Università di Pisa - Dipartimento di Matematica

Algebra 1

MATTIA SALVADORI

m.salvadori23@studenti.unipi.it

Rielaborazione delle lezioni dei professori
G. Gaiffi, V. Melani e F. G. Callegaro

a.a. 2021/2022

Indice

Prefazione

Questo elaborato comprende tutte le lezioni (ed anche qualche parola in più) del corso di Algebra 1 dell'a.a. 2021/2022 tenuto dai suddetti professori.
La realizzazione è stata impegnativa ma, al contempo, davvero molto soddisfacente e spero tanto che vi possa essere utile nello studio.

Ci tengo a ringraziare in modo particolare SABRINA BOTTICCHIO che è stata davvero fondamentale con il suo eccellente, puntuale e immancabile lavoro di correzione di ogni pagina che segue, ma anche tutti coloro che mi hanno segnalato errori, suggerimenti di modifica per maggiore chiarezza e correzioni varie: grazie davvero!
Se ci fosse qualcos'altro da cambiare e/o riscrivere, gradirei tantissimo che me lo segnalaste così da rendere queste dispense il più corrette possibile.

Detto tutto ciò,

Buona lettura!

Mattia

Capitolo 1

Gruppi

1.1 Azione di un gruppo su un insieme

Definizione 1.1.1. *Sia X un insieme e G un gruppo, un'**azione** di G su X è una funzione*

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g \cdot x \end{array}$$

che soddisfa le due proprietà seguenti:

(1) $e \cdot x = x \; \forall x \in X$;

(2) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

1.1.1 Azioni famose

Coniugio: $X = G$, $g \cdot x = gxg^{-1}$. È un'azione?

(1) $e \cdot x = exe^{-1} = x$ ok;

(2) $(g_1 g_2) \cdot x = g_1 g_2 x (g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1} = g_1 \cdot g_2 x g_2^{-1} = g_1 \cdot (g_2 \cdot x)$ ok.

Azione sui laterali: prendiamo $H < G$, ${}^{G}/_{H} = X$ è un insieme, $g \cdot kH = gkH$.

Esercizio 1. *Verificare che questa sia una "buona azione".*

Definizione 1.1.2. *Sia G un gruppo che agisce su X, diremo **orbita** di $x \in X$*

$$orb(x) = \{g \cdot x \mid g \in G\}$$

*e diremo **stabilizzatore** di $x \in X$*

$$Stab(x) = \{g \in G \mid g \cdot x = x\} \subseteq G$$

Lemma 1.1.1. *$Stab(x) < G$.*

Dimostrazione.

- $e \in Stab(x)$: evidente;
- $g_1, g_2 \in Stab(x) \Longrightarrow (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$;
- $g \in Stab(x) \Longrightarrow x = g \cdot x$, applichiamo g^{-1}:
  $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = e \cdot x = x \Longrightarrow g^{-1} \in Stab(x)$.

□

Teorema 1.1.2. *Sia G che agisce su X ($= G \curvearrowright X$), sia $x \in X$, esiste una funzione bigettiva*

$$\begin{array}{ccc} {}^{G}/_{Stab(x)} & \longrightarrow & orb(x) \\ gStab(x) & \longmapsto & g \cdot x \end{array}$$

Dimostrazione. È ben definita: $\overline{g}Stab(x) = gStab(x) \iff \overline{g} = gh$ con $h \in Stab(x)$ e $g^{-1}\overline{g} \in Stab(x)$, $\overline{g}Stab(x) \longmapsto \overline{g} \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$;
È surgettiva: se ho $g_1 \cdot x$ prendiamo $g_1 Stab(x) \longmapsto g_1 \cdot x$;
È iniettiva: se $\begin{array}{ccc} g_1Stab(x) & \longmapsto & g_1 \cdot x \\ g_2Stab(x) & \longmapsto & g_2 \cdot x \end{array}$ con $g_1 \cdot x = g_2 \cdot x$, $\Longrightarrow g_2^{-1} \cdot (g_1 \cdot x) = g_2^{-1} \cdot (g_2 \cdot x) \Longrightarrow$ $(g_2^{-1}g_1) \cdot x = x$, cioè $g_2^{-1}g_1 \in Stab(x)$, quindi $g_1Stab(x) = g_2Stab(x)$. □

Proposizione 1.1.3. *Le orbite costituiscono una partizione di X.*

Dimostrazione. $y \in X$ appartiene almeno ad un'orbita: $orb(y)$.
Ora mostriamo che se $x \in orb(y) \Longrightarrow orb(x) = orb(y)$: $x \in orb(y)$ significa che esiste $g \in G$ tale che $g \cdot y = x$, applichiamo g^{-1}, $y = g^{-1} \cdot (g \cdot y) = g^{-1} \cdot x \Longrightarrow y \in orb(x) \Longrightarrow orb(x) = orb(y)$. □

Teorema 1.1.4. *Siano G un gruppo e X un insieme tali che $|G|, |X| < +\infty$, allora*

$$|X| = \sum_{O_i \, orbita} |O_i| = \sum_{\substack{O_i \ orbita \\ rappr.\ da\ x_i}} \left| \frac{G}{Stab(x_i)} \right| = \sum_{\substack{O_i \ orbita \\ rappr.\ da\ x_i}} \frac{|G|}{|Stab(x_i)|}$$

Esempio 1. *Caliamo il tutto nell'esempio della famosa azione di G su se stesso:*
sia $x \in G$, $orb(x) = \{g \cdot x \,|\, g \in G\} = \{gxg^{-1} \,|\, g \in G\}$ è detta anche ***classe di coniugio*** *di x.*
$\big(x \in S_7$, $x = (1,2)(3,4)(5,6,7)$, $orb(x) = ?$, $\tau x \tau^{-1} = \big(\tau(1), \tau(2)\big)\big(\tau(3), \tau(4)\big)\big(\tau(5), \tau(6), \tau(7)\big)\big)$.
E a $Stab(x)$ che nome diamo?
$Stab(x) = \{g \in G \,|\, g \cdot x = x\} = \{g \in G \,|\, gxg^{-1} = x\} = \{g \in G \,|\, gx = xg\}$, questo $Stab(x)$ si chiama ***centralizzante*** *(o* ***centralizzatore****) di x, si indica con $C(x)$ ed è il più grande sottogruppo H di G tale che $x \in Z(H)$.*

Il **Teorema** precedente diventa

$$\boxed{|G| = \sum_{\substack{\text{classi di coniugio} \\ \text{rappresentate da } g_i}} \frac{|G|}{|C(g_i)|}} \text{ FORMULA DELLE CLASSI}$$

Proposizione 1.1.5. *Se $|G| = p^n$ con p primo, allora $Z(G) \neq \{e\}$.*

Dimostrazione. $|G| = \sum \frac{|G|}{|C(g_i)|}$, perciò o $|C(g_i)| = p^n$ e quindi $g_i \in Z(G)$ o $|C(g_i)| = p^{n_i} \underset{\neq}{|} p^n$ con $n_i < n$ e quindi $g_i \notin Z(G) \Longrightarrow p^n = |Z(G)| + \sum\limits_{n_i < n} \frac{p^n}{p^{n_i}}$.
Scopriamo che $p \mid |Z(G)| \Longrightarrow Z(G) \neq \{e\}$. □

Corollario 1.1.6. *Se $|G| = p^2$, allora G è abeliano.*

Dimostrazione. Per la **Proposizione 1.1.5.**, $|Z(G)| = p^2$ oppure $|Z(G)| = p$.
Supponiamo per assurdo che sia il secondo caso: prendiamo $a \in G \setminus Z(G)$.
Consideriamo $C(a)$: di sicuro $C(a) \supseteq Z(G)$, inoltre $a \in C(a)$ ma $a \notin Z(G)$ per come l'abbiamo scelto, allora $C(a) \supsetneq Z(G)$ e, per ragioni di cardinalità, sarebbe $|C(a)| = p^2 \Longrightarrow a$ commuterebbe con tutti gli elementi, cioè $a \in Z(G)$ ↯ □

Teorema 1.1.7 (Cauchy).
Sia G un gruppo finito e sia p un primo tale che $p \mid |G|$, allora $\exists$ in G un elemento di ordine p.

Esercizio 2. *Trovare tutti i sottogruppi di ordine 12 di S_5.*

Sia H un tale sottogruppo, $H < S_5$ e $X = \{1,2,3,4,5\}$, H agisce su X: per Cauchy sappiamo che esiste in H un elemento di ordine 3, ossia un 3-ciclo (a,b,c) e $orb(a) = \{a,b,c,\overset{?}{\dots}\}$ cioè esiste un'orbita su X di cardinalità ≥ 3:

- $|X| = 5$: non va bene perché la cardinalità di un'orbita deve dividere $12 = |H|$;
- $|X| = 3+1+1$: non va bene perché H dovrebbe "vivere" in S_3 ma $|H| = 12$;
- $|X| = 3+2$: c'è un'orbita da 3 e una da 2, cioè $K_1 \times K_2$, con $K_1 \cong S_3$ e $K_2 \cong S_2 \cong \mathbb{Z}/2\mathbb{Z}$, è un sottogruppo di S_5, $|K_1 \times K_2| = 12$ perciò tutti e soli gli H che hanno orbite $3+2$ sono di questo tipo. Quanti sono tali H? Sono $\binom{5}{3} = 10$.
  Domanda aggiuntiva: sono tutti coniugati tra loro? Sì, in quanto, comunque si scelga H_1 e H_2, ad esempio $\begin{array}{ccc} H_1 & \longleftrightarrow & \overbrace{\{1,2,3\}\{4,5\}}^{\text{orbite}} \\ H_2 & \longleftrightarrow & \{1,2,5\}\{3,4\} \end{array}$, esiste un σ, per l'esempio $\sigma : \begin{cases} 1 \longmapsto 1 \\ 2 \longmapsto 2 \\ 3 \longmapsto 5 \\ 4 \longmapsto 3 \\ 5 \longmapsto 4 \end{cases}$,
  tale che $\sigma^{-1} H_2 \sigma = H_1$.

Definizione 1.1.3. *Dato G gruppo e $H < G$, il* ***normalizzatore*** *di H in G, indicato con $N(H)$ è il più grande (per inclusione) sottogruppo di G che contiene H e in cui H è sottogruppo normale.*

Osservazione 1. *H contiene H.*

Esempio 2. *Sia H un sottogruppo di ordine 12 in S_5 di quelli descritti sopra, cioè*
$H = K_1 \times K_2 \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$, chi è $N(H)$?

Sia $X = \{\text{tutti i coniugati di } H\}$, S_5 agisce per coniugio su X, $\sigma \in S_5$: $\sigma \cdot H = \sigma H \sigma^{-1}$. Abbiamo visto che c'è un'unica orbita, in altre parole $X = orb(H)$. Allora ricordiamo che $|orb(H)| = \frac{|S_5|}{|Stab(H)|}$, $Stab(H) = N(H) \Longrightarrow |N(H)| = \frac{|S_5|}{|orb(H)|} = \frac{5!}{10} = 12 \Longrightarrow N(H) = H$.

- $|X| = 4+1$: significa che un numero (ad esempio il 5) è lasciato fisso da H, allora H "vive" in S_4 (vediamo S_4 in S_5 come il sottogruppo che permuta $\{1,2,3,4\}$).
  Risulta che $H = A_4$. Ingredienti:
  1. cercare i sottogruppi di ordine 6 in S_4 e scoprire che sono copie di S_3 e dunque contengono elementi pari e dispari;
  2. Ora se H è un sottogruppo di ordine 12 in S_4, vale che $H \cap A_4 = A_4$ oppure $H \cap A_4$ è un sottogruppo di ordine 6 di A_4 e di S_4 per il seguente **Lemma 1.1.8.** ma questo è assurdo per il punto 1.

Lemma 1.1.8. *Sia $K < S_n$, $K < A_n$ oppure K ha metà elementi pari e metà dispari.*

Dimostrazione. Se $K \nsubseteq A_n$ vuol dire che $\exists \tau \in K$ dispari. La seguente mappa

$$\begin{array}{ccc} K \cap A_n & \longrightarrow & K \cap (S_n \setminus A_n) \\ \underset{\text{pari}}{g} \in K & \longmapsto & \underset{\text{dispari}}{\tau g} \in K \end{array} \quad \text{possiede l'inversa} \quad \begin{array}{ccc} K \cap A_n & \longleftarrow & K \cap (S_n \setminus A_n) \\ \tau^{-1}\gamma & \longleftarrow\!\shortmid & \gamma \end{array}$$

Nota: τ^{-1} è dispari perché ha la stessa forma ciclica di τ. □

Conclusione: i sottogruppi di S_5 di cardinalità 12 con orbite 4+1 sono isomorfi ad A_4, più precisamente sono di questo tipo: dati a, b, c, d tra $\{1, 2, 3, 4, 5\}$ distinti, il gruppo in questione è quello dato dalle permutazioni pari di a, b, c, d.
Sono 5 e tutti coniugati tra loro: sia H uno di essi, ad esempio $H = A_4$ che permuta $\{1, 2, 3, 4\}$, come prima $|N(H)| = \frac{|S_5|}{|orb(H)|} = \frac{5!}{5} = 4! = 24$ e $|H| = 12$, dunque $N(H) = S_4$.

Esercizio 3. *Quali sono i sottogruppi di S_5 di cardinalità 24?*

Teorema 1.1.9 (Cauchy).
Sia p primo, $p \mid |G|$, allora G ha un elemento di ordine p. Più precisamente le soluzioni di $x^p = e$ in G sono in numero di kp con $k \geq 1$.

Dimostrazione. Sia $S = \{(a_1, ..., a_p) | a_i \in G \text{ e } a_1 \cdot ... \cdot a_p = e\}$, $|S| = |G|^{p-1}$. $\mathbb{Z}/p\mathbb{Z}$ agisce su S mediante questa regola:

$$[i] \cdot (a_1, ...a_p) = (a_{i+1}, ..., a_p, a_1, ..., a_i) \overset{?}{\in} S$$

Sì, appartiene ad S: presa l'equazione $a_1 \cdot ... \cdot a_p = e$, moltiplico da entrambi i lati a sinistra per $a_i^{-1} \cdot ... \cdot a_1^{-1}$ e a destra per $a_1 \cdot ... \cdot a_i$.

Esercizio 4. *Verificare che sia un'azione.*

A noi interessano le p-uple $(a, a, ..., a) \in S$, cioè $a^p = e$. Guardiamo le equazioni delle orbite:

$$|S| = |U| + \sum_{\substack{\text{altre} \\ \text{orbite}}} p \text{ dove } U = \{(a, a, ..., a) \mid a^p = e\}$$

$$|S| = |G|^{p-1} = |U| + pn \text{ per un certo } n \geq 0 \text{ intero.}$$

Quindi $p \mid |U|$, $|U| \geq 1$ perché c'è almeno $(e, e, ..., e)$, perciò $|U| = pk$ con $k \geq 1$. $\square$

1.2 Il Teorema di Cayley

Teorema 1.2.1. *Sia G un gruppo che agisce su X, dato $g \in G$ chiamo* $\begin{array}{rccc} \phi_g : & X & \longrightarrow & X \\ & x & \longmapsto & g \cdot x \end{array}$ *vale che:*

1) ϕ_g *è bigettiva;*

2) $\begin{array}{rccc} \Gamma : & G & \longrightarrow & Big(X) \\ & g & \longmapsto & \phi_g \end{array}$ *è un omomorfismo di gruppi.*

Dimostrazione. 1) (sulle dispense) ϕ_g è bigettiva perché esiste $\phi_{g^{-1}}$;
2) $\Gamma(g_1 g_2)(x) \overset{\text{def.}}{=} \phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x \overset{\text{def.}}{=} g_1 \cdot (g_2 \cdot x) = \phi_{g_1}(g_2 \cdot x) = \phi_{g_1} \circ \phi_{g_2}(x) = \Gamma(g_1) \circ \Gamma(g_2)(x)$. □

Teorema 1.2.2 (Cayley).
Sia G un gruppo finito con n elementi, allora G è isomorfo ad un sottogruppo di S_n.

Dimostrazione. G agisce su G per moltiplicazione a sinistra ($G \curvearrowright G$). Per il **Teorema** precedente: $\begin{array}{rccc} \Gamma : & G & \longrightarrow & Big(G) \cong S_n \\ & g_1 & \longmapsto & \phi_{g_1} \\ & g_2 & \longmapsto & \phi_{g_2} \end{array}$, se supponiamo $\phi_{g_1} = \phi_{g_2}$, applicandola ad e, $\phi_{g_1}(e) = \phi_{g_2}(e) \Longrightarrow g_1 e = g_2 e \Longrightarrow g_1 = g_2 \Longrightarrow \Gamma$ è iniettiva. □

Se $G = S_n$, il **Teorema 1.2.2.** dice che $S_n \hookrightarrow Big(S_n) \cong S_{n!}$.

Teorema 1.2.3. *Sia G un gruppo finito e $H < G$ tale che $|{}^{G}/_{H}| = p$ primo, se p è il più piccolo primo che divide $|G|$, allora $H \lhd G$.*

Dimostrazione. Usiamo la famosa azione sui laterali. $X = {}^{G}/_{H}$, G agisce così:
sia $g \in G$ e $xH \in {}^{G}/_{H}$, $g \cdot xH = gxH$.
Per il **Teorema 1.2.1.**, si ha un omomorfismo $\Gamma : G \longrightarrow Big({}^{G}/_{H}) \cong S_{|G/H|}$.
<u>Strategia</u>: mostreremo che $H = Ker\,\Gamma$.

<u>Inclusione facile</u>: $Ker\,\Gamma \subseteq H$ perché se $k \in Ker\,\Gamma$, $\begin{array}{ccc} G & \longrightarrow & Big({}^{G}/_{H}) \\ k & \longmapsto & \phi_k : \begin{array}{ccc} {}^{G}/_{H} & \longmapsto & {}^{G}/_{H} \\ xH & \longmapsto & kxH \end{array} \end{array}$, $k \in Ker\,\Gamma \Longrightarrow \phi_k = Id$, in particolare, $\phi_k(H) = H$ ma $\phi_k(H) = kH \Longrightarrow kH = H \Longleftrightarrow k \in H$.
⚠<u>Attenzione</u>!⚠ Tutto ciò è vero ogni volta che c'è in ballo l'azione sui laterali.

Esercizio 5. *Guardare l'altra inclusione.*

□

Esempi di azioni: (1) G agisce su se stesso per coniugio;
(2) $H < G$, G agisce sui laterali;
(1bis) $G = S_n$, siano $\sigma, \tau \in S_n$, allora $\tau\sigma\tau^{-1}$ e σ hanno la stessa decomposizione in cicli disgiunti. $\sigma_1, \sigma_2 \in S_n$ con la stessa decomposizione in cicli disgiunti $\Longrightarrow \sigma_1$ e σ_2 sono coniugate, cioè $\exists \tau$ tale che $\tau\sigma_1\tau^{-1} = \sigma_2$.
Idea: date due permutazioni $\sigma_1 = (1,2,3)(4,5)(6,7)$ e $\sigma_2 = (8,1,2)(3,7)(4,5)$, cerchiamo esplicitamente una permutazione τ tale che $\tau\sigma_1\tau^{-1} = \sigma_2$:

$$\tau\sigma_1\tau^{-1} = \big(\underset{8}{\underset{\shortparallel}{\tau(1)}}, \underset{1}{\underset{\shortparallel}{\tau(2)}}, \underset{2}{\underset{\shortparallel}{\tau(3)}}\big)\big(\underset{3}{\underset{\shortparallel}{\tau(4)}}, \underset{7}{\underset{\shortparallel}{\tau(5)}}\big)\big(\underset{4}{\underset{\shortparallel}{\tau(6)}}, \underset{5}{\underset{\shortparallel}{\tau(7)}}\big)$$

τ ovviamente non è unica.

Esercizio 6. $(1,2,3) \in S_n$*,* $n \geq 3$*, chi è il centralizzante di* $(1,2,3)$*?*

$|Stab(1,2,3)| = \frac{|S_n|}{|orb(1,2,3)|}$, $|orb(1,2,3)| = |\{\text{3-cicli di } S_n\}| = \binom{n}{3} \cdot 2 = \frac{n(n-1)(n-2)}{3}$, perciò $|Stab(1,2,3)| = 3 \cdot (n-3)!$.
$|\text{elementi di } S_n \text{ che non toccano 1,2,3}| = (n-3)!$, $(1,2,3), (1,3,2) \in C\big((1,2,3)\big)$.

- ho i σ che non toccano 1,2,3;
- ho i $(1,2,3)\sigma$ con σ che non tocca 1,2,3;
- ho i $(1,3,2)\sigma$ con σ che non tocca 1,2,3.

Esercizio 7. *Descrivere il centralizzatore di* $(1,2)(3,4)$ *in* S_5*.*

Esercizio 8. *Descrivere la classe di coniugio di* $(1,2,3)$ *in* A_4*.*

$\{\sigma(1,2,3)\sigma^{-1}, \sigma \in A_4\} \subseteq \{\sigma(1,2,3)\sigma^{-1}, \sigma \in S_4\}$, $|C_{S_4}(1,2,3)| = 3$,
$C_{S_4}(1,2,3) = \{e, (1,2,3), (1,3,2)\} \subset A_4$, perciò $\big|orb_{A_4}\big((1,2,3)\big)\big| = \frac{|A_4|}{3} = 4$.

Esercizio 9. *Trovare questi 4 elementi.*

Esercizio 10. *In generale: per quali* $\sigma \in A_n$ $orb_{A_n}(\sigma) = orb_{S_n}(\sigma)$*?*

- Se σ non tocca due elementi i, j, allora (i,j) commuta con σ;
- se uno dei cicli (detto τ) nella decomposizione di σ è dispari, allora τ commuta con σ.

Definizione 1.2.1. *Un gruppo* G *si dice* ***semplice*** *se gli unici suoi sottogruppi normali sono* $\{e\}$ *e* G*.*

- $\mathbb{Z}/n\mathbb{Z}$ è semplice se e solo se n è primo;
- Gruppi abeliani di cardinalità non prima non sono semplici;
- S_n, per $n \geq 3$, non è semplice;
- A_4 non è semplice.

Teorema 1.2.4. A_n *è semplice* $\forall n \geq 5$*.*

1.3 I teoremi di Sylow

Teorema 1.3.1 (**Sylow I**).
Siano G un gruppo finito e p un primo tale che $p \mid |G|$, diciamo che $p^b \mid |G|$ e $p^{b+1} \nmid |G|$, con $b \geq 1$, allora $\forall a = 0, ..., b$ $\exists$ in G un sottogruppo di cardinalità p^a.

