord}(\sigma^2) = \text{ord}(\rho^2) = \text{ord}(\eta^2) =$
$x_1 = (1\ 3\ 2\ 4)$
$x_2 = (1\ 4\ 2\ 3)$
$x_3 = (1\ 3\ 2\ 4)(5\ 6)$
$x_4 = (1\ 4\ 2\ 3)(5\ 6)$
ma quindi $\sigma^2 = \rho^2 = \eta^2 = (a\ b)(c\ d)$, risolvendo per $x^2$ ho
ovvero ho 4 soluzioni ma in $S_6$ ne avrei 6 in $Q_8$.
Ma quindi $Q_8 \not\hookrightarrow S_7$ perché $|S_7| = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, dato che $S_6 \subset S_7$ i 2-Sylow di $S_6$ sono quelli di $S_7$.

Ma quindi $n = 8$. Un esempio di immersione $\begin{matrix} i \longmapsto (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \\ j \longmapsto (1\ 5\ 3\ 7)(2\ 8\ 4\ 6) \end{matrix}$

**Esercizio 3:** Quali sono i sottogruppi di ordine 4 e indice 4 in $D_{100}$

(i) i sottogruppi di ordine 4 so che ci sono solo $\mathbb{Z}/4\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

- noto che $\langle r^{25} \rangle \cong \mathbb{Z}/4\mathbb{Z}$ e per la lezione 06/10 $\langle r^{25} \rangle \lhd D_{100}$

- per $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ho bisogno di 3 elementi di ordine 2 che commutano
ma quindi ho $\{e, r^{50}, sr^n, sr^{n+50}\} = Z_{D_{100}}(sr^n)$
dunque vanno tutti bene al variare di $n$ ma i gruppi sono a 2 a 2
perciò sono 50 gruppi in $D_{100}$ isomorfi a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Questi non sono normali: noto che $r\,sr^k\,r^{-1} = rsr^{k-1} = sr^{-1}r^{k-1} = sr^{k-2} \neq sr^k$

(ii) voglio gli $H \leq D_{100} \mid [D_{100} : H] = 4 \Rightarrow |H| = 50 \Rightarrow P_5 \leq H$. Noto che $\langle r \rangle = P_5$
Ma quindi i sottogruppi di indice 4 sono isomorfi a $D_{100}/P_5 = D_{100}/\langle r^4 \rangle \cong D_4$

Data dunque $\pi : D_{100} \longrightarrow D_{100}/\langle r^4 \rangle \cong P_4$ per corrispondenza i sottogruppi di
$\begin{matrix} r \longmapsto \bar{r} \\ s \longmapsto \bar{s} \end{matrix}$

indice 2 in $D_4$ hanno indice 4 in $D_{100}$. In $D_4$ ho $\langle \bar{r}^2 \rangle \lhd D_4$ $\langle \bar{s}\bar{r}^n \rangle < D_4$ sono 5 diversi al variare di $n$
dunque ho $\pi^{-1}(\langle \bar{r}^2 \rangle) = \langle r^2 \rangle \lhd D_{100}$ e $\pi^{-1}(\langle \bar{s}\bar{r}^n \rangle) = \langle sr^2 \rangle P_5 < D_{100}$

**Esercizio 4:** Sia $G$ gruppo $|G| = 144 \Rightarrow G$ non è semplice

Noto che $144 = 2^4 \cdot 3^2$. Se $G$ è semplice per es 2 lezione 20/10 $\Rightarrow G \hookrightarrow A_n$
Prendiamo il 3-Sylow $P_3$. Noto che $n_3 \equiv 1 \,(3)$ e $n_3 \mid |G|$. Questo significa che $n_3 = 1, 4, 16$. Se $n_3 = 1 \Rightarrow P_3 \lhd G \Leftrightarrow G$ non semplice ↯
Se $n_3 = 16 \Rightarrow 16 \cdot 8$ el nei 3-Sylow $\Rightarrow$ 5 el. fuori dei 3-Sylow $\Rightarrow P_2 \lhd G$ ↯
Se $n_3 = 4 \Rightarrow G \hookrightarrow A_4$ ma $144 \nmid 24$ ↯

Dunque resta solo il caso $n_3 = 16$ e $\exists P_3, P_3' \mid |P_3 \cap P_3'| \neq 3$. Questo significa che $P_3, P_3'$ sono abeliani $P_3, P_3' \subset Z(H) \leq N_G(H) \Rightarrow |N_G(H)| = 9 \cdot 2^a$.
- $a = 0, 1$ no per lup
- $a = 2$ no perché $G \not\hookrightarrow A_4$
- $a = 3$ no altrimenti è normale
- $a = 4 \Rightarrow H \lhd G$ ↯

## Algebra Lezione 27/10/25 (esercitazione - Patimo)

**Esercizio 1:** $\forall n \geq 3 \quad A_n = \langle (i\ j\ k) \mid i \neq j \neq k,\ i,j,k \in \{1, \dots, n\} \rangle$

- caso $\sigma$ di lunghezza dispari: $\sigma = (1 \dots 2k+1) = (1\ 2\ 3)(3 \dots 2k+1) =$
$= (1\ 2\ 3), \dots (2k-3\ 2k-2\ 2k-1)(2k-1\ 2k\ 2k+1) \in H$

- caso $\sigma$ prodotto di n cicli pari:
  - Base $n = 0 \Rightarrow id \in H$
  - P.I. $\sigma = (1 \dots 2a)(2a+1 \dots 2a+2b) = (1 \dots 2a-2)(2a-2\ 2a-1\ 2a)(2a+1\ 2a+2\ 2a+3$
$(2a+3\ 2a+4\ 2a+5) \dots (2(a+b)-2\ 2(a+b)-1\ 2(a+b)) =$
$= (1\ 2\ 3) \dots (2a-2\ 2a-1\ 2a)(2a+1\ 2a+2\ 2a+3) \dots (2(a+b)-2\ 2(a+b)-1\ 2(a+b)) \in H$

**Esercizio 2:** $\forall n \geq 5$ $A_n = \langle (ab)(cd) \mid a \neq b \neq c \neq d,\ a,b,c,d \in \{1,\dots,n\} \rangle$

Sia $K = \langle (ab)(cd) \rangle \trianglelefteq A_n$. $A_n = \langle (i\ j\ k) \rangle$ dunque se trovo $(1\,2\,3)$ in $K$ concludo

$(1\,2\,3) = (1\,2)(2\,3)(4\,5)(4\,5) = (1\,2)(4\,5)(2\,3)(4\,5)$
(qui serve $n \geq 5$)

**Esercizio 3:** Descrivi $S'_n$, $A'_n$ $\forall n \geq 3$

(i) $S_n / S'_n$ è il più grande gruppo abeliano di $S_n$ (lezione 06/10). $S_n / A_n = \mathbb{Z}/2\mathbb{Z}$ che è abeliano $\Rightarrow S'_n \leq A_n$. Noto che $(1\,2\,3) = (1\,3)(1\,2)(1\,3)(1\,2) \in S'_n$. Ma quindi in $S'_n$ ho i generatori di $A_n \Rightarrow S'_n = A_n$

(ii) $A'_3 = \{e\}$, $A'_4 \subset K$ ma $A'_4 \neq \{e\}$ perché non è abeliano, $A'_4 \neq \{e, (ab)(cd)\}$ se no non sarebbe normale

per $n \geq 5$ noto che $(1\,2)(3\,4) = (1\,2\,3)(2\,3\,4)(1\,3\,2)(2\,4\,3) \in A'_n$, dunque ho i generatori di $A_n$ in $A'_n \Rightarrow A'_n = A_n$.

(K è il Klein così indico anche con V)

**Esercizio 4:** Dimostra che $A_5$ è semplice

Supponiamo per assurdo che $\exists N \neq A_5 \mid N \trianglelefteq A_5$. Noto che in $N$ non ci posso essere i tre-cicli ne le coppie di due-cicli, altrimenti genererebbero $A_5$.
Supponiamo che $\exists \sigma \in N$, $\sigma$ cinque-ciclo dunque ho $|Cl_{A_5}(\sigma)| = 12$ e noto che

$$12 = |Cl_{A_5}(\sigma)| = \frac{|A_5|}{|Z_{A_5}(\sigma)|} = \frac{60}{5} \quad \lightning$$

**Esercizio 5:** Sia $G$ gruppo $|G| = 60$, $G$ semplice $\Rightarrow G \cong A_5$

Sappiamo che $60 = 2^2 \cdot 3 \cdot 5$ $n_5 = 1, 6$ ma $G$ è semplice $\Rightarrow n_5 = 6$.

$n_3 = 1, 4, 10$ ma $G$ è semplice $\Rightarrow n_3 \neq 1$
se $n_3 = 4 \Rightarrow \exists f: G \to S_4 \Rightarrow G \hookrightarrow S_4$ $\lightning$ $60 \nmid 24$
$\Rightarrow n_3 = 10$

$n_2 = 1, 3, 5, 15$ ma $G$ è semplice $\Rightarrow n_2 \neq 1$
se $n_2 = 3 \Rightarrow G \hookrightarrow S_3$ $\lightning$ $60 \nmid 6$
se $n_2 = 5 \Rightarrow G \hookrightarrow S_5 \Rightarrow G \cong H < S_5$ ma $[S_5 : H] = 2$
$\Rightarrow H \supset S'_5 = A_5 \Rightarrow H = A_5$

se $n_2 = 15$ (e l'intersezione dei 2-Sylow sono banali) $\lightning$ perché non ci sono abbastanza elementi

- se l'intersezione dei 2-Sylow è non banale siano $P_1, P_2$ 2-Sylow, $Q = P_1 \cap P_2 \Rightarrow |Q| = 2$. Sia $N := N_G(Q)$. Dato che $[P_1 : Q] = 2$ e $[P_2 : Q] = 2 \Rightarrow P_1, P_2 \subset N$

$|N| = \{\cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, 10, 12, \cancel{15}, 20, \cancel{30}, \cancel{60}\}$

($P_1, P_2 \subset N$; $P_1 P_2 \subset N$; 4 non li divide ma ho Sylow ordinati in $N$; $G$ semplice)

$\rightarrow |N| = 20 \Rightarrow [G : N] = 3$ $G$ agisce per classi laterali di $N$
$\Rightarrow G \hookrightarrow S_3$ e $G \hookrightarrow A_3 \hookrightarrow S_3$ $\lightning$

$\rightarrow |N| = 12 \Rightarrow [G : N] = 5$ $G$ agisce per classi laterali di $N$
$\Rightarrow G \hookrightarrow S_5$ e per quanto detto se $n_2 = 5 \Rightarrow G \cong A_5$

# Algebra lezione 29/10/25 (teoria - Del Corso)

- **Definizione anello**: Un anello è un insieme non vuoto munito di due operazioni $(A,+,\cdot)$ tale che: (i) $(A,+)$ è un gruppo abeliano; (ii) $(\cdot)$ è associativa; (iii) vale la proprietà distributiva di $(\cdot)$ su $(+)$ (a dx e a sx)

- **Definizione anello commutativo**: Un anello $A$ è commutativo se $(\cdot)$ è commutativa

- **Definizione anello con identità**: Un anello $A$ è con identità se $\exists 1 \in A \mid \forall a \in A \ a \cdot 1 = 1 \cdot a = a$

- Noi useremo quasi esclusivamente anelli commutativi con identità

- Alcuni esempi di anelli sono $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{K}[x_1,\dots,x_n]$, $\mathbb{Z}[[]]$, $\mathbb{K}[[x]]$ (la serie di potenze)

- **Definizione divisore di zero**: Sia $A$ anello, diremo che $x \in A$ è divisore di zero se $\exists y \in A \setminus \{0\} \mid xy(=yx) = 0$. Indicheremo con $D(A)$ l'insieme dei divisori di zero

- **Definizione dominio**: Sia $A$ anello commutativo, diremo che $A$ è dominio (d'integrità) se $D(A) = \{0\}$

- **Definizione nilpotente**: Sia $A$ anello, diremo che $x \in A$ è nilpotente se $\exists n \in \mathbb{N} \mid x^n = 0$. Indicheremo con $\mathcal{N}$ l'insieme dei nilpotenti e lo chiamiamo nilradicale (è ideale)

- **Definizione invertibile**: Sia $A$ anello, diremo che $x \in A$ è invertibile se $\exists y \in A \mid xy = (yx =) 1$. Indicheremo con $A^*$ l'insieme degli elementi invertibili ($(A^*,\cdot)$ è gruppo)

- Notiamo che $\mathcal{N} \subset D(A)$ questo perché sia $n_0 = \min\{n \in \mathbb{N} \mid x^n = 0\}$. Allora $x^{n_0-1} \neq 0$ e $x \cdot x^{n_0-1} = x^{n_0} = 0 \Rightarrow x \in D(A)$

- **Definizione anello ridotto**: Sia $A$ anello commutativo, diremo che $A$ è ridotto se $\mathcal{N} = \{0\}$

- **Proposizione proprietà anello con identità**: Sia $A$ anello commutativo con identità $\Rightarrow$
  (i) $(A^*,\cdot)$ è un gruppo abeliano
  (ii) $A^* \cap D(A) = \varnothing$
  (iii) Se $|A| < +\infty \Rightarrow A = D(A) \cup A^*$

  → **Dim** (i)
  - chiusura $\forall x,y \in A^* \Rightarrow \exists x^{-1}, y^{-1} \in A \Rightarrow y^{-1}x^{-1}$ è inverso di $xy \Rightarrow xy \in A^*$
  - associatività poiché $A^* \subseteq A$ e $A$ associativo per $(\cdot) \Rightarrow A^*$ associativo $(\cdot)$
  - el. neutro $1 \in A^*$, infatti $1$ ha inverso poiché $1 \cdot 1 = 1$
  - inverso sia $x \in A^* \Rightarrow \exists x^{-1} \in A$ ma $x^{-1}$ ha inverso $\Rightarrow x^{-1} \in A^*$
  - abel poiché $A^* \subseteq A$ e $A$ commutativo per $(\cdot) \Rightarrow A^*$ commutativo per $(\cdot)$

  (ii) Supponiamo per assurdo che $D(A) \cap A^* \neq \varnothing$, sia $x \in D(A) \cap A^*$, allora
  $x \in D(A) \Rightarrow \exists z \in A \setminus \{0\} \mid xz = zx = 0$ e $x \in A^* \Rightarrow \exists y \in A \mid xy = yx = 1$
  $(zx)y = z(xy)$ perché $(\cdot)$ associativa
  $0 = 0 \cdot y$ ↙ ↘ $z \cdot 1 = z$
  $\Rightarrow z = 0$ ↯

  (iii) $\supseteq$ ovvio perché $D(A) \subset A$ e $A^* \subset A$
  $\subseteq$ Sia $x \in A$
  - caso $x \in D(A) \Rightarrow x \in D(A) \cup A^*$
  - caso $x \in D(A) \setminus A$ sia $\varphi_x : A \to A$, $a \mapsto xa$, noto che $\ker\varphi_x = \{y \in A \mid \varphi_x(y) = xy = 0\} = \{0\}$ perché $x \notin D(A)$. Poiché $|A| < +\infty$ $\varphi_x$ inj $\Rightarrow \varphi_x$ surj $\Rightarrow 1 \in \mathrm{Im}\varphi_x \Rightarrow \exists a \mid \varphi_x(a) = 1$
  $\Rightarrow xa = 1 \Rightarrow x \in A^*$

- Un esempio di questo è $\frac{\mathbb{K}[x]}{(f(x))}$ (è un $\mathbb{K}$-spazio finitamente generato) perché $g(x) \in \left(\frac{\mathbb{K}[x]}{(f(x))}\right)^* \iff (g(x), f(x)) = 1$ e $g(x) \in D\left(\frac{\mathbb{K}[x]}{(f(x))}\right) \iff (g(x), f(x)) \neq 1$

## Esercizi

1_ Dimostra che $g(x) \in D\left(\frac{\mathbb{K}[x]}{(f(x))}\right) \iff (g(x), f(x)) \neq 1$

$\Rightarrow$ Se $g(x) \in D \Rightarrow \exists a(x) \mid g(x)a(x) = kf(x) \Rightarrow g(x) \mid f(x) \Rightarrow (g(x), f(x)) \neq 1$

$\Leftarrow$ Se $(g(x), f(x)) \neq 1 \Rightarrow (g(x), f(x)) = a(x) \Rightarrow g(x) = a(x)b(x)$ $f(x) = a(x)c(x)$
$\Rightarrow g(x)b(x)^{-1}c(x) = f(x) = 0 \Rightarrow g(x) \in D$

- **Definizione ideale**: Sia $A$ anello commutativo, $I \subset A$ è ideale se (i) $(I,+) < (A,+)$ (ii) $\forall a \in A \ \ aI \subset I$ e $Ia$

$\{0\}$ è ideale banale $A$ è ideale improprio

- **Definizione ideale generato**: Sia $A$ anello, $S \subset A$, definiamo l'ideale generato da $S$ come $(S) = \{\sum_{i=1}^{n} a_i s_i \mid a_i \in A, s_i \in S, n \in \mathbb{N}\}$

- **Proposizione** $(S) = \bigcap I$: $(S)$ è il più piccolo ideale che contiene $S$, dunque $(S) = \bigcap_{S \subseteq I \subseteq A} I$

→ **Dim** $\subseteq$ dato che $(S)$ è un ideale, mi è sufficiente che $S \subseteq \bigcap_{S \subseteq I \subseteq A} I$ ma questo è ovvio

$\supseteq$ dato che $(S)$ è uno degli ideali che stiamo intersecando è ovvio

- **Operazioni con gli ideali**: sia $A$ anello, $I, J \subseteq A$ ideali allora:

(i) $I \cup J = \{a \mid a \in I \vee a \in J\}$ in generale non è un ideale ($2\mathbb{Z} \cup 3\mathbb{Z}$ non è ideale

(ii) $I \cap J = \{a \mid a \in I \wedge a \in J\}$ è ideale

(iii) $I + J = (I, J) = \{i + j \mid i \in I \wedge j \in J\}$

(iv) $IJ = (\{xy \mid x \in I, y \in J\})$ è ideale (ma $\{xy \mid x \in I, y \in J\}$ non lo è) N.B. $IJ = I \cap J$

(v) $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\}$ è ideale (quindi noto che $\mathcal{N} = \sqrt{\{0\}}$ è ideale

(vi) $(I : J) = \{x \in A \mid xJ \subseteq I\}$ è ideale ad es $(25\mathbb{Z} : 10\mathbb{Z}) = \{x \in \mathbb{Z} \mid x \cdot 10 \in 25\mathbb{Z}\} = 5\mathbb{Z}$

$(m\mathbb{Z} : n\mathbb{Z}) = \frac{m}{mcd(m,n)}\mathbb{Z}$ ← caso generale

- **Definizione omomorfismo di anelli**: Siano $A, B$ anelli, $f : A \to B$ omomorfismo di anelli se:

(i) $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \quad \forall a_1, a_2 \in A$

(ii) $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2) \quad \forall a_1, a_2 \in A$

(iii) $\varphi(1_A) = 1_B$ ← solo se $A, B$ anelli con unità

- Sia $\varphi : A \to B$ omo di anelli, allora:

(i) $\ker\varphi$ è ideale di $A$

(ii) $\varphi(A)$ è sottoanello di $B$

(iii) se $J \subseteq B$ è ideale $\Rightarrow \varphi^{-1}(J) \subseteq A$ è ideale

(iv) Se $\varphi$ è surj $I \subseteq A$ ideale $\Rightarrow \varphi(I) \subseteq B$ è ideale

- **Definizione gruppo quoziente**: Sia $A$ anello, $I \subseteq A$ ideale, il gruppo quoziente $(A/I, +)$ ha anche una struttura di anello con l'operazione $(\cdot)$ definita $(a+I)\cdot(b+I) = ab + I$

- Ricordiamo che gli ideali sono tutti e soli i $\ker$ degli omomorfismi di anelli

- **Primo Teorema di omomorfismo per anelli**: Siano $A, A'$ anelli, $\varphi : A \to A'$ omomorfismo anelli, $I \subseteq \ker\varphi \Rightarrow \exists! \bar{\varphi} : A/I \to A'$ (i) $\varphi = \bar{\varphi} \circ \pi_I$

(ii) $\mathrm{Imm}\,\varphi = \mathrm{Imm}\,\varphi'$

(iii) $\ker\varphi' = \frac{\ker\varphi}{I}$

→ **Dim** per il 1° th omo, sappiamo che esiste ed è unico l'omomorfismo $\bar{\varphi} : A/I \to A'$. Dobbiamo dimostrare che tale omomorfismo è omo di anelli:

$$\bar{\varphi}((a+I)(b+I)) = \bar{\varphi}(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(a+I)\bar{\varphi}(b+I)$$

- **Teorema di corrispondenza per gli anelli**: Sia $A$ anello, $I \subset A$ ideale, $\pi_I$ la proiezione a quoziente $\Rightarrow \pi_I$ induce una corrispondenza biunivoca tra gli ideali di $A/I$ e gli ideali di $A$ che contengono $I$

→ **Dim** per il teorema di corrispondenza abbiamo una bigezione fra i sottogruppi. Voglio quindi solo controllare che le immagini di questi ideali e le controimmagini siano ancora ideali.

Sia $\mathcal{J} \subset A/I$ ideale, $(\pi_I^{-1}(\mathcal{J}), +) < (A, +)$. Dimostriamo dunque che vale la proprietà di assorbimento: $x \in \pi_I^{-1}(\mathcal{J}) \Rightarrow \pi_I(x) \in \mathcal{J} \overset{a \in A}{\Rightarrow} \pi_I(a)\pi_I(x) = \pi_I(ax) \in \mathcal{J} \quad \forall x \in \pi_I^{-1}(\mathcal{J}) \Rightarrow ax \in \pi_I^{-1}(\mathcal{J})$

Sia $J \subset A$ ideale, $(\pi_I(J), +) < (A/I, +)$, sia $x \in J$, $b \in A/I$, dato che $\pi_I$ è surj $\exists a \in A \mid \pi_I(a) = b$. Ma quindi $b\pi_I(x) = \pi_I(a)\pi_I(x) = \pi_I(ax)$ ma $ax \in J \Rightarrow \pi_I(ax) \in \pi_I(J)$

- **Definizione prodotto diretto an.**: Dati $A,B$ anelli, il prodotto cartesiano $A\times B$ può essere dotato di una struttura di anello con le operazioni:
(+) $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,\ b_1+b_2)$
(·) $(a_1,b_1)\cdot(a_2,b_2)=(a_1\cdot a_2,\ b_1\cdot b_2)$

- **Teorema Cinese del Resto per anelli**: Sia $A$ anello commutativo con unità, $I,J$ ideali
$\Rightarrow f: A \longrightarrow A/I \times A/J$, $a \longmapsto (a+I,\ a+J)$ è omo di anelli e $\ker f = I\cap J$
Inoltre $I+J=A \iff f$ surj $\Rightarrow A/IJ \cong A/I \times A/J$

→ **Dim** (i) $f$ è omo: $f(a+b)=((a+b)+I,\ (a+b)+J)=(a+I,\ a+J)+(b+I,\ b+J)$
$=f(a)+f(b)$
$f(ab)=(ab+I,\ ab+J)=(a+I,\ a+J)\cdot(b+I,\ b+J)=$
$=f(a)\,f(b)$

(ii) $\ker f$: $\ker f=\{a\in A \mid f(a)=(a+I,\ b+I)=(I,J)\}=\{a\in A \mid a\in I,\ a\in J\}=I\cap$

(iii) $\Rightarrow$ Supponiamo $I+J=A$, voglio dimostrare che $\forall a,b\in A\ \exists x \mid f(x)=(a+I,\ b+J)$. Innanzitutto noto che dato che $A=I+J$ $\exists i\in I\ \exists j\in J \mid 1=i+j$.
Per la stessa ragione, $\exists i\in I,\ \exists j\in J \mid x=aj+bi \Rightarrow$
$f(x)=(x+I,\ x+J)=(aj+bi+I,\ aj+bi+J)=(aj+I,\ bi+J)$
(vengono ass.)
ma $1=i+j \Rightarrow i=1-j$ e $j=1-i \Rightarrow (aj+I,\ bi+J)=(a(1-i)+I,$
$b(1-j)+J)=(a-ai+I,\ b-bj+J)=(a+I,\ b+J)$

$\Leftarrow$ Supponiamo $f$ surj. $\Rightarrow \exists i\in A \mid f(i)=(I,1+J) \Rightarrow i\in I$ e $i=1($
$\Rightarrow i=1+j$ per un $j\in J \Rightarrow 1=i-j \Rightarrow 1\in I+J$

Ma quindi per 1° th omo $A/\ker f \cong A/I \times A/J$ ma $\ker f=I\cap J$

ma notiamo che se $A=I+J \Rightarrow I\cap J=IJ$, dunque $\ker f=IJ$
$\Rightarrow A/IJ \cong A/I \times A/J$

- **Definizione maggiorante**: Sia $(\mathcal{I},\leq)$ un insieme parzialmente ordinato (poset) (partially ordered set), $X\subset\mathcal{I}$ un suo sottoinsieme, diciamo che $M$ è maggiorante per $X$ se:
$A\leq M\ \ \forall A\in X$

- **Definizione massimale**: Sia $(\mathcal{I},\leq)$ poset, $A\in\mathcal{I}$ è massimale per $\mathcal{I}$ se $\forall B\in\mathcal{I}: A\leq B \Rightarrow A=B$

- **Definizione massimo**: Sia $(\mathcal{I},\leq)$ poset, $A\in\mathcal{I}$ è massimo per $\mathcal{I}$ se $\forall B\in\mathcal{I}: B\leq A$

- **Definizione catena**: Sia $(\mathcal{I},\leq)$ poset, una catena di $\mathcal{I}$ è un sottoinsieme di $\mathcal{I}$ totalmente ordinato

- **Definizione induttivo**: Sia $(\mathcal{I},\leq)$ poset, $(\mathcal{I},\leq)$ è induttivo se ogni catena di $\mathcal{I}$ ammette un maggiorante in $\mathcal{I}$

- **Lemma di Zorn**: Sia $(\mathcal{I},\leq)\neq\emptyset$ poset induttivo $\Rightarrow \mathcal{I}$ contiene elementi massimi

- **Definizione primo**: Sia $I\subsetneq A$ ideale proprio, $I$ è primo se $xy\in I \Rightarrow x\in I \vee y\in I$

- **Definizione ideale massimale**: Sia $I$ ideale, $I$ è massimale se è un elemento massimale della famiglia di $\mathcal{I}$ di tutti gli ideali propri di $A$:
$I$ massimale $\iff \forall J\subsetneq A: I\subseteq J \Rightarrow I=J$

# Algebra Lezione 29/10/25 (esercitazione - Pattino)

**Esercizio 1**: Siano $p,q,r$ primi distinti, $G$ gruppo $\mid |G|=pqr \Rightarrow G$ non è semplice.

WLOG $r<q<p$. Calcoliamo i gruppi di Sylow: $n_p\in\{1,q,r,qr\}$ perché $p>q,r$
$n_q\in\{1,p,r,pr\}$ perché $q>r$
$n_r\in\{1,q,p,pq\}$

Se $G$ fosse semplice $n_p=qr$, $n_q\geq p$, $n_r\geq q$ ovvero ho:
$\underbrace{qr(p-1)}_{\text{el ord } p}+\underbrace{p(q-1)}_{\text{el ord } q}+\underbrace{q(p-1)}_{\text{el ord } r}$ elementi in $G$ $\lightning$
(almeno)

**Esercizio 2:** Chi sono i gruppi di ordine 45?

Sia $G$ gruppo $| |G| = 45 = 3^2 \cdot 5$. Allora noto che $|P_3| = 9$ e $|P_5| = 5 \Rightarrow$

$P_3 \cong \mathbb{Z}/9\mathbb{Z}$ oppure $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ $\quad P_5 \cong \mathbb{Z}/5\mathbb{Z}$. Inoltre $n_3, n_5 \in \{1, 3, 5, 9, 15, 45\} \Rightarrow n_3 = 1$ $n_5 =$

$\Rightarrow P_3, P_5 \trianglelefteq G$, ma quindi: (i) $P_3 . P_5 \trianglelefteq G$

(ii) $|P_3 P_5| = \frac{|P_3||P_5|}{|P_3 \cap P_5|} = \frac{9 \cdot 5}{1} = |G| \Rightarrow P_3 P_5 = G$

(iii) $P_3 \cap P_5 = \{e\}$

Dunque per il th dec prod semidir ho $P_3 \rtimes_\varphi P_5 \cong G \cong P_5 \rtimes_\varphi P_3$ (quindi ne studiamo solo uno perché sono gli stessi)

- caso $P_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\varphi: P_5 \longrightarrow Aut(P_3) \Rightarrow \varphi: \mathbb{Z}/5\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \cong GL_2(\mathbb{F}_3)$

ma $|GL_2(\mathbb{F}_3)| = 8 \cdot 6$, dato che $\varphi$ è omo $ord(\varphi(1)) \mid ord(1) = 5 \Rightarrow$
$\varphi = id \Rightarrow G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$

- caso $P_3 \cong \mathbb{Z}/9\mathbb{Z}$

$\varphi: P_5 \longrightarrow Aut(P_3) \Rightarrow \varphi: \mathbb{Z}/5\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$,

dato che $\varphi$ è omo $ord(\varphi(1)) \mid ord(1) = 5 \Rightarrow \varphi = id \Rightarrow G \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/45\mathbb{Z}$

**Esercizio 3:** Chi sono i gruppi di ordine 75?

Sia $G$ gruppo $| |G| = 75 = 3 \cdot 5^2$. Allora noto che $|P_3| = 3$ e $|P_5| = 25 \Rightarrow P_3 \cong \mathbb{Z}/3\mathbb{Z}$

$P_5 \cong \mathbb{Z}/25\mathbb{Z}$ oppure $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Guardo i Sylow $n_3 \in \{1, 5, 25\}$ $n_5 \in \{1, 3\} \Rightarrow P_5 \trianglelefteq G$

ma quindi: (i) $P_5 \trianglelefteq G$ (ii) $P_3 P_5 = G$ (iii) $P_3 \cap P_5 = \{e\}$

Dunque per il th dec prod semidir ho $P_5 \rtimes_\varphi P_3 \cong G$

- caso $P_5 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$\varphi: P_3 \longrightarrow Aut(P_5) \Rightarrow \varphi: \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \cong GL_2(\mathbb{F}_5)$

ma $|GL_2(\mathbb{F}_5)| = 24 \cdot 20$ e dato che $\varphi$ è omo $ord(\varphi(1)) \mid ord(1) = 3$ ma quindi
$ord(\varphi(1)) = 1, 3$. Quindi $ord(\varphi(1)) = 1 \Rightarrow \varphi = id \Rightarrow G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$

uso questo per dire che i due prodotti semidiretti che ci sono sono isomorfi

$ord(\varphi(1)) = 3 \Rightarrow G \cong (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

- caso $P_5 \cong \mathbb{Z}/25\mathbb{Z}$

$\varphi: P_3 \longrightarrow Aut(P_5) \Rightarrow \varphi: \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/25\mathbb{Z}) \cong (\mathbb{Z}/25\mathbb{Z})^* \cong \mathbb{Z}/20\mathbb{Z}$, dato che $\varphi$ è omo $ord(\varphi(1)) \mid ord(1) = 3 \Rightarrow \varphi = id \Rightarrow G \cong \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/75\mathbb{Z}$

- **Proposizione criterio di isomorfismo per prodotti semidiretti:**

Siano $G, G'$ gruppi $| G \cong H \rtimes_\varphi K$, $G' \cong H \rtimes_\psi K$ con
$\varphi, \psi: K \longrightarrow Aut(H)$ Se $\exists \alpha \in Aut(K), \exists \beta \in Aut(H) \mid \forall x \in K$
$\psi(\alpha(x)) = \beta \circ \varphi \circ \beta^{-1}(x) \Rightarrow G \cong G'$ ← non vale

→ Dim Sia $f: G \longrightarrow G'$, $(h, k) \mapsto (\beta(h), \alpha(k))$

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

ma $\psi(\alpha(k)) = \beta \circ \varphi \circ \beta^{-1}(k) \Rightarrow \beta \circ \varphi(k) = \psi(\alpha(k)) \circ \beta \Rightarrow f$ omo

- $f$ inj $\ker f = \{(h,k) \in H \rtimes_\varphi K \mid f((h,k)) = (\beta(h), \alpha(k)) = (e,e)\} = \{(h,k) \mid h \in \ker\beta$
$k \in \ker\alpha\} = \{(e,e)\}$
($\alpha, \beta$ inj $\Rightarrow (h,k) = (e,e)$)

- $f$ surj Sia $(h', k') \in H \rtimes_\psi K$ dato che $\beta \in Aut(H) \Rightarrow \exists h \in H \mid \beta(h) = h'$,
dato $\alpha \in Aut(K) \Rightarrow \exists k \in K \mid \alpha(k) = k' \Rightarrow (h', k') = (\beta(h), \alpha(k)) = f((h,k))$

**Esercizio 4**: Chi sono i gruppi di ordine $4p$ con $p \neq 3$ ($4$) ($p \neq 3$)

Sia $G$, $|G| = 4p$, $|P_2| = 4$ $|P_p| = p$ e $n_2 \in \{1, p\}$ $n_p \in \{1, p, 4\}$ ($n_p \equiv 1 \ (p)$)

$\Rightarrow$ $P_p$ Sylow normale Notiamo che $P_p \cong \mathbb{Z}/p\mathbb{Z}$ e $P_2 \cong \leq \mathbb{Z}/4\mathbb{Z} \leq \mathbb{Z}/2\mathbb{Z}$

Dato che (i) $P_p \trianglelefteq G$ (ii) $P_p P_2 = G$ (iii) $P_p \cap P_2 = \{e\} \Rightarrow G \cong P_p \rtimes_\varphi P_2$

- caso $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\varphi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p-1\mathbb{Z}$

  a. $(1\ 0) \longmapsto 0$ $(0\ 1) \longmapsto 0$
  b. $(1\ 0) \longmapsto 1$ $(0\ 1) \longmapsto 0$
  c. $(1\ 0) \longmapsto 0$ $(0\ 1) \longmapsto 1$
  d. $(1\ 0) \longmapsto 1$ $(0\ 1) \longmapsto 1$

con la mappa a ho $\varphi = id \Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2p\mathbb{Z}$

con la mappa b, c, d ottengo 3 mappe isomorfe | $G \cong \mathbb{Z}/2\mathbb{Z} \times D_p$ (i passaggi nel dettaglio sono gli stessi dell'esercizio 4 lezione 17/10)

- caso $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ $\varphi: \mathbb{Z}/4\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p-1\mathbb{Z}$, dato che $4 \nmid p-1$ allora posso mandare il generatore solo nell'unico elemento di ordine 2

  a. $1 \longrightarrow 0$
  b. $1 \longmapsto \frac{p-1}{2}$

con la mappa a ho $\varphi = id \Rightarrow G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
$\cong \mathbb{Z}/4p\mathbb{Z}$

con la mappa b ho $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$

**Esercizio 5**: Sia $\sigma \in A_n$, $Z_{S_n}(\sigma) < A_n \iff \sigma$ è prodotto di cicli disgiunti di lunghezza dispari tutti di lunghezza diversa

$\Rightarrow$ Se $\sigma$ ha un ciclo di lunghezza pari $\Rightarrow \sigma \in Z_{S_n}(\sigma) \setminus A_n \Rightarrow Z_{S_n}(\sigma) \not\subseteq A_n$
Se $\sigma$ ha due cicli della stessa lunghezza $\tau_1 = (1 \dots 2a+1)$ $\tau_2 = (2a+2 \dots 4a+2)$
$\Rightarrow \tau' = (1\ 2a+2) \dots (2a+1\ 4a+2) \in Z_{S_n}(\sigma) \setminus A_n \Rightarrow Z_{S_n}(\sigma) \not\subseteq A_n$

$\Leftarrow$ Sia $\sigma = \tau_1 \dots \tau_k$ con $\tau_i$ dispari e $\ell_1 > \dots > \ell_k$, $\sum \ell_i = n$ (proprietà per cui voglio lunghezze diverse perché quindi non posso avere 2 cicli di stessa lunghezza)
Studio $Z_{S_n}(\sigma)$: $|Z_{S_n}(\sigma)| = \frac{|S_n|}{|Cl(\sigma)|}$ ma

$$|Cl(\sigma)| = \binom{n}{\ell_1}(\ell_1 - 1)! \dots \binom{n-\ell_1-\dots-\ell_{k-1}}{\ell_k}(\ell_k - 1)! = \frac{n(n-1)\dots(n-\ell_1+1)}{\ell_1 \dots} (\ell_1-1)! \cdot \dots \cdot \frac{\ell_k \ell_{k-1} \dots}{\ell_k \dots} (\ell_k - 1)!$$

$$= \frac{n!}{\ell_1 \cdot \dots \cdot \ell_k} \Rightarrow |Z_{S_n}(\sigma)| = \ell_1 \cdot \dots \cdot \ell_k$$

So per definizione che $\tau_1, \dots, \tau_k \in Z_{S_n}(\sigma) \Rightarrow \langle \tau_1 \rangle, \dots, \langle \tau_k \rangle < Z_{S_n}(\sigma) \Rightarrow$

$Z_{S_n}(\sigma) = \langle \tau_1, \dots, \tau_k \rangle < A_n$

- Noto che $|Cl_{A_n}(\sigma)| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|A_n|}{|Z_{S_n}(\sigma) \cap A_n|} = \begin{cases} \frac{\frac{1}{2}|S_n|}{|Z_{S_n}(\sigma)|} = \frac{1}{2}\left|\frac{S_n}{Z_{S_n}(\sigma)}\right| \\ \frac{\frac{1}{2}|S_n|}{\frac{1}{2}|Z_{S_n}(\sigma)|} = \left|\frac{S_n}{Z_{S_n}(\sigma)}\right| \end{cases}$

## Algebra Lezione 03/11/25 (esercitazione - Patimo)

- **Definizione gruppo libero**: Sia $n \in \mathbb{N}$, chiameremo gruppo libero ($n$ generatori) $\mathbb{F}_n$ il gruppo i cui elementi sono le parole dell'alfabeto $\{x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}\}$
Poniamo in $\mathbb{F}_n$ la relazione di equivalenza: $x_i x_i^{-1} = \emptyset = x_i^{-1} x_i$
- L'operazione nel gruppo libero è la concatenazione e il neutro in $\mathbb{F}_n$ è $\emptyset$.
- **Definizione parola ridotta**: Diremo che $w_1, w_2 \in \mathbb{F}_n$ è ridotta se non contiene la successione $x_i x_i^{-1}$ al suo interno (sostanzialmente se sono "semplificate")
- Gli elementi di $\mathbb{F}_n$ sono in biiezione con le parole ridotte
- Un esempio è $\mathbb{F}_1 \cong \mathbb{Z}$ $x_1 \longmapsto 1 \wedge x_1^{-1} \longmapsto -1$
- Noto che $Z(\mathbb{F}_i) = \{e\}$ (per $i > 1$)

- **Proprietà universale:** Sia $G$ gruppo, $\mathrm{Hom}(\mathbb{F}_n, G)$ è in biiezione $G^n$

→ **Dim** $f: \mathrm{Hom}(\mathbb{F}_n, G) \longrightarrow \underbrace{G \times \dots \times G}_{n \text{ volte}}$

$\varphi: \mathbb{F}_n \longrightarrow G \longmapsto (\varphi(x_1), \dots, \varphi(x_n))$

- $f$ inj presi due morfismi $\varphi \neq \psi \in \mathrm{Hom}(\mathbb{F}_n, G)$, se $f(\varphi) = f(\psi) \Rightarrow (\varphi(x_1), \dots, \varphi(x_n)) = (\psi(x_1), \dots, \psi(x_n)) \Rightarrow \forall x_i \in \mathbb{F}_n \ \varphi(x_i) = \psi(x_i)$ ↯

- $f$ surj preso $(g_1, \dots, g_n) \in G \times \dots \times G$ sia $\varphi \mid \varphi(x_i) = g_i \quad \forall i \in \{1, \dots, n\}$. $\varphi$ è omo perché $\varphi(x_1^{\pm 1} x_2^{\pm 1} \dots x_n^{\pm n}) = (g_1^{\pm 1}, \dots, g_n^{\pm 1})$

- **Corollario $G$ è quoziente:** Ogni gruppo finito è quoziente di un gruppo libero.

→ **Dim** Siano $g_1, \dots, g_n \in G$ generatori (se fossero $m$ prendo $\mathbb{F}_m$ e $\mathbb{Z}$ finitamente generato perché finito), $\varphi: \mathbb{F}_n \longrightarrow G$, $x_i \longmapsto g_i$. $\varphi$ è surj perché $g_1, \dots, g_n \in \mathrm{Imm}\,\varphi \Rightarrow G = \mathrm{Imm}\,\varphi$. Ma quindi per 1th omo $G \cong \frac{\mathbb{F}_n}{\ker\varphi}$

- Un esempio di questo risultato è il seguente: $D_n \cong \frac{\mathbb{F}_2}{\ker\varphi}$ con $\varphi: \mathbb{F}_2 \longrightarrow D_n$, $x_1 \mapsto r$, $x_2 \mapsto s$

dunque $x_1^n \in \ker\varphi$, $x_2^2 \in \ker\varphi$, $x_1 x_2 x_1 x_2 \in \ker\varphi$

- **Proposizione $\ker\varphi \lhd \mathbb{F}_2$:** $\ker\varphi$ è il più piccolo sottogruppo normale di $\mathbb{F}_2$ che contiene $\{x_1^n, x_2^2, x_1 x_2 x_1 x_2\}$

→ **Dim** Sia $N \lhd \mathbb{F}_2$, supponiamo che $x_1^n, x_2^2, x_1 x_2 x_1 x_2 \in N$. Voglio dimostrare che $|\mathbb{F}_2 / N| \leq 2n$.
Innanzitutto noto che $x_1^{-1} N = x_1^{n-1} N$; $x_2^{-1} N = x_2 N$, dunque "posso usare solo esponenti positivi".
$x_1 x_2 x_1 x_2 \in N \Rightarrow x_1 x_2 N = x_2^{-1} x_1^{-1} N = x_2 x_1^{-1} N$ ma quindi preso un elemento generico in $\mathbb{F}_2/N$ $x_1^a x_2^b N = x_1^{a-1} x_1 x_2 x_2^{b-1} N = x_1^{a-1} x_2 x_1^{-1} x^{b-1} N$
$= x_2 x^{-a+1} x_1^{-1} x_2^{b-1} N = x_2 x^{-a} x_2^{b-1} N = x_2^b x_1^{(-1)^b a} N$
(per induzione scambio $x_1 x_2$ a volte; per induzione scambio $x_1 x_2$ $b$ volte)

Ma questo significa che preso $x_1^{a_1} x_2^{a_2} \dots x_1^{a_{2k+1}} x_2^{a_{2k+2}} N = x_2^{\alpha} x_1^{\beta} N$ con $0 \leq \alpha \leq 1$, $0 \leq \beta \leq n-1$ $\Rightarrow$ ho $2n$ elementi (al massimo).

- **Definizione quoziente gruppo libero:** Sia $n \in \mathbb{N}$, $r_1, \dots, r_k$ relazioni in $\mathbb{F}_n$, $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$ è il quoziente del gruppo libero $\mathbb{F}_n$ per il sottogruppo normale generato da $r_1, \dots, r_k$.

- **Esempi:** • $D_n = \langle r, s \mid r^n = s^2 = e, \ rsrs = e \rangle$ • $\langle x \mid x^n = e \rangle \cong \mathbb{Z}/n\mathbb{Z}$
• $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \langle x_1, x_2 \mid x_1^n = x_2^m = e, [x_1, x_2] \rangle$
(quoziento per il commutatore $\Rightarrow$ il gruppo è abel)

- Sia $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$, $H$ gruppo. $\mathrm{Hom}(G, H) \cong \mathrm{Hom}(\frac{\mathbb{F}_n}{\ker\varphi}, H) =$
$= \{\varphi: \mathbb{F}_n \longrightarrow H \mid \langle r_1, \dots, r_k \rangle < \ker\varphi\} = \{\varphi: \mathbb{F}_n \longrightarrow H \mid r_1, \dots, r_k \in \ker\varphi\} \cong \{(h_1, \dots, h_n) \in H^n \mid \text{soddisfano } r_1, \dots, r_k\}$
(proprietà universale)

## Esercizi:

1 - $|\mathrm{Aut}(Q_8)| = ?$

In $Q_8$ ho $\langle i \rangle, \langle j \rangle, \langle k \rangle < Q_8$ di ordine 4. Sia $\varphi: \mathrm{Aut}(Q_8) \longrightarrow S_3$, questa applicazione è surj perché $f: (i \mapsto j \wedge j \mapsto i) \mapsto (1\,2)$ e $g: (j \mapsto k \wedge k \mapsto j) \mapsto (2\,3)$ generano $S_3$. Dunque $\ker\varphi = \{\varphi \in \mathrm{Aut}(Q_8) \mid \varphi(\langle i \rangle) = \langle i \rangle \wedge \varphi(\langle j \rangle) = \langle j \rangle\}$
$\Rightarrow \varphi(i) \in \{i, -i\}$, $\varphi(j) \in \{j, -j\}$. Ma quindi $\ker\varphi \cong V_4$ (il Kleein)
(questo perché ho 4 automorfismi di ordine 2 che scambiano gli elementi a 2 a 2.)

Noto che $f, g \notin \mathrm{Inn}(G)$ e $\langle \varphi(f) \varphi(g) \rangle = S_3$
$\Rightarrow K = \langle f, g \rangle \cong S_3$ e $K < \mathrm{Aut}(Q_8)$

Ma (i) $\ker\varphi \lhd \mathrm{Aut}(Q_8)$
(ii) $\ker\varphi \cap K = \{id\}$
(iii) $\ker\varphi K = \mathrm{Aut}(Q_8)$
$\Rightarrow$ th dec prod semidir

$\mathrm{Aut}(Q_8) \cong V_4 \rtimes S_3 \cong S_4$

**Esercizio 1**: Caratterizza il 3-Sylow di $S_9$

Innanzitutto noto che $|P_3| = 81$. Sia $H = \langle (1\,2\,3)(4\,5\,6), (7\,8\,9) \rangle \cong (\mathbb{Z}/3\mathbb{Z})^2$ e quindi $|H| = 27$. Per il ③ di Sylow (inclusione) sappiamo che $H \leq P_3$ e $[P_3 : H] = 3$ ma 3 è il più piccolo primo che divide la cardinalità di $P_3$, dunque (per esercizio 1 lezione 20/10) $H \lhd P_3 \Rightarrow P_3 \leq N_{S_9}(H)$. Sia $\tau = (1\,4\,7)(2\,5\,8)(3\,6\,9) \in N_{S_9}(H)$, noto che $\tau \notin H$.
Ma dunque $P_3 = H \rtimes_\varphi \langle \tau \rangle \cong (\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ con $\varphi : \mathbb{Z}/3\mathbb{Z} \to Aut((\mathbb{Z}/3\mathbb{Z})^3) \cong GL_3(\mathbb{F}_3)$

$G$ ① $H \lhd P_3$ ② $H\langle\tau\rangle = P_3$ ③ $H \cap \langle\tau\rangle = \{e\}$

tb dec prod semidir

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

**Esercizio 2**: Caratterizza il 3-Sylow di $S_n$ per $n \geq 9$

- $n = 9$ $\quad P_3 = (\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$
- $n = 10, 11$ Dato che $S_9 \leq S_{10} \leq S_{11}$ e il 3-Sylow ha sempre cardinalità 81, è lo stesso di prima
- $n = 12$ $\quad P_3 \cong \underbrace{((\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z})}_{\text{il 3-Sylow di prima}} \times \underbrace{\mathbb{Z}/3\mathbb{Z}}_{\langle (10\,11\,12) \rangle}$
- $n = 18$ $\quad P_3 \cong \underbrace{((\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z})}_{\text{3-Sylow di } S_9} \times \underbrace{((\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z})}_{\text{3-Sylow di } S_9}$ (per 13,14 ovvio, per 15 moltiplico $\langle (3\,4\,5)(7\,8\,9) \rangle$ per 16,17 ovvio)
- $n = 27$ $\quad P_3 \cong ((\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}) \times ((\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}) \times ((\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z})) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

3-Sylow di $S_9$ × 3-Sylow di $S_9$ × 3-Sylow di $S_9$ $\langle (1\,10\,19)(2\,11\,20) \dots (9\,18\,27) \rangle$

perché sto scambiando i 3-Sylow di $S_9$ fra loro

**Esercizio 3**: Sia $G$ gruppo finito, $H \lneq G \Rightarrow G \neq \bigcup_{g \in G} gHg^{-1}$

Sia $G \circlearrowright \{gHg^{-1} \mid g \in G\}$ azione di coniugio. Noto che $|\{gHg^{-1} \mid g \in G\}| = |Orb(H)|$ per l'azione di coniugio, dunque $|\{gHg^{-1} \mid g \in G\}| = \frac{|G|}{|St_G(H)|} = \frac{|G|}{|N_G(H)|}$ (lo stabilizzatore per l'azione di coniugio è il normalizzatore)

lemma orbita-stabilizzatore

Questo significa che: $|\bigcup_{g \in G} gHg^{-1}| \leq |\{gHg^{-1} \mid g \in G\}| \cdot |H| = \frac{|G|}{|N_G(H)|} \cdot |H| \leq |G|$

- se almeno uno dei $\leq$ è $<$ $\Rightarrow |\bigcup_{g \in G} gHg^{-1}| < |G| \Rightarrow G \neq \bigcup_{g \in G} gHg^{-1}$
- se $|\bigcup_{g \in G} gHg^{-1}| = |\{gHg^{-1} \mid g \in G\}||H|$ e $|N_G(H)| = |H|$ ↯ perché almeno due di questi gruppi sono coniugati perché $H \lhd G$ e l'identità appartiene a tutti i gruppi, dunque avrei $|\bigcup_{g \in G} gHg^{-1}| > |G|$

- **Definizione azione transitiva**: Sia $G$ gruppo, $X$ insieme, $G \circlearrowright X$ azione, è transitiva se $\forall x, y \in X \ \exists g \mid gx = y$

**Esercizio 4**: Sia $G$ gruppo, $X$ insieme, $G \circlearrowright X$ transitiva $\Rightarrow \forall x, y \in X \ \exists g \mid Stab(x) = g\,Stab(y)\,g^{-1}$

Siano $x, y \in X \Rightarrow \exists g \in G \mid gx = y$ (perché l'azione è transitiva). Ma quindi $Stab(y) = Stab(gx) \supseteq g\,Stab(x)\,g^{-1}$, infatti: se $s \in Stab(x) \Rightarrow gsg^{-1}(gx) = gsx = gx$ perché $s \in Stab(x)$
Dato che $gx = y \Rightarrow x = g^{-1}y$, dunque:
$Stab(x) = Stab(g^{-1}y) \supseteq g^{-1}\,Stab(y)\,g$ (per la stessa argomentazione sopra). Dunque $g\,Stab(x)\,g^{-1} \supseteq Stab(y)$ ← semplicemente moltiplico a sx per $g$ e a dx per $g^{-1}$
$\Rightarrow Stab(y) = g\,Stab(x)\,g^{-1}$

- **Definizione punti fissi**: Sia $G$ gruppo, $X$ insieme, $G \circlearrowright X$ azione, $g \in G$ ha punto fisso se $\exists x \in X \mid g \in Stab(x)$

**Esercizio 5**: Sia $G$ gruppo finito, $X$ insieme $G \circlearrowright X$ transitiva. Se $|X| \geq 2 \Rightarrow \exists g \in G$ che agisce senza punti fissi (la negazione di quello sopra: $\forall x \in X \ g \notin Stab(x)$)

Sia $x_0 \in X$; $\bigcup_{x \in X} Stab(x) = \bigcup_{g \in G} g\,Stab(x_0)\,g^{-1}$. Dato che $|X| \geq 2 \Rightarrow |Orb(x)| \geq 2$

$\Rightarrow Stab(x_0) \lneq G \Rightarrow \bigcup_{g \in G} g\,Stab(x_0)\,g^{-1} \neq G$ (per es 4, es ③) $\Rightarrow \exists g \in G \setminus \bigcup_{g \in G} g\,Stab(x_0)\,g^{-1} \Rightarrow g$ non ha punti fissi

Esercizio 6: $S_n$ è generato da $\tau = (1 \dots n)$ e $(1\,2)$

Innanzitutto sia $H = \langle \tau, (1\,2) \rangle$. Noto che $\tau(1\,2)\tau^{-1} = (\tau(1)\ \tau(2)) = (2\ 3)$ $\Rightarrow (2\ 3) \in H$. Ma quindi $\tau(2\ 3)\tau^{-1} = (3\ 4) \Rightarrow \dots \Rightarrow \tau(n-2\ n-1)\tau^{-1} = (n-1\ n)$.
Perciò in $H$ ho tutti gli elementi della forma $(i\ i+1)$.
Sia $i<j$. Noto che $(i \dots j) = (i\ i+1)(i+1\ i+2) \dots (j-1\ j) \in H$.
Dunque in $H$ ho le permutazioni del tipo $(i\ i+1\ i+2 \dots j-1\ j)$
Infine $(i\ j) = (i+1\ i+2 \dots j)^{-1}(i\ i+1)(i+1\ i+2 \dots j) \in H$.
Ma quindi in $H$ ho tutte le trasposizioni e $H$ generato di tutte le trasposizioni è proprio $S_n$.

## Algebra Lezione 05/11/25 (teoria - Del Corso)

- N.B. $I \subsetneq A \iff I \cap A^* = \emptyset$ (questo perché $I \cap A^* \neq \emptyset \Rightarrow I = A$ e $I = A \Rightarrow 1 \in I \cap A^*$)
  $(x)$ proprio $\iff x \notin A^*$ (questo perché $x \in A^* \iff (x) = A$)

- **Proposizione proprietà degli ideali massimali:**

  (i) Ogni ideale proprio di $A$ è contenuto in un ideale massimale.

  (ii) Ogni elemento non invertibile di $A$ è contenuto in un ideale massimale.