Dimostrazione. Il caso $a = 0$ è banale;
Sia dunque $1 \leq a \leq b$, $|G| = p^b m$, con m primo con p e $X = \{L \subseteq G \,\big|\, |L| = p^a\}$,

$$|X| = \binom{p^b m}{p^a} = \frac{(p^b m)!}{(p^a)!(p^b m - p^a)!} = \frac{(p^b m) \cdot ... \cdot (p^b m - p^a + 1)}{p^a \cdot ... \cdot 2 \cdot 1}$$

$\frac{p^b m}{p^a} = p^{b-a} m$, si osserva poi che $p^k \mid p^b m - i \iff p^k \mid p^a - i$:
se $p^k \mid p^a - i$ innanzitutto $k < a$, $p^k s = p^a - i \implies p^k \mid i \implies p^k \mid p^a m - i$.
Risulta quindi che la massima potenza di p che divide $|X|$ è p^{b-a}.
Come facciamo agire G su X? Per moltiplicazione a sinistra: se $L \in X$ e $g \in G$, $g \cdot L = gL$ che ha ancora p^a elementi e dunque appartiene a $X \implies X$ viene partizionato in orbite e noi cerchiamo i sottogruppi che sono gli stabilizzatori degli elementi. Chiamiamo $\mathscr{L}_1, \mathscr{L}_2, ..., \mathscr{L}_n$ le orbite di questa azione: $\mathscr{L}_1 = orb(L_1)$, $\mathscr{L}_2 = orb(L_2)$,...,$\mathscr{L}_k = orb(L_k)$ e $|X| = \sum_{i=1}^{k} |\mathscr{L}_i| = \sum_{i=1}^{k} |orb(L_i)|$.
Non è possibile che p^{b-a+1} divida tutti gli $|orb(L_i)|$.
Sia j tale che $p^{b-a+1} \nmid |orb(L_j)|$: $|orb(L_j)| = \frac{|G|}{|Stab(L_j)|} = \frac{p^b m}{|Stab(L_j)|}$, $|Stab(L_j)| = \dfrac{p^b m}{\underbrace{|orb(L_j)|}_{\substack{\text{la massima potenza di } p \\ \text{che la divide è } \leq p^{b-a}}}}$.

Di sicuro $p^a \mid |Stab(L_j)|$. Ora mostriamo che $p^a = |Stab(L_j)|$: fissato $l \in L_j$, consideriamo la funzione $\begin{array}{ccc} Stab(L_j) & \longrightarrow & L_j \\ \gamma & \longmapsto & \gamma l \end{array}$ $\big(\gamma l \in L_j$ perché $\gamma \in Stab(L_j)\big)$.
La funzione è iniettiva: $\gamma_1 l = \gamma_2 l \iff \gamma_1 = \gamma_2$.
Quindi, in conclusione, $|Stab(L_j)| \leq |L_j| = p^a \implies p^a \mid |Stab(L_j)| \leq p^a \implies |Stab(L_j)| = p^a$. $\square$

Definizione 1.3.1. *Nelle ipotesi sopra, un sottogruppo $K < G$ tale che $|K| = p^b$ si dice un* ***p-Sylow***.

Esempio 3. *(dal passato): Trovare qualche 2-Sylow in S_4.*

$|S_4| = 24$, $2^3 \mid 24$ ma $2^4 \nmid 24$. Cerchiamo dunque sottogruppi di ordine 8: D_4, il gruppo delle simmetrie del quadrato $\begin{array}{ccc} 4 & \text{———} & 1 \\ | & & | \\ 3 & \text{———} & 2 \end{array}$, ha 8 elementi e si identifica con un sottogruppo di S_4:

$$D_4 = \{e, (1,3), (2,4), (1,2)(3,4), (1,4)(2,3), (1,3)(2,4), (1,2,3,4), (4,3,2,1)\}$$

$K_1 = D_4$ è dunque un 2-Sylow di S_4. Numerando diversamente i vertici del quadrato, si ottengono in tutto 3 2-Sylow K_1, K_2, K_3, tutti isomorfi a D_4.

Teorema 1.3.2 (**Sylow II**).
Sia G come sopra, sia H un p-Sylow e $K < G$, con $|K| = p^a$, allora:

(1) $\exists g \in G$ tale che $K \subseteq gHg^{-1}$;

(2) se anche K è p-Sylow, allora $\exists g \in G$ tale che $K = gHg^{-1}$.

Dimostrazione. *(1)* Faremo agire K sull'insieme dei laterali $X = {}^{G}/_{H}$, se $k \in K$ e $gH \in X$,

$$k \cdot gH = kgH$$

X viene partizionato in orbite: siano $g_1H, g_2H, ..., g_rH$ i rappresentanti di tali orbite.
L'equazione delle orbite dice

$$\left|{}^{G}/_{H}\right| = \sum_{i=1}^{r} |orb(g_iH)| = \sum_{i=1}^{r} \frac{|K|}{|Stab(g_iH)|} = \sum_{i=1}^{r} p^{a_i}$$

Osserviamo che $|{}^{G}/_{H}| = m$ è primo con p perché H è un p-Sylow, allora almeno uno degli a_i deve essere $= 0$. Supponiamo dunque che $a_j = 0$ per un certo j, allora $orb(g_jH) = \{g_jH\}$.
Vediamo che $K < g_jHg_j^{-1}$: infatti $\forall k \in K$ e $\forall h \in H$ $\exists h' \in H$ tale che $kg_jh = g_jh'$ (perché $kg_jH = g_jH$). Dunque $k = g_jh'h^{-1}g_j^{-1}$ e, dato che k era un qualunque elemento di K, abbiamo dimostrato che $K < g_jHg_j^{-1}$.
(2) segue immediatamente da *(1)*. □

Definizione 1.3.2. *Dato $H < G$, il* ***normalizzatore*** *$N(H)$ di H in G è*

$$N(H) = \{g \in G \,|\, gHg^{-1} = H\}$$

Osservazione 2.

- *$N(H)$ è sottogruppo di G;*
- *$N(H)$ è il più grande (per inclusione) sottogruppo di G in cui H è normale.*

Corollario 1.3.3. *Sia G come sopra, sia n_p il numero dei p-Sylow di G, allora $n_p = \frac{|G|}{|N(H)|}$, dove H è un qualunque p-Sylow (dunque, in particolare, $n_p \mid |G|$).*

Dimostrazione. Preso H p-Sylow, $X = \{p\text{-Sylow di } G\}$. G agisce su X per coniugio e, per **Sylow II**, c'è un'unica orbita. $|orb(H)| = \frac{|G|}{|Stab(H)|}$ ma $Stab(H) = N(H)$ per definizione, visto che l'azione in questione è il coniugio. $n_p = |X| = |orb(H)| = \frac{|G|}{|N(H)|}$. □

Torniamo all'**Esempio 3** dei 2-Sylow in S_4: dunque K_1, K_2, K_3 sono coniugati tra loro e si potrebbe già dimostrare che sono tutti e soli i 2-Sylow.

Teorema 1.3.4 (**Sylow III**).
Sia G come sopra, il numero n_p dei p-Sylow soddisfa $n_p \equiv 1 \,(mod\, p)$.

Dimostrazione. (Studiarla sulle dispense). □

Ancora sui 2-Sylow di S_4: cosa sappiamo di n_2? Sappiamo che $n_2 \mid 24$ per il **Corollario 1.3.3.** e che $n_2 \equiv 1\,(2)$ per **Sylow III**. Restano quindi solo due casi:

- $n_2 = 1$: NO, perché conosco K_1, K_2, K_3;
- $n_2 = 3$: SÌ, per esclusione e perché conosco già K_1, K_2, K_3 appunto.

Rileggiamo il "vecchio" omomorfismo da S_4 a S_3: facciamo agire S_4 per coniugio sui 2-Sylow.
Abbiamo un omomorfismo $\Gamma : S_4 \longrightarrow S_3$.
Per vedere che è surgettivo ci aiuta **Sylow II**? Va fatto il conto dell'anno scorso.

$$Ker\,\Gamma = Klein$$

Teorema 1.3.5. *A_n è semplice $\forall n \geq 5$.*

Proposizione 1.3.6. *I 3-cicli generano A_n.*

Dimostrazione. (**Proposizione 1.3.6.**) Sia $H < A_n$ tale che H contiene tutti i 3-cicli, allora H contiene tutte le permutazioni del tipo $(a,b)(a,c) = (a,c,b) \in H$ ma anche le permutazioni del tipo $(a,b)(c,d) = (a,b)(b,c)(b,c)(c,d) = (a,b,c)(b,c,d) \in H \Longrightarrow H = A_n$. □

Dimostrazione. (**Teorema 1.3.5.**) Sia $H \lhd A_n$, $H \neq \{e\} \Longrightarrow$ vorremmo $H = A_n$, cioè vorremmo che H contenesse tutti i 3-cicli, perciò vorremmo che H contenesse un 3-ciclo.

Che succede in A_5? Prendiamo $\sigma \in H$, $\sigma \neq e$:
$$\sigma = \begin{cases} \nearrow (1,2,3) & \text{(ok)} \\ \longrightarrow (1,2)(3,4) & \\ \searrow (1,2,3,4,5) & \text{(per esercizio)} \end{cases}$$

Cerchiamo un τ pari tale che $\tau(1,2)(3,4)\tau^{-1} = \big(\tau(1),\tau(2)\big)\big(\tau(3),\tau(4)\big)$ sia un 3-ciclo ma è impossibile, quindi speriamo che siano 2 trasposizioni del tipo $(1,2)(3,4) \cdot (3,4)(1,5) = (1,2)(1,5)$ che è un 3-ciclo, perciò avremmo $\tau = (1,3)(2,4,5)$ ma è dispari... Proviamo con $\tau = (2,3,1,4,5)$ che effettivamente funziona: $\tau(1,2)(3,4)\tau^{-1} = (4,3)(1,5) \in H$.
Quindi $(1,2)(3,4) \cdot (4,3)(1,5) \in H \Longrightarrow A_5$ è semplice.
Vogliamo dimostrare il **Teorema 1.3.5.** per induzione su $n \geq 5$:

P.B.: $n = 5$, appena svolto;

Lemma 1.3.7. *$n \geq 5$, $\sigma \in A_n$, con $\sigma \neq e$, allora σ ha un coniugato $\sigma' \neq \sigma$ tale che $\sigma(i) = \sigma'(i)$ per qualche $i = 1, ..., n$.*

Dimostrazione. (**Lemma 1.3.7.**) Sia l la lunghezza massima dei cicli che compaiono in una decomposizione di σ in cicli disgiunti $\sigma = (1,2,...,l)\tau$.
Se $l \geq 3$, coniughiamo σ per $(3,4,5)$ e troviamo $\sigma' = (1,2,4,...)\tau'$ e $\sigma(1) = \sigma'(1)$.
Se $l = 2$? (Per esercizio) □

P.I.: A_n agisce su $\{1,2,...,n\}$, $H_i = Stab(i) < A_n$, $H_i \cong A_{n-1} \Longrightarrow H_i$ è semplice per ipotesi induttiva.
Prendiamo $N \lhd A_n$, $N \neq \{e\}$. Sia $\sigma \in N$, $\sigma \neq e \Longrightarrow \exists \sigma' \neq \sigma$ tale che σ' è coniugato a σ, cioè $\sigma'(i) = \sigma(i)$ per qualche $i \Longrightarrow \sigma' \in N$ perché N è normale $\rightsquigarrow \sigma' \cdot \sigma^{-1} \in N \cap H_i$.
Quindi $N \cap H_i < H_i$ è un sottogruppo non banale. Inoltre $N \cap H_i \lhd H_i$ (perché $N \lhd A_n$) $\Longrightarrow N \cap H_i = H_i$ perché H_i è semplice, cioè $H_i \subseteq N \Longrightarrow N$ contiene un 3-ciclo.

□

Esercizio 11. *Sia G un gruppo con $|G| = 148$, allora G non è semplice.*

Dimostrazione. $148 = 4 \cdot 37$, $n_{37} = \#$ sottogruppi di 37 elementi:
$n_{37} \mid 148$ e $n_{37} \equiv 1\,(37) \Longrightarrow n_{37} = 1 \Longrightarrow$ l'unico sottogruppo di 37 elementi è normale. □

Esercizio 12. *Sia G un gruppo con $|G| = 72$, allora G non è semplice.*

$72 = 2^3 \cdot 3^2$, $n_3 = \#$ sottogruppi di 9 elementi: $n_3 \mid 72$ e $n_3 \equiv 1\,(3) \Longrightarrow$

$$n_3 = \begin{cases} \nearrow 1 & \text{ok, come prima} \\ \searrow 4 & \end{cases} \qquad n_3 = \frac{|G|}{|N(P)|} \text{ (con } P \text{ un 3-Sylow).}$$

Idea: se $n_3 = 4$, G agisce sull'insieme dei 3-Sylow $\rightsquigarrow \varphi : G \longrightarrow S_4$ omomorfismo:
$Ker\,\varphi \lhd G$ è banale?

Esercizio 13. *Sia G un gruppo con $|G| = p^2 q$, con p, q primi distinti, allora G non è semplice.*

1.4 ~~Quattro~~ Cinque passi in S_5

① Cerchiamo sottogruppi di ordine 30. Sia H un tale sottogruppo.
S_5 agisce su ${}^{S_5}\!/_{H}$ con l'azione sui laterali: $\sigma \cdot \tau H = \sigma\tau H$.
Dunque abbiamo un omomorfismo $\Gamma : S_5 \longrightarrow Big({}^{S_5}\!/_{H}) = S_4 \ (4 = \frac{120}{30})$.

- $Ker\,\Gamma \neq \{e\}$ per ragioni di cardinalità;
- Da una proprietà generale di questa azione, sappiamo che $Ker\,\Gamma \subseteq H$;
- $Ker\,\Gamma \lhd S_5$.

$Ker\,\Gamma =$
- $\longrightarrow \{e\}$ NO, appena detto;
- $\longrightarrow A_5$ NO, $|A_5| \nmid |H|$;
- $\longrightarrow S_5$ NO, se $H < G$ proprio, allora $Ker\,\Gamma \neq G$.

Spieghiamo come mai c'erano solo tre alternative:

$K \lhd S_5$
- $\longrightarrow K < A_5$
  - $\longrightarrow K = \{e\}$
  - $\longrightarrow K = A_5$
- $\longrightarrow |K \cap A_5| = |K \cap (S_5 \setminus A_5)|$ In questo caso $K \cap A_5 \lhd A_5$ e dunque

$K \cap A_5 =$
- $\longrightarrow \{e\}$ K avrebbe e ed un elemento dispari di ordine $2 \Longrightarrow K \ntriangleleft S_5$;
- $\longrightarrow A_5$ Per esclusione, SÌ, dunque $K = S_5$.

Abbiamo in pratica dimostrato la

Proposizione 1.4.1. *Se $n \geq 5$, gli unici sottogruppi normali di S_n sono $\{e\}$, A_n e S_n.*

In complesso abbiamo ottenuto un assurdo: non esistono sottogruppi di ordine 30. Lo stesso ragionamento ci porta ad escludere che esistano sottogruppi di ordine 40.
In generale, analogamente, si dimostra la

Proposizione 1.4.2. *Se $n \geq 5$, in S_n non esistono sottogruppi di indice k, con $2 < k < n$.*

② Cerchiamo sottogruppi di ordine 15. Sia H un tale sottogruppo.
Ogni $h \in H$ è pari, per Lagrange, $h^{15} = e$. Applicando l'omomorfismo $sgn : S_5 \longrightarrow \{1, -1\}$, $sgn(h)^{15} = 1 \Longrightarrow sgn(h) = 1$.
Dunque $H < A_5$ e consideriamo l'azione di A_5 su ${}^{A_5}\!/_{H}$.
Abbiamo un omomorfismo $\Gamma : A_5 \longrightarrow Big({}^{A_5}\!/_{H}) = S_4 \ (4 = \frac{60}{15})$. Per la semplicità di A_5,

$Ker\,\Gamma =$
- $\longrightarrow \{e\}$ NO, perché Γ sarebbe iniettiva mentre $|A_5| = 60 > |S_4| = 24$;
- $\longrightarrow A_5$ NO, per i soliti motivi generali.

③ Cerchiamo sottogruppi di ordine 5. Sono quelli generati dai 5-cicli.
I 5-cicli sono 24 e in ogni sottogruppo di ordine 5 ce ne sono 4 del tipo $\sigma = (1, 2, 3, 4, 5), \sigma^2, \sigma^3, \sigma^4$.
Allora ci sono 6 sottogruppi di ordine 5:
presi due tali sottogruppi H_1 e H_2 $\exists g$ tale che $gH_1g^{-1} = H_2$, ad esempio

$$\left.\begin{array}{l} H_1 = \big((1,2,3,4,5)\big) \\ H_2 = \big((1,3,4,5,2)\big) \end{array}\right\} \; g(1) = 1,\; g(2) = 3,\; g(3) = 4,\; g(4) = 5 \text{ e } g(5) = 2 \Longrightarrow g^{-1}H_2g = H_1$$

Oppure avremmo potuto notare che i sottogruppi di ordine 5 sono i 5-Sylow e dunque tutti coniugati per **Sylow II**.
Se S_5 agisce sui sottogruppi di ordine 5 forma un'unica orbita O, $6 = |O| = \frac{|S_5|}{|N(H)|}$, dove H è un qualunque sottogruppo di ordine 5. $|N(H)| = \frac{120}{6} = 20$.
<u>Cacciavite</u>: supponiamo $\sigma = (1, 2, 3, 4, 5)$ e che $H = (\sigma)$, noto che $(1, 2, 4, 3)\sigma(3, 4, 2, 1) = \sigma^2$ e che $(1, 2, 4, 3)\sigma^2(3, 4, 2, 1) = (1, 2, 4, 3)\sigma(3, 4, 2, 1)(1, 2, 4, 3)\sigma(3, 4, 2, 1) = \sigma^2\sigma^2$.
Dunque $(1, 2, 4, 3) \in N(H)$.
Perciò $N(H) \overset{?}{=} \big((1, 2, 3, 4, 5), (1, 2, 4, 3)\big) = L$.
$L < N(H)$, L ha ordine multiplo di 20 perché contiene un elemento di ordine 4 e un elemento di ordine 5, ma $|N(H)| = 20 \Longrightarrow L = N(H)$.

④ Cerchiamo sottogruppi di ordine 10. Sia H un tale sottogruppo.
Per Cauchy, H contiene un elemento σ di ordine 5, ossia un 5-ciclo, e un elemento g di ordine 2. Supponiamo che $g = (a, b)$: di sicuro una potenza di σ è del tipo (a, b, c, d, e) e $(a, b, c, d, e)(a, b) = (a, c, d, e)$ $\lightning$ perché ha ordine 4 e $4 \nmid 10$.
Quindi $g = (\, , \,)(\, , \,)$, a meno di rinumerare, prendiamo $\sigma = (1, 2, 3, 4, 5)$.
A meno di coniugare per un'opportuna potenza di σ, possiamo supporre che $g = (\, , \,)(\, , \,)(5)$.
Abbiamo 3 casi possibili e verifichiamo che:

- $(1, 2, 3, 4, 5)(1, 2)(3, 4) = (1, 3, 5)$ $\lightning$ perché ha ordine 3 e $3 \nmid 10$;
- $(1, 2, 3, 4, 5)(1, 3)(2, 4) = (1, 4, 3, 2, 5)$ notiamo che $(1, 4, 3, 2, 5) \notin \big((1, 2, 3, 4, 5)\big) \Longrightarrow \lightning$ perché in H c'è un solo 5-Sylow;
- $(1, 2, 3, 4, 5)(1, 4)(2, 3) = (1, 5)(4, 2)$ funziona!

Si tratta di una presentazione di $D_5 < S_5$. I sottogruppi di ordine 10 sono tutti e soli quelli prodotti così, ossia generati da σ e g come sopra. Il tutto dipende solo dalla scelta del sottogruppo di ordine 5 che nel nostro esempio è $\big((1, 2, 3, 4, 5)\big)$. Dunque c'è una bigezione tra

$$\{\text{Sottogruppi di ordine 5}\} \longleftrightarrow \{\text{Sottogruppi di ordine 10}\}$$

Dunque ci sono 6 sottogruppi di ordine 10. Sia H un tale sottogruppo, allora $N(H) = 20$ perché sono un'unica orbita (stesso argomento). Sia H di ordine 10 e σ un 5-ciclo in H, $(\sigma) \subseteq H$.
Sia $g \in N(H)$, diciamo che $g \in N\big((\sigma)\big)$, $gHg^{-1} = H$ e $\underbrace{g(\sigma)g^{-1}}_{\substack{\text{sottogruppo} \\ \text{di ordine 5}}} \subseteq H$, dunque $g(\sigma)g^{-1} = (\sigma)$.

Fatto 1.4.3 (generale). *Sia $K < H < G$ e sia K l'unico sottogruppo di ordine m in H, allora $N(H) \subseteq N(K)$.*

Infatti, se $gHg^{-1} = H$, $gKg^{-1} \subseteq H \Longrightarrow gKg^{-1} = K$.
Nel nostro caso, $N(H) \subseteq N\big((\sigma)\big)$, studiati al passo precedente, è in realtà $N(H) = N\big((\sigma)\big)$.

⑤ Cerchiamo sottogruppi di ordine 20. Sia H un tale sottogruppo.
Se fosse $H < A_5$, avrei l'omomorfismo $\Gamma : A_5 \longrightarrow Big(A_5/H) = S_3$ $(3 = \frac{60}{20})$.

$$\begin{tikzcd} & \{e\} \qquad \text{NO} \\ Ker\,\Gamma = \arrow[ur] \arrow[dr] & \\ & A_5 \qquad \text{NO} \end{tikzcd}$$

Allora deve valere che $|H \cap A_5| = 10$.

Mostriamo che $H = N(\overbrace{H \cap A_5}^{\text{ordine } 10})$, questo ci permetterebbe di dire che H è del tipo visto ai passi 3 e 4 ossia $H = \big((1,2,3,4,5),(1,2,4,3)\big)$.
Dato che $H \cap A_5 \lhd H$ vale $N(H \cap A_5) \supseteq H$ e, per motivi di ordine, vale $N(H \cap A_5) = H$.

Studiamo da vicino $H = \big((1,2,3,4,5),(1,2,4,3)\big)$. Quanti sono i 5-Sylow?
$n_5 \mid 20$ e $n_5 \equiv 1\,(5) \Longrightarrow n_5 = 1$.
Dunque $L = \big((1,2,3,4,5)\big) \cong \mathbb{Z}/5\mathbb{Z} \lhd H$, lo sapevamo dal passo 3.
Poi c'è il sottogruppo $K = \big((1,2,4,3)\big) \cong \mathbb{Z}/4\mathbb{Z}$:
$L \cap K = \{e\}$, $LK = \{lk \big| l \in L,\, k \in K\}$, $|LK| = 20 \Longrightarrow LK = H$, $L \cong \mathbb{Z}/5\mathbb{Z} < H$ e $K \cong \mathbb{Z}/4\mathbb{Z} < H$
ma quindi $H \overset{?}{\cong} L \times K \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/20\mathbb{Z}$ <u>NO</u>.
Allora come funziona la moltiplicazione in LK? $l_1k_1, l_2k_2 \in LK$, so che $L \lhd H \Longrightarrow$

$$l_1k_1l_2k_2 = l_1\,\overbrace{k_1l_2k_1^{-1}}^{\in L}\,k_1k_2 = l_1(k_1l_2k_1^{-1})k_1k_2$$

È la situazione tipo dei prodotti semidiretti.