  → Dim (i) Sia $I \subsetneq A$ ideale proprio $\mathcal{J} = \{J \subsetneq A \mid I \subseteq J\}$ ($I \in \mathcal{J} \Rightarrow \mathcal{J} \neq \emptyset$)

  · $(\mathcal{J}, \subseteq)$ è induttivo. Sia $\mathcal{C} = \{I_\lambda\}_{\lambda \in \Lambda}$ catena di $\mathcal{J}$

  ogni catena di $\mathcal{J}$ ammette maggiorante:
  · $C = \bigcup_{\lambda \in \Lambda} I_\lambda$ $C \in \mathcal{J}$ ($C \subsetneq A \wedge I \subseteq C$)
  · $\forall I_\lambda \in \mathcal{C}$ $I_\lambda \subseteq C$ per definizione di $C$
  · S.A. $C$ non è proprio $\Rightarrow 1 \in C \Rightarrow 1 \in \bigcup_{\lambda \in \Lambda} I_\lambda \Rightarrow \exists I_k \mid 1 \in I_k \not\subsetneq$
  · Per Zorn abbiamo in $\mathcal{J}$ un elemento massimale $M$

  $M$ è massimale nell'anello: Sia $L \subsetneq A \mid M \subseteq L \Rightarrow I \subseteq L \Rightarrow L \in \mathcal{J}$ ma $M$ è massimale in $\mathcal{J}$ $\Rightarrow L = M$

  (ii) Sia $x \in A \setminus A^*$, per quanto notato sopra $(x) \subsetneq A$. Per (i) $(x) \subseteq M \Rightarrow x \in M$

- **Proposizione caratterizzazione degli ideali primi e massimali:** Sia $I \subsetneq A$ ideale

  (i) $I$ è primo $\iff A/I$ è dominio

  (ii) $I$ è massimale $\iff A/I$ è campo

  → Dim (i) Sia $x, y \in A$. $A/I$ dominio $\iff (x+I)(y+I) = I \iff xy + I = I$
  $\iff xy \in I \Rightarrow x \in I \vee y \in I \iff I$ primo

  (ii) $I$ è massimale $\iff$ in $A/I$ gli unici ideali sono $I$ e $A/I \iff$
  $\forall \bar{x} = x + M \in A/M$ $\bar{x}$ invertibile $\iff A/I$ campo

- **Corollario caratterizzazione degli ideali primi e massimali:** Sia $A$ anello

  (i) $A$ è dominio $\iff (0)$ è primo

  (ii) $A$ è campo $\iff (0)$ è massimale

  (iii) $I$ massimale $\Rightarrow I$ primo

  → Dim (i) $(0)$ primo $\iff A/(0)$ dominio $\iff A$ dominio ($A/(0) \cong A$)

  (ii) $(0)$ massimale $\iff A/(0)$ campo $\iff A$ campo

  (iii) $I$ massimale $\iff A/I$ campo $\Rightarrow A/I$ dominio $\iff I$ primo

- Noto che $\mathbb{Z}$ dominio $\Rightarrow (0)$ è primo. Ma quindi $\mathbb{Z}/n\mathbb{Z}$ è dominio $\iff n\mathbb{Z}$ è primo $\iff n = 0 \vee n$ primo
  $\mathbb{Z}/n\mathbb{Z}$ è campo $\iff n$ primo $\iff n\mathbb{Z}$ massimale

- **Esempio**: dato $\mathbb{Z}[x]$, so che è dominio. Sia $\bar{a}=(x)$. Consideriamo l'omo di valutazione $\varphi_0 : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$, $q(x) \longmapsto q(0)$. Noto che è suriettivo e $\ker\varphi_0 = \{a(x) \mid a(0)=0\} = \{a(x) \mid x \mid a(x)\} = (x) \Rightarrow \mathbb{Z}[x]/(x) \cong \mathbb{Z}$ (1° teorema)

ma $\mathbb{Z}$ non è un campo $\Rightarrow \mathbb{Z}[x]/(x)$ non è campo $\Rightarrow (x)$ non massimale

- **Corollario la proiezione conserva primi/mass.**: Sia $A$ anello $I \subsetneq A$, $\pi_I : A \longrightarrow A/I$ conserva ideali primi e massimali (fra gli ideali che contengono $I$)

→ **Dim**: Sia $J \subset A$ $(I \subseteq J)$, dunque $\pi_J(J) = J/I$

- $J$ primo in $A \overset{\text{def}}{\iff} A/J$ dominio $\iff A/I / J/I$ dominio $\iff J/I$ primo

$A/J \overset{\uparrow}{\cong} A/I / J/I$ 2° teorema

- **Definizione parte moltiplicativa**: Consideriamo $A$ anello commutativo con identità che sia anche dominio. Sia $S \subset A$ | (i) $0 \notin S$ (ii) $1 \in S$ (iii) $xy \in S$ $\forall x, y \in S$

allora diremo che $S$ è la parte moltiplicativa di $A$

- **Definizione frazioni dominio**: Sia $A$ anello commutativo con identità che sia dominio, $S$ una sua parte moltiplicativa. Chiameremo insieme delle frazioni di un dominio $S^{-1}A = \{\frac{a}{s} \mid a \in A, s \in S\}/\sim$ con la relazione $\sim$ $\frac{a}{s} \sim \frac{b}{t} \iff at = bs$

## Esercizi:

1. $\sim$ è una relazione di equivalenza

- riflessiva $as = as \Rightarrow \frac{a}{s} \sim \frac{a}{s}$
- simmetria $\frac{a}{s} \sim \frac{b}{t} \Rightarrow at = bs \Rightarrow bs = at \Rightarrow \frac{b}{t} \sim \frac{a}{s}$
- transitiva $\frac{a}{s} \sim \frac{b}{t}$ e $\frac{b}{t} \sim \frac{c}{u} \Rightarrow at = bs$ e $bu = ct \Rightarrow aut = bus \Rightarrow aut = cts$
$\Rightarrow t(au - cs) = 0 \overset{t \in S \Rightarrow t \neq 0}{\Rightarrow} au = cs \Rightarrow \frac{a}{s} \sim \frac{c}{u}$

- **Proposizione anello delle frazioni di un dominio**: $(S^{-1}A, +, \cdot)$ è un anello con identità, definendo:

⊕ $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$

⊙ $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

→ **Dim** è sufficiente dimostrare che le operazioni sono ben definite:

$\frac{a}{s} \sim \frac{a'}{s'}$ e $\frac{b}{t} \sim \frac{b'}{t'}$, allora $as' = a's$ e $bt' = b't$

⊕ $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ e $\frac{a'}{s'} + \frac{b'}{t'} = \frac{a't'+b's'}{s't'}$ se sono uguali $\Rightarrow$

$\frac{at+bs}{st} = \frac{a't'+b's'}{s't'} \Rightarrow s't'(at+bs) = st(a't'+b's') \Rightarrow$

$s't'(at+bs) = a's tt' + b'ts s' \Rightarrow s't'(at+bs) = as'tt' + bt's s' \rightarrow$

$s't'(at+bs) = s't'(at+bs)$

⊙ $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ e $\frac{a'}{s'} \cdot \frac{b'}{t'} = \frac{a'b'}{s't'}$ se sono uguali $\Rightarrow \frac{ab}{st} = \frac{a'b'}{s't'} \Rightarrow abs't' = a'bst$

$\Rightarrow abs't' = a'sb't \Rightarrow abs't' = as'bt' \Rightarrow abs't' = abs't'$

- Sia $A$ dominio, $S = A - \{0\}$, in questo caso chiameremo $S^{-1}A = Q(A)$ il campo dei quozienti di $A$
- Sia $A$ dominio, $P \subset A$ primo, $S = A - P$, in questo caso diremo che $S$ è parte moltiplicativa, ovvero $x, y \in S \Rightarrow xy \in S$
- Sia $A = \mathbb{Z}$, $S = \{10^n\}_{n \geq 0} \Rightarrow S^{-1}A = \{\frac{a}{10^n} \mid a \in \mathbb{Z}, n \geq 0\}$ ovvero ho i decimali con sviluppo finito

- **Proposizione $S^{-1}A$ come estensione:** Siano $S,T$ parti moltiplicative di $A$, $S \subseteq T \Rightarrow S^{-1}A \hookrightarrow T^{-1}A$

→ **Dim** Sia $\varphi: S^{-1}A \to T^{-1}A$, $\frac{a}{s} \mapsto \frac{a}{s}$ (sono equivalenti in $A$)

- b.d. Sia $\frac{a}{s} \sim \frac{a'}{s'}$, allora $\varphi(\frac{a}{s}) = \frac{a}{s} \overset{\sim}{\in} \frac{a'}{s'} = \varphi(\frac{a'}{s'})$
- omo $\varphi(\frac{a}{s})\varphi(\frac{b}{t}) = \frac{a}{s}\cdot\frac{b}{t} = \frac{ab}{st} = \varphi(\frac{ab}{st}) = \varphi(\frac{a}{s}\cdot\frac{b}{t})$

$\varphi(\frac{a}{s}) + \varphi(\frac{b}{t}) = \frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} = \varphi(\frac{at+bs}{st}) = \varphi(\frac{a}{s}+\frac{b}{t})$

- inj $\ker\varphi = \{\frac{a}{s} \mid \varphi(\frac{a}{s}) = 0\} = \{\frac{a}{s} \mid \frac{a}{s} = 0\} = \{\frac{a}{s} \mid a = 0\} = \{0\}$ perché $\frac{0}{s} \sim \frac{0}{t}$ $\forall s,t$

- In particolare $I = \{1\}$ è parte moltiplicativa dunque $A \cong I^{-1}A \hookrightarrow S^{-1}A$ $\forall S$ p.m.
- Chi sono gli invertibili di $S^{-1}A$?

$(S^{-1}A)^* = \{\frac{a}{s} \mid \exists \frac{b}{t} : \frac{a}{s}\cdot\frac{b}{t} = 1\} = \{\frac{a}{s} \mid \exists \frac{b}{t} : ab = st\} \ominus \{\frac{a}{s} \mid \exists b : ab \in S\}$

$\subseteq$ $\frac{a}{s} \in (S^{-1}A)^* \Rightarrow \exists \frac{b}{t} \mid \frac{a}{s}\cdot\frac{b}{t} = \frac{1}{1} \Rightarrow \frac{ab}{st} = \frac{1}{1} \Rightarrow ab\cdot 1 = st\cdot 1 \Rightarrow ab = st$

ma $st \in S \Rightarrow ab \in S$

$\supseteq$ Sia $\frac{a}{s} \mid \exists b : ab \in S \Rightarrow \frac{a}{s}\cdot\frac{bs}{as} = \frac{abs}{abs} = \frac{1}{1}$ ($bs \in A$ sempre; $as \in S$ per ipotesi)

- Infatti se $S = \{10^n\}_{n\geq 1}$, $(S^{-1}\mathbb{Z})^* = \{\frac{a}{s} \mid a = 2^\alpha 5^\beta \text{ con } \alpha,\beta \geq 0\}$
- **Proposizione $A \subseteq Q(A)$:** Sia $A$ dominio, $S = A\setminus\{0\}$ p.m. $\Rightarrow S^{-1}A = Q(A)$ è il più piccolo campo che contiene $A$

→ **Dim**
- $A \subseteq Q(A)$ ovvio perché $A \hookrightarrow S^{-1}A$ per la prop. prec.
- $Q(A)$ è campo ovvio perché $(Q(A))^* = \{\frac{a}{s} \mid \exists b : ab \in S\} = Q(A)\setminus\{0\}$ (perché per ogni $a \in S$)
- $K$ campo $\mid A \subseteq K \Rightarrow Q(A) \subseteq K$. Sia $\frac{1}{a} \in K$ $\forall a \in A\setminus\{0\} \Rightarrow \forall b \in A$ $b\cdot\frac{1}{a} \in K$ $\Rightarrow \frac{b}{a} \in K$ ma $\frac{b}{a} \in Q(A) \Rightarrow Q(A) \subseteq K$

## Algebra Lezione 07/11/25 (esercitazione - Patimo)

- Notiamo che il coniugio fattore:
  - $G$ abel $\Rightarrow G' = \{e\}$
  - $G/K$ abel $\Leftrightarrow K \supset G'$
  - $S_n' = A_n$
  - $A_n' = A_n$ (per $n \geq 5$) $A_4' = V_4$ $A_n' = \{e\}$ ($n \neq 3$)
  - $D_n' = \langle r^2 \rangle$ (per $n$ pari) $D_n = \langle r \rangle$ (per $n$ dispari)

- **Lemma normalizzatore-centralizzatore:** Sia $G$ gruppo $H < G \Rightarrow Z_G(H) \trianglelefteq N_G(H)$. Inoltre $N_G(H)/Z_G(H) \hookrightarrow Aut(H)$

**Esercizio 1:** Sia $G$ $p$-gruppo, $H$ $q$-gruppo, $p \neq q$ $|G| = p^n$ $|H| = q^m$, $A = G_A \rtimes_\varphi H_A$ e $B = G_B \rtimes_\psi H_B$ allora $A \cong B \Rightarrow \ker\varphi \cong \ker\psi$

Sia $f: A \to B$ iso, allora $f(G_A) = G_B$ e $gf(H_A)g^{-1} = H_B$; questo perché: il $p$-Sylow è unico (in quanto $G_B \trianglelefteq B$) e $f(H_A)$ sarà uno dei $q$-Sylow.

Dunque $\ker\varphi = H_A \cap Z_A(G_A)$, perciò $f(\ker\varphi) = f(H_A) \cap f(Z_A(G_A)) = f(H_A) \cap Z_B(f(G_A)) = f(H_A) \cap Z_B(G_B)$

ma quindi $gf(\ker\varphi)g^{-1} = g f(H_A) g^{-1} \cap g Z_B(G_B) g^{-1} = H_B \cap Z_B(G_B) = \ker\psi$

ma quindi $c_g \circ f : \ker\varphi \to \ker\psi$ iso.

**Esercizio 2:** $SL_2(\mathbb{F}_4) \cong A_5$ (ricordiamo che det è omo surj)

$SL_2(\mathbb{F}_4) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{F}_4,\ ad - bc = 1\}$. Dunque $SL_2(\mathbb{F}_4) = \ker(\det)$ con $\det: GL_2(\mathbb{F}_4) \to \mathbb{F}_4^*$

Perciò $\frac{GL_2(\mathbb{F}_4)}{SL_2(\mathbb{F}_4)} \cong \mathbb{F}_4^*$ $\Rightarrow |SL_2(\mathbb{F}_4)| = \frac{|GL_2(\mathbb{F}_4)|}{|\mathbb{F}_4^*|}$ $\Rightarrow |SL_2(\mathbb{F}_4)| = 60$

Sia $H \in SL_2(\mathbb{F}_4)$ che agisce sullo spazio 1-dimensionale per moltiplicazione a sinistra cioè $H\langle v\rangle = \langle Hv\rangle$.
Dunque $SL_2(\mathbb{F}_4) \curvearrowright \{1\text{-dim sottospazi di } \mathbb{F}_4^2\}$ perciò $\varphi: SL_2(\mathbb{F}_4) \longrightarrow S(X) \cong S_5$, $H \longmapsto \varphi_H$

Se $\varphi(H) = id \Rightarrow H\langle\begin{pmatrix}1\\0\end{pmatrix}\rangle = \langle\begin{pmatrix}1\\0\end{pmatrix}\rangle \Rightarrow \langle\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\rangle = \langle\begin{pmatrix}a\\c\end{pmatrix}\rangle = \langle\begin{pmatrix}1\\0\end{pmatrix}\rangle$

$H\langle\begin{pmatrix}0\\1\end{pmatrix}\rangle = \langle\begin{pmatrix}0\\1\end{pmatrix}\rangle \Rightarrow \langle\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\rangle = \langle\begin{pmatrix}b\\d\end{pmatrix}\rangle = \langle\begin{pmatrix}0\\1\end{pmatrix}\rangle$

$\Rightarrow H = \begin{pmatrix}a&0\\0&d\end{pmatrix} = \begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix}$ (perché $\det(H)=1$). Ma quindi $H\langle\begin{pmatrix}1\\0\end{pmatrix}\rangle = \langle\begin{pmatrix}a\\0\end{pmatrix}\rangle \iff \begin{pmatrix}a\\0\end{pmatrix} \in \langle\begin{pmatrix}1\\0\end{pmatrix}\rangle \Rightarrow a^{-1} = a \Rightarrow a^2 = 1$

$\Rightarrow a = \pm 1 \Rightarrow a = 1$ (perché $-1 = 1$ in $\mathbb{F}_4$)

Ma quindi l'azione è fedele $\Rightarrow \varphi$ è omo inj. Dato che $[S_5 : \varphi(SL_2(\mathbb{F}_4))] = 2$

$\Rightarrow A_5 \leq \varphi(SL_2(\mathbb{F}_4))$ ma $|SL_2(\mathbb{F}_4)| = 60 = |A_5| \Rightarrow A_5 \cong SL_2(\mathbb{F}_4)$

**Esercizio 3:** $A_6$ è semplice

Innanzitutto ricordiamo che le classi di coniugio degli elementi in $A_6$ sono gli elementi con la stessa decomposizione in cicli disgiunti:

- 5-cicli $\Rightarrow |Cl(\sigma)| = \binom{6}{5}\frac{5!}{5} = 144 \longrightarrow$ in $S_6$
- 4-ciclo 2-ciclo $\Rightarrow |Cl(\sigma)| = \binom{6}{4}\frac{4!}{2}\binom{2}{2}\frac{2!}{2} = 90$
- 3-ciclo 3-ciclo $\Rightarrow |Cl(\sigma)| = \frac{1}{2}\binom{6}{3}\frac{3!}{3}\cdot\binom{3}{3}\frac{3!}{3} = 40$
- 3-ciclo $\Rightarrow |Cl(\sigma)| = \binom{6}{3}\frac{3!}{3} = 40$
- 2-ciclo 2-ciclo $\Rightarrow |Cl(\sigma)| = \frac{1}{2}\binom{6}{2}\frac{2!}{2}\binom{4}{2}\frac{2!}{2} = 45$
- $e \Rightarrow |Cl(e)| = 1$

Sia $N \lhd A_6$. $N \lhd A_6 \iff N$ è unione disgiunta delle classi di coniugio dei suoi elementi. Dunque $|N| = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60, 120\}$ perché $N \leq A_6$. Ma quindi non posso sommare in nessun modo gli elementi delle classi di coniugio per ottenere sottogruppi normali diversi da $\{e\}$ e $A_6$

**Esercizio 4:** $A_n$ è semplice per $n \geq 5$

→ Base $A_5$ semplice $A_6$ semplice

→ P.I. Sia $H \lhd A_{n+1}$, $K_i = \{\sigma \in A_{n+1} \mid \sigma(i) = i\}$. Tale $K_i \cong A_n$

Dato che $H$ è normale $\Rightarrow H \cap K_i$ è normale $\Rightarrow H \cap K_i$ è normale in $A_n$ perché $\dots$

Dunque o $H \cap K_i$ è banale o $H \cap K_i = K_i$. Ma questo significa che $\exists i \mid K_i \leq H \Rightarrow H$ contiene un 3-ciclo. ma $H$ normale $\Rightarrow H$ contiene tutti i 3-cicli $\Rightarrow H = A_n$. Se $H \cap K_i = \{e\} \Rightarrow H = \{id\}$ perché altrimenti: $\exists \sigma \in H - \{id\} \mid \sigma(1) = j$

Sia $\tau = (j\ k\ \ell)$ con $1 \neq j \neq k \neq \ell$. $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \in H$. Sia $\rho = \sigma\tau\sigma^{-1}$ ($\sigma \in H$, $\tau^{-1} \in H$ perché normale)

$\Rightarrow [\sigma, \tau] = \rho\tau^{-1}$ quindi è prodotto di due 3-cicli quindi ci sono al più 6 elementi non fissi.

Dato che $n \geq 6$ $A_7 \leq A_{n+1} \Rightarrow [\sigma, \tau]$ ha almeno un punto fisso ma dato che $H \cap K_i = \{e\} \Rightarrow [\sigma, \tau] = e \Rightarrow \sigma, \tau$ commutano.

Ma $(\sigma\tau)(1) = \sigma(1) = j$ e $(\tau\sigma)(1) = \tau(j) = k$ ↯ Dunque $H = \{id\}$

$\Rightarrow A_{n+1}$ è semplice $\Rightarrow A_n$ è semplice

**Esercizio 5:** Sia $G$ gruppo $|G| = p^5$, $|Z(G)| = p^2$ (i) $|G'| \mid p^3$, $|(G/Z)'| \mid p$

(ii) $|G'| = p^3 \Rightarrow Z \subset G'$ e $G'$ abel

(i) Sia $N \lhd G \mid |N| = p^3$, quindi $|G/N| = p^2 \Rightarrow G/N$ abel $\Rightarrow G' < N \Rightarrow |G'| \mid |N| = p^3$.

$|G/Z| = p^3$ $\exists N \lhd G/Z$ con $|N| = p$ $|\frac{G/Z}{N}| = p^2 \Rightarrow (G/Z)' < N$ e $|(G/Z)'| \mid p$

(ii) $(G/Z)'$ è generato dai commutatori: $aZbZa^{-1}Zb^{-1}Z = aba^{-1}b^{-1}Z = [a,b]Z$

$\Rightarrow (G/Z)'$ è generato dall'immagine dei commutatori tramite $\pi: G \to G/Z$

ma quindi $\pi(G') = G'Z/Z = (G/Z)' \Rightarrow |G'Z/Z| \leq p$. D'altra parte $|G'Z/Z| = \frac{|G'Z|}{|Z|} =$

$= \frac{|G'||Z|}{|G' \cap Z||Z|} = \frac{p^3 p^2}{|G' \cap Z| p^2} = p \Rightarrow |G' \cap Z| = p^2 \Rightarrow Z \subset G'$

Dato che $Z \subset G' \Rightarrow Z(G) < Z(G') \Rightarrow Z_{G'}(G')$ ha almeno $p^2$ elementi:

- $|Z_{G'}(G')| = p^3 \Rightarrow G'$ abel
- $|Z_{G'}(G')| = p^2 \Rightarrow G'/Z(G)$ ciclico $\lightning$

**Esercizio 6:** Sia $G = \mathbb{Z}/4\mathbb{Z} \times D_7$ (i) è vero che $G \cong \mathbb{Z}/7\mathbb{Z} \times D_4$?

(ii) Conta gli omo inj $f: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$

(i) $Z(G) = Z(\mathbb{Z}/4\mathbb{Z} \times D_7) = Z(\mathbb{Z}/4\mathbb{Z}) \times Z(D_7) = \mathbb{Z}/4\mathbb{Z} \times \{e\}$

$Z(\mathbb{Z}/7\mathbb{Z} \times D_4) = Z(\mathbb{Z}/7\mathbb{Z}) \times Z(D_4) = \mathbb{Z}/7\mathbb{Z} \times \{e\}$

hanno centri diversi quindi non sono isomorfi

(ii) $f: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow G$ con $a \neq b$ e $ord(a), ord(b) = 2$ e $[a,b] = e$

$(1,0) \longmapsto a$

$(0,1) \longmapsto b$

gli elementi di ordine 2 in $G$ sono gli elementi della forma $(x,y)$

con $ord(x), ord(y) \mid 2$ e $(x,y) \neq (e,e)$. In $\mathbb{Z}/4\mathbb{Z}$ ho 2 elementi $x = 0, 2$

In $D_7$ ho $y = id, s, sr, \dots, sr^6$. Dunque se $a = (x, sr^n) \Rightarrow b = (x+2, sr^k)$ v $b = (x, id)$

quindi ho $7 \cdot 2 - 2$ possibilità

Se $a = (x, id) \Rightarrow b$ ha 14 possibilità. Quindi in totale sono 42 omo.

## Algebra Lezione 12/11/25 (teoria - Del Corso)

- **Definizione dominio euclideo:** Sia $A$ dominio di integrità, diremo che $A$ è dominio euclideo (ED) se $\exists d: A \setminus \{0\} \longrightarrow \mathbb{N}$ funzione grado con le proprietà:
  (i) $d(x) \leq d(xy) \quad \forall x, y \in A \setminus \{0\}$
  (ii) $\forall x \in A \ \forall y \in A \setminus \{0\} \ \exists q, r \in A \mid x = qy + r$ con $d(r) < d(y)$ (o $r = 0$)

  $K$ campo ↗

- Alcuni ED sono $\mathbb{Z}$, $K[x]$, $\mathbb{Z}[i]$ (col reticolo), $K[[x]]$

- **Definizione PID:** Sia $A$ dominio, diremo che $A$ è dominio a ideali principali (PID) se tutti i suoi ideali sono principali.

- **Definizione UFD:** Sia $A$ dominio, diremo che $A$ è dominio a fattorizzazione unica (UFD) se $\forall x \in A, x \notin A^* \cup \{0\}$ si scrive in modo unico a meno dell'ordine di fattori e di moltiplicazione per elementi invertibili come prodotto di elementi irriducibili

- **Proposizione ideali di un dominio euclideo:** Dato $A$ dominio euclideo $\Rightarrow A$ PID e $A$ è generato da un elemento di grado minimo

  → **Dim** Sia $I \subset A$ ideale, $I = \{0\} \Rightarrow I$ principale.

  - $x \in I \setminus \{0\}$ | $x$ ha grado minimo (esiste per principio del minimo)
  - $(x) \subseteq I$ (ovvio)
  - $(x) \supseteq I$ sia $a \in I$ facciamo div. ev. $a = qx + r$ $d(r) < d(x)$ v $r = 0$
    ma $a - qx = r \in I$ (↑ $I$) ma $x$ ha deg minimo $\Rightarrow r = 0 \Rightarrow a = qx \Rightarrow a \in (x)$

- **Proposizione elementi invertibili**: Dato $A$ dominio euclideo $\Rightarrow$ gli elementi di deg minimo in $A$ sono gli invertibili.

→ **Dim** $A$ è generato da $x \iff x \in A^*$
Per la proposizione $A$ è generato da $x \iff x$ ha deg minimo in $A$

- **Definizione primo**: Dato $A$ dominio, $x \in A$, $x \notin A^* \cup \{0\}$ diremo che $x$ è primo se $\forall a,b \in A \quad x \mid ab \Rightarrow x \mid a \vee x \mid b$

- **Definizione irriducibile**: Dato $A$ dominio, $x \in A$, $x \notin A^* \cup \{0\}$ diremo che $x$ è irrid se $\forall a,b \in A \quad x = ab \Rightarrow a \in A^* \vee b \in A^*$

- **Proposizione primo $\Rightarrow$ irrid**: Sia $A$ dominio, $x \in A$ primo $\Rightarrow x$ è irriducibile

→ **Dim** Sia $x = ab$, $x$ primo $\Rightarrow x \mid a \vee x \mid b$. Allora WLOG $x \mid a$.
$\cdot\ a = xc \Rightarrow x = xcb \Rightarrow x(1-bc) = 0$
$\cdot\ A$ dominio, $x \neq 0 \Rightarrow 1 - bc = 0 \Rightarrow bc = 1 \Rightarrow b, c \in A^*$

- **Proposizione caratterizzazione di primi e irrid. in domini**: Sia $A$ dominio, allora:

(i) $x$ primo $\iff (x)$ primo (non nullo)

(ii) $x$ irrid $\iff (x)$ massimale (fra gli ideali principali di $A$)

→ **Dim** (i) $(x)$ primo $\iff (ab \in (x) \iff a \in (x) \vee b \in (x)) \iff x \mid a \vee x \mid b \iff x$ primo

(ii) $\Rightarrow$ Sia $x$ irrid, $(x) \subseteq (y) \subsetneq A \Rightarrow \exists z \in A \mid x = yz$. Dato che $(y) \subsetneq A$ $y \notin A^* \Rightarrow z \in A^*$ perché $x$ irrid

Ma $(x) = (y) \Rightarrow (x)$ massimale (fra gli id. princ.)

$\Leftarrow$ Sia $x$ rid $\Rightarrow x = yz \mid y, z \notin A^* \Rightarrow (x) \subsetneq (y) \subsetneq (A) \Rightarrow (x)$ non è massimale ($y \notin A^* \Rightarrow 1 \notin (y)$)

- **Teorema caratterizzazione degli UFD**: Sia $A$ dominio, sono equivalenti:

(i) $A$ è UFD

(ii) Ogni irriducibile è primo e ogni catena discendente di divisibilità è stazionaria ($\{a_i\} \subset A \mid a_{i+1} \mid a_i \Rightarrow \exists n_0 \mid a_i \sim a_{n_0}\ \forall i \geq n_0$)
($a_i = \lambda a_{n_0}$ $\lambda \in A^*$)

- **Corollario PID $\Rightarrow$ UFD**: Sia $A$ PID $\Rightarrow$ $A$ UFD.

→ **Dim** (i) irrid $\Rightarrow$ primo Sia $x \in A$ irrid $\overset{\text{prop car primi e irrid}}{\Rightarrow} (x)$ mass. $\overset{\text{car caratt. id primi e mass}}{\Rightarrow} (x)$ primo $\Rightarrow x$ primo

(ii) Sia $(a_1) \subseteq (a_2) \subseteq \dots$ catena asc. di ideali principali; Sia $I = \bigcup (a_i)$

$I$ è ideale di $A$ e $I$ è principale $\Rightarrow \exists a \in A \mid I = (a) \Rightarrow \exists a_{n_0} \mid a \in (a_{n_0}) \Rightarrow I = (a) \subseteq (a_{n_0})$ ma $(a_{n_0}) \subseteq I = \bigcup (a_i)$

$\Rightarrow I = (a_{n_0}) \Rightarrow \forall i \geq n_0 \quad (a_i) = (a_{n_0}) \Rightarrow \{(a_i)\}_{i \geq 0}$ è staz.

(i) + (ii) per caratterizzazione degli UFD $\Rightarrow A$ UFD

- **Proposizione UFD $\Rightarrow \exists$ MCD**: Sia $A$ UFD, siano $a, b \in A$, $(a,b) \neq (0,0) \Rightarrow \exists \text{MCD}(a,b)$

→ **Dim** Sia $d$ il prodotto dei fattori irrid comuni fra $a, b$ presi col minimo esponente $\Rightarrow d = \text{MCD}(a,b)$

- Noto che ED $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow \exists$ MCD Ma quindi ED $\Rightarrow \exists$ MCD e PID $\Rightarrow \exists$ MCD

- Esempi: $\cdot\ K[\{x^{1/n}\}_{n \in \mathbb{N}}]$ non è UFD perché $\{x^{1/2^n}\}_{n \geq 0}$ è catena discend. inf.
$\cdot\ \mathbb{Z}[\sqrt{-5}]$ non è UFD perché 2 è irrid ma 2 non è primo

- **Teorema A UFD $\Rightarrow$ A[x] UFD**: Sia A UFD $\Rightarrow$ A[x] UFD

→ **Dim** • A UFD $\Rightarrow$ A dominio $\Rightarrow$ A[x] dominio

• (i) irrid $\Rightarrow$ primo Sia $f(x) \in A[x]$ irrid

• $\deg(f(x)) = 0 \Rightarrow f(x) = f \in A$, f irrid $\Rightarrow$ f primo

• $\deg(f(x)) = n > 0$ sia $f(x)$ prim. e irrid in $K[x]$, $K[x]$ è ED
$\Rightarrow f(x)$ primo in $K[x]$. Quindi se $f(x) | g(x)h(x)$ in A
$\Rightarrow f(x) | g(x)$ v $f(x) | h(x)$ in $K[x]$.
Dato che $f(x)$ primitivo per il corollario divisibilità nel campo dei quozienti $\Rightarrow$ divisibilità
$\Rightarrow f(x) | g(x)$ v $f(x) | h(x)$ in $A[x] \Rightarrow f(x)$ è primo

• (ii) per il lemma di Gauss $f(x) | g(x) \Rightarrow c(f(x)) | c(g(x))$ e $f'(x) | g'(x)$

• $\{c(f_i(x))\}$ è stazionaria perdo' cat dist. in A UFD.
Sia $n_0$ il punto in cui si stabilizza
• $\{f_i'(x)\}$ è stazionaria perché $\{\deg f_i'(x)\}$ è succ. di nat. decrescenti (qui mi si stabilizza). Sia $d_0$ il punto in cui si stabilizza
• $n_0 = \max\{n_0, d_0\} \Rightarrow c(f_i(x)) \sim c(f_{n_0}(x))$ ∧ $f_i'(x) \sim f_{n_0}'(x)$

$\Rightarrow f_i(x) = c(f_i(x)) f_i'(x) \sim c(f_{n_0}(x)) f_{n_0}'(x)$

- **Definizione contenuto**: Sia A UFD, $f(x) \in A[x]$, $f(x) = \sum_{i=0}^{n} a_i x^i$, chiameremo contenuto di $f(x)$ $c(f(x)) = (a_0, \dots, a_n)$

- **Definizione primitivo**: Sia A UFD, $f(x) \in A[x]$ diremo che $f(x)$ è primitivo se $c(f(x)) \sim 1$

- **Lemma di Gauss**: Sia A UFD, $f(x), g(x) \in A[x] \Rightarrow c(f(x)g(x)) = c(f(x))c(g(x))$

→ **Dim** • caso $f(x), g(x)$ primitivi $\Rightarrow c(f(x)) = c(g(x)) = 1$. Supponiamo $f(x)g(x)$ non prim.

▪ $\exists p \mid c(f(x)g(x)) \Rightarrow \pi_p : A[x] \to \frac{A}{(p)}[x]$, $f(x) \mapsto \overline{f(x)}$

▪ $\overline{f(x)} \neq 0$ ∧ $\overline{g(x)} \neq 0$ perché $p \nmid c(f(x))$, $p \nmid c(g(x))$

▪ $p \mid f(x)g(x) \Rightarrow \overline{f(x)}\,\overline{g(x)} = 0$ ma $\frac{A}{(p)}[x]$ dominio ↯

• caso generale $\Rightarrow f(x) = c(f(x)) f'(x)$, $g(x) = c(g(x)) g'(x)$ con $f'(x), g'(x)$ prim.

▪ $h(x) = f(x)g(x) = c(f(x))\,c(g(x))\,f'(x)g'(x) = c(h(x))\,h'(x)$

▪ $c(h(x)) = c(c(h(x))\,h'(x)) = c(c(f(x))\,c(g(x))\,f'(x)g'(x))$
posso portare fuori le costanti
▪ $c(h(x)) = c(h(x))\,c(h'(x)) = c(f(x)g(x))\,c(f'(x)g'(x))$
(i) ⟵ per caso prec ⟶ (i)

$c(h(x)) = c(f(x))\,c(g(x))$

- **Corollario divisibilità nel campo dei quozienti $\Rightarrow$ divisibilità**: Siano $f(x), g(x) \in A[x]$, $c(f(x)) = 1$, $f(x) \mid g(x)$ in $K[x]$ (K campo dei quozienti di A)
$\Rightarrow f(x) \mid g(x)$ in $A[x]$

→ **Dim** • Supponiamo che $f(x) \mid g(x)$ in $K[x] \Rightarrow \exists h(x) \in K[x] \mid g(x) = f(x)h(x)$

• $\exists d \in A \mid h_1(x) = d\,h(x) \in A[x] \Rightarrow dg(x) = f(x)h_1(x) \in A[x]$

• Lemma di Gauss $c(dg(x)) = c(f(x)h_1(x)) = c(f(x))\,c(h_1(x)) = c(h_1(x))$
(i) per hp

• $d \mid c(h_1(x)) \Rightarrow h(x) \in A[x]$

- Corollario riducibilità nel campo dei quozienti $\Rightarrow$ riducibilità: Sia $f(x) \in A[x]$, $f(x) = g(x)h(x)$ in $K[x]$ ($K$ campo dei quozienti di $A$) $\deg(g(x)), \deg(h(x)) \geq 1$ $\Rightarrow \exists \delta \in K^* \mid g_1(x) = \delta g(x) \in A[x]$ $h_1(x) = \delta^{-1} h(x) \in A[x]$ e $f(x) = g_1(x) h_1(x)$

→ Dim • $\exists d \in A \mid g_1(x) = dg(x) \in A[x]$

• $f(x) = dd^{-1} g(x) h(x) = dg(x) d^{-1} h(x) = g_1(x)(d^{-1} h(x)) = c(g_1(x)) g_1'(x)(d^{-1}h(x))$

• $f(x) = g_1'(x) \underbrace{[c(g_1(x)) d^{-1} h(x))]}_{\in K[x]}$ $\Rightarrow g_1'(x) \mid f(x)$ in $K[x]$

• per il corollario $g_1'(x) \mid f(x)$ in $A[x]$

• $h_1(x) = \underbrace{\frac{c(g_1(x))}{d}}_{d^{-1}} h(x)$

- Teorema caratterizzazione degli irriducibili di $A[x]$: Sia $A$ UFD gli irriducibili di $A[x]$ sono tutti e soli: (i) $f(x) \in A$ irrid in $A$

(ii) $f(x) \in A[x]$ $\deg(f(x)) \geq 1$, $c(f(x)) = 1$, $f(x)$ irrid in $K[x]$

→ Dim (i) $f(x) \in A \Rightarrow f(x)$ costante, $f(x) = g(x)h(x) \Rightarrow \deg(g(x)) + \deg(h(x)) = 0$
$\Rightarrow f(x)$ irrid in $A[x] \iff f(x)$ irrid in $A$

(ii) Sia $f(x)$ irrid in $A[x] \Rightarrow f(x) = c(f(x)) f'(x) \Rightarrow c(f(x)) \in (A[x])^* = A^*$
$\Rightarrow f(x)$ primitivo

rid come qu. $\Rightarrow$ rid

• Sono i soli: Sia $f(x) = g(x)h(x)$ in $K[x] \Rightarrow f(x) = g_1(x)h_1(x)$ con $\deg(g_1(x)) = \deg(g(x))$, $\deg(h_1(x)) = \deg(h(x))$

• $f(x)$ irrid $\Rightarrow g_1(x)$ o $h_1(x)$ inv. $\Rightarrow \deg(g_1(x))$ o $\deg(h_1(x)) = 0$

• Sia $f(x)$ prim. irrid in $K[x]$, $f(x) = g(x)h(x)$ in $A[x] \Rightarrow f(x)$ irrid in $K[x] \Rightarrow g(x)$ v $h(x)$ inv. in $K[x] \Rightarrow$ w.l.o.g. $g(x) \in A$

• $1 = c(f(x)) = c(g(x)h(x)) = c(g(x)) c(h(x)) = g\, c(h(x)) \Rightarrow g \in A^* \Rightarrow f$ irrid

## Algebra lezione 14/11/25 (esercitazione - Patimo)

**Esercizio 1**: siano $I, J \subseteq A$ ideali $\Rightarrow \sqrt{I \cdot J} \overset{(i)}{=} \sqrt{I \cap J} \overset{(ii)}{=} \sqrt{I} \cap \sqrt{J}$

(i) $\subseteq$ $IJ = \{\sum a_k b_k \mid a_k \in I \wedge b_k \in J\} \subseteq I \cap J$ ($I, J$ sono ideali $\Rightarrow a_k b_k \in I$ $a_k b_k \in J$)

$\supseteq$ $\sqrt{I \cap J} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I \cap J\}$, se $x \in \sqrt{I \cap J} \Rightarrow \exists n : x^n \in I \cap J \Rightarrow x^{2n} = x^n \cdot x^n \in (I \cap J)\cdot(I \cap J) \subseteq IJ \Rightarrow x \in \sqrt{IJ}$

(ii) $\subseteq$ $x \in \sqrt{I \cap J} \Rightarrow \exists n \in \mathbb{N} : x^n \in J \cap J \Rightarrow x^n \in I \wedge x^n \in J \Rightarrow x \in \sqrt{I} \cap \sqrt{J}$

$\supseteq$ $x \in \sqrt{I} \wedge \sqrt{J} \Rightarrow \exists n \in \mathbb{N} : x^n \in I \wedge \exists m \in \mathbb{N} : x^m \in J \Rightarrow x^{n+m} \in I \cdot J \subseteq I \cap J \Rightarrow x \in \sqrt{I \cap J}$

- In generale, $I \cdot J \neq \{ab \mid a \in I \wedge b \in J\}$ (è un'uguaglianza $\iff I, J$ sono id. princ.

Ad esempio, sia $A = \mathbb{Z}[x, y]$ $I = J = (x, y) \Rightarrow x^2 + y^2 \in I \cdot J$ ma $x^2 + y^2 \notin \{ab \mid a \in I \wedge b \in J\}$

**Esercizio 2**: $\sqrt{\sqrt{I}} = \sqrt{I}$

$\supseteq$ $I \subseteq \sqrt{I} \Rightarrow \sqrt{I} \subseteq \sqrt{\sqrt{I}}$

$\subseteq$ $x \in \sqrt{\sqrt{I}} \Rightarrow \exists n \in \mathbb{N} : x^n \in \sqrt{I} \Rightarrow \exists m \in \mathbb{N} : (x^n)^m \in I \overset{a = nm}{\Rightarrow} \exists a \in \mathbb{N} : x^a \in I \Rightarrow x \in \sqrt{I}$

**Esercizio 3**: Sia $A = \frac{\mathbb{K}[x,y]}{(x-y,\ x^3+y^3-x)}$, $\mathbb{K} \in \{\mathbb{Q}, \mathbb{F}_5, \mathbb{F}_7\}$. Scrivere $A$ come prodotto di cam

Sia $I=(x-y)$, $J=(x^3+y^3-x) \Rightarrow A \cong \frac{\mathbb{K}[x,y]}{I+J} \cong \frac{\frac{\mathbb{K}[x,y]}{I}}{\frac{I+J}{I}}$ (2° thm)

$\mathbb{K}[x,y]/I \cong \mathbb{K}[y]$, infatti $\Phi: \mathbb{K}[x,y] \to \mathbb{K}[y]$, $f(x,y) \mapsto f(y,y)$ è omo di anelli surj

e $\ker \Phi = (x-y) = I$ dunque per 1° thm ho l'iso cercato

$\supseteq$ ovvio $\subseteq$ $f \in \ker\Phi \Rightarrow f = \sum a_{nm} x^n y^m$ con $x^n \equiv y^n \pmod{x-y}$

$\Rightarrow f(x,y) \equiv \sum a_{nm} y^{n+m} \pmod{x-y}$ ma $\Rightarrow x-y \mid f(x,y)$, $f(y,y)=0$

ma quindi $A \cong \frac{\mathbb{K}[y]}{\Phi(I+J)} = \frac{\mathbb{K}[y]}{(0, 2y^3-y)} = \frac{\mathbb{K}[y]}{(2y^3-y)}$

$2y^3-y = y(2y^2-1)$ ma $MCD(y, 2y^2-1)=1$ dunque per TCR $A \cong \frac{\mathbb{K}[y]}{(y)} \times \frac{\mathbb{K}[y]}{(2y^2-1)} \cong \mathbb{K} \times$

- Se $\mathbb{K}=\mathbb{Q}$ $2y^2-1$ è irriducibile, dunque $\frac{\mathbb{Q}[y]}{(2y^2-1)} \cong \mathbb{Q}\left(\frac{1}{\sqrt{2}}\right) = \mathbb{Q}(\sqrt{2}^{-1})$

  dato che $2y^2-1$ è irrid $\Rightarrow (2y^2-1)$ è mass. ma quindi $\ker \varphi_{\sqrt{2}} = (2y^2-1)$

- Se $\mathbb{K}=\mathbb{F}_5$ $2y^2-1$ è irrid $\iff$ non ha rad. (faccio il conto a mano con $\{0,1,2,3,4\}$

  ma quindi $2y^2-1$ è irrid $\Rightarrow$ è mass. e $\frac{\mathbb{F}_5[y]}{(2y^2-1)} \cong \frac{\mathbb{F}_5[y]}{(y^2-3)}$ ha dimensione 2 $\hookrightarrow \{1, y\}$ è base

  $\Rightarrow \left|\frac{\mathbb{F}_5[y]}{(2y^2-3)}\right| = 25 = \mathbb{F}_5^2$

  Inoltre noto che $\forall p \in \mathbb{F}_5[y] \Rightarrow p = q(y^2-3)+r$ con $\deg(r) \le 1 \Rightarrow \bar{p} = \bar{r}$ in $\frac{\mathbb{F}_5[y]}{(y^2-3)} = A$
  $\Rightarrow \{\bar{1}, \bar{y}\}$ generano a su $\mathbb{F}_5$. Inoltre sono lin indip perché $y^2-3 \neq \alpha 1 + \beta y \Rightarrow$ è base
  $\Rightarrow \dim_{\mathbb{F}_5}(A) = 2$

- Se $\mathbb{K}=\mathbb{F}_7$ $2y^2-1$ ha radici $3, -3 \Rightarrow 2y^2-1 = 2(y-3)(y+3) \Rightarrow \frac{\mathbb{F}_7[y]}{(2y^2-1)} \cong \frac{\mathbb{F}_7[y]}{(y-3)(y+3)} \cong$ ← TCR

  $\cong \frac{\mathbb{F}_7[y]}{(y-3)} \times \frac{\mathbb{F}_7[y]}{(y+3)} \cong \mathbb{F}_7 \times \mathbb{F}_7$

**Esercizio 4**: Sia $\mathbb{Q}[x,y]$. (i) Dimostra che $(x-1, y-1)$ è massimale
(ii) Dimostra che $(1-xy)$ è primo ma non massimale

(i) Sia $I=(x-1)$, $J=(y-1) \Rightarrow \frac{\mathbb{Q}[x,y]}{I+J} \cong \frac{\frac{\mathbb{Q}[x,y]}{I}}{\frac{I+J}{I}}$ (2° thm) e per lo stesso argomento dell'esercizio precedente, $\frac{\mathbb{Q}[x,y]}{I} \cong \mathbb{Q}[y]$

ma quindi $\frac{\mathbb{Q}[x,y]}{I+J} \cong \frac{\mathbb{Q}[y]}{\Phi(I+J)} \cong \frac{\mathbb{Q}[y]}{J} \cong \mathbb{Q}$ che è campo $\Rightarrow (x-1, y-1)$ m

(ii) $f = 1-xy$ non è massimale, infatti $f(1,1)=0 \Rightarrow f \in (x-1, y-1)$ ← perché è il ker dell
$\Rightarrow (1-xy) \subsetneq (x-1, y-1)$. Ma quindi $1-xy = -y(x-1) - (y-1)$
Infine dobbiamo verificare che è contenuto strettamente. $g \in (1-xy) \Rightarrow$
$g(2, \frac{1}{2}) = 0$ ma $(x-1)(2, \frac{1}{2}) = 1 \Rightarrow x-1 \notin (1-xy)$

Definisco $\mathbb{Q}[x, x^{-1}] = \left\{ \sum_{k=-n}^{m} a_k x^k \mid m,n \in \mathbb{N}, a_k \in \mathbb{Q} \right\} \subset \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Q}[x])$
(anello dei polinomi Laurent; ← è dominio perché contenuto in un campo)

Sia $\Phi: \mathbb{Q}[x,y] \to \mathbb{Q}[x,x^{-1}]$, $f(x,y) \mapsto f(x,x^{-1})$ omo di anelli. $1-xy \in \ker\Phi \Rightarrow (1-xy) \subseteq \ker\Phi$

Sia $f \in \ker\Phi$, $f(x,y) = \sum a_{nm} x^n y^m$ $\mid$ $f(x,x^{-1})=0 \iff \sum a_{nm} x^n x^{-m} = 0$

$\iff \sum_{d \in \mathbb{Z}} x^d \left( \sum_{d=n-m} a_{m+d,m} \right) \iff \forall d \ \sum a_{m+d,m} = 0$

ma quindi $f(x,y) = \sum a_{n,m} (xy)^m x^d = \sum x^d \underbrace{\left( \sum a_{m+d,m} (xy)^m \right)}_{q_d(xy)}$

ma $q_d(1)=0 \Rightarrow (1-xy) \mid q_d(xy) \Rightarrow (1-xy) \mid f(x,y) \Rightarrow \ker\Phi \subseteq (1-xy)$

$\mathbb{Q}[x,x^{-1}] \cong \frac{\mathbb{Q}[x,y]}{(1-xy)}$ che è dominio $\Rightarrow (1-xy)$ primo

(1° thm)

**Esercizio 5**: Sia $A=\mathbb{Z}[i]$, $I=(x-2-i)$, $J=(x-2+i)$ ideali di $A[x]$

(i) Dimostra che $I\cap J$ è principale
(ii) Trova gli ideali massimali che contengono $I+J$
(iii) Dimostra che $I+J$ non è principale

In generale $I+J=1 \Rightarrow I\cap J = IJ$

(i) $A\in ID \Rightarrow A[x]$ UFD. Sia $p\in I\cap J \Rightarrow (x-2-i)\mid p \wedge (x-2+i)\mid p$ ma $(x-2-i)$ e $(x-2+i)$ sono irridin $A[x]$ ma associati $\Rightarrow (x-2-i)(x-2+i)\mid p$ ma $(x-2-i)(x-2+i)\in I\cap J \Rightarrow I\cap J = IJ$

(ii) Sia $M$ ideale massimale, $I+J\subset M \Rightarrow x-2+i, x-2-i\in M \Rightarrow -2i\in M \Rightarrow 2\in M$ e $(1+i)^2=2i\in M \Rightarrow 1+i\in M$

In generale $\frac{A[x]}{(I)}\cong\left(\frac{A}{I}\right)[x]$ con $f: A[x]\to \frac{A}{I}[x]$ omo anelli con $\ker f=(I)$

Ma quindi $\frac{A[x]}{M}\cong \frac{\frac{A[x]}{(1+i)}}{M/(1+i)} \cong \frac{\mathbb{Z}[i][x]}{(1+i)} \cong \left(\frac{\mathbb{Z}[i]}{(1+i)}\right)[x] \cong \mathbb{F}_2[x]$

Dunque $\bar{M}=\frac{M}{(1+i)}$ è massimale in $\mathbb{F}_2[x]$ e $x-2-i\in M \Rightarrow x-1\in\bar{M} \Rightarrow \bar{M}=(x-1)$ ($\mathbb{F}_2$)

$\Rightarrow M=(1+i, x-1)$ è l'unico ideale mass. che contiene $I+J$

(iii) Supponiamo per assurdo che $I+J=(p)$ per $p\in A[x] \Rightarrow p\mid x-2-i \wedge p\mid x-2+i$

$\Rightarrow p\mid (x-2+i)-(x-2-i)=-2i \Rightarrow p\mid 2$. Ma $p$ deve dividere tutti i coefficienti di $x-2+i$, $x-2-i \Rightarrow p\mid 1 \Rightarrow p=1 \Rightarrow I+J=(1) \Rightarrow I+J=A[x]$ ↯ perché $I+J\subseteq M\subsetneq A[x]$

## Algebra Lezione 17/1/25 (esercitazione - Patimo)

**Esercizio 1**: Sia $A$ dominio, $S$ p.m., $I$ ideale di $A \Rightarrow S^{-1}I$ è ideale di $S^{-1}A$

- $\frac{\text{neutro}}{s}=\frac{0}{s}\in S^{-1}I$ perché $0\in I$
- opposto $\frac{a}{s}\in S^{-1}I \Rightarrow -\frac{a}{s}\in S^{-1}I$ perché $-a\in I$ e $\frac{a}{s}+\frac{-a}{s}=\frac{as-as}{s^2}=\frac{0}{s^2}=0$
- associatività vale perché $I$ ideale
- chiusura per somma $\frac{x}{s},\frac{y}{t}\in S^{-1}I$ $\frac{x}{s}+\frac{y}{t}=\frac{\overset{\in I}{\overbrace{xt}}+\overset{\in I}{\overbrace{ys}}}{st}\in S^{-1}I$
- assorbimento per prodotto $\frac{x}{s}\in S^{-1}I$ $\frac{a}{t}\in S^{-1}A$ $\frac{a}{t}\cdot\frac{x}{s}=\frac{\overset{\in I}{\overbrace{ax}}}{ts}\in S^{-1}I$

**Esercizio 2**: Sia $A$ dominio, $S$ p.m. $J$ ideale di $S^{-1}A \Rightarrow J\cap A$ è ideale di $A$

Definiamo $J\cap A=\{\frac{a}{1}\mid a\in A \wedge \frac{a}{1}\in J\}$ $(A\hookrightarrow S^{-1}A)$

- neutro $0\in J$, $0\in A \Rightarrow 0\in J\cap A$
- opposto $a\in J\cap A \Rightarrow a\in J\wedge a\in A \Rightarrow -a\in J\wedge -a\in A \Rightarrow -a\in J\cap A$
- chiusura per somma $a,b\in J\cap A \Rightarrow a,b\in J\wedge a,b\in A \Rightarrow a+b\in J\wedge a+b\in A \Rightarrow a+b\in J\cap A$
- assorbimento per prodotto $a\in J\cap A$ $x\in A$ $x\cdot\frac{a}{1}\in\frac{x\cdot a}{1}=\frac{x}{1}\cdot\frac{a}{1}\in J$ e $xa\in A \Rightarrow xa\in J\cap A$

**Esercizio 3**: Dimostra che $\forall J\subseteq S^{-1}A$ ideale $\exists I\subseteq A$ ideale $\mid J=S^{-1}I\,(J=S^{-1}(J\cap A))$

$\subseteq$ Sia $\frac{x}{s}\in J$, $x\in A$, $s\in S \Rightarrow x=s\cdot\frac{x}{s}\in J\cap A \Rightarrow \frac{x}{s}\in S^{-1}(J\cap A)$

$\supseteq$ Sia $\frac{a}{s}\in S^{-1}(J\cap A)$, $a\in J\cap A$, $s\in S \Rightarrow \frac{a}{s}=\frac{1}{s}\cdot a\in J$ perché $J$ ideale

- Noto che $\{\text{ideali di } A\}\underset{J\cap A\leftarrow J}{\overset{I\to S^{-1}I}{\rightleftarrows}}\{\text{ideali di } S^{-1}A\}$, $\alpha\circ\beta=\mathrm{id}$ ma $\beta\circ\alpha\neq\mathrm{id}$ perché $I\cap S\neq\emptyset \Rightarrow S^{-1}I=S^{-1}A$

**Esercizio 4**: Dimostra che $\{\text{ideali primi di } A: P\cap S=\emptyset\}\underset{J\cap A\leftarrow J}{\overset{I\to S^{-1}I}{\rightleftarrows}}\{\text{ideali primi di } S^{-1}A\}$

- $J\subseteq S^{-1}A$ primo $\Rightarrow J\cap A$ primo $\wedge (J\cap A)\cap S=\emptyset$

  Siano $x,y\in A \mid x\cdot y\in J\cap A \Rightarrow \frac{x}{1}\cdot\frac{y}{1}\in J \Rightarrow \frac{x}{1}\in J \vee \frac{y}{1}\in J \Rightarrow x\in J\cap A \vee y\in J\cap A$

  Se $(J\cap A)\cap S\neq\emptyset \Rightarrow \exists s\in(J\cap A)\cap S \Rightarrow 1=\frac{1}{s}\cdot\frac{s}{1}\in J \Rightarrow J=S^{-1}A$ ↯ (perché $J$ primo)

- $I \subset A$ primo $\wedge$ $I \cap S \neq \emptyset \Rightarrow S^{-1}I$ primo

$\frac{x}{s}, \frac{y}{t} \in S^{-1}A : \frac{x}{s}\cdot\frac{y}{t} \in S^{-1}I \Rightarrow \exists z \in I, \exists u \in S \mid \frac{xy}{st} = \frac{z}{u} \Rightarrow uxy = stz \in I$

Se $I$ è primo $\Rightarrow x \in I \vee y \in I \Rightarrow \frac{x}{s} \in S^{-1}I \vee \frac{y}{t} \in S^{-1}I$

Dunque le restrizione di $\alpha, \beta$ sono ben definite. Sappiamo che $\alpha\circ\beta = id$, per mostrare che sono biiezioni resta solo da far vedere che $\beta\circ\alpha = id$ ovvero $\beta\circ\alpha(I) = I$

$\supseteq$ $x \in I \Rightarrow x = \frac{x}{1} \in S^{-1}A$ e $x \in I \subset A$

$\subseteq$ $S^{-1}(I\cap A) \subset I$ $\frac{a}{s} \in S^{-1}(I\cap A)$ con $a \in I$ $s \in S \Rightarrow \exists b \in A \mid \frac{a}{s} = \frac{b}{1} \Rightarrow a = bs$

$a \in I \Rightarrow bs \in I$ ma $s \notin I \Rightarrow b \in I \Rightarrow \frac{a}{s} \in I$

- Un esempio può essere $A = \mathbb{Z}$, $S = \{3^k \mid k \geq 0\}$ $I = (6) \Rightarrow S^{-1}(6) = \left\{\frac{6a}{3^k} \mid a \in \mathbb{Z}, k \geq 0\right\} = \left\{\frac{2a}{3^{k-1}} \mid a \in \mathbb{Z}, k \geq 0\right\} = S^{-1}(2)$

Infatti: $S^{-1}(6) \cap \mathbb{Z} \ni 2 = \frac{6}{3} \notin (6)$

Esercizio 5: Descrivi gli ideali di $\mathbb{Z}_{(2)} = S^{-1}\mathbb{Z}$ (con $S = \mathbb{Z} \setminus (2) = \{\text{numeri dispari}\}$)

Ma infatti gli ideali di $\mathbb{Z}_{(2)}$ sono gli $S^{-1}I$ con $I$ ideale di $\mathbb{Z}$. Quindi è $S^{-1}(n)$ dove $n \in \mathbb{Z}$.