Sia H di ordine 20, chi è $N(H)$? I sottogruppi di ordine 20 sono tutti coniugati e sono 6, allora $|N(H)| = \frac{120}{6} = 20 \Longrightarrow N(H) = H$.
Al punto 3 c'era l'azione di S_5 sui sottogruppi di ordine 5 e avevamo visto che c'è un'unica orbita.
I sottogruppi di ordine 20 sono i normalizzatori degli elementi dell'orbita, ossia gli $Stab(x)$ con x nell'orbita. Vale in generale la seguente

Proposizione 1.4.4. *Sia G un gruppo che agisce su un insieme X. Siano $x, y \in O$ orbita (insomma x, y appartengono alla stessa orbita), allora $Stab(x)$ e $Stab(y)$ sono coniugati.*

Dimostrazione. Se $g \cdot x = y$, allora vale $g^{-1}Stab(y)g = Stab(x)$.
Analogamente $gStab(x)g^{-1} = Stab(y)$. $\square$

Esempio 4. *$GL_n(\mathbb{K})$, con $\mathbb{K}$ campo, è un gruppo (potenzialmente infinito se $|\mathbb{K}| = +\infty$).*
$GL_n(\mathbb{F}_p)$, $\mathbb{F}_p = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$, è un gruppo finito.

① Quanti elementi ha $GL_n(\mathbb{F}_p)$?
Date $\varphi : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n$ lineari e invertibili $\Longrightarrow |GL_n(\mathbb{F}_p)| = \#\varphi = (p^n-1)(p^n-p)...(p^n-p^{n-1})$.

② Studiare i p-Sylow in $GL_n(\mathbb{F}_p)$ (esercizio).

Esercizio 14. *Sia G gruppo con $|G| = 40 = 2^3 \cdot 5$, dimostrare che G non è semplice.*

Dimostrazione. $n_5 \mid 40$ e $n_5 \equiv 1\,(5) \Longrightarrow n_5 = 1 \Longrightarrow$ c'è un unico 5-Sylow che quindi è normale $\Longrightarrow G$ non è semplice. □

Esercizio 15. *Sia G gruppo semplice con $|G| = n$, dove n non è primo, e sia p un primo che divide n, allora $n \leq n_p!$.*

Dimostrazione. G agisce sull'insieme dei suoi p-Sylow per coniugio. Questa azione corrisponde ad un omomorfismo di gruppi $\varphi : G \longrightarrow S_{n_p}$. $Ker\,\varphi < G \Longrightarrow$

$$\begin{tikzcd}[row sep=small] & \{e\} \quad \rightsquigarrow |Imm\,\varphi| = n < |S_{n_p}| = n_p! \text{ (perché } Imm\,\varphi < S_{n_p}) \\ Ker\,\varphi = \arrow[ur] \arrow[dr] & \\ & G \quad \text{è assurdo } \lightning \end{tikzcd}$$

□

Esercizio 16. *Sia G gruppo con $|G| = 24 = 2^3 \cdot 3$, dimostrare che G non è semplice.*

Dimostrazione. $n_3 \mid 24$ e $n_3 \equiv 1\,(3) \Longrightarrow$
$$\begin{tikzcd}[row sep=small] & 1 \\ n_3 = \arrow[ur] \arrow[dr] & \\ & 4 \end{tikzcd}$$
Per l'esercizio precedente, se G è semplice, $|G| = 24 \leq n_3! \Longrightarrow n_3 = 4$, qui non funziona...

$n_2 \mid 24$ e $n_2 \equiv 1\,(2) \Longrightarrow$
$$\begin{tikzcd}[row sep=small] & 1 \\ n_2 = \arrow[ur] \arrow[dr] & \\ & 3 \end{tikzcd}$$
Per l'esercizio precedente, se G fosse semplice, dovrebbe valere $|G| = 24 \leq n_2! \Longrightarrow n_2 \neq 3 \Longrightarrow n_2 = 1 \Longrightarrow$ il 2-Sylow è unico e quindi normale $\Longrightarrow G$ non è semplice. □

Esercizio 17. *Sia G gruppo con $|G| = 56 = 2^3 \cdot 7$, dimostrare che G non è semplice.*

Dimostrazione.

$n_7 \mid 56$ e $n_7 \equiv 1\,(7) \Longrightarrow$
$$\begin{tikzcd}[row sep=small] & 1 \\ n_7 = \arrow[ur] \arrow[dr] & \\ & 8 \end{tikzcd}$$
mentre $n_2 \mid 56$ e $n_2 \equiv 1\,(2) \Longrightarrow$
$$\begin{tikzcd}[row sep=small] & 1 \\ n_2 = \arrow[ur] \arrow[dr] & \\ & 7 \end{tikzcd}$$
Se $n_7 = 1$, il sottogruppo di 7 elementi è unico e quindi normale $\Longrightarrow G$ non è semplice.
Se invece $n_7 = 8$, due qualunque 7-Sylow hanno intersezione $\{e\}$, infatti, presi $P, Q < G$ due 7-Sylow distinti sono tali che $P \cap Q < P$ e $P \cap Q < Q$.
Quanti elementi di ordine 7 ci sono in G? Sono $48 = 8 \cdot 6$ ($8 = \#\{$sottogruppi di 7 elementi$\}$ e $6 = \#\{$elementi di ordine 7 in ogni sottogruppo$\}$).
Restano "fuori" 8 elementi i quali quindi formano (per **Sylow I**) un solo 2-Sylow possibile che appunto, essendo unico, è normale $\Longrightarrow G$ non è semplice. □

Esercizio 18. *Sia G gruppo semplice con $|G| = n \geq 3$, dimostrare che se n è pari, allora $4 \mid n$.*

$n = 2^a d$ con $(2, d) = 1$.
Pista: prendiamo $H < G$ un 2-Sylow e supponiamo H ciclico, $H =< h >$.
Vogliamo interpretare h come una permutazione dispari.

Esercizio 19. *Mettere tutto insieme e dimostrare che non esistono gruppi semplici "nuovi" (=diversi dai gruppi di ordine p e gli altri noti) con ordine < 60.*

Esercizio 20. *Mostrare che A_5 è l'unico (a meno di isomorfismo) gruppo semplice di ordine 60.*

G gruppo, $\varphi : G \longrightarrow S_{|G|} = Big(G) \supseteq Aut(G)$, $\varphi\big(g_1 g_2\big)(x) = \varphi\Big(g_1\Big)\big(\varphi\big(g_2\big)(x)\big)$
$\varphi\big(g\big)(xy) = \varphi\big(g\big)(x)\varphi\big(g\big)(y)$, se l'azione rappresenta il coniugio, $gxyg^{-1} = gxg^{-1}gyg^{-1}$ ✓

$$\begin{tikzcd} G \arrow[r] \arrow[dr] & S_{|G|} \\ & Aut(G) \end{tikzcd}$$
con $Aut(G) < S_{|G|}$, chi è $Aut(S_n) =?$

$$\begin{array}{rccccccc} \psi : & S_n & \hookrightarrow & Aut(S_n) & & & \\ & \sigma & \longmapsto & C_\sigma : & S_n & \longrightarrow & S_n \\ & & & & \tau & \longmapsto & \sigma\tau\sigma^{-1} \end{array}$$

$\sigma \in Ker\,\psi \Longleftrightarrow \sigma \in Z(S_n) = \{e\}$ per $n \geq 3 \Longrightarrow \psi$ è iniettiva.

Teorema 1.4.5. *Se $n > 2$ e $n \neq 6$, allora $Aut(S_n) \cong S_n$.*

1.5 Prodotti semidiretti

Siano G un gruppo e $M, N < G$. Sappiamo bene che in generale non è vero che $MN < G$. Ad esempio in S_3, dati $M = \{e, (1,2)\}$ e $N = \{e, (1,3)\}$

$$MN = \{e \cdot e, e \cdot (1,3), (1,2) \cdot e, (1,2)(1,3)\} = \{e, (1,3), (1,2), (1,3,2)\} \not< S_3$$

Lemma 1.5.1. *Siano $M \lhd G$ e $N < G$, allora $MN < G$.*

Dimostrazione. Verifichiamo che è chiuso rispetto al prodotto: $m, m_1 \in M$ e $n, n_1 \in N$

$$mn \cdot m_1 n_1 = mnm_1n_1 = mnm_1n^{-1}nn_1 = m \underbrace{nm_1n^{-1}}_{\in M} nn_1 \in MN$$

$\square$

Lemma 1.5.2. *(Come esercizio, altrimenti da studiare sulle dispense)*
Se $M \lhd G$, $N \lhd G$ e vale anche $M \cap N = \{e\}$, allora $\forall m \in M$ e $\forall n \in N$ $mn = nm$.

Osservazione 3. *In questo caso dunque $MN < G$ e $MN \cong M \times N$.*

Errore di stampa a pagina 32 delle dispense: Corollario ~~4.1.1.~~ 1.2.1.

1.5.1 Costruzione di un prodotto semidiretto

Siano H, K gruppi e sia $\begin{array}{cccc} \tau: & K & \longrightarrow & Aut(H) \\ & k & \longmapsto & \tau(k) \end{array}$ omomorfismo, consideriamo sull'insieme $H \times K$ il seguente prodotto "strano" $(h,k)(\overline{h},\overline{k}) = \Big(h\tau\big(k\big)\big(\overline{h}\big), k\overline{k}\Big)$.
Prima: $m\, nm_1n^{-1}\, nn_1 = m\, C\big(n\big)\big(m_1\big)\, nn_1$ visto che $M \lhd G$.

Definizione 1.5.1. *Chiamiamo $H \rtimes_\tau K$ il* ***prodotto semidiretto di*** *H* ***e*** *K* ***rispetto a*** *τ definito qui sopra.*

Esercizio 21. *Dimostrare che $H \rtimes_\tau K$ è un gruppo.*

Consideriamo adesso $H \times \{e_K\} = \{(h, e_K) | h \in H\} < H \rtimes_\tau K$ che è $\cong H$:

$$(h_1, e_K)(h_2, e_K) = \Big(h_1 \underbrace{\tau\big(e_K\big)}_{=Id}(h_2), e_K\Big) = (h_1h_2, e_K)$$

$\begin{array}{cccc} \psi: & H & \longrightarrow & H \times \{e_K\} \\ & h & \longmapsto & (h, e_K) \end{array}$ è un isomorfismo.

Esercizio 22. $H \times \{e_K\} \lhd H \rtimes_\tau K$.

<u>Hint</u>: l'inverso di $(\overline{h}, \overline{k})$ è $\Big(\tau\big(\overline{k}^{-1}\big)\big(\overline{h}^{-1}\big), \overline{k}^{-1}\Big)$.
$(\overline{h}, \overline{k})(h, e_K)\Big(\tau\big(\overline{k}^{-1}\big)\big(\overline{h}^{-1}\big), \overline{k}^{-1}\Big) \overset{?}{\in} H \times \{e_K\}$.

Osservazione 4. $\{e_H\} \times K < H \rtimes_\tau K$.

Teorema 1.5.3. *Siano G gruppo, $H \lhd G$, $K < G$, $H \cap K = \{e\}$ e $G = HK$,*

$\Big($Commento: nei sottogruppi di ordine 20 di S_5 accadeva proprio questo, ovvero $H = \big((1,2,3,4,5)\big)$, $K = \big((1,2,4,3)\big)$ e $H \cap K = \{e\}$, HK ha 20 elementi e dunque $HK = G.\Big)$

allora $G \cong H \rtimes_{C_G} K$, *dove* $\begin{array}{rccc} C_G: & K & \longrightarrow & Aut(H) \\ & k & \longmapsto & {\scriptstyle \text{automorfismo tale che} \atop \forall h \in H,\ h \mapsto khk^{-1}} \end{array}$.

Dimostrazione. Consideriamo $\begin{array}{rccc} \theta: & HK & \longrightarrow & H \rtimes_{C_G} K \\ & hk & \longmapsto & (h,k) \end{array}$ ... □

Proposizione 1.5.4. *Dati H, K gruppi, siano $\tau_1, \tau_2 : K \longrightarrow Aut(H)$ due omomorfismi. Se esistono $\alpha \in Aut(H)$ e $\beta \in Aut(K)$ tali che $\alpha \circ \tau_1(k) \circ \alpha^{-1} = \tau_2\big(\beta(k)\big)$ $\forall k \in K$, allora $H \rtimes_{\tau_1} K \cong H \rtimes_{\tau_2} K$.*

Dimostrazione. $\begin{array}{rccc} \theta: & H \rtimes_{\tau_1} K & \longrightarrow & H \rtimes_{\tau_2} K \\ & (h,k) & \longmapsto & \big(\alpha(h), \beta(k)\big) \end{array}$ è l'isomorfismo cercato (verificarlo come esercizio oppure studiarlo sulle dispense). □

Esempio 5. *Classificazione dei gruppi di cardinalità pq, con p e q primi:*

Proposizione 1.5.5. *Sia $p > q$. Se $q \nmid p-1$ esiste un solo gruppo (a meno di isomorfismo) di cardinalità pq ed è $\mathbb{Z}/_{pq\mathbb{Z}}$.*
Se $q \mid p-1$ esistono esattamente due gruppi (a meno di isomorfismo) di ordine pq: $\mathbb{Z}/_{pq\mathbb{Z}}$ e uno non abeliano.

Nota: se $q = 2$ esiste sempre il gruppo non abeliano ed è D_{2p}.

Dimostrazione. Sia G gruppo, con $|G| = pq$, siano N_p un p-Sylow e N_q un q-Sylow.
Si nota subito che $N_p \lhd G$ visto che ha indice q, cioè il più piccolo primo che divide l'ordine del gruppo (**Teorema 1.2.3.**). Dunque $N_pN_q = G$ per ragioni di cardinalità ($N_p \cap N_q = \{e\}$):

$$|N_pN_q| = \frac{|N_p| \cdot |N_q|}{|N_p \cap N_q|} = pq \Longrightarrow G \cong N_p \rtimes_{C_G} N_q \Longrightarrow N_p \cong \mathbb{Z}/_{p\mathbb{Z}} \text{ e } N_q \cong \mathbb{Z}/_{q\mathbb{Z}}$$

Studiamo tutti i possibili $\tau : \mathbb{Z}/_{q\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{p\mathbb{Z}}) \cong (\mathbb{Z}/_{p\mathbb{Z}})^* \cong \mathbb{Z}/_{(p-1)\mathbb{Z}}$:
Se $q \nmid p-1$, allora $\tau : \mathbb{Z}/_{q\mathbb{Z}} \longrightarrow Aut(\mathbb{Z}/_{p\mathbb{Z}}) \cong \mathbb{Z}/_{(p-1)\mathbb{Z}}$ è tale che $\tau(i) = Id$ $\forall i \in \mathbb{Z}/_{q\mathbb{Z}}$ perché non ci sono elementi di ordine q in $Aut(\mathbb{Z}/_{p\mathbb{Z}})$ quindi l'immagine di 1 (= un generatore di $\mathbb{Z}/_{q\mathbb{Z}}$) è $Id \in Aut(\mathbb{Z}/_{p\mathbb{Z}})$ (oppure $0 \in \mathbb{Z}/_{(p-1)\mathbb{Z}}$).
Perciò $\mathbb{Z}/_{p\mathbb{Z}} \rtimes_\tau \mathbb{Z}/_{q\mathbb{Z}}$ coincide col prodotto diretto $\mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{q\mathbb{Z}} \cong \mathbb{Z}/_{pq\mathbb{Z}}$.
Se $q \mid p-1$, allora $\begin{array}{rccc} \tau_i: & \mathbb{Z}/_{q\mathbb{Z}} & \longrightarrow & \mathbb{Z}/_{(p-1)\mathbb{Z}} \\ & 1 & \longmapsto & i \cdot \frac{p-1}{q} \end{array}$. $\tau_0(1) = 0$, come prima, e questo produce $\mathbb{Z}/_{q\mathbb{Z}} \times \mathbb{Z}/_{p\mathbb{Z}}$.
Mostriamo adesso, usando la **Proposizione 1.5.4.**, che

$$\mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_1} \mathbb{Z}/_{q\mathbb{Z}} \cong \mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_2} \mathbb{Z}/_{q\mathbb{Z}} \cong ... \cong \mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_{q-1}} \mathbb{Z}/_{q\mathbb{Z}}$$

$\forall i = 1, ..., q-1$ scelgo $\beta_i \in Aut(\mathbb{Z}/_{q\mathbb{Z}})$ definito da $\beta_i(1) = i$.
Ricordiamo che $Aut(\mathbb{Z}/_{q\mathbb{Z}}) \cong (\mathbb{Z}/_{q\mathbb{Z}})^*$ e la mappa era $\begin{array}{ccc} Aut(\mathbb{Z}/_{q\mathbb{Z}}) & \cong & (\mathbb{Z}/_{q\mathbb{Z}})^* \\ 1 \mapsto i \neq 0 & \longleftrightarrow & i \end{array}$.
Affermiamo che $\tau_i(1) = \tau_1\big(\beta_i(1)\big)$, infatti $\tau_i(1) = i \cdot \frac{p-1}{q} = \tau_1(i) = \tau_1\big(\beta_i(1)\big)$.
Dunque $\tau_1 \circ \beta_i = \tau_i$ su tutto $\mathbb{Z}/_{q\mathbb{Z}}$ perché coincidono su 1 che è un generatore di $\mathbb{Z}/_{q\mathbb{Z}}$.
Quindi $\mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_1} \mathbb{Z}/_{q\mathbb{Z}} \cong \mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_i} \mathbb{Z}/_{q\mathbb{Z}}$ $\forall i$. Perciò ci sono al massimo due gruppi (a meno di isomorfismi) di cardinalità pq: $\mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{q\mathbb{Z}}$ e $\mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_1} \mathbb{Z}/_{q\mathbb{Z}}$.
Per mostrare che non sono isomorfi tra loro basta far vedere che $\mathbb{Z}/_{p\mathbb{Z}} \rtimes_{\tau_1} \mathbb{Z}/_{q\mathbb{Z}}$ non è abeliano: siano $a \in \mathbb{Z}/_{p\mathbb{Z}}$ e $b \in \mathbb{Z}/_{q\mathbb{Z}}$,

$$(a,b)(0,b) = \Big(a + \tau_1\big(b\big)(0), 2b\Big) = (a, 2b)$$

$$(0,b)(a,b) = \Big(0 + \tau_1\big(b\big)(a), 2b\Big) = \Big(\tau_1\big(b\big)(a), 2b\Big)$$

Scegliamo b tale che $\tau_1(b) \neq Id$ (possiamo farlo perché infatti τ_1 non è l'isomorfismo banale). Perciò $\tau_1(b) \neq Id \iff \exists$ un elemento, che chiameremo ovviamente a, che non viene mandato in se stesso $\Longrightarrow \tau_1\big(b\big)(a) \neq a$. Dunque $\mathbb{Z}/p\mathbb{Z} \rtimes_{\tau_1} \mathbb{Z}/q\mathbb{Z}$ non è commutativo. $\square$

<u>Nota</u>: si poteva anche osservare che se $G = \mathbb{Z}/p\mathbb{Z} \rtimes_{\tau_1} \mathbb{Z}/q\mathbb{Z}$ fosse stato abeliano, allora τ_1 avrebbe descritto il coniugio in G che è l'Id e dunque τ_1 sarebbe stato l'omomorfismo banale $\lightning$.

1.6 Gruppi di ordine 6

Sia G un tale gruppo. Siano N_2 un 2-Sylow e N_3 un 3-Sylow.
$n_3 = 1$ (o comunque N_3 ha indice 2) e dunque $N_3 \lhd G$.
Inoltre $N_3 \cap N_2 = \{e\}$ e $|N_3N_2| = \frac{|N_3|\cdot|N_2|}{|N_3 \cap N_2|} = 6 \Longrightarrow N_3N_2 = G$, allora, per il **Teorema 1.5.3.** sappiamo che $G \cong N_3 \rtimes_{C_G} N_2$.
$C_G : N_2 \longrightarrow Aut(N_3)$ già... ma chi è C_G?
Studiamo adesso tutti i possibili omomorfismi $\tau : N_2 \longrightarrow Aut(N_3)$.

$$N_3 \cong \mathbb{Z}/3\mathbb{Z} \quad N_2 \cong \mathbb{Z}/2\mathbb{Z} \quad Aut(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} = \{Id, -Id\}$$

Stiamo dunque studiando (a meno di isomorfismi) i possibili omomorfismi

$$\begin{array}{cccc} \tau : & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & 1 & \longmapsto & \{1, 0\} \end{array}$$

$\Longrightarrow$ in totale abbiamo 2 omomorfismi.
Tradotti: $\begin{array}{cccc} \tau_1 : & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/3\mathbb{Z}) \\ & 1 & \longmapsto & Id \end{array}$ e $\begin{array}{cccc} \tau_2 : & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/3\mathbb{Z}) \\ & 1 & \longmapsto & -Id \end{array}$.
Esistono quindi al massimo due gruppi di ordine 6, perché:

- sappiamo che un tale gruppo è del tipo $\mathbb{Z}/3\mathbb{Z} \rtimes_\tau \mathbb{Z}/2\mathbb{Z}$;
- sappiamo che di τ di quel tipo, ossia $\tau : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z})$, ne esistono due.

Conosciamo due gruppi di orine 6: $\underset{\text{abeliano}}{\mathbb{Z}/6\mathbb{Z}}$ e $\underset{\text{non abeliano}}{S_3}$, dunque deve essere

$$\mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_1} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \qquad \text{e} \qquad \mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_2} \mathbb{Z}/2\mathbb{Z} \cong S_3$$

τ_1 infatti è banale, $\tau_1(1) = Id$:

$$(a,b)(c,d) = \Big(a\tau_1\big(b\big)(c), bd\Big) = (ac, bd) \Longrightarrow \mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_1} \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

S_3: $H = \big((1,2,3)\big)$, $K = \big((1,2)\big)$, $S_3 = HK \cong H \rtimes_{\substack{\text{coniugio} \\ \text{in } S_3}} K$,

$$\begin{array}{cccc} \tau_2 : & K & \longrightarrow & Aut(H) \\ & (1,2) & \longmapsto & \substack{\text{automorfismo di } H \text{ che man-} \\ \text{da ogni elemento nell'inverso}} \end{array}$$

Ad esempio: $(1,2,3) \in H$, $(1,2)(1,2,3)(1,2) = (1,3,2) = (1,2,3)^{-1}$.

Esercizio 23. *Wreath product*
$H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $K = \mathbb{Z}/2\mathbb{Z}$, $H \rtimes_? K$.