- $n = 0$ $S^{-1}(0) = \left\{\frac{0}{s}\right\} = \{0\}$
- $n = 2k+1$ $S^{-1}(n) = \mathbb{Z}_{(2)}$
- $n = 2^k d$ $2^k = \frac{2^k d}{d} \in S^{-1}(2^k d)$ ma quindi $S^{-1}(2^k) \subseteq S^{-1}(n) \subseteq S^{-1}(2^k)$

Inoltre $S^{-1}(2^{k+1}) \subsetneq S^{-1}(2^k)$ perché $2^k \notin \left\{\frac{2^{k+1}c}{d} \mid d \text{ dispari}, c \in \mathbb{Z}\right\}$

Quindi gli ideali di $\mathbb{Z}_{(2)}$ sono $(0) \subset \dots \subset (2^k) \subset \dots \subset (8) \subset (4) \subset (2)$

Esercizio 6: Dato $I$ ideale di $\mathbb{Z}$, chi è $S^{-1}(I \cap \mathbb{Z})$?

$I = (n)$ con $n = 2^k d$ ($d$ dispari). Dunque $S^{-1}((n)\cap\mathbb{Z}) = S^{-1}((2^k)\cap\mathbb{Z}) = \left\{\frac{2^k c}{d} \mid c \in \mathbb{Z}, d \text{ dispari}\right\} \cap \mathbb{Z}$

Se $\frac{2^k c}{d} \in \mathbb{Z}$, dato che $d$ dispari $\Rightarrow d \mid c \Rightarrow \frac{2^k c}{d} = 2^k \cdot \frac{c}{d} \in (2^k)$

$\Rightarrow S^{-1}((2^k)\cap\mathbb{Z}) = (2^k)$

Se $n = 0$ $S^{-1}((0)\cap\mathbb{Z}) = (0)$

Esercizio 7: Descrivi gli ideali massimali di $\mathbb{Z}[x]$

Sia $M \subset \mathbb{Z}[x]$ ideale massimale, $\mathbb{Z} \subset \mathbb{Z}[x]$ sottoanello delle costanti. Supponiamo che $M \cap \mathbb{Z} \neq (0) \Rightarrow \exists n \in \mathbb{Z} \mid n \in M$ con $n = p_1^{d_1}\cdots p_n^{d_n}$ fatt. in $\mathbb{Z}$. Poiché $M$ massimale $\Rightarrow$ $M$ primo $\Rightarrow \exists i \mid p_i \in M$

$$\frac{\mathbb{Z}[x]}{M} \cong \frac{\frac{\mathbb{Z}[x]}{(p)}}{M/(p)} \cong \frac{\mathbb{Z}_{(p)}[x]}{\bar{M}} \quad (\bar{M} = M/(p)) \cong \frac{\mathbb{F}_p[x]}{\bar{M}} \text{ con } \bar{M} \text{ mass. in } \mathbb{F}_p[x]$$

$\Rightarrow \bar{M} = (\bar{f})$ con $\bar{f}$ irriducibile in $\mathbb{F}_p[x]$ $\Rightarrow M = (p, \tilde{f}(x))$ ($\tilde{f}(x) \in \mathbb{Z}[x] \mid \tilde{f}(x) \equiv f(x) \pmod p$)

In generale: $S^{-1}(A[x]) \overset{IS}{=} (S^{-1}A)[x]$

Ma quindi se $M$ mass. in $\mathbb{Z}[x]$ e $M \cap \mathbb{Z} \neq \{0\} \Rightarrow M = (p, g(x))$ con $g(x)$ irriducibile mod $p$

Se $M \cap \mathbb{Z} = \{0\}$, prendiamo $S = \mathbb{Z}\setminus\{0\}$. Allora per quanto detto prima

$\{\text{ideali primi di } \mathbb{Z}[x] \text{ che intersecano } S\} \leftrightarrow \{\text{ideali primi di } S^{-1}\mathbb{Z}[x]\}$

$M \longleftrightarrow S^{-1}M$

Dunque $M$ primo in $\mathbb{Z}[x]$ $\Leftrightarrow S^{-1}M$ primo in $S^{-1}(\mathbb{Z}[x]) \cong (S^{-1}\mathbb{Z})[x] \cong \mathbb{Q}[x]$

$\Leftrightarrow S^{-1}M = (0)$ o $S^{-1}M = (f)$ con $f \in \mathbb{Q}[x]$ irriducibile

Perché $M = S^{-1}(M \cap \mathbb{Z}[x])$. Se $S^{-1}M = (0) \Rightarrow M = (0)$ ↯ dunque $S^{-1}M = (f)$

$\Rightarrow M = (f) \cap \mathbb{Z}[x]$ (WLOG $f$ primitivo)

Ma $(f)_{\mathbb{Q}[x]} \cap \mathbb{Z}[x] = (f(x))_{\mathbb{Z}[x]}$

? chiaro

$\subseteq$ Sia $g \in \mathbb{Q}[x] \mid f(x)g(x) \in \mathbb{Z}[x] \Rightarrow \exists \frac{p}{q} \in \mathbb{Q} \mid \frac{p}{q} \cdot g(x) \in \mathbb{Z}[x]$ ed è primitivo.

Per il Lemma di Gauss $c(f \cdot \frac{p}{q} g) = c(f) \cdot c(\frac{p}{q} g)$ (i primi $c(f)$ e $c(\frac{p}{q}g)$ sono $=1$)

S.A. $(p,q)=1 \Rightarrow f \cdot \frac{p}{q} \cdot g = \frac{p}{q}(fg)$, $fg \in \mathbb{Z}[x]$ ma quindi tutti i coeff. sono divisi da $p \Rightarrow p=1$ Ma quindi $f(x) \cdot (\frac{1}{q} \cdot g(x)) \in \mathbb{Z}[x]$ e $fg \in (f)_{\mathbb{Z}[x]}$

Ma quindi $M = (f(x))$ con $f$ primitivo e irrid. Ma tale $M$ è massimale?

Voglio trovare $p \in \mathbb{Z} \mid (f(x)) \subsetneq (p, f(x)) \subsetneq \mathbb{Z}[x]$. Sia dunque $p \nmid a_n$ $(f = a_n x^n + \dots + a_0)$

Dunque $\frac{\mathbb{Z}[x]}{(p, f(x))} \cong \frac{\mathbb{F}_p[x]}{(\bar{f}(x))}$ $(\bar{f}(x) \equiv f(x) \pmod p)$ dato che $p \nmid a_n \Rightarrow$ $\deg f(x) = \deg \bar{f}(x) \Rightarrow \dim\left(\frac{\mathbb{F}_p[x]}{(\bar{f}(x))}\right) = n \neq 0 \Rightarrow (p, f(x)) \neq \mathbb{Z}[x]$

Dunque gli ideali massimali di $\mathbb{Z}[x]$ sono della forma $M = (p, f(x))$

## Algebra Lezione 19/11/25 (teoria - Del Corso)

- **Definizione algebrico:** Sia $K$ campo, $L$ estensione di $K$, $\alpha \in L$ è algebrico su $K$ se $\exists f(x) \in K[x] \setminus \{0\} \mid f(\alpha) = 0$.

- **Definizione trascendente:** Sia $K$ campo, $L$ estensione di $K$, $\alpha \in L$ è trascendente su $K$ se non è algebrico.

- **Definizione: omo di val:** Sia $K$ campo, $L$ estensione di $K$, $\alpha \in L$ allora definiamo l'omomorfismo di valutazione di $\alpha$ su $K[x]$

$$\varphi_\alpha : K[x] \longrightarrow K[\alpha] (\subset L) \quad \text{tale omo è surj (perché prendiamo l'immagine)}$$
$$f(x) \longmapsto f(\alpha)$$

- Noto che quindi vale la seguente mappa per 1° teo di omo $K[x] \xrightarrow{\varphi_\alpha} K[\alpha]$

$\Rightarrow K[\alpha] \cong \frac{K[x]}{\ker \varphi_\alpha}$. Ma noto che $\ker \varphi_\alpha$ è ker di un omo di anelli $\Rightarrow \ker \varphi_\alpha$ è ideale $\Rightarrow \ker \varphi_\alpha$ è principale perché $K[x]$ è PID $\Rightarrow \ker \varphi_\alpha = (\mu_\alpha(x))$ per un certo $\mu_\alpha(x) \in K[x]$

$\pi_{\ker \varphi_\alpha} : K[x] \to \frac{K[x]}{\ker \varphi_\alpha}$, $\bar{\varphi}_\alpha : \frac{K[x]}{\ker \varphi_\alpha} \to K[\alpha]$

$L$ campo $\Rightarrow K[\alpha]$ dominio

$\frac{K[x]}{(\mu_\alpha)}$ dominio $\Rightarrow (\mu_\alpha)$ primo

$(\mu_\alpha)$ primo $\Rightarrow (\mu_\alpha)$ irrid (in dom. primo $\Rightarrow$ irrid)

Inoltre $\ker \varphi_\alpha$ è massimale (perché $K[x]$ PID) $\Rightarrow \frac{K[x]}{(\mu_\alpha(x))}$ campo $\Rightarrow K[\alpha]$ campo

$\frac{K[x]}{(\mu_\alpha)} \overset{\text{def}}{=} K[\alpha] = K(\alpha)$

Come scegliamo $\mu_\alpha(x)$? - Prendiamo un polinomio monico
- $\mu_\alpha(\alpha) = 0$
- $\forall p(x) \in K[x] \mid p(\alpha) = 0 \Rightarrow \mu_\alpha(x) \mid p(x)$ (ha grado minimo)
- $\mu_\alpha(x)$ irrid

Il polinomio con queste caratteristiche viene chiamato polinomio minimo ed è unico a meno di associati.

- Sia $f(x) = a_n x^n + \dots + a_0 \in K[x] \setminus \{0\}$; $f(\alpha) = a_n \alpha^n + \dots + a_0 = 0$ se è vero solo quando tutti i coefficienti $\Rightarrow \{\alpha^n, \dots, \alpha, 1\}$ sono lin. indip. in $K$

- **Definizione estensione algebrica:** Sia $K$ campo, $L$ estensione di $K$, l'estensione $L/K$ è algebrica se $\forall \alpha \in L$, $\alpha$ è algebrico su $K$

- Noto per come è definita la mappa e per quanto detto sopra $\alpha$ algebrico su $K \iff \ker \varphi_\alpha \neq \{0\} \iff \varphi_\alpha$ non inj

- In $\frac{K[x]}{(\mu_\alpha(x))}$ ho le classi $1, \bar{x}, \dots, \bar{x}^{n-1} \Rightarrow$ In $K[\alpha]$ ho le classi $1, \alpha, \dots, \alpha^{n-1}$ perché gli iso preservano le classi

- **Proposizione:** Siano $K \subseteq L$ campi $\alpha \in L$ algebrico su $K$ $L/K$ estensione. $p(x)$ è il polinomio minimo $\iff$ • $p(x)$ irrid • $p(\alpha) = 0$ • $p(x)$ monico

  → **Dim** $\Rightarrow$ visto
  $\Leftarrow$ Se $p(\alpha) = 0 \Rightarrow p(x) \in \ker \varphi_\alpha \Rightarrow \mu_\alpha(x) \mid p(x) \Rightarrow p(x) = \mu_\alpha(x) q(x)$ ma $p(x)$ irrid $\Rightarrow q(x) \in K[x]^* = K^* = K \setminus \{0\} \Rightarrow p(x) = \mu_\alpha(x) q$ ma $p(x), \mu_\alpha(x)$ sono monici $\Rightarrow q = 1$.

- **Definizione estensione finita:** Siano $K \subseteq L$ campi $L/K$ estensione, chiameremo grado di $L/K$ $[L:K] = \dim_K L$
  Se $[L:K] < +\infty$ diremo che $L/K$ è un'estensione finita.

- Noto che per quanto detto precedentemente $[K(\alpha):K] = \begin{cases} +\infty & \text{se } \alpha \text{ trascend. su } K \\ \deg \mu_K(x) & \text{se } \alpha \text{ alg. su } K \end{cases}$

- **Proposizione proprietà torri:** Sia $K \subset F \subset L$ torre di estensioni, $L/K$ è finita $\iff$ $L/F$ e $F/K$ sono finite. In tal caso $[L:K] = [L:F][F:K]$

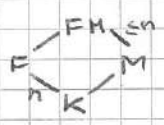
  → **Dim** ($\Leftarrow$) Sia $[L:F] = n$ e $[F:K] = m$, questo significa che $L$ è un $F$-spazio vettoriale di dimensione $n$, dunque ammette base $\mathcal{B} = \{v_1, \dots, v_n\}$ invece $F$ è un $K$-spazio vettoriale di dimensione $m$, dunque ammette base $\mathcal{D} = \{w_1, \dots, w_m\}$.
  Sia $\mathcal{B}' = \{v_i w_j\}_{\substack{i=1,\dots,n \\ j=1,\dots,m}}$

  - $\mathcal{B}'$ genera, dato che $L$ è un $F$-spazio vettoriale $\Rightarrow \forall \alpha \in L$
    $\alpha = \sum_{j=1}^{m} \lambda_j w_j$ con $\lambda_j \in F$. Ma $F$ è un $K$-spazio vettoriale
    $\lambda_j = \sum_{i=1}^{n} a_{ji} v_i \Rightarrow \alpha = \sum_{j=1}^{m} \left( \sum_{i=1}^{n} a_{ij} v_i \right) w_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} v_i w_j$
  - $\mathcal{B}'$ lin indip, $\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ji} v_i w_j = \left( \sum_{i=1}^{n} a_{i1} v_i \right) w_1 + \dots + \left( \sum_{i=1}^{n} a_{mi} v_i \right) w_n = 0$
    ma $\mathcal{D}$ è base $\Rightarrow$ la somma è $0 \iff \sum_{i=1}^{n} a_{i1} v_i = \dots = \sum_{i=1}^{n} a_{ni} v_i = 0$
    ma $\mathcal{B}$ base $\Rightarrow$ l'uguaglianza è rispettata $\iff$
    $a_{ij} = 0 \ \forall i,j \Rightarrow \mathcal{B}'$ lin indip.

  $\Rightarrow$ se $L/K$ finito $\Rightarrow$ $L/F$ finito $\Rightarrow$ $F/K$ finito

- **Definizione:** Dati $K, S \subseteq \Omega$, $K$ campo, $S$ insieme $K(S) = \bigcap_{\substack{L \subseteq \Omega \text{ campo} \\ K,S \subseteq L}} L$ = il più piccolo campo che contiene $K, S$

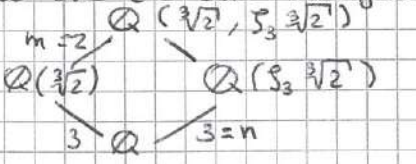
- Noto che se $F, L \subseteq \Omega$ campi $\Rightarrow FL = F(L) = L(F)$




- **Proposizione proprietà shift:** Sia $K \subset M$, $K \subset F$
  $[F:K] = n \Rightarrow [FM:M] \leq n$

  → **Dim** $\langle v_1, \dots, v_n \rangle_K = F \Rightarrow \text{Span}(\langle v_1, \dots, v_n \rangle_K) = FM = M(F) \Rightarrow \dim_M FM \leq n$
  perché genera ma non è detto siano tutti linearmente indipendenti

- Noto che c'è una disuguaglianza, non la divisibilità! Un esempio

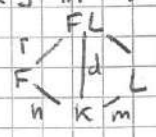



$n = 3$, $m = 2$, $m \leq n$ ma $m \nmid n$!

- **Proposizione proprietà composto:** Sia $K \subset F$, $K \subset L$ $[F:K] = n$ $[L:K] = m$ $\Rightarrow$
  $[FL:K] = d$ e $\text{mcm}(n,m) \mid d$

  → **Dim** $[FL:K] = [FL:F][F:K] = an$ (torri) $\Rightarrow d = an = bm$
  $= [FL:L][L:F] = bm$

  $\Rightarrow n \mid d \wedge m \mid d \Rightarrow \text{mcm}(n,m) \mid d$




- **Proposizione est. fin $\Rightarrow$ alg:** Ogni estensione di grado finito è algebrica

  → **Dim** Sia $\alpha \in L$ algebrico su $K$ $\Rightarrow K \subseteq K(\alpha) \subseteq L$ ($[L:K] < +\infty$ per hp) è finita
  $\Rightarrow K \subseteq K(\alpha)$ è finita $\Rightarrow$ è algebrica
  Ma quindi $\forall \alpha$ $K(\alpha)/K$ è algebrica $\Rightarrow$ $L/K$ è algebrica

- Sorge spontanea la domanda est alg $\Rightarrow$ fin? No! Facciamo un esempio:

  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ alg. su } \mathbb{Q}\}$, $L = \mathbb{C}$, $K = \mathbb{Q}$, $\overline{\mathbb{Q}} = A$ per come sono definiti gli elementi $\overline{\mathbb{Q}}$ è algebrica su $\mathbb{Q}$. Supponiamo sia finito $\Rightarrow [\overline{\mathbb{Q}}:\mathbb{Q}] = n$
  Prendiamo $\alpha \in \mathbb{C}$ $\Rightarrow \alpha \in \overline{\mathbb{Q}}$ ma $[\mathbb{Q}(\alpha):\mathbb{Q}] = n+1$ ↯ perché $\mathbb{Q}(\alpha) \subsetneq \overline{\mathbb{Q}}$ (i.e. il polinomio $x^{n+1} - 2 \in \mathbb{Q}[x]$, è irr. per Eisenstein, monico e ha radice in $\mathbb{C}$)

- **Proposizione campo delle estensioni algebriche:** Sia $L/K$ estensione, $A = \{\alpha \in L \mid \alpha \text{ alg su } K\}$
  $\Rightarrow A$ è campo (e est. alg di $K$)

  → **Dim** Siano $\alpha, \beta \in A \Rightarrow [K(\alpha):K] = n$ $[K(\beta):K] = m$ ma quindi la torre
  $K \subseteq K(\alpha) \subseteq K(\alpha,\beta)$ è finita per la proprietà del composto
  $\Rightarrow K(\alpha,\beta)/K$ è alg. $\Rightarrow \alpha \pm \beta, \alpha\beta, \frac{1}{\alpha}$ sono alg su $K \Rightarrow A$ campo

- **Proposizione est alg e fin gen ⇒ fin:** Sia $L/K$ fin. gen. da el alg. $\Rightarrow$ $L/K$ è fin.

→ **Dim** $n=1$ $L=K(\alpha)$ $\Rightarrow$ è finita perché semplice e $\alpha$ alg su $K$

$L=K(\alpha_1,\dots,\alpha_{n-1},\alpha_n)=K(\alpha_1,\dots,\alpha_{n-1})(\alpha_n)$ per hp ind è estensione torri: $K'=K(\alpha_1,\dots,\alpha_{n-1})$ è finita su $K$. Dunque $[L:K]=[L:K'][K':K]$ fin per hp ind, fin perché semplice

- **Proposizione proprietà est alg:** (i) Data una torre $K\subset L\subset F$, $F/K$ alg $\iff$ $F/L$, $L/K$ alg.

(ii) $K\subset L$, $K\subset M$, $L/K$ alg $\Rightarrow$ $ML/M$ alg

(iii) $L/K$, $M/K$ alg $\iff$ $LM/K$ alg.

→ **Dim** (i) $\Leftarrow$ $\alpha\in F$ è alg su $L$ $f(x)\in L[x]$ $f(x)=\sum_{i=0}^{n}\gamma_i x^i \Rightarrow \alpha$ alg $K[\gamma_1,\dots,\gamma_n]=L_0$ ma $L_0/K$ fin perché fin gen da alg. ma quindi $L_0(\alpha)\supseteq L_0\supseteq K$ sono tutti finiti: $\Rightarrow$ algebrici

$\Rightarrow$ è ovvio

(ii) $ML=M(L)$ ma gli el. di $L$ sono algebrici su $K$ $\Rightarrow$ $\alpha$ è alg su $M$

(iii) segue da (i)+(ii)

## Algebra Lezione 21/11/25 (teoria - Del Corso)

- **Definizione algebricamente chiuso:** Sia $\Omega$ campo, diremo che $\Omega$ è algebricamente chiuso se $\forall f(x)\in\Omega[x]$, $\deg(f(x))\geq 0 \Rightarrow \exists\alpha\in\Omega \mid f(\alpha)=0$

- **Definizione chiusura algebrica:** Sia $\Omega/K$ estensione, $\Omega$ è una chiusura algebrica di $K$ se $\Omega$ è algebricamente chiuso e $\Omega/K$ è algebrico

- Noto che $\Omega$ è alg. chiuso $\iff$ i pol. irrid di $\Omega[x]$ sono solo gli $f(x)\mid \deg(f(x))=1$

- Per il teo. fond. dell'algebra $\mathbb{C}$ è algebricamente chiuso

- $\mathbb{C}$ non è la chiusura algebrica di $\mathbb{Q}$, questo perché $|\mathbb{C}|=\mathfrak{c}>\aleph_0=|\mathbb{Q}|$ (la chiusura algebrica ha la stessa cardinalità del campo)

- **Teorema esistenza e unicità della chiusura algebrica:** Sia $K$ campo $\Rightarrow \exists!\ \overline{K}$ chiusura alg di $K$ (a meno di iso) ($\exists\varphi:\Omega\to\Omega'$ iso $\varphi_{|K}=id$)

- Prendiamo come esempio $\overline{\mathbb{Q}}=\{\alpha\in\mathbb{C}\mid \alpha \text{ alg. su } \mathbb{Q}\}$. Per quanto visto, $\overline{\mathbb{Q}}$ è campo e $\overline{\mathbb{Q}}/\mathbb{Q}$ è est. alg. Notiamo che $\overline{\mathbb{Q}}$ è alg. chiuso. Infatti preso $f(x)\in\overline{\mathbb{Q}}[x]$. Sia $\alpha\in\mathbb{C}\mid f(\alpha)=0$; $f(x)=a_nx^n+\dots+a_0$ dunque considero $L=\mathbb{Q}(a_0,\dots,a_n)$, perciò $L(\alpha)/\mathbb{Q}$ è fin. gen. el. alg. $\Rightarrow$ è Finito $\Rightarrow$ è alg. $\Rightarrow f(x)\in L$. Inoltre anche $L(\alpha)/L$ è alg. $\Rightarrow L(\alpha)/\mathbb{Q}$ è alg $\Rightarrow \alpha\in\overline{\mathbb{Q}}$

- **Definizione cds:** Sia $f(x)\in K[x]$, $\deg(f(x))\geq 1$, $\alpha_1,\dots,\alpha_n\in\overline{K}$ radici di $f(x)$. chiameremo campo di spezzamento di $f(x)$ su $K$ il sottocampo di $\overline{K}$ $K(\alpha_1,\dots,\alpha_n)$

- Vediamo chi è il cds di $x^n-1$. Innanzitutto noto che $x^n-1=\prod_{i=0}^{n-1}(x-\zeta_n^i)\Rightarrow\langle\zeta_n\rangle$ è l'insieme delle radici di $x^n-1$. Dunque il cds è $\mathbb{Q}(\zeta_n)$. Che grado ha? per $n$ primo sappiamo essere $n-1$.

- **Teorema criterio della derivata:** Sia $f(x)\in K[x]\Rightarrow f(x)$ ha rad mul. in $\overline{K}$ $\iff$ $(f(x),f'(x))\neq 1$. Se $f(x)$ è irrid, $f(x)$ ha rad mul $\iff f'(x)=0$

→ **Dim** Sia $f(x)\in K[x]$, $\alpha$ rad di $f(x)$, $\alpha\in\overline{K}\Rightarrow f(x)=(x-\alpha)g(x)$ ma quindi $f'(x)=(x-\alpha)g'(x)+g(x)$. Ma quindi $\alpha$ è rad mul. $\iff g(\alpha)=0$ $\iff f'(\alpha)=\underbrace{(\alpha-\alpha)g'(\alpha)}_{=0}+\underbrace{g(\alpha)}_{=0}=0\Rightarrow MCD(f,f')$ è multiplo del pol min.