Vi propongo questo $\begin{array}{cccc} \tau : & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \\ & 1 & \longmapsto & \text{scambio di coordinate} \end{array}$.
Prendiamo: $a = \big((0,0),1\big) \in H \rtimes_\tau K$, $b = \big((1,0),1\big) \in H \rtimes_\tau K$, $aba^{-1} = ?$

$$\big((0,0),1\big)\big((1,0),1\big)\big((0,0),1\big) = \Big((0,0) + \tau\big(1\big)\big((1,0)\big), 1+1\Big)\big((0,0),1\big) = \big((0,1),0\big)\big((0,0),1\big) =$$

$$= \big((0,1) + \tau\big(0\big)\big((0,0)\big), 0+1\big) = \big((0,1),1\big) \Longrightarrow \text{il gruppo } \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \rtimes_\tau \mathbb{Z}/2\mathbb{Z} \text{ non è abeliano.}$$

1.7 Gruppi di ordine 12

Siano G gruppo di ordine 12, N_2 un 2-Sylow, con $|N_2| = 4$, e N_3 un 3-Sylow, con $|N_3| = 3$.

Si ha $n_2 = \begin{array}{l} \nearrow 1 \\ \\ \searrow 3 \end{array}$ e $n_3 = \begin{array}{l} \nearrow 1 \\ \\ \searrow 4 \end{array}$

Caso 1: Sia $n_2 = 1 \Longrightarrow N_2 \lhd G$ e $G \cong N_2 \rtimes N_3$, ma allora $N_2 \cong \begin{array}{l} \nearrow \mathbb{Z}/4\mathbb{Z} \\ \\ \searrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{array}$.

Studiamo il caso $G = \mathbb{Z}/4\mathbb{Z} \rtimes_\tau \mathbb{Z}/3\mathbb{Z}$, $Aut(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$:
si ha che $\begin{array}{rccc} \tau: & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & 1 & \longmapsto & 0 \end{array}$ è l'unico possibile per motivi di ordine. Abbiamo dunque solamente $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$.
Studiamo adesso il caso $G = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\tau \mathbb{Z}/3\mathbb{Z}$, $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong GL_2(\mathbb{Z}/2\mathbb{Z})$:
si ha che $|GL_2(\mathbb{Z}/2\mathbb{Z})| = 3 \cdot 2 = 6$ (in quanto per una matrice del tipo $\begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}$ abbiamo $2^2 - 1$ scelte per la prima colonna e $2^2 - 2$ scelte per la seconda), inoltre $GL_2(\mathbb{Z}/2\mathbb{Z})$ non è abeliano e dunque, dato che sappiamo che esiste un solo gruppo non abeliano (a meno di isomorfismo) di cardinalità 6, deve essere $GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.
Nota: vediamo più da vicino: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ è generato da $< (1,0), (0,1) >$. Un automorfismo è un cambio di base e le basi sono tutte e sole le coppie a, b, dove $a \neq b$ e $a, b \in \{(1,0), (0,1), (1,1)\}$. Questo identifica i cambi di base con le permutazioni di X.
$\begin{array}{rccc} \tau_i: & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3 \\ & 1 & \longmapsto & (1,2,3)^i \end{array}$; $\tau_0(1) = e$ dà $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
Ora osserviamo che $\tau_1 \circ \beta = \tau_2$, dove $\beta \in Aut(\mathbb{Z}/3\mathbb{Z})$ e $\beta(1) = 2$, infatti $\tau_1\big(\beta(1)\big) = \tau_1(2) = (1,3,2)$, dunque $\tau_1 \circ \beta = \tau_2$.
Avremmo potuto anche prendere $\alpha \in S_3$ tale che $\alpha(1,2,3)\alpha^{-1} = (1,3,2)$ (quindi $\alpha = (2,3)$), allora $\alpha \circ \tau_2(1) \circ \alpha^{-1} = \tau_1(1)$, $\alpha(1,3,2)\alpha^{-1} = (1,2,3)$.
Grazie alla **Proposizione 1.5.4.**, deduciamo che c'è solo un gruppo del tipo $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\tau_1} \mathbb{Z}/3\mathbb{Z}$ ossia in cui il 2-Sylow è normale ed è $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dato che conosciamo A_4, È LUI.
Abbiamo terminato i casi in cui il 2-Sylow è normale.
Caso 2: Sia dunque adesso $n_2 = 3 \Longrightarrow n_3 = 1$ perché se fosse $n_3 = 4$ avremmo 8 elementi di ordine 3 e resterebbero 4 elementi non di ordine 3 che costituirebbero un unico 2-Sylow ma allora sarebbe $n_2 = 1$ $\lightning$.
Dunque $n_2 = 3$ e $n_3 = 1$, allora $G \cong N_3 \rtimes N_2$ e l'analisi si dirama nei due casi:

(A) $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$: $\begin{array}{rccc} \tau_i: & \mathbb{Z}/4\mathbb{Z} & \longleftrightarrow & Aut(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \\ & 1 & \longmapsto & (-1)^i Id \leftrightarrow i \end{array}$, $\tau_0(1) = Id$ dà $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$.
$\tau_1(1) = -Id$ invece dà $\mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_1} \mathbb{Z}/4\mathbb{Z}$:

$$(a,b)(c,d) = \Big(a + \tau_1\big(b\big)(c), b + d\Big) = \big(a + (-1)^b c, b + d\big)$$

Un modello per questo gruppo si trova ad esempio dentro $SL_2(\mathbb{C})$ (= sottogruppo di $GL_2(\mathbb{C})$ dato dalle matrici con det $= 1$):

$$\begin{array}{l} x = (1,0) \\ y = (0,1) \end{array} \quad x = \begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix},\ \omega = e^{\frac{2\pi}{3} i},\ y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Il gruppo $(x, y) \subseteq SL_2(\mathbb{C})$. Vale anche la relazione $yxy^{-1} = x^{-1}$.

(B) $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$: $\quad \begin{array}{rccc} \tau : & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \\ & a = (1,0) & \longmapsto & ? \\ & b = (0,1) & \longmapsto & ? \end{array}$.

Per dire chi sia τ devo indicare $\tau(a)$ e $\tau(b)$.
Se $\tau_0(a) = \tau_0(b) = 0$ si ha il prodotto diretto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Se $\tau_1(a) = 0$ e $\tau_1(b) = 1$, $\tau_2(a) = 1$ e $\tau_2(b) = 0$ o $\tau_3(a) = \tau_3(b) = 1$, vorrei dire che si ha

$$\mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_1} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_2} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\tau_3} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}).$$

Cerco $\alpha \in Aut(\mathbb{Z}/3\mathbb{Z})$ e $\beta \in Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ tali che $\alpha \circ \tau_2(k) \circ \alpha^{-1} = \tau_1\big(\beta(k)\big)$.
Scelgo $\alpha = Id$ (tanto non mi aiuta perché $Aut(\mathbb{Z}/3\mathbb{Z})$ è commutativo) e $\beta =$ il cambio di base che mi scambia a e b.
Per $\alpha \circ \tau_3(k) \circ \alpha^{-1} = \tau_2\big(\beta(k)\big)$ basta scegliere $\alpha = Id$ e $\beta =$ il cambio di base che manda a in a e b in $a + b$.
Il gruppo trovato è D_6:
$\{e, r^3, s, r^3 s\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} < D_6$, dove $r^3 =$ rotazione di 180° e $s =$ una simmetria.
Ricordiamo che $D_6 = \{r, s \mid r^6 = e,\ s^2 = e,\ srs = r^{-1}\}$.
Dunque D_6 ha le caratteristiche richieste.

Sia G gruppo, sappiamo che $Aut(G) \subseteq Big(G)$ è un gruppo per gli automorfismi di G.

$g \in G$, $\begin{array}{rccc} C_g : & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1} \end{array}$ e $S_n \hookrightarrow Aut(S_n)$.

Teorema 1.7.1. *$Aut(S_n) \cong S_n$ se $n > 2$ e $n \neq 6$.*

Dimostrazione. (Idee): ① Presi $\varphi \in Aut(S_n)$ e un $x \in S_n$ di ordine 2 $\Longrightarrow \varphi(x)$ ha ordine 2 $\big($infatti $\varphi(x)^2 = \varphi(x)\varphi(x) = \varphi(x^2) = \varphi(e) = e\big)$.
② Presi $\varphi \in Aut(S_n)$ e $x, y \in S_n$ coniugati tra loro $\Longrightarrow \varphi(x)$ e $\varphi(y)$ sono coniugati $\big($infatti se $gxg^{-1} = y$, allora $\varphi(gxg^{-1}) = \varphi(y)$, cioè $\varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(y)\big)$.
③ Se $\varphi \in Aut(S_n)$, allora φ permuta le classi di coniugio degli elementi di ordine 2.
Γ_k = classe di coniugio dei k 2-cicli di S_n, $\#\Gamma_k = \frac{1}{k!}\binom{n}{2}\binom{n-2}{2}...\binom{n-2(k-1)}{2}$. □

Lemma 1.7.2. *Se $n \neq 6$, allora $\#\Gamma_k \neq \#\Gamma_1$ $\forall k > 1$.*

Conseguenza: se $n \neq 6$, allora $\varphi(\Gamma_1) = \Gamma_1$, cioè φ manda trasposizioni in trasposizioni.

Esercizio 24. *Dimostrare il **Lemma 1.7.2.***

Domanda: se $\varphi \in Aut(S_n)$ manda trasposizioni in trasposizioni, è vero che $\varphi = C_g$ per qualche $g \in S_n$?
Risposta: SÌ: supponiamo $\varphi\big((1,2)\big) = (a,b)$ e prendiamo $i \neq 1,2$, allora $(1,2)(1,i)$ è un 3-ciclo e dunque $\varphi\big((1,2)(1,i)\big) = \varphi\big((1,2)\big)\varphi\big((1,i)\big) = (a,b)\varphi\big((1,i)\big)$ è un 3-ciclo anche lui.
Possiamo quindi supporre che $\varphi\big((1,i)\big) = (a,c)$, con $c \neq a, b$.
Affermiamo: $\forall j \neq 1$, $\exists d \neq a$ tale che $\varphi\big((1,j)\big) = (a,d)$.
Per $j = 2$ e $j = i$ lo sappiamo già. Supponiamo quindi $j \neq 2$ e $j \neq i$.
$\varphi\big((1,j)(1,2)\big)$ è un 3-ciclo; vogliamo escludere la possibilità che $\varphi\big((1,j)\big) = (b,f)$,
$\varphi\big((1,j)(1,i)\big) = (b,f)(a,c)$ è un 3-ciclo $\Longrightarrow f \stackrel{?}{=} c$:

$$(a,b)(a,c)(a,b) = (b,c) \Longrightarrow \varphi\big((1,2)\big)\varphi\big((1,i)\big)\varphi\big((1,2)\big) = \varphi\big((1,j)\big) \Longrightarrow$$

$$\Longrightarrow \varphi\big((1,2)(1,i)(1,2)\big) = \varphi\big((1,j)\big) \Longrightarrow \varphi\big((2,i)\big) = \varphi\big((1,j)\big) \lightning$$

Esercizio 25. *Concludere la dimostrazione del **Teorema 1.7.1.***

1.8 Gruppi di ordine 8

Sia G un tale gruppo. Preso un $g \in G$, $ord(g) = \{1, 2, 4, 8\}$.

• Se il massimo ordine degli elementi di G è 1 $\Longrightarrow |G| = 1$ ↯.

• Se il massimo ordine degli elementi di G è 8 $\Longrightarrow G$ è ciclico, quindi $G \cong \mathbb{Z}/8\mathbb{Z}$.

• Se il massimo ordine degli elementi di G è 2 $\Longrightarrow x^2 = e$ $\forall x \in G \setminus \{e\}$, cioè $x = x^{-1}$ $\forall x \in G \Longrightarrow G$ è abeliano perché $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

Esercizio 26. *Dimostrare che in questo caso* $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

• Se il massimo ordine degli elementi di G è 4 $\Longrightarrow \exists x \in G$ di ordine 4 e sia $H =< x >$ il sottogruppo di G generato da $x \Longrightarrow H \lhd G$ perché ha indice 2.
Prendiamo $y \in G \setminus H$ di ordine 2 (si può?)

$$\begin{array}{c} K = \{e, y\} < G \\ H = \{e, x, x^2, x^3\} \end{array} \Longrightarrow G = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\} \Longrightarrow G \cong H \rtimes_\varphi K$$

Devo capire chi sia yxy^{-1}.
$\varphi : K \longrightarrow Aut(H)$ cioè $\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.
Se l'azione φ è banale, $G \cong H \times K \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Altrimenti $yxy^{-1} = yxy = x^{-1} = x^3$, $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

Esercizio 27. *Dimostrare che* $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong D_4$.

Ma perché esiste un elemento di ordine 2 fuori da H?

Esercizio 28. *Pensateci...*

• (Bis) Se il massimo ordine degli elementi di G è 4 $\Longrightarrow \exists x \in G$ tale che $ord(x) = 4$ e chiediamo che $\nexists y \notin < x >$ tale che $ord(y) = 2 \Longrightarrow \exists z \notin < x >$ tale che $ord(z) = 4$.
Per elencazione, sarebbe $G = \{e, x, x^2, x^3, z, z^2 = x^2, z^3, xz, (xz)^2 = x^2, (xz)^3\}$.
Chiamiamo $i = x$, $j = z$, $k = xz$, $i^2 = j^2 = k^2 = -1$, $i^3 = -i$, $j^3 = -j$ e $k^3 = -k$.
Quindi $G = \{e, i, j, k, -1, -i, -j, -k\}$. Osserviamo ora che $\boxed{ij = k}$,
$(ji)(ij) = ji^2j = -jj = -j^2 = 1 \Longrightarrow ji = (ij)^{-1} = -k \Longrightarrow \boxed{ji = -k}$,
$jk = jij = -kj = -ijj = -ij^2 = i \Longrightarrow \boxed{jk = i}$, $\boxed{kj = -i}$, $\boxed{ki = j}$ e $\boxed{ik = -j}$.
Quello che otteniamo quindi è Q_8, detto **Gruppo dei quaternioni**:
ha 6 elementi di ordine 4, 1 elemento di ordine 2 e 1 elemento di ordine 1.
In $GL_2(\mathbb{C})$, le matrici $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ e $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ generano un gruppo isomorfo a Q_8.

Domanda: $S_3 \times \mathbb{Z}/2\mathbb{Z}$ quale gruppo è nella classificazione?
Prendiamo $H \subseteq S_3$, $H = \big((1,2,3)\big)$: $H \times \{0\} \lhd S_3 \times \mathbb{Z}/2\mathbb{Z} \Longrightarrow$ il 3-Sylow è normale.
$K \subseteq S_3$, $K = \big((1,2)\big)$, $K \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} < S_3 \times \mathbb{Z}/2\mathbb{Z}$.
Inoltre, il gruppo $S_3 \times \mathbb{Z}/2\mathbb{Z}$ non è abeliano, dunque $S_3 \times \mathbb{Z}/2\mathbb{Z} \cong D_6$.

Domanda peggiore: Presi i gruppi S_3, $\mathbb{Z}/2\mathbb{Z}$ e l'omomorfismo $\begin{array}{rccc} \tau: & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/3\mathbb{Z}) \cong S_3 \\ & 1 & \longmapsto & (1,2) \end{array}$,
possiamo fare $S_3 \rtimes_\tau \mathbb{Z}/2\mathbb{Z}$ e questo gruppo chi è?
Sia $b = \big((1,2),0\big) \in S_3 \rtimes_\tau \mathbb{Z}/2\mathbb{Z}$, allora $b^2 = (e,0)$, infatti

$$\big((1,2),0\big)\big((1,2),0\big) = \Big((1,2)\underbrace{\tau(0)}_{\substack{\shortparallel \\ Id}}\big(1,2\big), 0+0\Big) = (e,0)$$

Sia $g = (e,1)$, allora $g^2 = (e,0)$. Sia ora $x = bg = \big((1,2),0\big)(e,1) = \big((1,2),1\big) \notin S_3 \times \{0\}$.
Notiamo che $x^2 = bg\,bg = bggb = bg^2b = beb = b^2 = e$, infatti b e g commutano:
$gb = (e,1)\big((1,2),0\big) = \Big(e\,\tau(1)\big(1,2\big),1\Big)$, ma $\tau(1)$ è il coniugio per $(1,2)$ e quindi
$(1,2)(1,2)(1,2) = (1,2)$, da cui $gb = \big((1,2),1\big) = bg$.
Mostriamo che x commuta con $S_3 \times \{0\}$: basta vedere che x commuta con $b = \big((1,2),0\big)$ (già visto) e che x commuta con $a = \big((1,2,3),0\big)$:

$$ax = \big((1,2,3),0\big)\big((1,2),1\big) = \Big((1,2,3)\tau(0)\big(1,2\big), 0+1\Big) = \big((1,2,3)(1,2),1\big) = \big((1,3),1\big)$$

$$xa = \big((1,2),1\big)\big((1,2,3),0\big) = \Big((1,2)\tau(1)\big(1,2,3\big), 1+0\Big) = \big((1,2)^2(1,2,3)(1,2),1\big) = \big((1,3),1\big)$$

Siano $K =< x >$ che ha ordine 2 e $H = S_3 \times \{0\}$ che ha ordine 6:
$H \cap K = \{e\}$, $HK = S_3 \rtimes_\tau \mathbb{Z}/2\mathbb{Z}$ e, poiché x commuta con H, $HK \cong H \times K \cong S_3 \rtimes_\tau \mathbb{Z}/2\mathbb{Z}$.

Osservazione 5. *Usando la* ***Proposizione 1.5.4.****, avremmo mai potuto scoprire che* $S_3 \times \mathbb{Z}/2\mathbb{Z} \cong S_3 \rtimes_{\tau_{ban}} \mathbb{Z}/2\mathbb{Z}$ *e* $S_3 \rtimes_\tau \mathbb{Z}/2\mathbb{Z}$ *sono isomorfi?*

$$\begin{array}{rccc} \tau_{ban}: & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & S_3 \\ & 1 & \longmapsto & e \end{array} \qquad \begin{array}{rccc} \tau: & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & S_3 \\ & 1 & \longmapsto & (1,2) \end{array}$$

Cerchiamo $\alpha \in Aut(S_3) \cong S_3$ e $\beta \in Aut(\mathbb{Z}/2\mathbb{Z}) = \{Id\}$ (quindi β in realtà non aiuta) tali che $\alpha \circ \tau(1) \circ \alpha^{-1} = \tau_{ban}\big(\beta(1)\big)$. Proviamo α come elemento di S_3 $\tau(1) = (1,2)$ e $\tau_{ban}\big(\beta(1)\big) = e$:
$\alpha(1,2)\alpha^{-1} \overset{?}{=} e \Longrightarrow \big(\alpha(1),\alpha(2)\big) = e$ impossibile. $\lightning$

Proposizione 1.8.1. *(∼****Esercizio****) Dati $p \geq 3$ primo e $\alpha \geq 2$ intero, allora*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/\phi(p^\alpha)\mathbb{Z} = \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

e quindi è ciclico.

Dimostrazione. Strategia: troveremo un elemento γ di ordine $p^{\alpha-1}$ e un elemento β di ordine $p-1$, allora $\gamma\beta$ avrà ordine $p^{\alpha-1}(p-1)$ *perché il gruppo è abeliano* e quindi $(\mathbb{Z}/p^\alpha\mathbb{Z})^* = (\gamma\beta)$.

Lemma 1.8.2. *Sia $k \in \mathbb{N} \setminus \{0\}$, allora $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, con $MCD(\lambda, p) = 1$.*

Dimostrazione. Per induzione su $k \geq 1$.
Passo base: $k = 1$,

$$(1+p)^p = 1 + \binom{p}{1}p + \binom{p}{2}p^2 + ... + p^p = 1 + p^2 + \underbrace{\binom{p}{2}p^2 + ... + p^p}_{\text{sono divisi da } p^3} =$$

$$= 1 + p^2 \underbrace{(1 + \delta p + ...)}_{=\lambda} = 1 + p^2\lambda, \text{ con } MCD(\lambda, p) = 1.$$

<u>Passo induttivo</u>:

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p = (1+\lambda p^{k+1})^p = 1 + \binom{p}{1}\lambda p^{k+1} + \binom{p}{2}(\lambda p^{k+1})^2 + ... =$$

$$= 1 + \lambda p^{k+2} + \underbrace{\binom{p}{2}(\lambda p^{k+1})^2 + ...}_{\text{sono divisi da } p^{k+3}} = 1 + p^{k+2}\underbrace{(\lambda + pu)}_{=\lambda'} = 1 + p^{k+2}\lambda', \text{ con } MCD(\lambda', p) = 1. \quad \square$$

<u>Nota</u>: abbiamo dimostrato che $1+p$ ha ordine $p^{\alpha-1}$ in $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$:

$$(1+p)^{p^{\alpha-1}} \overset{\textbf{Lemma 1.8.2.}}{=} 1 + p^\alpha\lambda \equiv 1\,(p^\alpha)$$

Inoltre, se $r < \alpha - 1$ $(1+p)^r \overset{\textbf{Lemma 1.8.2.}}{=} 1 + p^{r+1}\lambda' \not\equiv 1\,(p^\alpha)$.
$\Longrightarrow \boxed{\gamma = 1 + p}$.

$$\begin{array}{rccc} \psi: & (\mathbb{Z}/p^\alpha\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \\ & [m]_{p^\alpha} & \longmapsto & [m]_p \end{array} \text{ è omomorfismo surgettivo.}$$

Sia $x \in (\mathbb{Z}/p\mathbb{Z})^*$ di ordine $p-1$ e sia $y \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tale che $\psi(y) = x$. Che ordine ha y?
Siccome x ha ordine $p-1$, allora y ha ordine multiplo di $p-1$, allora nel gruppo ciclico (y) trovo un $\boxed{\text{elemento } \beta \text{ di ordine } p-1}$. $\square$

Proposizione 1.8.3. *(∼**Esercizio**) Sia $\alpha \geq 3$, allora $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.*

Lemma 1.8.4. *$\forall k \in \mathbb{N} \setminus \{0\}$ vale $5^{2^k} = 1 + \lambda 2^{k+2}$ con λ dispari.*

Dimostrazione. Per esercizio. $\square$

$$\begin{array}{rccc} \psi: & (\mathbb{Z}/2^\alpha\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \\ & [b]_{2^\alpha} & \longmapsto & [b]_4 \end{array} \text{ è omomorfismo surgettivo.}$$

$Ker\,\psi$ ha $\frac{\phi(2^\alpha)}{2} = \frac{2^\alpha - 2^{\alpha-1}}{2} = 2^{\alpha-2}$ elementi.