Per il secondo punto $f$ ha rad mul. $\iff MCD(f,f')\neq 1 \iff f\mid f'$ ma quindi per questioni di grado $f'=0$

- **Definizione caratteristica:** Sia $K$ campo, $\varphi:\mathbb{Z}\to K$ chiameremo caratteristica di $K$

$$\operatorname{char}K=\begin{cases}0 & \text{se } \ker\varphi=\mathbb{Z}\\ p & \text{se } \ker\varphi=p\mathbb{Z}\end{cases}$$

- **Corollario:** Se $K$ ha caratteristica 0 $\Rightarrow$ $f$ irrid ha tutte rad distinte

- Se $K$ è campo di caratteristica $p$, sia $K = \mathbb{F}_p[t]$, sia $f(x) = x^p - t \in K[x]$ allora $f(x)$ è irrid perché $f'(x) = px^{p-1} = 0$ e preso $\alpha \in \overline{K} \mid \alpha^p = t$, $(x-\alpha)^p = f(x)$

- **Proposizione:** $|K| = \mathbb{F}_p$ $f(x) \in K[x]$, $f'(x) = 0 \Rightarrow f(x) = g(x)^p$ con $g(x) \in K[x]$

  → **Dim** $\cdot f'(x) = 0 \Rightarrow f(x) = \sum_{i=0}^{n} a_i x^i \rightsquigarrow f'(x) = \sum_{i=1}^{n} i a_i x^{i-1} = 0$ ovvero

  $i a_i = 0 \ \forall i$; dunque $\begin{cases} a_i = 0 \\ i \equiv 0 \ (p) \end{cases} \Rightarrow f(x) = \sum_{\ell} a_{p\ell} x^{p\ell}$ ma $a^p \equiv a \ (p)$ Fermat

  $\Rightarrow f(x) = \sum_{\ell} a_{p\ell}^p x^{p\ell} = \left(\sum_{\ell} a_{p\ell} x\right)^p = g(x)^p$

- **Definizione campo finito:** Sia $K$ campo, diremo che $K$ è finito se $|K| < +\infty$

- Noto che $F$ Finito $\Rightarrow$ $\mathrm{char} F = p$ (se fosse 0 $\mathbb{Q} \hookrightarrow F$ $\lightning$)

- **Teorema classificazione dei campi finiti:** $\forall p$ primo $\exists! F \mid |F| = p^n$

  → **Dim** Sia $F$ campo, $|F| = p^n \Rightarrow \mathbb{F}_p \subseteq F \subset \overline{\mathbb{F}_p}$, allora $|F^*| = p^n - 1$

  • Ma quindi voglio che $\forall \alpha \in F^* \ \alpha^{p^n - 1} = 1$ ovvero $\alpha$ radice di $f(x) = x^{p^n-1} - 1 \in \overline{\mathbb{F}_p}[x]$

  • $F \subset \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n - 1} - 1 = \alpha^{p^n} - \alpha = 0\}$. $g(x) = x^{p^n} - x$ ha $p^n$ rad in $\overline{\mathbb{F}_p}[x]$ distinte
  $g'(x) = -1$ per criterio derivata segue ↗

  • $F = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\}$ se è campo abbiamo chiuso

  - $0, 1 \in F$ verifica a mano
  - $(\alpha \pm \beta)^{p^n} - \alpha \pm \beta = \alpha^{p^n} \pm \beta^{p^n} - \alpha \pm \beta = (\alpha^{p^n} - \alpha) \pm (\beta^{p^n} - \beta) = 0 \pm 0 = 0$
  - $(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = (\alpha^{p^n} - \alpha)(\beta^{p^n} - \beta) = 0 \cdot 0 = 0$
  - $(\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0$

  ← come gruppi non come anelli

- Noto che $\mathbb{F}_{p^n}$ è il CDS di $f(x)$ su $\mathbb{F}_p$. Inoltre $(\mathbb{F}_{p^n}, +) \cong ((\mathbb{Z}/p\mathbb{Z})^n, +)$

- **Teorema sgr. fin. mol. campo:** Ogni sottogruppo moltiplicativo finito di un campo è ciclico

- **Corollario:** $(\mathbb{F}_p^*, \cdot)$ è un gruppo ciclico $\forall p$ primo $\forall n \geq 1$.

- **Corollario $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$:** $\forall p$ primo $\forall n \geq 1$ $\mathbb{F}_{p^n}$ è un'estensione semplice di $\mathbb{F}_p$ $\Rightarrow \exists \alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$

- Ma $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha] \Rightarrow \mathbb{F}_{p^n}^* = \langle \alpha \rangle$ no! Ad esempio preso $\mathbb{F}_{5^2}$, $|\mathbb{F}_{5^2}^*| = 24$, dunque un generatore $\gamma$ di $\mathbb{F}_{5^2}^*$ $\mathrm{ord}(\gamma) = 24$. Sia $\alpha \mid \mathbb{F}_{5^2} = \mathbb{F}_5(\alpha) \Rightarrow \alpha$ ha pol. min. di grado 2 ad es. $f(x) = x^2 + x + 1$. Ma $3 + 4 \Rightarrow \alpha \notin \mathbb{F}_5^* \Rightarrow \alpha \notin \mathbb{F}_5$

- **Corollario $f(x)$ irr. $\mathbb{F}_p[x]$:** $\forall p$ primo $\forall n \geq 1$ $\exists f(x) \in \mathbb{F}_p[x]$ irrid. con $\deg(f(x)) = n$

  → **Dim** $\forall p$ primo, $\forall n \geq 1$ $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha] \cong \dfrac{\mathbb{F}_p[x]}{(\mu_\alpha(x))}$ con $\deg(\mu_\alpha(x)) = n$ e $\mu_\alpha(x)$ irrid perché pol min.

- In particolare $f(x) \in \mathbb{F}_p[x]$ irriducibile di grado $n$ ha $n$ rad distinte "$\mathbb{F}_{p^n}$ conta le rad di tutti i pol irrid di deg $n$ su $\mathbb{F}_p$"

## Algebra lezione 24/11/25 (esercitazione-Patimo)

**Esercizio 1** Siano $A, B$ anelli allora $K \subseteq A \times B$ ideale $\Leftrightarrow$ $I \subseteq A$ ideale $\wedge$ $J \subseteq B$ ideale, $K = I \times J$

⇐ Innanzitutto noto che $I \times J$ è un ideale di $A \times B$, dato che faccio il prodotto componente per componente

⇒ Definisco $I = \{a \in A \mid \exists b \in J : (a, b) \in K\}$, infatti $(a,b) \in K \Rightarrow (a, 0) \in K$ perché $(1, 0)(a, b) \in K \Rightarrow I = \{a \in A \mid (a, 0) \in K\} \Rightarrow I \subseteq A$ ideale. Analogamente $J = \{b \in B \mid (0, b) \in K\}$. Manca solo da vedere che $K = I \times J$

$\subseteq$ $(a, b) \in K \Rightarrow a \in I \wedge b \in J$

$\supseteq$ $a \in I \wedge b \in J \Rightarrow (a, 0), (0, b) \in K \Rightarrow (a, 0) + (0, b) \in K \Rightarrow (a, b) \in K$

**Esercizio 2:** Sia $f(x) = x^5 - x^4 - 3x^3 + 6x - 3 \in \mathbb{Z}[x]$

(i) Scrivi $A = \frac{\mathbb{Z}[x]}{(g(x))}$ come prod. di domini

(ii) Trova gli ideali massimali di $A$

(iii) Trova gli ideali di $\mathbb{Z}[x]$ che contengono $(3, f)$

(iv) Trova gli ideali di $\mathbb{Z}[x]$ che contengono $(2, f)$

(i) Fattorizziamo $f$: $f(1) = 0 \Rightarrow (x-1) \mid f(x) \Rightarrow f(x) = (x-1)\underbrace{(x^4 - 3x + 3)}_{g(x)}$

Noto che $g(x)$ è irriducibile per Eisenstein (con $p = 3$).
Sia dunque $I = (x-1)$, $J = (g(x))$. Valutare $g(x) \bmod (x-1)$ è equivalente a valutare $g(1)$. Ho: $g(1) = 1 \Rightarrow g(x) = (x-1)q(x) + 1$ (infatti perché $g(x) \equiv 1 \bmod (x-1)$). Dunque $I + J = (1)$ ← non è automatica come in $\mathbb{Q}$, ti basta dire $x-1 \nmid g(x)$

$\Rightarrow I \cdot J = I \cap J \Rightarrow \frac{\mathbb{Z}[x]}{(f)} = \frac{\mathbb{Z}[x]}{IJ} \cong \frac{\mathbb{Z}[x]}{I} \times \frac{\mathbb{Z}[x]}{J}$

ma $\frac{\mathbb{Z}[x]}{I} \cong \mathbb{Z}$ e $\frac{\mathbb{Z}[x]}{J}$ è dominio perché $(g)$ è primo dato che è irriducibile in un UFD.

(ii) Gli ideali di $\mathbb{Z} \times \frac{\mathbb{Z}[x]}{J}$ sono gli $I \times K \mid I \trianglelefteq \mathbb{Z} \wedge K \trianglelefteq \frac{\mathbb{Z}[x]}{J}$ (es 1)
Gli ideali massimali di un prodotto diretto sono quelli che hanno tutto in una componente e massimale nell'altra.
I massimali di $\frac{\mathbb{Z}[x]}{J}$ sono i massimali di $\mathbb{Z}[x]$ $(p, h(x))$ in cui $g \in (p, h(x))$ quando $h(x) \bmod (p) \in \mathbb{F}_p[x] \mid g(x) \bmod (p) \in \mathbb{F}_p[x]$

Ma quindi $M$ massimale in $\mathbb{Z}[x]$, $f(x) \in M \Rightarrow g(x) \in M \vee (x-1) \in M$

dunque $M$ massimale in $\mathbb{Z}[x]$ che contiene $f(x)$ sono quelli della forma $(p, \underbrace{r(x)}_{\bmod (p)})$ con $r(x) \mid f(x) \Rightarrow r(x) \mid x-1 \vee r(x) \mid g(x)$ perché $r(x)$ è irriducibile. Ma $r(x) \mid (x-1) \Rightarrow r(x) = x-1 \Rightarrow M = (p, x-1)$

$\Rightarrow \frac{\mathbb{Z}[x]}{J} \times (p) \times \frac{\mathbb{Z}[x]}{(x-1)}$

Ma $r(x) \mid g(x) \bmod (p) \Rightarrow M = (p, r(x)) \Rightarrow \frac{(p, r(x))}{g(x)} \times \frac{\mathbb{Z}[x]}{(x-1)}$

(iii) Gli ideali che contengono $(3, f)$ sono gli ideali di:

$\frac{\mathbb{Z}[x]}{(3, f)} \cong \frac{\frac{\mathbb{Z}[x]}{(3)}}{\frac{(3, f)}{(3)}} \cong \frac{\mathbb{F}_3[x]}{(\bar{f})} \Rightarrow \bar{f} = (x-1)\bar{g}(x)$ ma $\bar{g}(x) = x^4$

($\bar{f} = f \bmod (p)$, $\bar{g} = g \bmod (p)$)

$\Rightarrow \frac{\mathbb{Z}[x]}{(3, f)} \cong \mathbb{F}_3 \times \frac{\mathbb{F}_3[x]}{(x^4)}$. Gli ideali di $\mathbb{F}_3$ sono $\{0\}$ e $\mathbb{F}_3$ perché campo

Gli ideali di $\mathbb{F}_3[x]$ che contengono $x^4$ sono gli $(h(x)) \mid x^4 \in (h(x))$ perché $\mathbb{F}_3[x]$ PID. Ma quindi sono gli $(h(x)) \mid h(x) \mid x^4 \Rightarrow h(x) = 1, x, x^2, x^3, x^4$

(iv) Gli ideali che contengono $(2, f)$ sono gli ideali di:

$\frac{\mathbb{Z}[x]}{(2, f)} \cong \frac{\frac{\mathbb{Z}[x]}{(2)}}{\frac{(2, f)}{(2)}} \cong \frac{\mathbb{F}_2[x]}{(\bar{f})} \Rightarrow \bar{f} = (x+1)\bar{g}(x)$ ma $\bar{g}(x) = x^4 + x + 1$

($\bar{f} = f \bmod (p)$, $x+1 \bmod (p)$, $\bar{g} = g \bmod (p)$)

$\Rightarrow \frac{\mathbb{Z}[x]}{(2, f)} \cong \mathbb{F}_2 \times \frac{\mathbb{F}_2[x]}{(x^4 + x + 1)}$

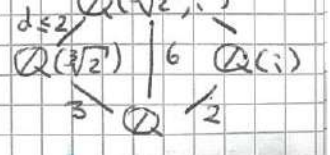
questo perché $\bar{g}(x)$ non ha radici e cerco i pol di deg 2 irrid in $\mathbb{F}_2[x]$ e ho solo $x^2 + x + 1$ ma $x^2 + x + 1 \nmid g(x) \Rightarrow \bar{g}(x)$ irrid

Ma $\mathbb{F}_2$, $\frac{\mathbb{F}_2[x]}{(x^4 + x + n)}$ sono campi quindi hanno solo 2 id.

**Esercizio 3:** Qual'è il grado di $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}]$? Qual'è il pol. min. di $\alpha = \sqrt[3]{2} + i$

$\mathbb{Q}(\sqrt[3]{2})$ ha come pol min $(x^3 - 2) \Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

$\mathbb{Q}(i)$ ha come pol min $(x^2 + 1) \Rightarrow [\mathbb{Q}(i) : \mathbb{Q}] = 2$




Se $d = 1 \Rightarrow \mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2})$ ma $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ e $\mathbb{Q}(\sqrt[3]{2}, i) \subset \mathbb{C}$ $\lightning \Rightarrow d = 2$

Ma quindi $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = 6$

$\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[3]{2}, i)$ perché $\sqrt[3]{2} + i \in \mathbb{Q}(\sqrt[3]{2}+i)$. Quindi

$\mathbb{Q}(\sqrt[3]{2}, i) \xrightarrow{a} \mathbb{Q}(\alpha) \xrightarrow{b} \mathbb{Q}$ $\Rightarrow ab = 6 \Rightarrow a = \frac{6}{b} \in \mathbb{Z}$.

$x = \sqrt[3]{2} + i \longrightarrow (x-i)^3 = 2 \rightarrow x^3 + 3ix^2 - 3x + i = 2 \rightarrow (x^3 - 3x + 2)^2 = (-(3x^2+1)i)^2$

$\longrightarrow \underbrace{x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5}_{t(x)} = 0$. $t(x)$ è pol min $\iff \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}, i)$

Noto che $(\alpha^3 - i)^3 = 2 \Rightarrow \alpha^3 - 3i\alpha^2 - 3\alpha + i - 2 = 0 \Rightarrow \alpha^3 - 3\alpha - 2 = (3\alpha^2 - 1)i \Rightarrow$

$i = \frac{\alpha^3 - 3\alpha - 2}{3\alpha^2 - 1} \in \mathbb{Q}(\alpha)$ ($3\alpha^2 - 1 \neq 0$) $\Rightarrow \alpha - i \in \mathbb{Q}(\alpha) \Rightarrow \sqrt[3]{2} \in \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\alpha)$

$\Rightarrow t(x)$ è pol min. di $\mathbb{Q}(\alpha)$

**Esercizio 4:** Sia $\alpha \in \overline{\mathbb{Q}}$, $\alpha$ rad di $f(x) = x^4 + x + 1$. Trova il pol. min. di $2\alpha + 1$, $\alpha^2$

Innanzitutto controlliamo che $f(x)$ è irrid su $\mathbb{Q}[x]$ Per Gauss, $f(x)$ irriducibile in $\mathbb{Z}[x] \Rightarrow f(x)$ irrid in $\mathbb{Q}[x]$. $f(x)$ è irrid in $\mathbb{F}_2[x] \Rightarrow f(x)$ irriducibile in $\mathbb{Z}[x]$.

Dunque se $\alpha$ è rad di un pol. irrid in $\mathbb{Q}[x] \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

$x+1 \in \mathbb{Q}(2\alpha+1) \Rightarrow \alpha \in \mathbb{Q}(2\alpha+1) \Rightarrow \mathbb{Q}(2\alpha+1) = \mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(2\alpha+1) : \mathbb{Q}] = 4 \Rightarrow$

$\deg(\mu_\alpha(x)) = 4$.

per $f(x)$ $\alpha^4 + \alpha + 1 = 0 \rightarrow \alpha^4 = -\alpha - 1$

$x = 2\alpha + 1 \rightarrow x - 1 = 2\alpha \rightarrow (x-1)^4 = (2\alpha)^4 \longrightarrow (x-1)^4 = 16\alpha^4 \xrightarrow{!} (x-1)^4 = -16(\alpha+1)$

$\rightarrow (x-1)^4 = -8(2\alpha+1+1) \longrightarrow (x-1)^4 = -8(x+1) \rightarrow x^4 - 4x^3 + 6x^2 + \dots - 4x + 1 + 8x + 8 = 0$

$\longrightarrow x^4 - 4x^3 + 6x^2 + 4x + 9 = 0$ ← pol min $2\alpha+1$

$\alpha^2 \in \mathbb{Q}(\alpha^2)$ ma $x = \alpha^2 \Rightarrow x^2 = \alpha^4 = \alpha + 1 \Rightarrow \alpha = \alpha^2 - 1 \in \mathbb{Q}(\alpha^2) \Rightarrow \mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$
$\Rightarrow [\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4$

pol min $\alpha^2$

$x^4 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 \longrightarrow x^4 = x + 2(x-1) + 1 = x + 2x^2 - 2 + 1 \xrightarrow{(!)} x^4 - 2x^2 - x + 1 = 0$

**Esercizio 5:** Sia $K$ campo con caratteristica $\neq 2$, $a, b \in K^*$ allora $K(\sqrt{a}) = K(\sqrt{b}) \iff \frac{a}{b} \in K^2$

$\sqrt{b} = \frac{\sqrt{a}}{c}$ $\qquad \sqrt{a} = c\sqrt{b}$

$\Leftarrow$ Sia $\frac{a}{b} \in K^2 \Rightarrow \exists c \in K \mid c^2 = \frac{a}{b} \Rightarrow \sqrt{a} = c\sqrt{b} \Rightarrow \sqrt{a} \in K(\sqrt{b})$ e $\sqrt{b} \in K(\sqrt{a})$

$\Rightarrow K(\sqrt{b}) = \{x + y\sqrt{b} \mid x, y \in K\}$, per che $\sqrt{a} \in K(\sqrt{b}) \Rightarrow \sqrt{a} = x + y\sqrt{b} \Rightarrow$

- $a = x^2 + y^2 b + 2xy\sqrt{b} \rightarrow 2xy\sqrt{b} = x^2 + y^2 - a \in K \Rightarrow 2xy\sqrt{b} \in K$ ma $\mathrm{char}(K) \neq 2$
$\Rightarrow xy\sqrt{b} \in K \iff \begin{cases} \sqrt{b} \in K \\ xy = 0 \end{cases}$
  - Se $\sqrt{b} \in K \Rightarrow b \in K^2$ ma $K(\sqrt{b}) = K = K(\sqrt{a}) \Rightarrow \sqrt{a} \in K \Rightarrow a \in K^2 \Rightarrow \frac{a}{b} \in K^2$
  - Se $x = 0$ $\sqrt{a} = y\sqrt{b} \Rightarrow \frac{a}{b} = y^2 \Rightarrow \frac{a}{b} \in K^2$
  - Se $y = 0$ $\sqrt{a} = x \Rightarrow a = x^2 \in K^2 \Rightarrow b \in K^2 \Rightarrow \frac{a}{b} \in K^2$

## Algebra Lezione 26/11/25 (teoria - Del Corso) -> incompleta!!

**Esercizio 1:** Conta i polinomi irriducibili su $\mathbb{F}_p[x]$ di grado 5

Noto che $f(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ rappresenta tutti i polinomi di deg 5 che posso trovare. Ma quindi ho $\mathbb{F}_p^5 / \mathbb{F}_p$ $p^5$ - p polinomi di deg 5 in $\mathbb{F}_p$

Se pongo la relazione $\alpha \sim \beta \iff \mu_\alpha(x) = \mu_\beta(x)$ $\mathbb{F}_p^5 / \mathbb{F}_p / \sim$ sono i polinomi irriducibili di deg 5 in $\mathbb{F}_p$ ovvero $\frac{p^5 - p}{5}$

**Esercizio 2:** Se $\alpha \in \mathbb{F}_{p^5}$ $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = ?$

Noto che $\mathbb{F}_p \xrightarrow{a} \mathbb{F}_p(\alpha) \xrightarrow{b} \mathbb{F}_{p^5}$ $\Rightarrow ab = 5$ dunque se $a = 1 \Rightarrow \alpha \in \mathbb{F}_p$

Altrimenti: $a=5 \Rightarrow b=1$ $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^5}$

Se $\alpha \in \mathbb{F}_{p^6}$ $\mathbb{F}_p \xrightarrow{a} \mathbb{F}_p(\alpha) \xrightarrow{b} \mathbb{F}_{p^6}$ $\Rightarrow ab = 6$

caso $a=1,6$ già visti (analoghi a prima) può essere $a=2$?

è vero $\Leftrightarrow \mathbb{F}_2 \subset \mathbb{F}_6$

- **Proposizione:** $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m \mid n$

→ **Dim:** $\Rightarrow$ Per torri $\mathbb{F}_p \overset{m}{\frown} \mathbb{F}_{p^m} \frown \mathbb{F}_{p^n}$

$\Leftarrow$ $n = am$, dunque $\alpha \in \mathbb{F}_{p^m}^{\times} \Rightarrow \alpha^{p^m-1} = 1$ ma quindi

$p^m \equiv 1 \ (p^m-1) \rightarrow p^n = p^{am} \equiv 1 \ (p^m-1)$

$\Rightarrow p^m-1 \mid p^n-1$ ma quindi $p^n-1 = \lambda(p^m-1) \Rightarrow (\alpha^{p^m-1})^{\lambda} = 1^{\lambda}$

$\Rightarrow \alpha^{p^n-1} = 1 \Leftrightarrow \alpha \in \mathbb{F}_{p^n}^* \subseteq \mathbb{F}_{p^n}$

- **Teorema:** Sia $f \in \mathbb{F}_p[x]$, il cos di $f$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ dove $d = mcm(\deg f_1, \dots, f_n)$

$(f = f_1 \cdots f_n$ irrid)

→ **Dim** Sia $f = f_1(x)^{e_1} \cdots f_n(x)^{e_n}$ con $f_i(x) \in \mathbb{F}_p[x]$, $\deg(f_i(x)) = d_i$

Il cos di $f_i$ è $\mathbb{F}_{p^{d_i}}$

Il cos di $f$ è $\mathbb{F}_{p^{d'}}$ con $d'$ minimo $\mid \mathbb{F}_{p^{d_i}} \subseteq \mathbb{F}_{p^{d'}} \ \forall i$: $d_i \mid d'$

dunque $d = [d_1, \dots, d_n]$

**Esercizio 3:** Trova il cos di $x^m-1$ su $\mathbb{F}_p$

Sia $G_n = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^n = 1\} \Rightarrow \mathbb{F}_p(G_n)$ è cos di $x^m-1$. Ma per quanto detto nel teorema $\mathbb{F}_p(G_n) = \mathbb{F}_{p^d}$. $f_n(x) = x^n-1$ dunque $f_n'(x) = nx^{n-1}$ e per il criterio della derivata $f_n(x)$ ha rad multiple $\Leftrightarrow (f_n, f_n') \neq 1 \Leftrightarrow p \mid n$

Se $p \nmid n$ $|G_n| = n$ e $n = p^r m$ $(m,p)$ $(x^{p^r m}-1) = (x^m-1)^{p^r}$

$x^n-1 = (x^m-1)^{p^r}$ $x^n-1$ ha radici distinte

ma quindi $G_m < \mathbb{F}_{p^d}^*$, $|\mathbb{F}_{p^d}^*| = p^d-1 \Rightarrow |G_m| \mid p^d-1$.

Viceversa $m \mid p^d-1 \Rightarrow G_m < \mathbb{F}_{p^d}^*$ $\alpha \in G_m \Rightarrow \alpha^m \equiv 1$ $\alpha \in \mathbb{F}_{p^d}^*$

$\mathbb{F}_{p^n} = \{0\} \cup \{\alpha \in \overline{\mathbb{F}_p}^* \mid \alpha^{p^n-1} = 1\}$

- **Teorema:** $n = p^r m$ $r \geq 0$ $(m,p) = 1$ il cos di $x^n-1$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ dove $d = \operatorname{ord}_m p$

- **Teorema numero di estensioni a $\overline{K}$ di un'estensione qualsiasi:** Sia $L/K$ estensione, $[L:K] = n \Rightarrow \forall \varphi: K \hookrightarrow \overline{K}$ $\exists \varphi_1, \dots, \varphi_n: L \hookrightarrow \overline{K}$ con $\varphi_i|_K = \varphi$

## Algebra lezione 28/11/25 (teoria - Del Corso)

- **Definizione normale:** Sia $L/K$ estensione, diremo che $L/K$ è normale se $\forall \varphi: L \hookrightarrow \overline{K}$ con $\varphi|_K = id_K \Rightarrow \varphi(L) = L$

Facciamo degli esempi:

(i) Le estensioni di grado 2 sono normali:

$[L:K] = 2 \Rightarrow L \cong \frac{K(x)}{x^2+dx+b} \Rightarrow L = K(\alpha) = K(\sqrt{\Delta})$ ma quindi preso $\varphi: L \hookrightarrow \overline{K}$ $\varphi|_K = id$ allora $\varphi(\lambda+\mu\sqrt{\Delta}) = \varphi(\lambda) + \varphi(\mu)\varphi(\sqrt{\Delta}) = \lambda + \mu\varphi(\sqrt{\Delta})$ dunque devo solo decidere dove mandare $\sqrt{\Delta}$ tramite $\varphi$ per estendere a $L$ (dato che tutti gli elementi di $L$ sono della forma $\lambda+\mu\sqrt{\Delta}$). Ma $\varphi(\sqrt{\Delta}) = \pm\sqrt{\Delta}$ perché $\mu_{\sqrt{\Delta}} = x^2 - \Delta$ ma $\varphi(L) = \varphi(K(\sqrt{\Delta})) = K(\pm\sqrt{\Delta}) = L$

(ii) Ogni estensione di campi finiti è normale

$\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ $m \mid n \Rightarrow n = md \Rightarrow [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = d$ ho $d$ immersioni e $\forall i$: $[\varphi_i(\mathbb{F}_{p^n}) : \varphi_i(\mathbb{F}_{p^m})] = d \Rightarrow \mathbb{F}_{p^{md}} = \mathbb{F}_{p^n}$

(iv) Le estensioni ciclotomiche sono normali (e $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$)

per $n=p$ abbiamo visto. Se $n \neq p$ sappiamo che $|\langle \zeta_n \rangle| = n$ ma quindi l'ordine dell'immersione $\varphi: \mathbb{Q}(\zeta_n) \hookrightarrow \mathbb{Q}$ è $n$. Ma è un'immersione $\Rightarrow$ $\mathrm{ord}(\varphi) = n$. Ma quindi $\mathrm{ord}(\zeta_n^i) = \mathrm{ord}(\varphi(\zeta_n)) = \mathrm{ord}(\zeta_n) = n \iff (n,i) = 1$ ma quindi ho $\varphi(n)$ mappe e $\varphi(\mathbb{Q}(\zeta_n)) = \mathbb{Q}(\zeta_n^i) = \mathbb{Q}(\zeta_n)$

(iv) $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ è normale

Infatti: ho 4 immersioni: $i \longmapsto \pm i$ e $\sqrt{2} \longmapsto \pm\sqrt{2}$ e $\varphi_i(L) \subseteq L$

(v) $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})/\mathbb{Q}$ non è normale

Infatti: "sono dipendenti" perché ho 4 scelte ma 8 radici dunque non ottengo tutto lo spazio

(vi) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è normale

Infatti: le radici del polinomio minimo sono $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$ ma $\varphi(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2}\zeta_3) \neq \mathbb{Q}(\sqrt[3]{2})$ (è vera senza ma lo dimostriamo con)