Osservazione 6. *$5 \in Ker\,\psi$ e nel **Lemma 1.8.4.** abbiamo dimostrato che in $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ 5 ha esattamente ordine $2^{\alpha-2}$.*

Dunque $Ker\,\psi$ è ciclico, generato da 5, perciò dentro $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ abbiamo $Ker\,\psi \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$, $H = \{1, -1\}$, $Ker\,\psi \cap H = \{1\} \Longrightarrow$ per ragioni di cardinalità, $Ker\,\psi H = (\mathbb{Z}/2^\alpha\mathbb{Z})^*$.
Dunque $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong Ker\,\psi \times H \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\square$

Esercizio 29. *Se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, chi è $Aut(\mathbb{Z}/n\mathbb{Z})$? Per quali n è ciclico?*

1.9 Gruppi abeliani finitamente generati

Definizione 1.9.1. *Un gruppo abeliano M si dice* ***finitamente generato*** *se $\exists m_1, ..., m_n \in M$ tali che $\forall m \in M$ si può scrivere*

$$m = a_1 m_1 + a_2 m_2 + ... + a_{n-1} m_{n-1} + a_n m_n, \ \text{con } a_i \in \mathbb{Z}\ \forall i$$

Si dice che $\{m_1, ..., m_n\}$ è un ***insieme di generatori****.*

Esempio 6. *$(\mathbb{Q}, +)$ non è finitamente generato, infatti se esistessero dei generatori $\frac{r_1}{s_1}, ..., \frac{r_n}{s_n}$ e fosse p un primo tale che p non divide $s_1, ..., s_n$, allora varrebbe $\frac{1}{p} = a_1 \frac{r_1}{s_1} + ... + a_n \frac{r_n}{s_n}$ ma è impossibile perché si troverebbe $s_1 ... s_n = (a_1 r_1 s_2 ... s_n + ... + a_n r_n s_1 ... s_{n-1})p$. $\lightning$*

Definizione 1.9.2. *Se A è un gruppo abeliano isomorfo a $\mathbb{Z}^r$ per un $r \geq 1$ lo chiameremo* ***gruppo abeliano libero di rango*** *r.*

Nota: vedremo più avanti che il rango è univocamente definito, dunque è una buona definizione.

1.9.1 Successioni esatte di gruppi abeliani

La successione $\{0\} \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \{0\}$, dove A, B, C sono gruppi abeliani e f, g sono omomorfismi, si dice che è **esatta** se $Ker\, f = \{0\}$, $Imm\, f = Ker\, g$ e $Imm\, g = C$.

Esempio 7. *Data la successione $\{0\} \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{f} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{g} \mathbb{Z}/p\mathbb{Z} \longrightarrow \{0\}$, si ha che*

$$f\big([a]_p\big) = [pa]_{p^2} \ \text{e}\ g\big([b]_{p^2}\big) = [b]_p$$

quindi la successione è esatta ma non è vero che $\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proposizione 1.9.1. *Data*

$$\begin{tikzcd} \{0\} \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & \mathbb{Z} \arrow[r] \arrow[l, bend left, dashed, "\psi"] & \{0\} \end{tikzcd}$$

successione esatta, allora vale $B \cong A \oplus \mathbb{Z}\,(= A \times \mathbb{Z})$.

Dimostrazione. Visto che g è surgettivo, $\exists b \in B$ tale che $g(b) = 1$.
Costruiamo allora l'omomorfismo $\begin{array}{rccc} \psi: & \mathbb{Z} & \longrightarrow & B \\ & 1 & \longmapsto & b \end{array}$.
Notiamo che $g \circ \psi(1) = g(b) = 1$, cioè $g \circ \psi : \mathbb{Z} \longrightarrow \mathbb{Z}$ è l'identità.
Costruisco $\begin{array}{rccc} \Gamma: & A \times \mathbb{Z} & \longrightarrow & B \\ & (a, n) & \longmapsto & f(a) + \psi(n) \end{array}$: è immediato verificare che sia un omomorfismo.
Verifichiamo che Γ è surgettiva: sia $b' \in B$, consideriamo $g(b') = m \in \mathbb{Z}$ e $\psi(m) = mb$ che sono distinti ma con la stessa immagine per g. Notiamo che $g(b') = g\big(\psi(m)\big) = m$, dunque $g(b' - mb) = 0 \Longrightarrow b' - mb \in Ker\, g$, ma $Ker\, g = Imm\, f$ per l'esattezza, allora $\exists a \in A$ tale che $f(a) = b' - mb$, $b' = f(a) + mb = f(a) + \psi(m)$, dunque $\Gamma\big((a, m)\big) = f(a) + \psi(m) = b'$.
Verificare che Γ è iniettiva per esercizio. $\square$

Esercizio 30. *Consideriamo lo schema*

$$\begin{tikzcd} \{0\} \arrow[r] & M' \arrow[r, "\gamma"] \arrow[d, "f"] & M \arrow[r, "\gamma'"] \arrow[d, "g"] & M'' \arrow[r] \arrow[d, "h"] & \{0\} \\ \{0\} \arrow[r] & N' \arrow[r, "\delta"] & N \arrow[r, "\delta'"] & N'' \arrow[r] & \{0\} \end{tikzcd}$$

supponiamo che le successioni orizzontali siano esatte e che tutti i diagrammi commutino. Dimostrare che se due fra f, g, h sono isomorfismi, allora anche l'altro è isomorfismo.

⚠Attenzione!⚠
$$\begin{array}{ccccccccc} \{0\} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\gamma} & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\gamma'} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \{0\} \\ & & \Big\| Id & & \Big\downarrow g & & \Big\| Id & & \\ \{0\} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\delta} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\delta'} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \{0\} \end{array}$$
, prendendo ad esempio $\gamma(a) = (a, 0)$ e $\gamma'(c, d) = d$, $\nexists g$ centrale che fa commutare $\big($infatti $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \not\cong \mathbb{Z}/p^2\mathbb{Z}\big)$.

Proposizione 1.9.2. *Sia $M < \mathbb{Z}^n$, allora $M \cong \mathbb{Z}^r$ per un certo $0 \leq r \leq n$.*
"Un sottogruppo di un gruppo abeliano libero è un gruppo abeliano libero oppure è $\{0\}$."

Dimostrazione. Per induzione su $n \geq 1$.

Passo base: $n = 1$, $M < \mathbb{Z}$, allora $M = \begin{cases} \{0\} \\ d\mathbb{Z} \cong \mathbb{Z} \end{cases}$ come gruppo abeliano.

Passo induttivo: $n > 1$, sia $\pi : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ la proiezione sull'ultima coordinata.
Visto che $M < \mathbb{Z}^n$, consideriamo $\pi_{|_M} : M \longrightarrow \mathbb{Z}$.
Se vale $Imm\,\pi_{|_M} = \{0\}$, allora $M \subseteq \{(a_1, ..., a_{n-1}, 0) | a_1, ..., a_{n-1} \in \mathbb{Z}\} \cong \mathbb{Z}^{n-1}$, allora, per ipotesi induttiva, sappiamo che $M \cong \mathbb{Z}^r$ con $0 \leq r \leq n-1$.
Se vale $Imm\,\pi_{|_M} = d\mathbb{Z}$ ho $\{0\} \longrightarrow Ker\,\pi_{|_M} \xrightarrow{i} M \xrightarrow{\pi} d\mathbb{Z} \cong \mathbb{Z} \longrightarrow \{0\}$.
Per la **Proposizione 1.9.1.**, $M \cong Ker\,\pi_{|_M} \times d\mathbb{Z} \cong Ker\,\pi_{|_M} \times \mathbb{Z}$. Notiamo che $Ker\,\pi_{|_M} \subseteq T \cong \mathbb{Z}^{n-1}$, per ipotesi induttiva, $Ker\,\pi_{|_M} \cong \mathbb{Z}^r$ con $0 \leq r \leq n-1$.
Quindi $M \cong \mathbb{Z}^r \times \mathbb{Z} \cong \mathbb{Z}^{r+1}$, con $1 \leq r+1 \leq n$. □

Sia M un gruppo abeliano finitamente generato e siano $m_1, ..., m_n$ dei generatori.
$\begin{array}{cccc} \phi : & \mathbb{Z}^n & \longrightarrow & M \\ & (a_1, ..., a_n) & \longmapsto & a_1m_1 + ... + a_nm_n \end{array}$ è omomorfismo. ϕ è surgettivo perché $m_1, ..., m_n$ sono generatori. $\{0\} \longrightarrow Ker\,\phi \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\phi} M \longrightarrow \{0\}$, per il **Primo teorema di omomorfismo**, $M \cong \mathbb{Z}^n/Ker\,\phi$ e, per le **Proposizioni** precedenti, $Ker\,\phi \cong \mathbb{Z}^r$.

Esempio 8. *Se $n = 2$ e $Ker\,\phi = \big((2, 0), (0, 3)\big)$, allora $M \cong \mathbb{Z}^2/((2,0),(0,3)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

$\begin{array}{cccc} \theta : & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ & (a, b) & \longmapsto & \big([a]_2, [b]_3\big) \end{array}$ è omomorfismo surgettivo.
Chi è $Ker\,\theta$? $Ker\,\theta = \big((2, 0), (0, 3)\big) \Longrightarrow \mathbb{Z}^2/((2,0),(0,3)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Esercizio 31. *Sia G un gruppo di ordine pqr, con $p < q < r$ primi. Dimostrare che l'r-Sylow è normale in G.*

Dimostrazione. $n_r \mid pq$ e $n_r \equiv 1\,(r) \Longrightarrow n_r \in \{1, p, q, pq\}$.
Se non fosse $n_r = 1$, allora $n_r = 1 + rk$, con $k \geq 1$, cioè $n_r > r > q > p$. Resterebbe solo il caso $n_r = pq$.
Studiamo allora n_q: $n_q \mid pr$ e $n_q \equiv 1\,(q) \Longrightarrow n_q \in \{1, p, r, pr\}$.
Se non fosse $n_q = 1$, allora $n_q = 1 + qs$, con $s \geq 1$, cioè $n_q > q > p$. Resterebbero i due casi $n_q = r$ o $n_q = pr$.
In G ci sarebbero come minimo $r(q-1)$ elementi di ordine q. Complessivamente in G avremmo $\underbrace{pq(r-1)}_{\text{elementi di ordine } r} + \underbrace{n_q(q-1)}_{\text{elementi di ordine } q} \geq pq(r-1) + r(q-1) = pqr - pq + qr - r$.
Notiamo che $qr - pq - r > qr - pr - r \Longrightarrow pqr - pq + qr - r > pqr + r\underbrace{(q-p-1)}_{\geq 0}$ e dobbiamo ancora aggiungere gli elementi di ordine p. ↯

Dunque $n_q = 1 \Longrightarrow N_q \lhd G$, facciamo ${}^{G}/_{N_q} = \overline{G}$ gruppo di cardinalità pr. In $\overline{G}$ $\exists \overline{H}$ r-Sylow ed è normale perché ha indice p.
Consideriamo $\pi : G \longrightarrow \overline{G} = {}^{G}/_{N_q}$ surgettiva, $\pi^{-1}(\overline{H}) < G$ e, come sappiamo dal **Teorema di corrispondenza**, $\pi^{-1}(\overline{H})$ ha rq elementi. Sappiamo anche che $\pi^{-1}(\overline{H}) \lhd G$.
Dentro $\pi^{-1}(\overline{H})$ c'è un r-Sylow R. Vale che $R \lhd \pi^{-1}(\overline{H})$ perché ha indice q. Inoltre, da **Sylow II**, sappiamo che è l'unico sottogruppo di π^{-1} di ordine r. Allora osserviamo che:

- $gRg^{-1} \subseteq \pi^{-1}(\overline{H})$ per la normalità di $\pi^{-1}(\overline{H})$ in G;
- $gRg^{-1} = R$ perché in $\pi^{-1}(\overline{H})$ abbiamo un unico sottogruppo di ordine r.

In conlusione, abbiamo dimostrato che $\forall g \in G$ $gRg^{-1} = R$, cioè $R \lhd G$ $(*)$ ma è assurdo $\lightning$ perché eravamo nel caso $n_r = pq$. $\square$

$(*)$ Nota: Ricordiamoci che se $K \lhd H$ e $H \lhd G$ non è detto che $K \lhd G$ $\big($ad esempio $G = S_4$, $H = Klein$ e $K = \{e, (1,2)\}\big)$ ma se K è caratteristico in H e $H \lhd G$, allora vale $K \lhd G$. Ricordiamo a tal proposito che un sottogruppo M di un gruppo L si dice **caratteristico** se $\forall \psi \in Aut(L)$ $\psi(M) = M$.

Esempio 9. *Sia* $n = 3$, $Ker\,\phi = Span_{\mathbb{Z}} < \begin{pmatrix}2\\4\\2\end{pmatrix}, \begin{pmatrix}0\\4\\4\end{pmatrix}, \begin{pmatrix}0\\2\\8\end{pmatrix} >$ *che corrisponde alla matrice* $\begin{pmatrix}2&0&0\\4&4&2\\2&4&8\end{pmatrix}$.

Fare una mossa di riga intera corrisponde a moltiplicare a sinistra per una matrice invertibile a coefficienti interi (e con inversa a coefficienti interi).
Dunque fare mosse di riga intere corrisponde a cambiare base in arrivo e fare mosse di colonna intere corrisponde a cambiare base in partenza.

$$\begin{pmatrix}2&0&0\\4&4&2\\2&4&8\end{pmatrix} \xrightarrow[R_3\to R_3-R_1]{R_2\to R_2-2R_1} \begin{pmatrix}2&0&0\\0&4&2\\0&4&8\end{pmatrix} \xrightarrow{C_2\leftrightarrow C_3} \begin{pmatrix}2&0&0\\0&2&4\\0&8&4\end{pmatrix}$$

$$\begin{pmatrix}2&0&0\\0&2&4\\0&8&4\end{pmatrix} \xrightarrow{C_3\to C_3-2C_2} \begin{pmatrix}2&0&0\\0&2&0\\0&8&-12\end{pmatrix} \xrightarrow[C_3\to -C_3]{R_3\to R_3-4R_2} \begin{pmatrix}2&0&0\\0&2&0\\0&0&12\end{pmatrix}$$

Dunque nella nuova base di $\mathbb{Z}^3$ in arrivo, $Ker\,\phi = Span_{\mathbb{Z}} < \begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\0\\12\end{pmatrix} >$.
Perciò $M \cong {}^{\mathbb{Z}^3}/_{Ker\,\phi} \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{12\mathbb{Z}}$.

Teorema 1.9.3. *Data una matrice* $L \in \mathcal{M}(t, s, \mathbb{Z})$ *di rango* h, *è possibile, attraverso una sequenza di mosse intere di riga e/o di colonna, trasformarla nella matrice* L' *tale che*

- $L'_{ij} = 0$ *se* $i \neq j$;
- $L'_{ii} > 0$ *se* $i \leq h$;
- $L'_{ii} = 0$ *se* $i > h$;
- $L'_{11} = MCD(L_{11}, ..., L_{1s}, L_{21}, ..., L_{2s}, ..., L_{t1}, ..., L_{ts})$;

- $L'_{11} \mid L'_{22} \mid L'_{33} \mid ... \mid L'_{hh}$.

*Tale matrice L' è detta **Forma di Smith** di una matrice a coefficienti in $\mathbb{Z}$.*

Dimostrazione. (Traccia) Presa una matrice con un certo coefficiente, in modulo, più piccolo degli altri, ad esempio mettiamo che sia un 3, le applichiamo qualche operazione di riga/colonna:

$$\begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 3 \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \longrightarrow \begin{pmatrix} \cdot & \cdot & \cdot & 3 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

Adesso, se nella prima riga/colonna è presente un coefficiente coprimo con 3, ad esempio 7, applichiamo un'operazione di riga/colonna così da far comparire al suo posto il resto della divisione euclidea tra 7 e 3, cioè 1, e lo scambio col 3:

$$\begin{pmatrix} 3 & 7 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

A questo punto, con sufficienti operazioni di riga e di colonna, otteniamo la matrice

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

Iterando il procedimento con la sottomatrice arriviamo a una situazione del tipo

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

Cioè, più in generale,

$$\begin{pmatrix} MCD & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & d_h \end{pmatrix}$$

Sicuramente $d_2 \mid d_3 \mid ... \mid d_h$ e $d_1 = MCD \mid d_2$.
Studiare sulle dispense la dimostrazione formale. □

Teorema 1.9.4. *Sia M un gruppo finitamente generato, allora*

a) Vale che $M \cong \mathbb{Z}^k$, con $k \geq 0$, oppure
$M \cong \underbrace{\mathbb{Z}^k}_{\substack{\text{parte} \\ \text{libera}}} \oplus \underbrace{\bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}}_{\substack{\text{parte di} \\ \text{torsione}}}$*, dove $k \geq 0$, $d_i \geq 2$ interi, e, se $i < j$, vale $d_i \mid d_j$.*

Esempio 10. *$Ker\,\phi = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, $\mathbb{Z}^5/_{Ker\,\phi} \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}^2$, infatti*

$$\begin{array}{ccc} \mathbb{Z}^5 & \longrightarrow & \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z} \times \mathbb{Z} \\ (a_1, a_2, a_3, a_4, a_5) & \longmapsto & \big([a_1]_2, [a_2]_4, [a_3]_4, a_4, a_5\big) \end{array} \quad \textit{è isomorfismo.}$$

b) I numeri $k, d_1, d_2, ..., d_r$ sono univocamente determinati.

Il punto *b)* per ora non è dimostrato.
La parte di torsione può essere presentata anche in un altro modo:

$$\mathbb{Z}/_{6\mathbb{Z}} \times \mathbb{Z}/_{12\mathbb{Z}} \times \mathbb{Z}/_{48\mathbb{Z}} \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{16\mathbb{Z}} \cong (\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{16\mathbb{Z}}) \times (\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}})$$

Notiamo che un gruppo abeliano finito è prodotto dei suoi p-Sylow.

Esempio 11.

$$\left(\boxed{\mathbb{Z}/_{2\mathbb{Z}}} \times \boxed{\mathbb{Z}/_{2^2\mathbb{Z}}} \times \boxed{\mathbb{Z}/_{2^2\mathbb{Z}}}\right) \times \left(\boxed{\mathbb{Z}/_{7^2\mathbb{Z}}} \times \boxed{\mathbb{Z}/_{7^3\mathbb{Z}}}\right) \times \left(\boxed{\mathbb{Z}/_{11^4\mathbb{Z}}} \times \boxed{\mathbb{Z}/_{11^6\mathbb{Z}}}\right) \Longleftrightarrow \boxed{\mathbb{Z}/_{2\mathbb{Z}}} \times \boxed{\mathbb{Z}/_{2^2 7^2 11^4\mathbb{Z}}} \times \boxed{\mathbb{Z}/_{2^2 7^3 11^6\mathbb{Z}}}$$

Per dimostrare il punto *b)* del **Teorema 1.9.2.** (vedi paragrafo 8.2. delle dispense) basta dimostrare il seguente

Lemma 1.9.5. *Sia A un gruppo abeliano finito di ordine p^a con p primo e $a \geq 1$. Supponiamo che*

$$A \cong \mathbb{Z}/_{p^{\alpha_1}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p^{\alpha_j}\mathbb{Z}}, \ \textit{con } 1 \leq \alpha_1 \leq ... \leq \alpha_j$$

e anche che

$$A \cong \mathbb{Z}/_{p^{\beta_1}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p^{\beta_h}\mathbb{Z}}, \ \textit{con } 1 \leq \beta_1 \leq ... \leq \beta_h$$

allora $j = h$ e $\alpha_i = \beta_i \ \forall i = 1, ..., h$.

Dimostrazione. Contando gli elementi di ordine $\leq p$, deduciamo subito che $j = h$, perciò

$$A \cong \mathbb{Z}/_{p^{\alpha_1}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p^{\alpha_h}\mathbb{Z}} \text{ e } A \cong \mathbb{Z}/_{p^{\beta_1}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p^{\beta_h}\mathbb{Z}}$$

Supponiamo che $u \in \{1, ..., h\}$ sia il minimo tale che $\beta_u \neq \alpha_u$, cioè per esempio $\alpha_u > \beta_u$.
Consideriamo il sottogruppo H di A dato da $p^{\beta_u}A$, allora

$$H \cong 0 \times ... \times \mathbb{Z}/_{p^{\alpha_u - \beta_u}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p^{\alpha_h - \beta_u}\mathbb{Z}}$$

$$\text{e } H \cong 0 \times ... \times 0 \times \mathbb{Z}/_{p^{\beta_{u+1} - \beta_u}\mathbb{Z}} \times ... \times \mathbb{Z}/_{p^{\beta_h - \beta_u}\mathbb{Z}}$$

Si ottiene un assurdo contando gli elementi di ordine $\leq p$ di H. □

Se $A \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/_{d_i\mathbb{Z}}$ e $A \cong \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/_{c_i\mathbb{Z}}$, allora esiste

$$\phi : \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/_{d_i\mathbb{Z}} \longrightarrow \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/_{c_i\mathbb{Z}} \text{ isomorfismo.}$$

Osservazione 7. $\mathbb{Z}^k \xhookrightarrow{i} \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/_{d_i\mathbb{Z}} \xrightarrow{\phi} \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/_{c_i\mathbb{Z}} \xrightarrow{\pi} \mathbb{Z}^s$

Studiare i dettagli sulle dispense.

1.10 Viaggio nei gruppi di ordine 24

1.10.1 Capitolo 1

Se $n_2 \neq 1$ e $n_3 \neq 1$, allora $G \cong S_4$. Infatti $n_3 \mid 8$ e $n_3 \equiv 1\,(3) \Longrightarrow$ visto che $n_3 \neq 1$, vale $n_3 = 4$.
Sia $X = \{P_1, P_2, P_3, P_4\}$ l'insieme dei 3-Sylow: G agisce su X per coniugio.
$\Gamma : G \longrightarrow Big(X) \cong S_4$, basta osservare che Γ è iniettivo.
Studiamo gli elementi g tali che $\Gamma(g) = e$ per capire chi sia $Ker\,\Gamma$: sono i g tali che si ha $gP_ig^{-1} = P_i \ \forall i = 1, 2, 3, 4$, cioè $Ker\,\Gamma = \bigcap_{i=1}^{4} N(P_i)$.
Per **Sylow II**, $|N(P_1)| = |N(P_2)| = |N(P_3)| = |N(P_4)| = \frac{|G|}{4} = 6 \Longrightarrow \#Ker\,\Gamma \mid 6$.

- Se fosse $|Ker\,\Gamma| = 3$:
  $Ker\,\Gamma \subseteq N(P_1)$ che ha 6 elementi, dunque ha un 3-Sylow che è $Ker\,\Gamma$ ed è anche P_1.
  $Ker\,\Gamma \subseteq N(P_2)$ che ha 6 elementi, dunque ha un 3-Sylow che è $Ker\,\Gamma$ ed è anche P_2. $\lightning$

- Se fosse $|Ker\,\Gamma| = 6$:

$$Ker\,\Gamma = \underbrace{N(P_1)}_{\substack{\text{ha un unico}\\ \text{3-Sylow: } P_1}} = \underbrace{N(P_2)}_{\substack{\text{ha un unico}\\ \text{3-Sylow: } P_2}} = \underbrace{N(P_3)}_{\substack{\text{ha un unico}\\ \text{3-Sylow: } P_3}} = \underbrace{N(P_4)}_{\substack{\text{ha un unico}\\ \text{3-Sylow: } P_4}} \Longrightarrow \lightning$$

- Se fosse $|Ker\,\Gamma| = 2$: $Ker\,\Gamma = \{e, x\}$, con x di ordine 2.