- **Proposizione caratterizzazione delle estensioni normali:** Sia $F/K$ est. alg. (fin) sono equiv
  - (i) $F/K$ normale
  - (ii) $\forall f(x) \in K[x]$ irr. d, $\alpha$ rad di $f$, $\alpha \in F \Rightarrow$ tutte le rad di $f$ sono in $F$
  - (iii) $F$ è CDS su $K$ di una famiglia di polinomi in $K[x]$

  → **Dim** (i)⇒(ii) Sia $f(x) \in K[x]$ $\alpha_1, \dots, \alpha_n$ le sue radici. per hp una radice di $f$ è in $F$, wlog $\alpha_1 \in F \Rightarrow K(\alpha_1) \subset F$. Allora sia
  - $\varphi_i : K(\alpha_1) \longrightarrow K(\alpha_i) \subseteq \overline{K}$, $\alpha_1 \longmapsto \alpha_i$, $\varphi_{i|K} = id_K$
  - $\tilde{\varphi}_i : F \longrightarrow \overline{K}$ estensione di $\varphi_i$ che è normale per hp
  - $\tilde{\varphi}_i(F) = F \Rightarrow \alpha_i \in F \ \forall i$

  (ii)⇒(iii) Sia $F_0$ CDS di $\mathcal{F} = \{\mu_\alpha(x) \in K[x] \mid \alpha \in F, \mu_\alpha(x)$ p.m. di $\alpha$ su $K\}$
  - $F \subseteq F_0$ perché ha tutte le rad di $f$
  - $F_0 = K(\beta \mid \beta \text{ rad } \mu_\alpha(x) \in \mathcal{F}) \Rightarrow \alpha \in F_0$
  - per hp $\alpha \in F \Rightarrow \beta$ rad $\mu_\alpha(x) \in F \Rightarrow F_0 \subseteq F$

  (iii)⇒(i) $F$ è CDS di $\mathcal{F} \Rightarrow F = K(\{\alpha_{ij}\} \mid i = 1, \dots, \kappa \wedge j = 1, \dots, n_i)$
  - $\varphi: F \hookrightarrow \overline{K}$ $\varphi_{|K} = id_K$ $\forall i,j$ $\varphi(\alpha_{ij}) = \alpha_{ij}$ (ovvero è un'altra rad dello stesso pol)
  - $\varphi(F) = \varphi(K(\{\alpha_{ij}\})) = K(\varphi(\alpha_{ij}) \mid i = 1, \dots, \kappa \wedge j = 1, \dots, n_i) \subseteq F$ (ho permutato le radici e basta)
  - $K \subseteq \varphi(F) \subseteq F \Rightarrow \varphi(F) = F$ (n, n)

- **Proposizione proprietà delle estensioni normali rispetto alle torri:** Data $K \subseteq F \subset L$ in una chiusura algebrica $\overline{K}$, $L/K$ normale $\Rightarrow L/F$ normale

  → **Dim** $L/K$ normale $\iff$ CDS di una famiglia di polinomi in $K[x] \subseteq F[x]$
  $\Rightarrow L/K$ è CDS della stessa famiglia di polinomi a coefficienti in $F[x]$
  $\iff L/F$ è normale

- In generale $L/F$ normale e $F/K$ normale $\not\Rightarrow L/K$ normale $\mathbb{Q} \xrightarrow[\text{nor}]{2} \mathbb{Q}(\sqrt{2}) \xrightarrow[\text{nor}]{2} \mathbb{Q}(\sqrt[4]{2})$ (non normale)
- $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \xrightarrow[\text{nor}]{} \mathbb{Q}(\sqrt[3]{2}) \xrightarrow[\text{non nor.}]{} \mathbb{Q}$

- **Proposizione proprietà delle estensioni normali rispetto allo shift:** Dato $K \subset L, F$ in una fissata chiusura algebrica $\overline{K}$ $L/K$ nor $\Rightarrow$ $LF/F$ nor

→ **Dim** Sia $\varphi: LF \hookrightarrow \overline{K}$ con $\varphi_{|F} = id_F$ allora $\varphi(LF) = \varphi(L)\varphi(F)$ perché $\varphi_{|F}=id$

$\varphi(LF) = \varphi(L)\varphi(F) = LF$
($\varphi$ omo; $L$ perché $L/K$ nor)

- **Proposizione proprietà delle estensioni normali rispetto al composto e all'intersezione** Siano $F/K$ $L/K$ in una chiusura algebrica $\overline{K}$ normali $\Rightarrow$ $LF/K$ e $L\cap F/K$ normali

→ **Dim** Sia $\varphi: LF \hookrightarrow \overline{K}$ con $\varphi_{|K} = id_K$

(i) $\varphi(LF) = \varphi(L)\varphi(F) = LF$ ($L/K$ nor $\Rightarrow \varphi(L)=L$; $F/K$ nor $\Rightarrow \varphi(F)=F$)

(ii) $\varphi(L\cap F) = \tilde{\varphi}(L) \cap \tilde{\varphi}(F) = L \cap F$ con $\tilde{\varphi}$ estensione di $\varphi$ a $L$ e $F$

- **Definizione estensione di Galois:** Un'estensione $E/K$ si dice di Galois se è normale e separabile

- Per noi le estensioni sono sempre separabili.

- Noto che $\varphi: E \longrightarrow \overline{K}$ con $\varphi_{|K} = id_K \Rightarrow \varphi(E) = E$ perché $E/K$ normale dunque posso definire $Aut_K(E) = \{\varphi: E \longrightarrow E \mid \varphi_{|K} = id_K\}$ chiameremo tale gruppo il gruppo di Galois $Gal(E/K) = Aut_K(E)$ e $|Gal(E/K)| = [E:K]$

- $[L:K]=2 \Rightarrow$ è normale $\Rightarrow$ è di Galois $\Rightarrow Gal(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ perché è l'unico gruppo di ordine 2

- $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ ($K=\mathbb{Q}$) $L/K$ è normale $[L:K]=6 \Rightarrow |Gal(L/K)| = 6$

dunque $Gal(L/K) \cong S_3 \cong \mathbb{Z}/6\mathbb{Z}$. Per capire mi basta vedere la struttura del gruppo: $\varphi_{ij} \in Gal(L/K)$ $\varphi_{ij}: \begin{cases} L \longrightarrow L \\ \sqrt[3]{2} \longmapsto \sqrt[3]{2}\,\zeta_3^i \\ \zeta_3 \longmapsto \zeta_3^j \end{cases}$ $i=0,1,2$ $j=0,1,2$

Noto che $(\varphi_{02})^2 = (\varphi_{22})^2 = id$ ma quindi $Gal(L/K) \cong S_3$ (perché ho un solo el di ord 2 in $\mathbb{Z}/6\mathbb{Z}$)

## Algebra Lezione 01/12/25 (esercitazione - Patimo)

**Esercizio 1:** Sia $f \in K[x]$ $\deg(f(x)) = n$, $L$ cos di $f$ su $K \Rightarrow [L:K] \mid n!$

→ **Base** $\deg(f(x)) = 1 \Rightarrow L = K$ e $1 \mid 1!$

→ **P. I.** Sia $f$ irrid, $\deg(f(x)) = n$; $\alpha \in \overline{K}$ radice di $f$. Ma quindi $f(x) = (x-\alpha)g(x)$ su $K(\alpha) \Rightarrow L$ è cos di $f(x)$ su $K(\alpha)$ e $\deg(g(x)) = n$ ma quindi per hp ind. $[L:K(\alpha)] \mid (n-1)!$ e poiché $[K(\alpha):K] \neq n$ $\Rightarrow [L:K] \mid n!$

Se $f$ non irrid $\Rightarrow f(x) = g(x)h(x)$. Sia $L_g$ cos di $g$ su $K$ allora

$[L:K] = [L:L_g][L_g:K] \mid (\deg h)!(\deg g)! \mid (\deg(f))!$ ($a+b=n \Rightarrow a!b! \mid n!$)

**Esercizio 2:** Siano $p, q$ primi disgiunti, $\alpha = \sqrt{p} + \sqrt{q}$; qual'è il pol. min. di $\alpha$ su $\mathbb{Q}$?

$\alpha \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ e $[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2$ e $[\mathbb{Q}(\sqrt{q}):\mathbb{Q}] = 2$

$\mathbb{Q}(\sqrt{p},\sqrt{q})$ — 2 — $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ — 2 — $\mathbb{Q}$, $|4$

dunque $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})] \leq 2$. Se fosse 1 $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{q})$ perché $p \neq q \Rightarrow [\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}] = 4$

$\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] \mid 4$ Ma $[\mathbb{Q}(\alpha):\mathbb{Q}] = \#$ imm. su $\overline{\mathbb{Q}}$ ovvero

$|\{\varphi: \mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}} \mid \varphi_{|\mathbb{Q}} = id\}|$ perciò noto che

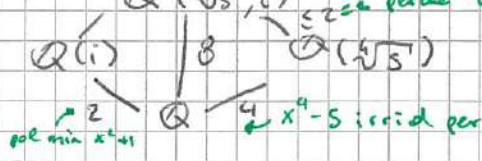
$\varphi_{++}$: $\sqrt{p} \mapsto \sqrt{p}$, $\sqrt{q} \mapsto \sqrt{q}$
$\varphi_{+-}$: $\sqrt{p} \mapsto \sqrt{p}$, $\sqrt{q} \mapsto -\sqrt{q}$
$\varphi_{-+}$: $\sqrt{p} \mapsto -\sqrt{p}$, $\sqrt{q} \mapsto \sqrt{q}$
$\varphi_{--}$: $\sqrt{p} \mapsto -\sqrt{p}$, $\sqrt{q} \mapsto -\sqrt{q}$
} tutte dist.

prese le immersioni di $\mathbb{Q}(\sqrt{p},\sqrt{q}) \hookrightarrow \overline{\mathbb{Q}}$ se le valuto in $\alpha$ ottengo $\varphi_{++}(\alpha) = \sqrt{p}+\sqrt{q}$, $\varphi_{+-}(\alpha) = \sqrt{p}-\sqrt{q}$; $\varphi_{-+}(\alpha) = -\sqrt{p}+\sqrt{q}$ $\varphi_{--}(\alpha) = -\sqrt{p}-\sqrt{q}$ che sono tutte distinte e quindi in $\mathbb{Q}$ $m_\alpha(x) = (x^2 - 2\sqrt{q}x + (q-p))(x^2 + 2\sqrt{q}x + (q-p))$

**Esercizio 3:** Sia $L$ il cos di $x^4-5$ su $\mathbb{Q}$. $[L:\mathbb{Q}]=?$

Dato che $L$ è cos di $x^4-5$ allora contiene tutte le sue radici che sono $\sqrt[4]{5}, \sqrt[4]{5}\,i, \sqrt[4]{5}\,i^2, \sqrt[4]{5}\,i^3$ dunque $\mathbb{Q}(\sqrt[4]{5}, \sqrt[4]{5}\,i, \sqrt[4]{5}\,i^2, \sqrt[4]{5}\,i^3) = L \Rightarrow L = \mathbb{Q}(\sqrt[4]{5}, i)$

ma $L$




**Esercizio 4:** Sia $L$ il cos di $x^3+x+1$ su $\mathbb{Q}$. $[L:\mathbb{Q}]=?$

Innanzitutto noto che $x^3+x+1$ è irriducibile: Derivando $f(x)$ noto che $f'(x)=3x^2+1>0$

$\Rightarrow f(x)$ ha una sola rad. reale $\Rightarrow \beta, \gamma, \bar{\gamma}$ sono radici di $f$ con $\beta \in \mathbb{R}$, $\gamma, \bar{\gamma} \notin \mathbb{R}$

$L = \mathbb{Q}(\beta, \gamma, \bar{\gamma})$

$\mathbb{Q}(\beta, \gamma)$ $\quad [L:\mathbb{Q}] \mid 3! = 6 \Rightarrow [L:\mathbb{Q}] = 6$

$|\ 2 \longrightarrow$ perché $\gamma \notin \mathbb{R} \Rightarrow \gamma \notin \mathbb{Q}(\beta)$

$\mathbb{Q}(\beta)$

$|\ 3 \longrightarrow f(x)$ pol min

$\mathbb{Q}$

**Esercizio 5:** Sia $L$ il cos di $f(x)=x^4+3x^2+1$ su $\mathbb{Q}$. $[L:\mathbb{Q}]=?$

Vediamo se $f(x)$ è fattorizzabile: $f(x) = (x^2+ax+b)(x^2+cx+d) \Leftrightarrow$

$$\begin{cases} bd=1 \\ a+c=0 \\ ad+bc=0 \\ ac+b+d=3 \end{cases} \longrightarrow \begin{cases} d=b^{-1} \\ c=-a \\ ab-ab=0 \\ b+b^{-1}=3+a^2 \end{cases} \qquad a(b^{-1}-b)=0 \Rightarrow a=0 \vee b=\pm 1$$

- $a=0 \Rightarrow b+b^{-1}=3 \Rightarrow b^2-3b+1$ non ha sol in $\mathbb{Q}$
- $b=\pm 1 \Rightarrow 3+a^2=\pm 2$ non ha sol in $\mathbb{Q}$

Dunque $f(x)$ irrid.
Cerchiamo le radici di $f(t)$ $(t:=x^2)$ $\quad t = \frac{-3\pm\sqrt{5}}{2} \Rightarrow x = \pm\sqrt{\frac{-3\pm\sqrt{5}}{2}}$

$\alpha := \sqrt{\frac{-3+\sqrt{5}}{2}}$ $\quad \beta := \sqrt{\frac{-3-\sqrt{5}}{2}}$ $\quad$ perciò $L = \mathbb{Q}(\alpha, \beta)$

Dato che $f(x)$ irrid $\quad [\mathbb{Q}(\alpha):\mathbb{Q}]=4$

$\alpha^2\beta^2 = \alpha(-\alpha)\beta(-\beta) = 1 \Rightarrow \beta = \sqrt{\alpha^{-2}} \Rightarrow \beta = \pm 1/\alpha \Rightarrow \beta \in \mathbb{Q}(\alpha)$

i.e. prod delle rad dev essere il termine noto

$\Rightarrow [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] = 1$

**Esercizio 6:** Sia $f(x) \in K[x]$ pol min di $\alpha$ su $K$. Trova il polinomio minimo di $\alpha^2$

Innanzitutto $K(\alpha^2) \subset K(\alpha)$ e $[K(\alpha):K(\alpha^2)] = 2$ perché $\mu_{\alpha, K(\alpha^2)} \mid x^2-\alpha^2$

- Se $[K(\alpha):K(\alpha^2)] = 2 \Rightarrow [K(\alpha):K] = 2[K(\alpha^2):K] \Rightarrow \deg \mu_\alpha = 2 \deg \mu_{\alpha^2}$

N.B. $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^2)] = 2$ $\quad \mu_{\alpha^2}(x) \in K[x^2]$ ma $\mu_{\alpha^2}(x)$ è pol min di $\alpha$ perché $\mu_{\alpha^2}(\alpha^2) = 0 \Rightarrow \deg(\mu_{\alpha^2}(x^2)) = \deg \mu_\alpha$

Viceversa $\mu_\alpha(x) \in K[x^2]$ $\exists\, g(x) \in K[x] \mid \mu_\alpha(x) = g(x^2)$ e $g(x^2) = \mu_{\alpha^2}(x)$

- Se $[K(\alpha):K(\alpha^2)] = 1 \Rightarrow \alpha \in \mathbb{Q}(\alpha^2)$ e $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2) \Rightarrow \deg \mu_\alpha = \deg \mu_{\alpha^2}$

$\mu_\alpha(x) = p(x^2) + x\,d(x^2)$ con $p, d \in K[x^2]$.

- $p \neq 0$ perché $\mu_\alpha(0) = p(0) \neq 0$
- $\deg p \leq \frac{1}{2} \deg \mu_\alpha \Rightarrow p(\alpha^2) \neq 0$ altrimenti: $\mu_{\alpha^2} \mid p$ ma $\deg \mu_{\alpha^2} = \deg \mu_\alpha$ $\lightning$

Ma quindi: $\mu_\alpha(\alpha) = p(\alpha^2) + \alpha\, d(\alpha^2) \quad \mu_{-\alpha}(x) = p(x^2) - x\,d(x^2)$

$\mu_\alpha \mu_{-\alpha} = [p(x^2)+x\,d(x^2)][p(x^2)-x\,d(x^2)] = p(x^2)^2 - x^2 d(x^2)^2 \in K[x^2]$

$\exists g \in K[x] \mid g(x^2) = p(x^2)^2 - x^2 d(x^2)^2 \in K[x^2] \Rightarrow g(x^2) = \mu_\alpha(x)\mu_{-\alpha}(x)$ e $g(\alpha^2) = 0$

$\deg g = \frac{1}{2}\deg g(x^2) = \frac{1}{2}\deg \mu_\alpha \deg \mu_{-\alpha} = \deg \mu_\alpha \Rightarrow g(x) = \mu_{\alpha^2}(x)$

**Esercizio 7:** Sia $K=\mathbb{Q}$ $\alpha = 2+\sqrt{5+\sqrt{-5}}$. Trova il pol min di $\alpha$ su $K$

$(\alpha-2)^2 = 5+\sqrt{-5} \Rightarrow \sqrt{-5} \in \mathbb{Q}(\alpha)$

$\alpha \in \mathbb{Q}(\sqrt{5}, i)$ $\iff$ $5+\sqrt{5}i$ è un quadrato in $\mathbb{Q}(\sqrt{5}, i)$ :
$(a+b\sqrt{-5})^2 = a^2-5b^2+2ab\sqrt{-5} \iff \begin{cases} a^2-5b^2=5 \\ 2ab=1 \end{cases} \iff \begin{cases} a^2-5/4a^2=5 \\ b=1/2a \end{cases}$

$\iff 4a^4-20a^2-5=0$ ma è irrid per Eisenstein $\Rightarrow \alpha \notin \mathbb{Q}(\sqrt{5}, i)$

Ma quindi $\mu_\alpha(x) = x^4-8x^3+14x^2+8x \notin \mathbb{Q}[x^2]$. $\mu_{\alpha^2} = (x^2+14x+6)^2-x(-8x+8)^2 =$
$= x^4-36x^3+336x^2+108x+36$

**Esercizio 8:** $\overline{K} := \bigcup_{n>0} \mathbb{F}_{p^n}$ è la chiusura algebrica di $\mathbb{F}_p$ ($\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ $\forall m,n$ con $m \mid n$)

- $\overline{K}$ è [redacted] algebrico ; $x \in \overline{K} \Rightarrow x \in \mathbb{F}_{p^n}$ per un $n \in \mathbb{N} \Rightarrow x$ è alg su $\mathbb{F}_p$
- $\overline{K}$ è alg chiuso ; sia $f \in K[x]$ $\exists \alpha$ rad. di $f$ in $\overline{K}$. Infatti: $f(x)=a_n x^n+\dots+a_0$
  $a_i \in K$ allora $\forall i$ $\exists m_j \mid a_i \in \mathbb{F}_{p^{m_j}}$. Mettendo $r = m_0 m_1 \dots m_n \Rightarrow$
  $a_i \in \mathbb{F}_{p^r}$ $\forall i \Rightarrow f(x) \in \mathbb{F}_{p^r}[x]$

## Algebra Lezione 03/12/25 (teoria - Del Corso)

- **Teorema dell'elemento primitivo:** Sia $K$ campo, $E/K$ estensione finita (e separabile) $\Rightarrow E/K$ è semplice

→ **Dim** • $K$ finito $\Rightarrow L$ finito $\Rightarrow L^*$ è ciclico $\Rightarrow L^* = \langle \alpha \rangle \Rightarrow L = K(\alpha)$

• $K$ infinito Sia $L = K(\alpha, \beta)$ $[L:K]=n \Rightarrow \varphi_1, \dots, \varphi_n : L \hookrightarrow \overline{K}$
con $\varphi_{i|K} = id \Rightarrow \forall t \in K$ $K \subseteq K(\alpha+t\beta) \subseteq K(\alpha,\beta)$

$$F(x) = \prod_{i<j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta)) \neq 0$$ perché $\varphi_i \neq \varphi_j$

poiché $\exists t \in K \mid F(t) \neq 0 \Rightarrow \alpha + t\beta$ ha deg $n$

- **Proposizione grado del campo di spezzamento:** Dato $f(x) \in K[x]$ irriducibile deg$(f(x))=n$ e detto $F$ il suo CDS su $K$ $n \mid [F:K] \mid n!$ e $Gal(F/K) \hookrightarrow S_n$

→ **Dim** $\alpha_1, \dots, \alpha_n$ radici di $f(x)$ in $\overline{K}$ $\Rightarrow F = (\alpha_1, \dots, \alpha_n)$ ma quindi $K \subseteq K(\alpha_i) \subseteq F$

$\Rightarrow n = [K(\alpha_i) : K] \mid [F:K] = |Gal(F/K)|$

$$\Phi : Gal(F/K) \longrightarrow S(\{\alpha_1, \dots, \alpha_n\}) \cong S_n$$
$$\varphi \longmapsto \varphi_{|\{\alpha_1, \dots, \alpha_n\}}$$

• $\Phi$ b.d. perché sto permutando le radici di $f(x)$

• $\Phi$ omo. $\Phi(\varphi \circ \psi) = (\varphi \circ \psi)_{|\{\alpha_1, \dots, \alpha_n\}} = (\varphi(\psi(\{\alpha_1, \dots, \alpha_n\}))) = \Phi(\varphi) \circ \Phi(\psi)$

• $\Phi$ inj $\ker \Phi = \{\varphi \in Gal(F/K) \mid \varphi(\alpha_i) = id(\alpha_i) = \alpha_i \ \forall i \in \{1, \dots, n\}\} = \{id\}$

- Noto che se $f$ è irrid, $f = \mu_{\alpha_i}$ $\forall i$ $\varphi_{ij} : K(\alpha_i) \hookrightarrow \overline{K}$ $\varphi_{ij|K} = id$ e posso
$\alpha_i \longmapsto \alpha_j$
estenderlo su $L$ quindi $\forall i,j$ $\exists \varphi \in Gal(L/K) \mid \varphi(\alpha_i) = \alpha_j$

- **Lemma il campo fissato è quello base $\iff$ è fissato rispetto a tutto il gruppo:**
Sia $L/M$ estensione di Galois, $H \in Gal(L/M)$ allora
$M = L^H \iff H = Gal(L/M)$

→ **Dim** $\Leftarrow$ $G := Gal(L/M)$, supponiamo $H=G$. Se $M \subsetneq L^G \Rightarrow [L^G : M] > 1$
ma quindi $\exists \varphi : L^G \hookrightarrow \overline{M}$ $\varphi_{|M} = id$
Estendiamo a $\tilde{\varphi} : L \hookrightarrow M$ $\tilde{\varphi}_{|L^G} = \varphi$ e $\tilde{\varphi}(L) = L$ perché normale
$\Rightarrow \tilde{\varphi} \in G$ $\lightning$ perché $[L^G : M] > 1$

$\Rightarrow$ per il th delle el prim. $\exists \alpha \mid L = M(\alpha)$. sia $H \subseteq G$ tale che
$L^H = M$
$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$ deg$(f(x)) = |H|$

$f(x)$ si annulla in $\alpha$ e $f(x) \in L^H[x]$ perché preso $\rho \in H$
$\rho(f(x)) = \prod_{\sigma \in H} (x - \rho(\sigma(\alpha))) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \overset{*}{=} f(x)$ * stai ri-permutando ma per quindi non cambi il prodotto

$|G| = [L:M] = [M(\alpha):M] = \deg \mu_{\alpha,M}(x) \leq \deg(f) = |H| \Rightarrow |H| = |G|$

- Lemma sottocampo fissato dal coniugato: Sia $L/K$ di Galois, $H \leq Gal(L/K)$, $\sigma \in Gal(L/K) \Rightarrow L^{\sigma H \sigma^{-1}} = \sigma(L^H)$

→ Dim $L^H = \{\alpha \in L \mid \varphi(\alpha) = \alpha \ \forall \varphi \in H\}$ ma quindi $\sigma(L^H) = \{\sigma(\alpha) \mid \alpha \in L^H\} =$

$= \{\sigma(\alpha) \mid \varphi(\alpha) = \alpha \ \forall \varphi \in H\}$

$\sigma(L^H) = \{\beta \in L \mid (\varphi \circ \sigma^{-1})(\beta) = \sigma^{-1}(\beta) \ \forall \varphi \in H\} = \{\beta \in L \mid (\sigma \circ \varphi \circ \sigma^{-1})(\beta) \ \forall \varphi \in H\} =$

$\cong L^{\sigma H \sigma^{-1}}$

## Algebra Lezione 05/12/25 (teoria - Patimo)

**Esercizio 1:** Sia $f(x) = (x^8-1)(x^3-1)$, $L$ cds di $f(x)$ su $\mathbb{F}_p$. Calcola $[L:\mathbb{F}_p]$ $\forall p$ primo

Ricorda: Se $f = f_1 \cdots f_n$ con $f_i$ irrid su $\mathbb{F}_p$ $[L:\mathbb{F}_p] = mcm(deg(f_1), \dots, deg(f_n))$

Ma $(x^3-1) = (x^2+x+1)(x-1)$. $x^2+x+1$ è irrid su $\mathbb{F}_p \iff$ non ci sono radici in $\mathbb{F}_p$

$\Rightarrow x^2+x+1$ è irrid in $\mathbb{F}_p$ con $p \neq 3$

Questo perché se $3 \mid |\mathbb{F}_p^*|$, $|\mathbb{F}_p^*| \cong \mathbb{Z}/p-1\mathbb{Z}$ $\exists g \in \mathbb{F}_p^*$ $ord(g) = 3 \Rightarrow g^3 = 1$

$\Rightarrow g$ rad $\frac{x^3-1}{x-1} = x^2+x+1$

N.B. $g(x) = (x^3-1)$ $L_g$ cds di $g(x)$ su $\mathbb{F}_p$ $[L_g:\mathbb{F}_p] = \begin{cases} 1 & \text{se } p \equiv 1 \ (3) \\ 2 & \text{se } p \equiv 2 \ (3) \end{cases}$

- Proposizione: Se $(m,n) = 1$ il cds su $\mathbb{F}_p$ è $\mathbb{F}_{p^r}$ $(r = ord_{(\mathbb{Z}/n\mathbb{Z})^*}(p))$

Invece $h(x) = x^8-1$ il cds $L_h$ su $\mathbb{F}_p$ se $p \neq 2$ è $\mathbb{F}_{p^r}$ con $r = ord_{(\mathbb{Z}/8\mathbb{Z})^*}(p)$

$(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\Rightarrow L_h = \begin{cases} \mathbb{F}_p & \text{se } p \equiv 1 \ (8) \\ \mathbb{F}_{p^2} & \text{se } p \not\equiv 1 \ (8) \end{cases}$

quindi per $p = 2$ $(x^8-1) = (x-1)^8$ $\Rightarrow L_h = \mathbb{F}_p$ ($ord = 2$)

Da qui ricavo il cds di $f$: $L = L_g L_h = \begin{cases} L_g = L_h = \mathbb{F}_p \iff (p=3) \vee (p \equiv 1 \ (3)) \wedge (p=2) \vee (p \equiv 1 \ (8))) \iff p \equiv 1 \ (\dots) \\ \mathbb{F}_{p^2} \text{ se } L_g = \mathbb{F}_{p^2} \vee L_h = \mathbb{F}_{p^2} \end{cases}$

**Esercizio 2:** $f(x) = x^6 + ax^3 + b \in \mathbb{F}_p[x]$. $L$ cds su $\mathbb{F}_p$ ($p$ primo). Dimostra che $[L:\mathbb{F}_p] \mid 6$

$f(x) \in \mathbb{F}_p[x^3]$, $f(x) = g(x^3)$ con $g(x) = x^2+ax+b$. Sia $\alpha$ rad di $g \Rightarrow \sqrt[3]{\alpha} = \beta$ è rad $f$

Se $\beta$ è rad di $x^3-\alpha$ allora le altre rad del polinomio sono $\beta\zeta_3$, $\beta\zeta_3^2$

Noto che $\alpha_1, \alpha_2, \zeta_3 \in \mathbb{F}_{p^2}$ perché radici di un polinomio di grado 2 irrid. su $\mathbb{F}_p$

Vale $g(x) = (x-\alpha_1)(x-\alpha_2) \in \mathbb{F}_{p^2}[x] \Rightarrow f(x) = (x^3-\alpha_1)(x^3-\alpha_2) \in \mathbb{F}_{p^2}[x]$

cds di $x^3-\alpha_1$ su $\mathbb{F}_{p^2} = \begin{cases} \mathbb{F}_{p^2} & \text{se tutte le rad stanno in } \mathbb{F}_{p^2} \\ \mathbb{F}_{p^2}(\beta_1) & \text{se } \exists \beta_1 \text{ rad non in } \mathbb{F}_{p^2} \end{cases}$

Se $\beta_1$ rad di $x^2-\alpha_1$ e $\beta_1 \notin \mathbb{F}_{p^2}$ ($\beta_1, \beta_1\zeta_3, \beta_1\zeta_3^2 \in \mathbb{F}_{p^2}(\beta_1)$)

Ma quindi il cds è $\mathbb{F}_{p^2}(\beta_1)$ se $\exists$ rad in $\mathbb{F}_{p^2}$ $\Rightarrow$ cds $\mathbb{F}_{p^2}$

se $\nexists$ rad in $\mathbb{F}_{p^2} \Rightarrow x^3-\alpha_1$ irrid $\Rightarrow$ cds $(\mathbb{F}_{p^2})^3 = \mathbb{F}_{p^6}$

$\Rightarrow$ cds di $f(x) \subseteq \mathbb{F}_{p^6}$ $\Rightarrow [L:\mathbb{F}_p] \mid 6$

**Esercizio 3:** $\alpha, \beta \in \overline{\mathbb{F}}_p$ $m = [\mathbb{F}_p(\alpha):\mathbb{F}_p]$ $n = [\mathbb{F}_p(\alpha):\mathbb{F}_p]$. Se $(n,m) = 1 \Rightarrow [\mathbb{F}_p(\alpha+\beta):\mathbb{F}_p] = nm$

(è equiv $\mathbb{F}_p(\alpha+\beta) = \mathbb{F}_p(\alpha,\beta)$)

Innanzitutto noto che $\mathbb{F}_p(\alpha+\beta) = \mathbb{F}_p[\alpha+\beta, \beta] = \mathbb{F}_p(\alpha+\beta, \alpha)$.