  Osservazione 8. *$x \in Z(G)$ perchè $Ker\,\Gamma \lhd G$, infatti $\forall g \in G \ gxg^{-1} \in Ker\,\Gamma \Longrightarrow$*

$$gxg^{-1} = \begin{cases} \nearrow e & \textit{No, } x = g^{-1}eg = e \ \lightning \\ \searrow x & \end{cases} \Longrightarrow \forall g \in G \ gxg^{-1} = x.$$

  Allora contiamo in G gli elementi di ordine 3: stanno in P_1, P_2, P_3, P_4 quindi sono $2 \cdot 4 = 8$.
  Sia y uno di questi 8 elementi di ordine 3.
  Consideriamo xy: ha ordine 6, quindi produciamo in questo modo 8 elementi di ordine 6.
  In G restano dunque $24 - 8 - 8 = 8$ elementi di ordine $\neq 3$ e $\neq 6$, quindi, per **Sylow I**, questi 8 elementi devono costituire l'unico 2-Sylow possibile ma questo è assurdo perché avevamo supposto $n_2 \neq 1$.

- In conclusione, $|Ker\,\Gamma| = 1$, cioè $Ker\,\Gamma = \{e\}$. $\square$

1.10.2 Capitolo 2. Alcuni prodotti del tipo $H \rtimes \mathbb{Z}/3\mathbb{Z}$ con $|H| = 8$

Se $n_2 = 1$ oppure $n_3 = 1$ si vede subito che G (di ordine 24) è prodotto semidiretto dei suoi Sylow. Studiamo in questo capitolo il caso $n_2 = 1$.

$$N_2 \cong \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ Q_8 \text{ e } N_3 \cong \mathbb{Z}/3\mathbb{Z}$$

Cominciamo con $\mathbb{Z}/8\mathbb{Z} \rtimes_\tau \mathbb{Z}/3\mathbb{Z}$:

$$\begin{array}{rccc} \tau : & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & Aut(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & \underset{\text{ord } 3}{1} & \longmapsto & Id = (0,0) \end{array} \Longrightarrow \begin{array}{c}\text{allora esiste solo}\\ \text{il } \tau \text{ banale}\end{array} \Longrightarrow G \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/24\mathbb{Z}$$

Studiamo adesso $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes_\tau \mathbb{Z}/3\mathbb{Z}$:

$$Aut\big((\mathbb{Z}/2\mathbb{Z})^3\big) \cong GL_3(\mathbb{Z}/2\mathbb{Z}) \qquad \Big(\big|GL_3(\mathbb{Z}/2\mathbb{Z})\big| = (2^3-1)(2^3-2)(2^3-2^2) = 168\Big)$$

Questa volta in $Aut\big((\mathbb{Z}/2\mathbb{Z})^3\big)$ ci sono elementi di ordine 3, perciò

$$\begin{array}{rccc} \tau: & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & GL_3(\mathbb{Z}/2\mathbb{Z}) \\ & 1 & \longmapsto & M \end{array}, \text{ con } M^3 = Id \text{ e } M \neq Id.$$

$M^3 - Id = 0 \Longrightarrow (M - Id)(M^2 + M + Id) = 0$. Sia f un'applicazione lineare associata a M.
$(f - Id)(f^2 + f + Id) = 0$, vale che $Ker(f - Id) \oplus Ker(f^2 + f + Id) = (\mathbb{Z}/2\mathbb{Z})^3$
$(t - 1)$ e $(t^2 + t + 1)$ sono primi tra loro in $\mathbb{Z}/2\mathbb{Z}[t]$.
Per **Bezout**, $\lambda(t)(t - 1) + \mu(t)(t^2 + t + 1) = 1 \Longrightarrow \lambda(f)(f - Id) + \mu(f)(f^2 + f + Id) = Id \Longrightarrow$

$$\underbrace{\lambda(f)(f - Id)v}_{\in Ker(f^2+f+Id)} + \underbrace{\mu(f)(f^2 + f + Id)v}_{\in Ker(f-Id)} = v$$

Potrebbe essere che uno dei due, ad esempio, $Ker(f^2 + f + Id) = \{0\}$? NO, perché altrimenti $Ker(f - Id) = (\mathbb{Z}/2\mathbb{Z})^3$ e dunque $f = Id$ mentre $M \neq Id$.
Quindi $\exists w \in Ker(f^2 + f + Id)$ tale che $w \neq 0$. Consideriamo $f(w)$ e notiamo che w e $f(w)$ sono linearmente indipendenti (perché i multipli di w sono 0 e w e si escludono entrambi i casi).
Scegliamo per completamento una base $u, w, f(w)$ di $(\mathbb{Z}/2\mathbb{Z})^3$

$$\begin{array}{c} \begin{array}{ccc} f(u) & f(w) & f^2(w) \end{array} \\ \begin{pmatrix} a & 0 & 0 \\ b & 0 & 1 \\ c & 1 & 1 \end{pmatrix} \end{array} \quad \text{perché } f^2 + f + Id = 0,\ f^2(w) + f(w) + Id(w) = 0 \Longrightarrow f^2(w) = -f(w) - w \overset{\text{in } \mathbb{Z}/2\mathbb{Z}}{=} f(w) + w$$

Dato che f è invertibile, deve essere $a = 1 \Longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ b & 0 & 1 \\ c & 1 & 1 \end{pmatrix}$ e, dal polinomio caratteristico, si vede che 1 è autovalore. Scegliamo allora al posto di u un autovettore u' di autovalore 1:

$$\underbrace{u',}_{\in Ker(f-Id)} \quad \underbrace{w, \quad f(w)}_{\in Ker(f^2+f+Id)} \text{ quindi, rispetto a questa base, ottengo la matrice } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Quindi, a meno di coniugio, possiamo immaginare che $\tau(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.
Per la **Proposizione 1.5.4.** $\alpha \circ \tau_2(k) \circ \alpha^{-1} = \tau_1\big(\beta(k)\big)$ esiste dunque, a meno di isomorfismo, un solo prodotto semidiretto del tipo $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes_\tau \mathbb{Z}/3\mathbb{Z}$.

Troviamo adesso concretamente questo gruppo: consideriamo $\mathbb{Z}/2\mathbb{Z} \times A_4$, $\mathbb{Z}/2\mathbb{Z} \times Klein < \mathbb{Z}/2\mathbb{Z} \times A_4$. Dunque $\mathbb{Z}/2\mathbb{Z} \times Klein$ è un 2-Sylow $\big($ed è $\cong (\mathbb{Z}/2\mathbb{Z})^3\big)$.
Contando gli ordini, vediamo che esistono in $\mathbb{Z}/2\mathbb{Z} \times A_4$ esattamente 8 elementi di ordine ≤ 2 e quindi $\mathbb{Z}/2\mathbb{Z} \times Klein$ è l'unico 2-Sylow. Perciò è proprio il gruppo descritto.

Esercizio 32. *Ogni gruppo semplice di ordine 60 ha un sottogruppo di ordine 12.*

Dimostrazione. Per la semplicità del gruppo si ha $n_5 > 1 \Longrightarrow n_5 = 6$ e ci sono quindi $6 \cdot 4 = 24$ elementi di ordine 5.
Se fosse $n_2 = 15$ avremmo i 2-Sylow $B_1, B_2, ..., B_{15}$: se fosse inoltre che $B_i \cap B_j = \{e\}\ \forall i, j$ avremmo 45 elementi di ordine 2 o 4 mentre dovrebbe valere $|G| \geq 24 + 45 + 1...$ ↯
Dunque $\exists i, j$ tali che $|B_i \cap B_j| = 2$. Consideriamo $N(B_i \cap B_j)$,

$$\begin{matrix} B_i \cap B_j \lhd B_i \\ B_i \cap B_j \lhd B_j \end{matrix} \quad \text{(perché } B_i \text{ è abeliano, oppure perché } B_i \cap B_j \text{ ha indice 2...)}$$

Allora $B_i < N(B_i \cap B_j)$ e $B_j < N(B_i \cap B_j)$, quindi anche

$$\underset{\substack{\text{prodotto} \\ \text{di insieme}}}{B_i B_j} \subseteq N(B_i \cap B_j) \text{ ma } |B_i B_j| = \frac{4 \cdot 4}{2} = 8$$

Dunque sappiamo che $8 \leq \#N(B_i \cap B_j) \mid 60$ e $4 \mid \#N(B_i \cap B_j)$ perché $B_i < N(B_i \cap B_j) \Longrightarrow \#N(B_i \cap B_j) \in \{12, 20, 60\}$:

60: NO, perché sarebbe che $N(B_i \cap B_j) = G$ cioè $B_i \cap B_j \lhd G$ ma G è semplice;

20: NO, perché consideriamo l'azione di G su ${}^{G}/_{N(B_i \cap B_j)}$ e abbiamo un omomorfismo: $\Gamma : G \longrightarrow Big\big({}^{G}/_{N(B_i \cap B_j)}\big) \cong S_3$ deve essere $Ker\,\Gamma = \{e\}$ per semplicità di G (ricordiamo che $Ker\,\Gamma = G$ non va bene per questo tipo di azione), ↯ per motivi di cardinalità.

□

Nota: potevamo direttamente usare il

Teorema 1.10.1 (dell'indice).
Se in un gruppo G c'è un sottogruppo H di indice h tale che $|G| \nmid h!$, allora G non è semplice.

Dimostrazione. $G \curvearrowright {}^{G}/_{H}$, $\Gamma : G \longrightarrow Big({}^{G}/_{H}) \cong S_h$, se G fosse semplice, $Ker\,\Gamma = \{e\}$ e dunque $\Gamma(G) \cong G$ ma $\Gamma(G) < S_h$ e dunque $\#G = \#\Gamma(G) \mid h!$ ↯ □
$\Longrightarrow$ per esclusione $|N(B_i \cap B_j)| = 12$ ☺
Se invece $n_2 = 3$ o $n_2 = 5$, prendiamo N_2 un 2-Sylow, allora $|N(N_2)| = \frac{|G|}{n_2} = \frac{60}{n_2} \neq 4$ in entrambi i casi. Dato che $N_2 < N(N_2)$ vale che $4 \mid \#N(N_2) \mid 60$, dunque $|N(N_2)| \in \{12, 20, 60\}$.
Esattamente come prima si conclude che $|N(N_2)| = 12$. □

Esercizio 33. *Se G è semplice di ordine 60, allora $G \cong A_5$.*

Dimostrazione. Sia $H < G$ con $|H| = 12$ (esiste per l'esercizio precedente). Consideriamo l'azione di G su ${}^{G}/_{H}$ $\Gamma : G \longrightarrow Big({}^{G}/_{H}) \cong S_5$. $Ker\,\Gamma = \{e\}$ perché G è semplice, dunque $\Gamma(G)$ ha 60 elementi ed è $\Gamma(G) < S_5$.
Perciò o $\Gamma(G) \leq A_5$ nel qual caso $\Gamma(G) = A_5$, o $|\Gamma(G) \cap A_5| = 30$ ↯↯ perché, avendo indice 2, sarebbe un sottogruppo normale di A_5 e di $\Gamma(G)$ mentre sono entrambi semplici. □

Esercizio 34. *Quali sono i gruppi del tipo ${}^{\mathbb{Z}}/_{4\mathbb{Z}} \rtimes {}^{\mathbb{Z}}/_{4\mathbb{Z}}$?*

Dimostrazione. $\begin{matrix} \tau_{ban} : & {}^{\mathbb{Z}}/_{4\mathbb{Z}} & \longrightarrow & Aut({}^{\mathbb{Z}}/_{4\mathbb{Z}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \\ & 1 & \longmapsto & Id = 0 \end{matrix}$ che dà il prodotto diretto ${}^{\mathbb{Z}}/_{4\mathbb{Z}} \times {}^{\mathbb{Z}}/_{4\mathbb{Z}}$.
$\begin{matrix} \tau_1 : & {}^{\mathbb{Z}}/_{4\mathbb{Z}} & \longrightarrow & Aut({}^{\mathbb{Z}}/_{4\mathbb{Z}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \\ & 1 & \longmapsto & -Id = 1 \end{matrix}$, consideriamo dunque $G = {}^{\mathbb{Z}}/_{4\mathbb{Z}} \rtimes_{\tau_1} {}^{\mathbb{Z}}/_{4\mathbb{Z}}$ che ha ordine 16.
Usiamo la notazione $x^a y^b = (a, b) \in G$.

$G = (x)(y)$, con $(x) \lhd G$, dove $x = (1,0)$ e $y = (0,1) \Longrightarrow x^4 = (0,0)$ e $y^4 = (0,0)$.
Ci interessa sapere quanto vale yxy^{-1}:

$$yx = (0,1)(1,0) = \Big(0 + \tau_1\big(1\big)(1), 1 + 0\Big) = (-1,1) = x^{-1}y$$

Dunque $yxy^{-1} = x^{-1}$.
La potevamo pensare anche: $yx = \underbrace{yxy^{-1}}_{\in(x)} y = x^a y$ perché $(x) \lhd G$.

Dunque il nostro gruppo $G = \mathbb{Z}/4\mathbb{Z} \rtimes_{\tau_1} \mathbb{Z}/4\mathbb{Z}$ è generato da x, y con le relazioni $x^4 = e$, $y^4 = e$, $yxy^{-1} = x^{-1}$. $\square$

Domande: ① Chi è il centro? Risposta: (x^2, y^2)
② Chi è $G/(x^2)$?
③ Chi è $G/(y^2)$?
④ Chi è $G/(x^2y^2)$?

1.10.3 Capitolo 3. Automorfismi di gruppi di ordine 8

$\boxed{Aut\big((\mathbb{Z}/2\mathbb{Z})^3\big)}$ Dal momento che $\mathbb{Z}/2\mathbb{Z}$ è un campo e quindi $(\mathbb{Z}/2\mathbb{Z})^3$ è anche uno spazio vettoriale, si ha che $Aut\big((\mathbb{Z}/2\mathbb{Z})^3\big) \cong GL_3(\mathbb{Z}/2\mathbb{Z}) = GL_3(\mathbb{F}_2)$ e $|GL_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168$.

$\boxed{Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})}$ In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ abbiamo 1 elemento di ordine 1, 3 di ordine 2 e 4 di ordine 4. $(1,0)$, che ha ordine 2, deve andare in un elemento di ordine 2 ma non può andare ad esempio in $(0,2)$ perché $<(0,2)>$ è un sottogruppo caratteristico di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, quindi

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ (0,1) & \longmapsto & \text{uno dei 4 elementi di ordine 4} \\ (1,0) & \longmapsto & \text{uno dei 2 elementi di ordine 2 rimasti} \end{array} \Longrightarrow 8 \text{ possibili automorfismi}$$

$$\begin{tikzcd} \mathbb{Z} \times \mathbb{Z} \arrow[r, "\tilde{f}"] \arrow[d, "/<\binom{2}{0},\binom{0}{4}>"] & \mathbb{Z} \times \mathbb{Z} \arrow[d, "/<\binom{2}{0},\binom{0}{4}>"] \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \arrow[r, "f"] \arrow[d, "/\binom{0}{2}"] & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \arrow[d, "/\binom{0}{2}"] \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[r, "\overline{f}"] & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{tikzcd}$$

$\tilde{f} : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ lo possiamo esprimere con una matrice del tipo $\begin{pmatrix} a & b \\ 2c & d \end{pmatrix}$ (la prima colonna garantisce che $f\binom{1}{0}$ abbia ordine 2): a, b ci interessano "*mod* 2" e $2c, d$ ci interessano "*mod* 4". L'isomorfismo $\overline{f} \in Aut\big((\mathbb{Z}/2\mathbb{Z})^2\big)(\cong S_3)$ lo possiamo esprimere con una matrice della forma $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, perché $2c \equiv 0\,(2)$ $\forall c$ e vogliamo che la matrice sia invertibile, quindi $a \equiv 1\,(2)$ e $d \equiv 1\,(2)$, perciò, dal momento che ogni isomorfismo in $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$ induce un isomorfismo in $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, otteniamo

$$\begin{pmatrix} a & b \\ 2c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \Longrightarrow \begin{array}{c} a=1 \;\; b=0,1 \;\; c=0,1 \;\; d=1,3 \Longrightarrow \\ 1 \cdot 2 \cdot 2 \cdot 2 = 8 \text{ automorfismi possibili} \end{array}$$

Se $\alpha = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$, allora $\alpha^2 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \Longrightarrow \alpha^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, cioè α ha ordine 4.
Se $\beta = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, allora $\beta^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, cioè β ha ordine 2.
Si vede che α e β non commutano $\Longrightarrow Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \cong D_4$.

Esercizio 35. *Quanti sono gli* $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$*? Quanti sono gli* $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})$*?*

$\boxed{Aut(D_4)}$ Studiamoli più in generale per $D_n =< r, s \,|\, r^n = s^2 = 1, srs = r^{-1} >$, con $n > 2$. Gli elementi di ordine n generano un sottogruppo ciclico, di ordine n e caratteristico (chiamiamolo K), quindi un isomorfismo $f \in Aut(D_n)$ dovrà mandare ogni elemento di K in un elemento di K e ogni elemento che non sta in K in un elemento che non sta in K, cioè

$$\begin{array}{rccl} f: & D_n & \longrightarrow & D_n \\ & s & \longmapsto & sr^i \quad i = 0, ..., n-1 \\ & r & \longmapsto & r^j \quad MCD(j,n) = 1. \end{array}$$

Quindi possiamo "sperare" di trovare al più $n \cdot \phi(n)$ automorfismi.
Basta verificare che $\forall i, j \ f : D_n \longrightarrow D_n$ determina un automorfismo.

- Descriviamo f su tutti gli elementi: $f(s^a r^b) = (sr^i)^a r^{bj}$, con $a = 0, 1$ e $b = 0, ..., n-1$.
- Verifichiamo che f sia un omomorfismo: $f(s^a r^b) f(s^{a'} r^{b'}) = f(s^a r^b s^{a'} r^{b'})$:
  - Se $a = a' = 0$,
  $$f(r^b) f(r^{b'}) = r^{bj} r^{b'j} = r^{(b+b')j} = f(r^b r^{b'});$$
  - Se $a = 0$ e $a' = 1$,
  $$f(r^b) f(sr^{b'}) = r^{bj} sr^i r^{b'j} = sr^{-bj} r^i r^{b'j} = sr^i r^{(-b+b')j} = f(sr^{-b} r^{b'}) = f(r^b sr^{b'});$$
  - Se $a = 1$ e $a' = 0$, per esercizio;
  - Se $a = a' = 1$, per esercizio.
- Verifichiamo che f sia bigettivo: andando da un insieme in se stesso basta verificare, ad esempio, che sia suriettivo:
  $r^j \in Imm\, f \Longrightarrow < r^j > \subseteq Imm\, f \Longrightarrow < r > \subseteq Imm\, f$, inoltre $sr^i \notin < r >$ e $sr^i \in Imm\, f$ $\Longrightarrow |Imm\, f| \geq 2n$ e $Imm\, f < D_n \Longrightarrow Imm\, f = D_n \Longrightarrow f$ è bigettiva.

Descriviamo meglio questi $n \cdot \phi(n)$ automorfismi: se abbiamo $f \in Aut(D_n)$, posso cercare di guardare cosa fa soltanto sugli elementi di ordine 2 fuori dal sottogruppo ciclico K di ordine n: sappiamo che $f(sr^a) = sr^i r^{aj} = sr^{i+aj}$, quindi abbiamo una funzione $\begin{array}{cccc} \varphi_{ij}: & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & a & \longmapsto & aj+i \end{array}$ con $j \in (\mathbb{Z}/n\mathbb{Z})^*$ e $i \in \mathbb{Z}/n\mathbb{Z}$, che risulta analogo a trasformare la retta reale usando una funzione del tipo $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax+b \end{array}$, con $a \neq 0$ e $b \in \mathbb{R}$: essa è una trasformazione affine su $\mathbb{R}$, quindi anche noi stiamo facendo una trasformazione affine su $\mathbb{Z}/n\mathbb{Z} \Longrightarrow$

$$Aut(D_n) \cong Aff(\mathbb{Z}/n\mathbb{Z})$$

Se abbiamo una trasformazione affine, possiamo vedere cosa succede solo al suo coefficiente moltiplicativo (cioè "quanto dilata le cose") con l'omomorfismo $\begin{array}{cccc} \pi: & Aff(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ & \varphi_{ij} & \longmapsto & j \end{array}$.
$Ker\, \pi$ è formato da tutte le trasformazioni con $j = 1$, cioè $Ker\, \pi$ è formato dalle traslazioni semplici di $\mathbb{Z}/n\mathbb{Z}$, quindi $Ker\, \pi = \mathbb{Z}/n\mathbb{Z}$. Perciò c'è una successione esatta corta

$$\begin{tikzcd} \mathbb{Z}/n\mathbb{Z} \arrow[r, hook] & Aff(\mathbb{Z}/n\mathbb{Z}) \arrow[r] & (\mathbb{Z}/n\mathbb{Z})^* \arrow[l, bend left] \end{tikzcd}$$

in cui $\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & Aff(\mathbb{Z}/n\mathbb{Z}) \\ j & \longmapsto & \varphi_{0j} \end{array}$ (dove $\varphi_{0j}(a) = aj$) è omomorfismo.
Quindi abbiamo appena mostrato che

$$Aut(D_n) \cong Aff(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\bullet} (\mathbb{Z}/n\mathbb{Z})^*$$

Come agisce $(\mathbb{Z}/n\mathbb{Z})^*$ su $\mathbb{Z}/n\mathbb{Z}$?
Proviamo a coniugare la "traslazione di i", cioè φ_{i1}, con la "moltiplicazione per j", cioè φ_{0j}:

$$\varphi_{0j} \circ \varphi_{i1} \circ \varphi_{0j}^{-1}(a) = \varphi_{0j} \circ \varphi_{i1}(aj^{-1}) = \varphi_{0j}(aj^{-1} + i) = a + ij$$

Con questo coniugio abbiamo fatto una traslazione di ij.
Quindi $(\mathbb{Z}/n\mathbb{Z})^*$ agisce su $\mathbb{Z}/n\mathbb{Z}$ per moltiplicazione.

Se abbiamo una successione esatta corta di gruppi (non necessariamente abeliani)

$$\begin{tikzcd}
\{0\} \arrow[r] & N \arrow[r, hook, "\alpha"] \arrow[d, equal] & G \arrow[r, two heads, "\beta"] & K \arrow[r] \arrow[l, bend left, "\beta'"] \arrow[d, equal] & \{0\} \\
\{0\} \arrow[r] & N \arrow[r] & N \rtimes_\varphi K \arrow[r] \arrow[u, "\gamma", "\wr"'] & K \arrow[r] & \{0\}
\end{tikzcd}$$

tale che $\beta\big(\beta'(k)\big) = k$, con β' omomorfismo di gruppi.
equivale a dire che $G \cong N \rtimes_\varphi H$. Chi è $\varphi : K \longrightarrow Aut(N)$?
Prendiamo $k \in K$ e $n \in N$, $\varphi_k(n) = \alpha^{-1}\big(\underbrace{\beta'(k)\alpha(n)\beta'(k)^{-1}}_{knk^{-1}}\big) \in N$.