Sia $d = [\mathbb{F}_p(\alpha+\beta):\mathbb{F}_p] \Rightarrow [\mathbb{F}_p(\alpha+\beta, \alpha):\mathbb{F}_p] = mcm(d,m) \wedge [\mathbb{F}_p(\alpha+\beta, \beta):\mathbb{F}_p] = mcm(d,n)$

Ma quindi $mn = mcm(d,n) = mcm(d,m)$ se $(m,n) = 1$ allora $m \mid mcd(d,n) \Rightarrow m \mid d$; $n \mid mcd(d,m) \Rightarrow n \mid d$ $\Big\} mn \mid d$

Poiché $\mathbb{F}_p(\alpha+\beta) \subseteq \mathbb{F}_p(\alpha,\beta) \Rightarrow d \mid mn \Rightarrow d = mn \Rightarrow \mathbb{F}_p(\alpha+\beta) = \mathbb{F}_p(\alpha,\beta)$

Esercizio 4: $f(x)=x^4+ax^2+b \in \mathbb{Q}[x]$. $L$ è campo di spezzamento su $\mathbb{Q}$, $G=Gal(L/\mathbb{Q})$

(i) $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ se $\sqrt{b} \in \mathbb{Q}$
(ii) $G \cong \mathbb{Z}/4\mathbb{Z}$ se $\sqrt{b} \notin \mathbb{Q}$ $\sqrt{b(a^2-4b)} \in \mathbb{Q}$
(iii) $G \cong D_4$ se $\sqrt{b}, \sqrt{b(a^2-4b)} \notin \mathbb{Q}$

$f(x)=g(x^2)$, $g(x)=x^2+ax+b$ $\Delta=a^2-4b$, le radici di $g$ sono $\frac{-a \pm \sqrt{\Delta}}{2}$

se $f(x)$ è irrid $\Delta \notin \mathbb{Q}$. Le radici di $f$ sono $\pm\sqrt{\frac{-a \pm \sqrt{\Delta}}{2}}$ $\alpha=\sqrt{\frac{-a+\sqrt{\Delta}}{2}}$ $\beta=\sqrt{\frac{-a-\sqrt{\Delta}}{2}}$

Ma quindi $L=\mathbb{Q}(\alpha,-\alpha,\beta,-\beta)=\mathbb{Q}(\alpha,\beta)$.

$\mathbb{Q}(\alpha,\beta)$ — 2 — $\mathbb{Q}(\alpha)$ — 4 — $\mathbb{Q}$ ; $\mathbb{Q}(\alpha,\beta)$ — 2 — $\mathbb{Q}(\beta)$ — 2 — $\mathbb{Q}$

$[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ ($\alpha$ rad pol min deg 4

$[\mathbb{Q}(\beta):\mathbb{Q}]=2 \Rightarrow [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=\begin{cases}4 & \text{se } \beta \in \mathbb{Q}(\alpha)\\ 8 & \text{se } \beta \notin \mathbb{Q}(\alpha)\end{cases}$

Quindi $G \hookrightarrow S_4$ come sgr transitivo: $-|G|=8 \Rightarrow G \cong D_4$ (i 2-Sylowdi $S_4$)

$-|G|=4 \to \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$
$\to \mathbb{Z}/4\mathbb{Z}$

Dimostriamo $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \iff \sqrt{b} \in \mathbb{Q}$

$\Rightarrow |G|=4$ $\exists \varphi \in G \mid \varphi(\alpha)=\beta$. $\varphi(\beta)=\pm\varphi\left(\frac{\sqrt{b}}{\alpha}\right) \overset{\text{perché } \varphi \text{ fissa } \sqrt{b}}{=} \pm\frac{\sqrt{b}}{\varphi(\alpha)} = \pm\frac{\sqrt{b}}{\beta} = \alpha$

Ma quindi $\varphi$ agisce come $(\alpha\ \beta)(-\alpha\ -\beta)$

$\exists \psi \in G$ $\psi(\alpha)=-\alpha \Rightarrow \psi(-\alpha)=-\psi(\alpha)=-(-\alpha)=\alpha$. Ma quindi $\psi$ agisce come $(\alpha\ -\alpha)(\beta\ -\beta)$

Ma quindi ho due el di ord 2 in un gruppo di ordine 4 $\Rightarrow G=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

$\Leftarrow$ S.A. $\sqrt{b} \notin \mathbb{Q}$ Sicuramente $\sqrt{b}=\pm\alpha\beta \in \mathbb{Q}(\alpha,\beta)$ questo perché $\exists \varphi \in Gal(\mathbb{Q}(\sqrt{b})/\mathbb{Q})$ che posso estendere a un $\tilde{\varphi} \in Gal(\mathbb{Q}(\alpha,\beta)/\mathbb{Q})$

$\exists \tau \in G$ $\tau(\sqrt{b})=-\sqrt{b}=\tau(\alpha\beta) \Rightarrow \tau(\alpha\beta)=-\alpha\beta$

- $\tau(\alpha)=\alpha$ NO perché l'azione non può avere punti fissi
- $\tau(\alpha)=-\alpha \Rightarrow \tau(\beta)=\beta$ ↯
- $\tau(\alpha)=\beta \Rightarrow \tau(\beta)=-\alpha \Rightarrow \tau^2(\alpha)=-\alpha \Rightarrow ord(\tau)=4$ ↯
- $\tau(\alpha)=-\beta \Rightarrow \tau(\beta)=\alpha \Rightarrow \tau(-\beta)=-\alpha \Rightarrow ord(\tau)=4$ ↯

} perché in $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ non ci sono el di ord 4

Dimostriamo $\sqrt{b} \notin \mathbb{Q}$, $\sqrt{b\Delta} \in \mathbb{Q} \Rightarrow G \cong \mathbb{Z}/4\mathbb{Z}$

Ricordiamo che $\mathbb{Q}(\sqrt{b})=\mathbb{Q}(\sqrt{\Delta}) \iff \sqrt{b\Delta} \in \mathbb{Q}$
Chiamo $K=\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\alpha,\beta)$ perché $\alpha^2=\frac{-a+\sqrt{\Delta}}{2}$

$\mathbb{Q}(\alpha)=K(\alpha)=K\left(\sqrt{\frac{-a+\sqrt{\Delta}}{2}}\right)$ $\mathbb{Q}(\beta)=K(\beta)=K\left(\sqrt{\frac{-a-\sqrt{\Delta}}{2}}\right)$

Voglio capire se $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=4,8 \iff [K(\alpha,\beta):K]=2,4$

- $[K(\alpha,\beta):K]=2 \iff K(\alpha)=K(\beta) \iff \alpha\beta=\pm\sqrt{b} \in K \iff \mathbb{Q}(\sqrt{b})=\mathbb{Q}(\sqrt{\Delta})=K$
  $\iff \sqrt{b\Delta} \in \mathbb{Q}$

  Ma quindi $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=4 \iff \sqrt{b\Delta} \in \mathbb{Q}$ e siccome $\sqrt{b} \notin \mathbb{Q}$ $G \cong \mathbb{Z}/4\mathbb{Z}$

- se $\sqrt{b} \notin \mathbb{Q}$, $\sqrt{b\Delta} \notin \mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=8 \Rightarrow Gal(\mathbb{Q}(\alpha,\beta)/\mathbb{Q}) \cong D_4$

## Algebra Lezione 10/12/25 (Teoria - Del Corso) → incompleta!!

- **Teorema di corrispondenza di Galois:** Sia $L/K$ di Galois (finita) esiste una corrispondenza biunivoca tra l'insieme delle sottoestensioni di $L/K$ e l'insieme dei sottogruppi di $Gal(L/K)$.
  Inoltre $H \lhd G \iff L^H/K$ normale $\Rightarrow Gal(L^H/K) \cong \frac{Gal(L/K)}{Gal(L/L^H)} \cong G/H$

→ Dim $\mathcal{E}:=\{F \mid K \subseteq F \subseteq L\} \longleftrightarrow \mathcal{G}:=\{H < Gal(L/K)\}$

$F \xrightarrow{\alpha} Gal(L/F)$

$H \xleftarrow{\beta} L^H$

- $\alpha, \beta$ b.d. $L^H$ è campo e $K \subseteq L^H \subseteq L$
  $Gal(L/F) < Gal(L/K)$ perché un $K$-automorfismo di $F$ fissa $K$

- $\alpha$ inv $\beta$ $\quad \alpha \circ \beta(H) = \alpha(L^H) = Gal(L/L^H) = Aut_{L^H}(L) = H$

- $\beta$ inv $\alpha$ $\quad \beta \circ \alpha(F) = \beta(Gal(L/F)) = L^{Gal(L/F)} = F$

$\Leftrightarrow$ $H \lhd Gal(L/K) \Leftrightarrow \sigma H \sigma^{-1} = H \ \forall \sigma \in Gal(L/K)$ allora per il lemma
$\sigma(L^H) = L^{\sigma H \sigma^{-1}} = L^H \ \forall \sigma \in Gal(L/K) \Rightarrow L^H/K$ è normale

- $res: Gal(L/K) \longrightarrow Gal(L^H/K)$
  $\varphi \longmapsto \varphi_{|L^H}$

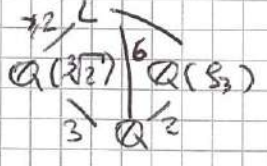
  - b.d. perché funz restrizione
  - omo chiaro
  - surj $\forall \psi \in Gal(L^H/K)$ ammette est. a $L$ e tutte sono aut.
  - $\ker res = \{\varphi \in Gal(L/K) \mid \varphi_{|L^H} = id\} = H$

    $\supseteq$ $\varphi(\alpha) = \alpha \ \forall \alpha \in L^H = \{x \mid hx = x \ \forall h \in H\}$
    $\subseteq$ cardinalità

  $\Rightarrow$ 1° th om $\quad Gal(L^H/K) \cong \dfrac{Gal(L/K)}{Gal(L/L^H)} = \dfrac{G}{H}$

**Esercizio 1:** Sia $f(x) = x^3 - 2$. Studiamo il galois del suo cos su $\mathbb{Q}$

Le sue radici sono $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2 \Rightarrow L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ è il suo CDS




$[L:\mathbb{Q}] = 6 \Rightarrow |Gal(L/\mathbb{Q})| = 6 \Rightarrow Gal(L/\mathbb{Q}) \cong S_3 \cong \mathbb{Z}/6\mathbb{Z}$

Ma $L/\mathbb{Q}$ ammette estensioni non normali $\Rightarrow Gal(L/\mathbb{Q})$ non è abel

$\Rightarrow Gal(L/\mathbb{Q}) \cong S_3 \Rightarrow K = L^{S_3}$

Perciò i sottogruppi di $Gal(L/\mathbb{Q})$ sono:

- $A_3 = \langle (123) \rangle \xrightarrow{\sim} L^{A_3} = \mathbb{Q}(\zeta_3)$ perché ha grado 3 in alto grado 2 in basso
- $\langle (12) \rangle, \langle (13) \rangle \langle (23) \rangle \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\zeta_3), \mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$ i coniugati
- $\{id\} \xrightarrow{\sim} \mathbb{Q}$

Ma chi sono gli elementi del Galois? Sono le funzioni

$$\varphi_{ij}: \begin{array}{ccc} L & \longrightarrow & \overline{\mathbb{Q}} \\ \sqrt[3]{2} & \longmapsto & \zeta_3^i \sqrt[3]{2} \quad (i = 0,1,2) \\ \zeta_3 & \longmapsto & \zeta_3^j \quad (j = 1,2) \end{array}$$

← N.B non vanno sempre bene tutte le scelte in questo caso sì perché sono 6

Noto che $\varphi_{11}$ ha deg 3 e $\varphi_{02}$ ha deg 2 e dato che $S_3 = \langle (123)(12) \rangle$

$\Rightarrow Gal(L/\mathbb{Q}) \cong \langle \varphi_{11}, \varphi_{02} \rangle$

- **Proposizione proprietà della corrispondenza di Galois:** Dati $H, S \leq Gal(L/K)$ allora:
  (i) $H \leq S \Leftrightarrow L^H \supseteq L^S$
  (ii) $L^{H \cap S} = L^H L^S$ (il composto)
  (iii) $L^{\langle S, H \rangle} = L^H \cap L^S$

→ **Dim (i)** $\Leftarrow$ $\sigma \in H$, $L^H \supseteq L^S$ allora $\sigma$ fissa gli elementi di $L^H \Rightarrow$ fissa gli elementi di $L^S \Rightarrow \sigma \in S$

$\Rightarrow \forall \sigma \in H \ \ \sigma \in S \Rightarrow \sigma$ fissa gli el di $S \Rightarrow L^H \supseteq L^S$

**(ii)** $\supseteq$ per (i) $H \cap S \leq H, S \Rightarrow L^{H \cap S} \supseteq L^H, L^S \Rightarrow L^{H \cap S} \supseteq L^H L^S$

$\subseteq L^H L^S \subseteq L \Rightarrow \exists N \ Gal(L/K) \mid L^H L^S = L^N \Rightarrow$ per th corr. Galois
$Gal(L/L^{H \cap S}) = Gal(L/L^N) = N \leq (Gal(L/L^H) \cap Gal(L/L^S)) \supseteq L^{H \cap S}$

(ii) $\subseteq$ $H,S \subseteq \langle H,S\rangle \Rightarrow L^S, L^H \supseteq L^{\langle H,S\rangle}$ per (i) $\Rightarrow L^{\langle H,S\rangle} \subseteq L^H \cap L^S$

$\supseteq$ $\alpha \in L^H \cap L^S \Rightarrow \varphi(\alpha)=\alpha \quad \forall \varphi \in H,S \Rightarrow \alpha$ è fissato dai generatori
$\Rightarrow L^H \cap L^S \subseteq L^{\langle H,S\rangle}$

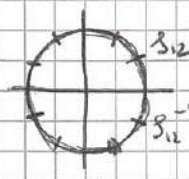
# Algebra Lezione 15/12/25 (esercitazione - Patimo)

**Esercizio 1:** Trova tutte le sottoestensioni di $\mathbb{Q}(\zeta_{12})$

Innanzitutto noto che $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$ è di Galois (perché $\mathbb{Q}(\zeta_{12})$ è cos di $x^{12}-1$)

$x^{12}-1 = (x^6-1)(x^6+1) = (x^3-1)(x^3+1)(x^2+1)(x^4-x^2+1)$

$\Rightarrow [\mathbb{Q}(\zeta_{12}):\mathbb{Q}] \leq 4$ ma se $f(x)$ è irriducibile che $\zeta_{12}$ è sua radice è proprio 4



$\zeta_{12} = e^{\frac{2\pi i}{12}} = \cos\left(\frac{\pi}{6}\right) + i\sin\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{i}{2}$

$\zeta_{12}^{-1} = \frac{\sqrt{3}}{2} - \frac{i}{2}$

$\Rightarrow \zeta_{12} + \zeta_{12}^{-1} \in \mathbb{Q}(\zeta_{12}) \Rightarrow \sqrt{3} \in \mathbb{Q}(\zeta_{12}) \Rightarrow i \in \mathbb{Q}(\zeta_{12}) \Rightarrow \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i,\sqrt{3})$

Ma $[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}] = 4 \Rightarrow f(x)$ irrid

Sia $G = Gal(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$, $|G|=4$. $G \neq \mathbb{Z}/4\mathbb{Z}$ perché ho già trovato 2 sottoestensioni di grado 2 $\Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

| sottogruppi di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | sottoestensioni di $\mathbb{Q}(\zeta_{12})$ su $\mathbb{Q}$ |
|---|---|
| $\{e\}$ | $\mathbb{Q}(\zeta_{12})$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Q}$ |
| $\langle(0,1)\rangle, \langle(1,0)\rangle, \langle(1,1)\rangle$ | $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{3}i)$ |

- **Proposizione:** Sia $p$ primo, allora $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ è di Galois e $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$

→ **Dim** $\zeta_p$ è radice di $\frac{x^p-1}{x-1} = x^{p-1}+\dots+x+1 \equiv \Psi_p(x)$

$\mathbb{Q}(\zeta_p)$ è cos di $\Psi_p(x)$ che ha rad $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$

- $\Psi_p(y+1) = \frac{(y+1)^p-1}{y} = \sum_{i=1}^{p}\binom{p}{i}y^{i-1}$ è irrid per Eisenstein ($p \nmid \binom{p}{p}=1$, $p \mid \binom{p}{i}\ \forall i$, $p^2 \nmid \binom{p}{1}=p$)

$\Rightarrow \Psi_p(x)$ irrid $\Rightarrow [\mathbb{Q}(\zeta_p):\mathbb{Q}] = \deg \Psi_p(x) = p-1$

Sia $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \{\varphi_1,\dots,\varphi_{p-1}\}$ con $\varphi_i(\zeta_p) = \zeta_p^i$

$i \in (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow G$ è iso di gruppi
$\quad\quad\quad\ \longmapsto \varphi_i$

- **Proposizione:** $(\mathbb{Z}/n\mathbb{Z})^* \cong Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

La cosa difficile è dimostrare che $\Psi_n(x) = \frac{x^n-1}{\prod_{d \mid n,\, d<n}\Psi_d(x)}$ è irrid di $\deg \Psi_n(x) = \varphi(n)$

**Esercizio 2:** Studia $\mathbb{Q}(\underbrace{\zeta_7+\zeta_7^{-1}}_{\alpha})/\mathbb{Q}$

- Noto che $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_7)$
- Poiché $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è abeliana $\Rightarrow$ le sue sottoestensioni sono di Galois
- $\varphi_{-1} : \mathbb{Q}(\zeta_7) \longrightarrow \mathbb{Q}(\zeta_7)$, $\varphi_{-1}(\alpha) = \zeta_7^{-1} + \zeta_7 = \alpha$
  $\quad\quad\quad\ \zeta_7 \longmapsto \zeta_7^{-1}$

ma quindi $\varphi_{-1}$ ha ordine 2 $\Rightarrow [\mathbb{Q}(\zeta_7):\mathbb{Q}(\alpha)] \geq 2$

D'altra parte $x^2 - \alpha x + 1 = (x-\zeta_7)(x-\zeta_7^{-1})$ e $\alpha$ è rad di questo polinomio

$\Rightarrow [\mathbb{Q}(\zeta_7):\mathbb{Q}(\alpha)] = 2 \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ (infatti $[\mathbb{Q}(\zeta_7):\mathbb{Q}] = 6$)

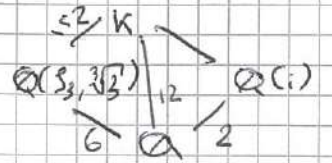
$\varphi_1(\alpha) = \alpha = \varphi_6(\alpha)$, $\varphi_2(\alpha) = \zeta_7^2 - \zeta_7^{-2} = \varphi_5(\alpha)$, $\varphi_3(\alpha) = \zeta_7^3 - \zeta_7^{-3} = \varphi_4(\alpha)$

$\Rightarrow \mu_\alpha(x) = x^3 + x^2 - 2x - 1$

A questo punto potremmo chiederci quale è l'altra sottoestensione di $\mathbb{Q}(\zeta_7)$. Perché $\mathbb{Q}(\sqrt{7}i)$?

**Esercizio 3:** Trova tutti i sottocampi di $\mathbb{Q}(i, \zeta_3, \sqrt[3]{3})$ | $[F:\mathbb{Q}] = 2$

$K = \mathbb{Q}(i, \zeta_3, \sqrt[3]{3})$ è campo di spezzamento su $\mathbb{Q}$ di $\{\underbrace{x^2+1}_{\pm i}, \underbrace{x^3-3}_{\sqrt[3]{3}, \sqrt[3]{3}\zeta_3, \sqrt[3]{3}\zeta_3^2}\}$




$[K : \mathbb{Q}(\zeta_3, \sqrt[3]{3})] = 1 \iff i \in \mathbb{Q}(\zeta_3, \sqrt[3]{3}) \iff \mathbb{Q}(i) \subset \mathbb{Q}(\zeta_3, \sqrt[3]{3})$

ma $Gal\left(\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q}\right) \cong S_3$ e per Galois $\mathbb{Q}(\zeta_3)$ è l'unica sottoestensione di deg 2; $\zeta_3 = \cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = \frac{1}{2} + i\frac{\sqrt{3}}{2}$

$\Rightarrow \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) \not\subset \mathbb{Q}(i) \Rightarrow \mathbb{Q}(i) \subset \mathbb{Q}(\zeta_3, \sqrt[3]{3}) \Rightarrow [K : \mathbb{Q}(\zeta_3, \sqrt[3]{3})] = 2$

Ma $Gal(K/\mathbb{Q}) \hookrightarrow Gal\left(\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q}\right) \times Gal\left(\mathbb{Q}(i)/\mathbb{Q}\right) \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$

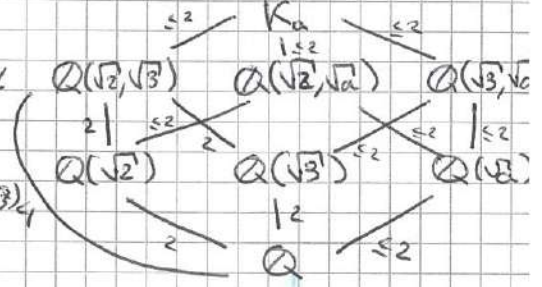
$\Rightarrow Gal(K/\mathbb{Q}) \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$ (per cardinalità

Chi sono i sottogruppi di cardinalità 6 su $S_3 \times \mathbb{Z}/2\mathbb{Z}$?

- $\mathbb{Z}/6\mathbb{Z} = \langle((123), \bar{1})\rangle \longrightarrow \mathbb{Q}(\zeta_3)$
  $\langle((132), \bar{1})\rangle \qquad\qquad \mathbb{Q}(\sqrt{-3})$
- $S_3 \times \{0\} = \langle((12), \bar{0}), ((13), \bar{0}), ((23), \bar{0})\rangle \longrightarrow \mathbb{Q}(i)$
- $\{(\sigma, \text{segno}) \in S_3 \times \mathbb{Z}/2\mathbb{Z}\} = \langle((12), \bar{1}), ((13), \bar{1}), ((23), \bar{1})\rangle \longrightarrow \mathbb{Q}(i)$

**Esercizio 4:** Sia $a \in \mathbb{Z}$ $K_a = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{a})$ studia $K_a$ al variare di $a$

$[K_a : \mathbb{Q}] = \begin{cases} 4 & \text{se } a \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ 8 & \text{altrimenti} \end{cases}$




$[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 \iff \sqrt{a} \in \mathbb{Q} \iff a$ non è quadrato in $\mathbb{Z}$

$[\mathbb{Q}(\sqrt{3}, \sqrt{a}) : \mathbb{Q}(\sqrt{a})] = 2 \iff \sqrt{3} \notin \mathbb{Q}(\sqrt{a}) \iff 3a$ non è quadrato in $\mathbb{Z}$

$[K_a : \mathbb{Q}(\sqrt{3}, \sqrt{a})] = 2 \iff \sqrt{2} \notin \mathbb{Q}(\sqrt{a}, \sqrt{3}) \iff 2a$ non è quadrato in $\mathbb{Q}(\sqrt{3})$

$2a = (x + y\sqrt{3})^2 = x^2 + 3y^2 + 2xy\sqrt{3} \Rightarrow xy = 0 \Rightarrow x = 0 \vee y = 0$

- $x = 0 \Rightarrow 2a = 3y^2 \iff 6a$ è quadrato in $\mathbb{Z}$
- $y = 0 \Rightarrow 2a = x^2 \iff 2a$ è quadrato in $\mathbb{Z}$

$[K_a : \mathbb{Q}] = [K_a : \mathbb{Q}(\sqrt{3}, \sqrt{2})][\mathbb{Q}(\sqrt{3}, \sqrt{a}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 8 \iff a, 2a, 3a, 6a$ non sono quadrati in $\mathbb{Z}$

"2 $\iff$ 6a, 2a no q. "2 $\iff$ 3a no q. "2 $\iff$ a no q

Se $[K_a : \mathbb{Q}] = 4 \Rightarrow K_a = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow Gal\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Se $[K_a : \mathbb{Q}] = 8 \Rightarrow Gal(K_a/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Ad esempio per $a = 7$ le sottoestensioni di deg 2 di $K_7$ sono in corrispondenza con i sottogruppi di indice 2 di $(\mathbb{Z}/2\mathbb{Z})^3$ che sono i sottospazi vettoriali di $\mathbb{F}_2^3$ di dimensione 2 (sono 7)
Quindi ho $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{14})$, $\mathbb{Q}(\sqrt{21})$, $\mathbb{Q}(\sqrt{42})$