Sicuramente $\varphi_k \in Aut(N)$ ✓
Diciamo anche che $\varphi : K \longrightarrow Aut(N)$ è un omomorfismo: cioè vorremmo $\varphi_k\big(\varphi_{k'}(n)\big) = \varphi_{kk'}(n)$:

$$\varphi_k\big(\varphi_{k'}(n)\big) = \alpha^{-1}\Big(\beta'(k)\alpha\big(\varphi_{k'}(n)\big)\beta'(k)^{-1}\Big) = \alpha^{-1}\big(\beta'(k)\beta'(k')\alpha(n)\beta'(k')^{-1}\beta'(k)^{-1}\big) =$$

$$= \alpha^{-1}\big(\beta'(kk')\alpha(n)\beta'(kk')^{-1}\big) = \varphi_{kk'}(n) \checkmark$$

Vogliamo quindi definire $\begin{array}{cccc} \gamma : & N \rtimes_\varphi K & \longrightarrow & G \\ & (n,k) & \longmapsto & \alpha(n)\beta'(n) \end{array}$ e dobbiamo verificare che sia un omomorfismo:

$$\gamma\big((n_1,k_1)\cdot(n_2,k_2)\big) = \gamma\big(n_1\varphi_{k_1}(n_2), k_1k_2\big) = \alpha\big(n_1\varphi_{k_1}(n_2)\big)\beta'(k_1k_2) =$$

$$= \alpha(n_1)\alpha\big(\varphi_{k_1}(n_2)\big)\beta'(k_1)\beta'(k_2) = \alpha(n_1)\beta'(k_1)\alpha(n_2)\cancel{\beta'(k_1)^{-1}}\cancel{\beta'(k_1)}\beta'(k_2) =$$
$$\alpha(n_1)\beta'(k_1)\alpha(n_2)\beta'(k_2) = \gamma(n_1,k_1)\gamma(n_2,k_2) \checkmark$$

$\boxed{Aut(Q_8)}$ Ricordiamo che $Q_8 =< i,j >= \{1,-1,i,j,-i,-j,k=ij,-k=ji\}$, quindi un $\varphi \in Aut(Q_8)$ manda l'elemento i, che ha ordine 4, in un qualsiasi elemento di ordine 4 di Q_8 (6 scelte) e l'elemento j, che ha anche lui ordine 4, in un elemento di ordine 4 di Q_8 ma non in $\varphi(i)$ né in $\varphi(-i)$ (4 scelte), quindi

$$|Aut(Q_8)| \leq 6\cdot 4 = 24$$

Consideriamo quindi i tre sottoinsiemi di Q_8 $L_1 = \{i,-i\}$, $L_2 = \{j,-j\}$ e $L_3 = \{k,-k\}$, allora un qualsiasi $\varphi \in Aut(Q_8)$ permuta tra loro questi tre insiemi, cioè abbiamo un omomorfismo

$$\pi : Aut(Q_8) \longrightarrow S_3$$

π è suriettivo: infatti le immagini rispetto a π dei seguenti automorfismi di Q_8 generano S_3:

$$\pi\left(\begin{cases} i \longmapsto j \\ j \longmapsto i \\ k \longmapsto -k \end{cases}\right) = (1,2) \quad \text{e} \quad \pi\left(\begin{cases} i \longmapsto j \\ j \longmapsto k \\ k \longmapsto i \end{cases}\right) = (1,2,3)$$

Vediamo che $Ker\,\pi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, infatti è generato da $\begin{cases} i \longmapsto -i \\ j \longmapsto j \\ k \longmapsto -k \end{cases}$ e $\begin{cases} i \longmapsto i \\ j \longmapsto -j \\ k \longmapsto -k \end{cases}$ che hanno chiaramente entrambi ordine 2.
Perciò abbiamo scoperto che c'è una successione esatta corta del tipo

$$\{0\} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow Aut(Q_8) \twoheadrightarrow S_3 \longrightarrow \{0\}$$

Vorremmo quindi dire che $Aut(Q_8) \cong S_4$: costruiamo un cubo ai cui vertici mettiamo le triple costituite da un elemento di L_1, un elemento di L_2 e un elemento di L_3.

$$
\begin{tikzcd}[arrows=-]
& \{i,-j,k\} \arrow[rr] \arrow[dl] \arrow[dd, dashed] & & \{-i,-j,k\} \arrow[dl] \arrow[dd] \\
\{i,j,k\} \arrow[rr] \arrow[dd] & & \{-i,j,k\} \arrow[dd] & \\
& \{i,-j,-k\} \arrow[rr, dashed] \arrow[dl, dashed] & & \{-i,-j,-k\} \arrow[dl] \\
\{i,j,-k\} \arrow[rr] & & \{-i,j,-k\} &
\end{tikzcd}
$$

Vogliamo trovare un isomorfismo tra $Aut(Q_8)$ e S_4, cioè vogliamo far agire $Aut(Q_8)$ su un insieme di 4 elementi, ad esempio l'insieme formato dalle diagonali del cubo. Consideriamo quindi insiemi del tipo $\big\{\{-i,j,-k\},\{i,-j,k\}\big\}$ in cui esplicitiamo due vertici opposti del cubo e quindi determiniamo univocamente una diagonale. Adesso consideriamo:

- $\begin{cases} i \longmapsto j \\ j \longmapsto k \\ k \longmapsto i \end{cases} \in Aut(Q_8)$ fissa $\big\{\{i,j,k\},\{-i,-j,-k\}\big\}$ e permuta le altre 3 diagonali ciclicamente, quindi ci dà un 3-ciclo in S_4;

- $\begin{cases} i \longmapsto -i \\ j \longmapsto j \\ k \longmapsto -k \end{cases} \in Ker\,\pi$ manda $\begin{matrix} \big\{\{i,j,k\},\{-i,-j,-k\}\big\} \longleftrightarrow \big\{\{-i,j,-k\},\{i,-j,k\}\big\} \\ \big\{\{i,j,-k\},\{-i,-j,k\}\big\} \longleftrightarrow \big\{\{-i,j,k\},\{i,-j,-k\}\big\} \end{matrix}$, quindi ci dà un 2-2-ciclo in S_4;

- $\begin{cases} i \longmapsto j \\ j \longmapsto i \\ k \longmapsto -k \end{cases} \in Aut(Q_8)$ manda $\big\{\{i,j,k\},\{-i,-j,-k\}\big\} \longmapsto \big\{\{i,j,-k\},\{-i,-j,k\}\big\}$ e lascia fisse le altre 2 diagonali, quindi ci dà un 2-ciclo in S_4;

- $\begin{cases} i \longmapsto j \\ j \longmapsto -i \\ k \longmapsto k \end{cases} \in Aut(Q_8)$ manda $\big\{\{i,j,k\},\{-i,-j,-k\}\big\} \longmapsto \big\{\{-i,j,k\},\{i,-j,-k\}\big\}$ $\longmapsto \big\{\{-i,-j,k\},\{i,j,-k\}\big\} \longmapsto \big\{\{i,-j,k\},\{-i,j,-k\}\big\} \longmapsto \big\{\{i,j,k\},\{-i,-j,-k\}\big\}$, quindi ci dà un 4-ciclo in S_4.

Facendo agire $Aut(Q_8)$ sull'insieme delle 4 diagonali del cubo abbiamo scoperto di avere un omomorfismo $g : Aut(Q_8) \longrightarrow S_4$ la cui immagine contiene un 2-ciclo, un 2-2-ciclo, un 3-ciclo e un 4-ciclo.

Esercizio 36. *$Imm\, g = S_4$.*

$\boxed{Aut(\mathbb{Z}/8\mathbb{Z})}$ Sappiamo già che $Aut(\mathbb{Z}/2^n\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ e che $Aut(\mathbb{Z}/p^n\mathbb{Z}) \cong \big(\mathbb{Z}/p\mathbb{Z}\big)^* \times \mathbb{Z}/p^{n-1}\mathbb{Z}$, con p primo dispari, quindi $Aut(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Esercizio 37. *Per quali valori di n il gruppo $Aut(\mathbb{Z}/n\mathbb{Z})$ è ciclico?*

Se n è diviso da almeno due primi dispari distinti, è della forma $n = 2^a p_1^{b_1} \cdot ... \cdot p_h^{b_h}$, con $p_1, ..., p_h$ primi dispari e $b_1, ..., b_h \geq 1$, allora

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/2^a\mathbb{Z} \times \mathbb{Z}/p_1^{b_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_h^{b_h}\mathbb{Z} \Longrightarrow Aut(\mathbb{Z}/n\mathbb{Z}) \cong Aut(\mathbb{Z}/2^a\mathbb{Z}) \times Aut(\mathbb{Z}/p_1^{b_1}\mathbb{Z}) \times ... \times Aut(\mathbb{Z}/p_h^{b_h}\mathbb{Z})$$

Notiamo che $\mathbb{Z}/2\mathbb{Z} \subseteq Aut(\mathbb{Z}/p_i^{b_i}\mathbb{Z})$ $\forall i = 1, ..., h$, quindi ci restringiamo al caso $n = 2^a p^b$, con p primo dispari. Dal momento che $Aut(\mathbb{Z}/2\mathbb{Z}) \cong \{0\}$ e $Aut(\mathbb{Z}/2^2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, gli n possibili sono

$$\boxed{n = 1, 2, 4, p^m, 2p^m}, \text{ con } p \text{ primo dispari.}$$

Definizione 1.10.1. *Sia G un gruppo, il **sottogruppo dei commutatori** o **sottogruppo derivato** $G' = [G, G]$ è il sottogruppo generato dagli elementi della forma $ghg^{-1}h^{-1} \doteqdot [g, h]$ al variare di $g, h \in G$.*

$gh = ghg^{-1}h^{-1}hg = [g, h]hg$ e anche $gh = hg[g^{-1}, h^{-1}]$.

Proposizione 1.10.2. *G' è caratteristico in G.*

Dimostrazione. Dato un qualsiasi $\varphi \in Aut(G)$, si ha che $\varphi\big([g, h]\big) = \big[\varphi(g), \varphi(h)\big]$. □

Proposizione 1.10.3. *G/G' è abeliano.*

Dimostrazione. $gG'hG' = ghG' = gh[h^{-1}, g^{-1}]G' = hG'gG'$. □

Proposizione 1.10.4. *Sia $f : G \longrightarrow H$ un omomorfismo surgettivo tale che H è abeliano, allora $G' < Ker\, f$ e quindi $\exists \tilde{f}$ tale che*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/G' \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Dimostrazione. Visto che H è abeliano, se prendiamo un qualsiasi commutatore $[g, h] \in G$ abbiamo che

$$f\big([g, h]\big) = f\big(ghg^{-1}h^{-1}\big) = f(g)f(h)f(g)^{-1}f(h)^{-1} = e_H \Longrightarrow G' < Ker\, f$$

In quanto se tutti i commutatori sono dentro al nucleo c'è anche il gruppo da loro generato. □

"Rendere un gruppo abeliano vuol dire quozientarlo almeno per i commutatori."

Definizione 1.10.2. *Chiamo **serie derivata** di G la successione*

$$G > G' > G^{(2)} > G^{(3)} > ..., \text{ dove } G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

*Può succedere che $G' = G$, in tal caso G è detto **perfetto**.*

Definizione 1.10.3. *Un gruppo G è **risolubile** se esiste una **serie subnormale** $G = G_0 \rhd G_1 \rhd ... \rhd G_n = \{0\}$, cioè $G_{i+1} \lhd G_i$ $\forall i$, tale che G_i/G_{i+1} è abeliano $\forall i$.*

Osservazione 9. *Se la serie derivata termina con $\{0\} \Longrightarrow G$ è risolubile.*

Proposizione 1.10.5. *Un gruppo G è risolubile $\Longleftrightarrow$ è risolubile per commutatori (cioè la serie derivata termina).*

Dimostrazione. $(\Longleftarrow)$ è l'**Osservazione 9.**.
$(\Longrightarrow)$ G è risolubile, quindi $G = G_0 \rhd G_1 \rhd ... \rhd G_n = \{0\}$:
${}^{G_0}/_{G_1}$ è abeliano $\Longrightarrow G_1 > G' \Longrightarrow G_1 \rhd G'$;
${}^{G_1}/_{G_2}$ è abeliano $\Longrightarrow G_2 > G'_1 > G^{(2)} \Longrightarrow G_2 \rhd G'_1 \rhd G^{(2)}$; e così via...
Quindi $G_n \rhd ... \rhd G^{(n)} = \{0\}$. □

Esercizio 38. *S_n, con $n \geq 5$, non è risolubile.*

Dimostrazione. Infatti la serie derivata di S_n è $S_n \rhd A_n \rhd A_n \rhd ...$ in quanto A_n è perfetto. □

Esercizio 39. *Sia $H < \mathbb{Z}^4$ tale che $H =< \begin{pmatrix}1\\2\\2\\4\end{pmatrix}, \begin{pmatrix}0\\4\\8\\2\end{pmatrix}, \begin{pmatrix}1\\-2\\8\\0\end{pmatrix} >$, chi è ${}^{\mathbb{Z}^4}/_H$?*

Dimostrazione. Costruiamo la matrice $\begin{pmatrix}1&0&1\\2&4&-2\\2&8&8\\4&2&0\end{pmatrix}$ e le applichiamo le seguenti operazioni di riga/colonna:

$$\begin{pmatrix}1&0&1\\2&4&-2\\2&8&8\\4&2&0\end{pmatrix} \xrightarrow{C_3 \to C_3 - C_1} \begin{pmatrix}1&0&0\\2&4&-4\\2&8&6\\4&2&-4\end{pmatrix} \xrightarrow[R_4 \to R_4 - 4R_1]{R_{2,3} \to R_{2,3} - 2R_1} \begin{pmatrix}1&0&0\\0&4&-4\\0&8&6\\0&2&-4\end{pmatrix} \xrightarrow{R_2 \leftrightarrow R_4} \begin{pmatrix}1&0&0\\0&2&-4\\0&8&6\\0&4&-4\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&2&-4\\0&8&6\\0&4&-4\end{pmatrix} \xrightarrow[R_4 \to R_4 - 2R_2]{R_3 \to R_3 - 4R_2} \begin{pmatrix}1&0&0\\0&2&-4\\0&0&22\\0&0&4\end{pmatrix} \xrightarrow[R_3 \to R_3 - 5R_4]{C_3 \to C_3 + 2C_2} \begin{pmatrix}1&0&0\\0&2&0\\0&0&2\\0&0&4\end{pmatrix} \xrightarrow{R_4 \to R_4 - 2R_3} \begin{pmatrix}1&0&0\\0&2&0\\0&0&2\\0&0&0\end{pmatrix}$$

Quindi

$${}^{\mathbb{Z}^4}/_H \cong {}^{\mathbb{Z}}/_{\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{2\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{2\mathbb{Z}} \oplus \mathbb{Z} \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times \mathbb{Z}$$

□

Capitolo 2

Campi

(<u>Ricordiamo</u>: se abbiamo due campi K ed $F \subseteq K$, $Aut(K/F)$ è il gruppo degli automorfismi di K che lasciano fisso F.)

2.11 Tuffo nelle dispense di Aritmetica

Capitolo 14, paragrafo 2

Siano F, F' due campi e $\phi : F \longrightarrow F'$ un isomorfismo. Chiamo $\widetilde{\phi}$ l'isomorfismo di anelli
$$\begin{array}{rccc} \widetilde{\phi}: & F[x] & \longrightarrow & F'[x] \\ & a_n x^n + ... + a_1 x + a_0 & \longmapsto & \phi(a_n)x^n + ... + \phi(a_1)x + \phi(a_0) \end{array}.$$

Teorema 2.11.1. *Siano F, F', ϕ come sopra, $F \subseteq L$ e $F' \subseteq L'$ due estensioni, $a \in L$ algebrico su F, $p(x) \in F[x]$ il polinomio minimo di a e $a' \in L'$ una radice di $\widetilde{\phi}\big(p(x)\big)$ ($L \supseteq F \overset{iso}{\longleftrightarrow} F' \subseteq L'$), allora $\exists \phi' : F[a] \longrightarrow F'[a']$ isomorfismo tale che $\phi'(a) = a'$ e $\phi'_{|_F} = \phi$.*
(Usiamo $F[a] = F(a)$ perché a è algebrico).

Dimostrazione. La composizione

$$\begin{array}{rccccc} \theta : & F[x] & \overset{\tilde{\phi}}{\longrightarrow} & F'[x] & \overset{\pi}{\longrightarrow} & F'[x]/\big(\tilde{\phi}(p(x))\big) \\ & x & \longmapsto & x & \longmapsto & x + \big(\tilde{\phi}(p(x))\big) \\ & k \in F & \longmapsto & \phi(k) & \longmapsto & \phi(k) + \big(\tilde{\phi}(p(x))\big) \end{array}$$

è omomorfismo. Visto che $Ker\,\theta = \big(p(x)\big)$, per il **Primo teorema di omomorfismo**, abbiamo che $\begin{array}{rccc} \theta' : & F[x]/\big(p(x)\big) & \longrightarrow & F'[x]/\big(\tilde{\phi}(p(x))\big) \\ & x + \big(p(x)\big) & \longmapsto & x + \big(\tilde{\phi}(p(x))\big) \end{array}$ è isomorfismo. Inoltre, $\theta'_{|_F}$ coincide con ϕ.

$$F[a] \overset{\gamma}{\cong} F[x]/(p(x)) \overset{\theta'}{\cong} F'[x]/\big(\tilde{\phi}(p(x))\big) \overset{\gamma'}{\cong} F'[a']$$

In cui $\gamma(a) = x + \big(p(x)\big)$ e $\gamma_{|_F} = Id$, $\gamma'(a') = x + \big(\tilde{\phi}(p(x))\big)$ e $\gamma'_{|_{F'}} = Id$.
<u>Ripasso:</u> $\begin{array}{ccc} F[x] & \longrightarrow & F[a] \\ q(x) & \longmapsto & q(a) \end{array}$, per il **Primo teorema di omomorfismo**, $\begin{array}{ccc} F[x]/(p(x)) & \longrightarrow & F[a] \\ a + p(x) & \longleftrightarrow & a \end{array}$
L'isomorfismo richiesto è quindi $(\gamma')^{-1} \circ \theta' \circ \gamma : F[a] \longrightarrow F'[a']$. □

Teorema 2.11.2. *Siano F, F', ϕ come sopra. Dato $f(x) \in F[x]$ non nullo, siano E un campo di spezzamento di $f(x)$ su F, E' un campo di spezzamento di $\tilde{\phi}\big(f(x)\big) \in F'[x]$ su F', allora $\exists \phi' : E \longrightarrow E'$ isomorfismo tale che $\phi'_{|_F} = \phi$.*

Dimostrazione. Per induzione su $\deg f(x) \geq 1$.
<u>Passo base</u>: $\deg f(x) = 1$, banalmente vero.
<u>Passo induttivo</u>: $\deg f(x) > 1$, sia $g(x)$ un fattore irriducibile di $f(x)$. Siano $a \in E$ una radice di $g(x)$ e sia $a' \in E'$ una radice di $\tilde{\phi}\big(g(x)\big)$. Il **Teorema** precedente dice che $\exists \theta : F[a] \longrightarrow F'[a']$ isomorfismo tale che $\theta(a) = a'$ e $\theta_{|_F} = \phi$.

$$\begin{array}{ccccc} F & \subseteq & F[a] & \subseteq & E \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \theta} & & \\ F' & \subseteq & F'[a'] & \subseteq & E' \end{array} \quad \text{e } \tilde{\theta} : F[a][x] \longrightarrow F'[a'][x].$$

In $F[a][x]$ il polinomio $f(x)$ si fattorizza come $f(x) = (x-a)\overline{f}(x)$, con $\deg \overline{f}(x) = \deg f(x) - 1$. Applichiamo $\tilde{\theta}$ a questa uguaglianza: $\tilde{\theta}\big(f(x)\big) = (x-a')\tilde{\theta}\big(\overline{f}(x)\big)$. Per ipotesi induttiva $\big($considerando il polinomio $\overline{f}(x)$ e i campi base $F[a]$ e $F'[a']\big)$, sappiamo che $\exists \phi' : E \longrightarrow E'$ tale che $\phi'_{|_{F[a]}}$ coincide con θ. Notiamo dunque che $\phi'_{|_F} = \phi$ e quindi ϕ' è l'isomorfismo cercato. $\square$

Corollario 2.11.3. *Sia F un campo e siano E ed E' due campi di spezzamento di un polinomio $f(x) \in F[x]$, allora $\exists \phi' : E \longrightarrow E'$ isomorfismo tale che $\phi'_{|_F} = Id$.*

2.12 Ritorno alle dispense di Algebra 1

Capitolo 10

Lemma 2.12.1. *Sia $f(x) \in F[x]$, se $f(x)$ ha fattori (non invertibili) multipli in $F[x]$, allora* $\deg\Big(MCD\big(f(x), f'(x)\big)\Big) \geq 1$ *(dove $f'(x)$ è la derivata formale di $f(x)$).*

Dimostrazione. Scriviamo $f(x) = g^2(x)q(x)$, allora $f'(x) = 2g(x)g'(x)q(x) + g^2(x)q'(x) =$
$= g(x)[2g'(x)q(x) + g(x)q'(x)]$ e quindi $g(x) \mid MCD\big(f(x), f'(x)\big)$. □

Teorema 2.12.2. *Sia $f(x) \in F[x]$, allora $f(x)$ non ha fattori multipli in $E[x]$ (dove E è un campo di spezzamento di $f(x)$ su F) $\Longleftrightarrow MCD\big(f(x), f'(x)\big) = 1$.*

Nota: $MCD\big(f(x), f'(x)\big) = 1$ in $F[x] \Longleftrightarrow MCD\big(f(x), f'(x)\big) = 1$ in $E[x]$.

Dimostrazione. $(\Longrightarrow)$ Sia f senza fattori multipli in $E[x]$, cioè $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$, con $\alpha_i \in E$ e $\alpha_i \neq \alpha_j$ se $i \neq j$, allora

$$f'(x) = (x-\alpha_2)\cdot ... \cdot(x-\alpha_n) + (x-\alpha_1)\cdot(x-\alpha_3)\cdot ... \cdot(x-\alpha_n) + ... + (x-\alpha_1)\cdot ... \cdot(x-\alpha_{n-1})$$

e dunque $f'(\alpha_i) \neq 0 \ \forall i$, perciò $f(x)$ ed $f'(x)$ non hanno radici in comune in E. Se avessero un divisore comune $d(x)$, questo avrebbe in E una radice che sarebbe comune a $f(x)$ e a $f'(x)$. Dunque $MCD\big(f(x), f'(x)\big) = 1$.
$(\Longleftarrow)$ Sia $MCD\big(f(x), f'(x)\big) = 1$. Se $f(x)$ ha fattori multipli in $F[x]$ sappiamo, per il **Lemma 2.12.1.**, che $\deg\Big(MCD\big(f(x), f'(x)\big)\Big) \geq 1$. $\lightning$ □

Domande: Se abbiamo un polinomio irriducibile $p(x) \in F[x]$, possiamo dire che $p(x)$ non ha radici multiple (in un campo di spezzamento E)?
Se $char\,F = 0$ è vero che $p(x)$ non ha radici multiple, infatti $MCD\big(p(x), p'(x)\big) \in \{1, p(x)\}$ perché $p(x)$ è irriducibile, ma $\deg p'(x) = \deg p(x) - 1$, dunque $p(x) \nmid p'(x)$, allora $MCD\big(p(x), p'(x)\big) = 1$ e, per il **Teorema 2.12.2.**, $p(x)$ non ha radici multiple.
Se $char\,F = p$, con p primo, cosa succede?
Sia $g(x)$ un polinomio irriducibile. Il discorso qui sopra funziona, A MENO CHE $g'(x) = 0$: sia F campo finito, con $char\,F = p$

$$g'(x) = 0 \Longleftrightarrow g(x) = a_n(x^p)^n + ... + a_1x^p + a_0, \text{ con } a_n, ..., a_0 \in F$$

Sia $\mathcal{F}$ l'omomorfismo di Frobenius, $\begin{array}{cccc}\mathcal{F}: & F & \longrightarrow & F \\ & a & \longmapsto & a^p\end{array}$ è omomorfismo iniettivo (vedi dispense di Aritmetica). F è finito $\Longrightarrow \mathcal{F}$ è surgettivo, dunque è isomorfismo, allora $a_n = \mathcal{F}(b_n) = b_n^p$, $a_{n-1} = \mathcal{F}(b_{n-1}) = b_{n-1}^p$, ... ,$a_1 = \mathcal{F}(b_1) = b_1^p$, $a_0 = \mathcal{F}(b_0) = b_0^p$.
In conclusione,

$$g(x) = b_n^p(x^p)^n + ... + b_1^px^p + b_0^p = b_n^p(x^n)^p + ... + b_1^px^p + b_0^p = (b_nx^n + ... + b_1x + b_0)^p$$

ma è assurdo, perché $g(x)$ è irriducibile.
Perciò anche in un campo F, con $char\,F = p$ ma finito, accade che $g(x)$ irriducibile $\Longrightarrow g(x)$ non ha radici multiple.
Ultima possibilità: sia F campo, con $char\,F = p$, infinito.
Sia $F = \mathbb{Z}/p\mathbb{Z}(t) = \left\{\frac{q(t)}{h(t)} \,\middle|\, q(t), h(t) \in \mathbb{Z}/p\mathbb{Z}[t] \text{ e } h(t) \neq 0\right\}$, dove t è una variabile.
Prendiamo il polinomio $g(x) = x^p - t \in F[x] = \mathbb{Z}/p\mathbb{Z}(t)[x]$.
$g(x)$ è irriducibile per il **Lemma di Gauss** e per il **Criterio di Eisenstein**.

$\Big($**Lemma di Gauss**: $g(x)$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}(t)[x] \iff$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[t][x]$.

Criterio di Eisenstein: applicato con l'irriducibile t di $\mathbb{Z}/p\mathbb{Z}[t]$.$\Big)$
Quindi $g(x) = x^p - t$ è irriducibile in $F[x]$. Vale che $g'(x) = 0$.
Sia E un campo di spezzamento di $g(x)$ su $F = \mathbb{Z}/p\mathbb{Z}(t)$.
Sia $\alpha \in E$ una radice di $g(x)$, cioè $g(\alpha) = 0 \iff \alpha^p - t = 0 \implies t = \alpha^p$, allora in $E[x]$ $g(x)$ si fattorizza come $g(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p$ (anche E ha caratteristica p).

Esercizio 40 (Condizione necessaria perché due prodotti semidiretti (di p-gruppi) siano isomorfi).
Sia N un gruppo di ordine p^α e sia H un gruppo di ordine q^β, con p e q primi distinti e $\alpha, \beta > 0$. Supponiamo che $N \rtimes_{\tau_1} H \cong N \rtimes_{\tau_2} H$, allora $Ker\,\tau_1 \cong Ker\,\tau_2$.

Notazione: Chiamiamo, in generale, $G = N \rtimes_\tau H$, $\overline{N} = \{(n, e) | n \in N\}$, $\forall K < H$ $\overline{K} = \{(e, k) | k \in K\}$, in particolare $\overline{H} = \{(e, h) | h \in H\}$, e $C(\overline{N}) = \{g \in G | gx = xg \; \forall x \in \overline{N}\}$.

Dimostrazione. Primo passo: si nota che $\overline{Ker\,\tau} = \overline{H} \cap C(\overline{N})$ (ricordiamo che $Ker\,\tau < H$). Infatti $(e, h) \in \overline{Ker\,\tau} \iff h \in Ker\,\tau \iff \forall n \in N \; \tau(h)(n) = n$ (insomma $\tau(h) = Id$) $\iff$ $\forall n \in N \; (n, h) = \big(\tau(h)(n), h\big) \iff \forall n \in N \; (n, e)(e, h) = (e, h)(n, e)$, infatti, per definizione, $(n, e)(e, h) = (n, h)$ e $(e, h)(n, e) = \big(e \cdot \tau(h)(n), h \cdot e\big) = (n, h)$, $\iff (e, h) \in C(\overline{N}) \cap (\overline{H})$.
Secondo passo: chiamiamo adesso $G_1 = N \rtimes_{\tau_1} H$ e $G_2 = N \rtimes_{\tau_2} H$, $\overline{N}$ e $\overline{H}$ in entrambi i casi, $C_1(\overline{N})$ in G_1 e $C_2(\overline{N})$ in G_2.
Sia $f : G_1 \longrightarrow G_2$ isomorfismo, dato che $\overline{N} \lhd G_1$ e inoltre, essendo il p-Sylow, è l'unico sottogruppo di quell'ordine e, dato che lo stesso vale in G_2, deve valere che $f(\overline{N}) = \overline{N}$.
Notiamo che $\overline{H}$ è un q-Sylow di G_1 e $f(\overline{H})$ è un q-Sylow di G_2 ma anche $\overline{H}$ è un q-Sylow di G_2, dunque $f(\overline{H})$ e $\overline{H}$ sono coniugati in G_2, cioè $\exists g \in G_2$ tale che $f(\overline{H}) = g\overline{H}g^{-1}$.
Terzo passo: studiamo $f(\overline{Ker\,\tau_1})$:

$$f(\overline{Ker\,\tau_1}) \overset{\substack{\text{Primo} \\ \text{passo}}}{=} f\big(\overline{H} \cap C_1(\overline{N})\big) = f(\overline{H}) \cap f\big(C_1(\overline{N})\big) = g\overline{H}g^{-1} \cap C_2\big(f(\overline{N})\big) = g\overline{H}g^{-1} \cap C_2(\overline{N})$$

Ci piacerebbe dire che $C_2(\overline{N}) = gC_2(\overline{N})g^{-1}$ perché in tal caso avremmo

$$g\overline{H}g^{-1} \cap C_2(\overline{N}) = g\overline{H}g^{-1} \cap gC_2(\overline{N})g^{-1} = g\big(\overline{H} \cap C_2(\overline{N})\big)g^{-1} \overset{\substack{\text{Primo} \\ \text{passo}}}{=} g(\overline{Ker\,\tau_2})g^{-1}$$

quindi avremmo $f(\overline{Ker\,\tau_1}) = g(\overline{Ker\,\tau_2})g^{-1}$, cioè $\overline{Ker\,\tau_1} \cong g(\overline{Ker\,\tau_2})g^{-1} \cong \overline{Ker\,\tau_2}$, ma $\overline{Ker\,\tau_1} \cong Ker\,\tau_1$ e $\overline{Ker\,\tau_2} \cong Ker\,\tau_2 \implies \boxed{Ker\,\tau_1 \cong Ker\,\tau_2}$.
Resta da dimostrare che $gC_2(\overline{N})g^{-1} = C_2(\overline{N})$: basta dimostrare un'inclusione, ad esempio $gC_2(\overline{N})g^{-1} \subseteq C_2(\overline{N})$, per ragioni di cardinalità, ossia basta dimostrare che se $x \in C_2(\overline{N})$ e $\overline{n} \in \overline{N}$, allora $(gxg^{-1})\overline{n} = \overline{n}(gxg^{-1})$. Notiamo che

$$gxg^{-1}\overline{n} = gx \overbrace{(g^{-1}\overline{n}g)}^{\substack{\in \overline{N} \text{ perché} \\ \overline{N} \text{ è normale}}} g^{-1} \overset{x \in C_2(\overline{N})}{=} g(g^{-1}\overline{n}g)xg^{-1} = \overline{n}gxg^{-1}$$

$\square$

Nota: l'**Esercizio 40.** funziona anche se N non è p-gruppo ma è comunque l'unico gruppo di ordine $|N|$ in $N \rtimes H$.

2.13 Polinomi separabili

Definizione 2.13.1. *Sia F un campo, un polinomio irriducibile $g(x) \in F[x]$ si dice **separabile** se $g'(x) \neq 0$. Un polinomio $f(x) \in F[x]$ si dice **separabile** se è prodotto di irriducibili separabili.*

Osservazione 10. *Se f è irriducibile e separabile, allora non ha radici multiple in un campo di spezzamento.*

Proposizione 2.13.1. *Sia $F \subseteq E$, se $f(x) \in F[x]$ si spezza in $E[x]$ come $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$, con $\alpha_1, ..., \alpha_n$ a due a due distinti, allora $f(x)$ è separabile.*

Dimostrazione. Sia $g(x) \in F[x]$ un fattore irriducibile di $f(x)$: mostriamo che $g'(x) \neq 0$. Ora, sappiamo che in $E[x]$ $g(x) = (x - \alpha_{i_1}) \cdot ... \cdot (x - \alpha_{i_k})$, con $\alpha_{i_1}, ..., \alpha_{i_k} \in \{\alpha_1, ..., \alpha_n\}$ distinte.
Si ha che $g'(\alpha_{i_1}) \neq 0$ come visto la volta scorsa, dunque $g'(x) \neq 0$, allora $g(x)$ è irriducibile e separabile. $\square$

Proposizione 2.13.2. *Siano $g(x) \in F[x]$ irriducibile e separabile, E un campo di spezzamento di $g(x)$ su F e $a \in E$ una radice di $g(x)$, allora*

$$\#\{\phi : F(a) \longrightarrow E \overset{\text{sono immersioni}}{\text{omomorfismi tali che}}\ \phi_{|_F} = Id_{|_F}\} = [F(a) : F] = \deg g(x)$$

Dimostrazione. Per un **Teorema** di Aritmetica, sappiamo che se $a, b \in E$ sono due radici distinte di $g(x)$, allora $\exists! \underset{\subseteq E}{F(a)} \longrightarrow \underset{\subseteq E}{F(b)}$ isomorfismo che lascia fisso F e manda a in b.
Quindi abbiamo almeno $\deg g(x)$ immersioni $F(a) \longrightarrow E$.
Viceversa, notiamo che se $\phi : F(a) \longrightarrow E$, con $\phi_{|_F} = Id_{|_F}$, allora, visto che $\tilde{\phi}\big(g(x)\big) = g(x)$, $\phi(a)$ è ancora una radice di $g(x)$. Dunque tutti i ϕ cercati sono del tipo $F(a) \longrightarrow F(b)$. $\square$

Corollario 2.13.3. *Siano $g(x) \in F[x]$ irriducibile e separabile, E un campo di spezzamento di $g(x)$ in F, $a \in E$ una radice di $g(x)$ e $k \in F(a) \setminus F$, allora $\exists \tau : F(a) \longrightarrow E$ tale che $\tau_{|_F} = Id$ e $\tau(k) \neq k$.*

Dimostrazione. Consideriamo l'estensione di campi $F \subseteq F(k) \subseteq F(a)$ e il polinomio minimo di a in $F(k)[x]$. Sia $q(x) \in F(x)[x]$ e $q(x) \mid g(x)$, ma $g(x)$ non ha radici multiple, dunque anche $q(x)$ non ha radici multiple. Per la **Proposizione 2.13.1**, allora $q(x)$ è separabile. Per la **Proposizione 2.13.2**, $\#\{\phi : F(a) \longrightarrow E \text{ e } \phi_{|_{F(k)}} = Id\} = [F(a) : F(k)]$.
Inoltre, $\#\{\phi : F(a) \longrightarrow E \text{ e } \phi_{|_F} = Id\} = [F(a) : F]$.
Notiamo che $[F(k) : F] > 1$ perché $k \notin F$, allora per il **Teorema delle torri di estensioni** $[F(a) : F] = [F(a) : F(k)] \cdot [F(k) : F]$ e quindi $[F(a) : F] > [F(a) : F(k)]$.
Dunque esistono immersioni $F(a) \longrightarrow E$ che non fissano $F(k)$ il che equivale a dire che non fissano k. $\square$

Corollario 2.13.4. *Siano E il campo di spezzamento su F di un polinomio separabile $g(x) \in F[x]$ e sia $a \in E \setminus F$, allora $\exists \tau : E \longrightarrow E$ automorfismo tale che $\tau(a) \neq a$ e $\tau_{|_F} = Id$.*

Dimostrazione. Costruiamo $E = F(a_1, ..., a_t)$, dove $a_1, ..., a_t$ sono le radici di $g(x)$. Sia i tale che $a \notin F(a_1, ..., a_{i-1})$ ma $a \in F(a_1, ..., a_i)$. Sia $g_i(x)$ il polinomio minimo di a_i in $F(a_1, ..., a_{i-1})[x]$ e sia $L \subseteq E$ il campo di spezzamento di $g_i(x)$ su $F(a_1, ..., a_{i-1})$.
Notiamo che $g_i(x)$ è separabile, perché $g_i(x) \mid g(x)$ $*$, allora $\exists \tau' : F(a_1, ..., a_{i-1})(a_i) \longrightarrow L$ tale che $\tau'(a) \neq a$ per il **Corollario 2.13.3**.
Siccome a è radice di un polinomio separabile, abbiamo un'immersione (omomorfismo di campi) $F(a_1, ..., a_{i-1})(a_i) \longrightarrow L$ che muove a. Consideriamo il polinomio $g(x)$: il suo campo di

spezzamento in $F(a_1, ..., a_{i-1})(a_i)$ è E ma anche quello in L è E, allora c'è un'estensione dell'omomorfismo $E \longrightarrow E$ che, ristretta ai campi di base, corrisponde all'estensione iniziale τ'. Questa è la τ richiesta perché, ristretta alla base, si comporta come faceva τ', cioè muove a. Si conclude usando il **Teorema 14.10** delle dispense di Aritmetica visto la volta scorsa. $\square$

$*$ $g(x) = p_1^{\alpha_1}(x)p_2^{\alpha_2}(x) \cdot ... \cdot p_k^{\alpha_k}(x)$, con $p_1(x), ..., p_k(x)$ irriducibili in $F[x]$ e separabili.
Guardiamo $g(x)$ in $F(a_1, ..., a_{i-1})[x]$: sappiamo che $g_i(x)$ è irriducibile e $g_i(x) \mid g(x)$.
D'altra parte, la fattorizzazione in irriducibili di $g(x)$ in $F(a_1, ..., a_{i-1})[x]$ si ottiene considerando tutte le fattorizzazioni dei $p_s(x)$, allora $g_i(x) \mid p_t(x)$ per un certo t, ma $p_t(x)$ è irriducibile e separabile, allora ha radici distinte.
Dunque $g_i(x)$ ha radici distinte e, per la **Proposizione 2.13.1.**, $g_i(x)$ è separabile.

Definizione 2.13.2. *Sia $F \subseteq E$ un'estensione di campi. Un elemento $a \in E$ è **separabile** su F se è algebrico e se il suo polinomio minimo è separabile.*

Teorema 2.13.5 **(dell'elemento primitivo).**

Sia $F \subseteq E$ un'estensione finita di campi, dove $E = F(\overbrace{\alpha, \beta_1, ..., \beta_n}^{algebrici})$, con i β_i separabili su F, allora $\exists \delta \in E$ tale che $E = F(\delta)$.

Dimostrazione. Se F è un campo finito, anche E, che è un'estensione finita, è finito, dunque E^* è ciclico: $E^* = (\gamma) \implies F(\gamma) = E$.
Sia allora F infinito. Basta dimostrare che $E = F(\alpha, \beta_1) = F(\gamma)$.
Siano $f(x)$ il polinomio minimo di α su F e $g(x)$ il polinomio minimo di β_1 su F.
Consideriamo $f(x) \cdot g(x)$: se E non è il campo di spezzamento di $f(x) \cdot g(x)$, lo estendo a $\tilde{E}$.
In $\tilde{E}$ vale $f(x) = \prod_{i=1}^{\deg f} (x - a_i)$ e $g(x) = \prod_{k=1}^{\deg g} (x - b_k)$.
Sappiamo che $b_1 = \beta_1, b_2 ..., b_k$ sono distinti a due a due.
Presi i e k, considero l'equazione

$$a_i + xb_k = \alpha + x\beta_1$$

che ha un'unica soluzione $x = \frac{a_i - \alpha}{\beta_1 - b_k}$, dunque abbiamo un numero finito di tali soluzioni $x \in \tilde{E}$.
Dato che F è infinito, scegliamo $r \in F$ diverso da queste soluzioni, allora $a_i + rb_k \neq \alpha + r\beta_1$ $\forall k \neq 1$ e $\forall i$. Diciamo che il δ "giusto" è proprio $\alpha + r\beta_1$. Dobbiamo dimostrare che $F(\alpha, \beta_1) = F(\gamma) = F(\alpha + r\beta_1)$. L'inclusione $F(\alpha + r\beta_1) \subseteq F(\alpha, \beta_1)$ è ovvia.
Notiamo che β_1 è radice di $g(x)$ ma è radice anche di $f(\delta - rx)$, infatti $f(\delta - r\beta_1) = f(\alpha) = 0$, allora, in $\tilde{E}(x)$, $x - \beta_1$ divide sia $g(x)$ sia $f(\delta - rx)$. Diciamo che, in $\tilde{E}(x)$, $MCD\big(f(\delta - r\beta_1), g(x)\big) = x - \beta_1$.
Dobbiamo controllare se per b_i, con $i > 1$, $x - b_i$ divide $f(\delta - rx)$, ossia se $f(\delta - rb_i) = 0$:

$$\delta - rb_i = \alpha + rb_1 - rb_i$$

È sempre vero che $\alpha + r\beta_1 \neq a_l + rb_i \implies \alpha + r\beta_1 - rb_i \neq a_l$ $\forall l$. Dunque $MCD\big(f(\delta - rx), g(x)\big)$ in $F(\delta)[x]$ non è 1, allora è un polinomio non costante che divide $x - \beta_1$, dunque ha grado 1, perciò diciamo che è $c_1x + c_0$, con $c_0, c_1 \in F(\delta)$ e $c_1 \neq 0$: $c_1x + c_0 \mid x - \beta_1$ in $\tilde{E}(x)$, quindi β_1 è radice di $c_1x + c_0 \implies \beta_1 = -\frac{c_0}{c_1}$, allora $\beta_1 \in F(\delta)$, ma $\delta = \alpha + r\beta_1$, dunque $\alpha = \delta - r\beta_1 \in F(\delta)$, da cui otteniamo $F(\alpha, \beta_1) \subseteq F(\delta)$. $\square$

2.14 Teoria di Galois

Data $F \subseteq E$ un'estensione di campi, chiamiamo $Aut({}^{E}/_{F})$ l'insieme degli automorfismi di E che lasciano fissi tutti gli elementi di F.
Chiamiamo anche $E' = \{h \in E \mid \phi(h) = h \ \ \forall \phi \in Aut({}^{E}/_{F})\}$.

Osservazione 11. *E' è un campo ed è detto il **campo fisso di** $Aut({}^{E}/_{F})$.*

Esempio 12. *① Se $E = \mathbb{Q}(\sqrt{2})$ ed $F = \mathbb{Q}$, $\phi \in Aut({}^{E}/_{F})$ è determinato da $\phi(\sqrt{2})$. $\phi(\sqrt{2})$ dovrà essere una radice di x^2-2 perché $\tilde{\phi}(x^2-2) = x^2-2$, dunque $\phi(\sqrt{2}) = \pm\sqrt{2}$, da cui $Aut({}^{\mathbb{Q}(\sqrt{2})}/_{\mathbb{Q}}) = \{Id, \theta\}$, con $\theta(a+b\sqrt{2}) = a - b\sqrt{2}$ $\forall a, b \in \mathbb{Q}$. Perciò $\mathbb{Q}(\sqrt{2})' = \mathbb{Q}$.*

② Se $E = \mathbb{Q}(\sqrt[3]{2})$ ed $F = \mathbb{Q}$, $Aut({}^{E}/_{F}) = \{Id\}$, perché un $\phi \in Aut({}^{\mathbb{Q}(\sqrt[3]{2})}/_{\mathbb{Q}})$ è determinato da $\phi(\sqrt[3]{2})$ che deve $\in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ e deve essere una radice di x^3-2 ma di queste tre radici solo una è reale, quindi $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Dunque $\mathbb{Q}(\sqrt[3]{2})' = \mathbb{Q}(\sqrt[3]{2})$.

Definizione 2.14.1. *Un'**estensione** $F \subseteq E$ si dice **di Galois** se E è finita su F e se il campo fisso di $Aut({}^{E}/_{F})$ è F.
$Aut({}^{E}/_{F}) = Gal({}^{E}/_{F})$ è detto **Gruppo di Galois di** E **su** F.*

Proposizione 2.14.1. *Sia $[E:F] < +\infty$, allora $Aut({}^{E}/_{F})$ è gruppo finito.*

Esercizio 41. *Dimostrare la **Proposizione 2.14.1.**.*

Teorema 2.14.2. *Sia $F \subseteq E$ di Galois, allora ogni $a \in E$ è radice di un polinomio $f(x)$ irriducibile e separabile e inoltre E contiene un campo di spezzamento di $f(x)$.*

Dimostrazione. Costruiamo $f(x) = \prod\limits_{\gamma \in O} (x-\gamma)$, dove $O = \{\phi(a) \mid \phi \in Aut({}^{E}/_{F})\}$.
Per costruzione, $f(x) \in E[x]$. Data $\phi \in Aut({}^{E}/_{F})$, $\tilde{\phi} : E[x] \longrightarrow E[x]$ è tale che

$$\tilde{\phi}\big(f(x)\big) = \prod_{\gamma \in O} \tilde{\phi}(x-\gamma) = \prod_{\gamma \in O} \big(x - \phi(\gamma)\big) = \prod_{\gamma \in O} (x-\gamma) = f(x)$$

perché $\phi_{|O} \in Big(O)$.
$f(x) = a_n x^n + ... + a_1 x + a_0$, con $a_i \in E$ $\forall i = 1, ..., n$, ma, da quanto appena osservato, sappiamo che $\forall \phi \in Aut({}^{E}/_{F})$

$$\tilde{\phi}\big(f(x)\big) = \phi(a_n)x^n + ... + \phi(a_1)x + \phi(a_0) = f(x) = a_n x^n + ... + a_1 x + a_0$$

Dunque, $\phi(a_i) = a_i$ $\forall i = 1, ..., n$ e $\forall \phi \in Aut({}^{E}/_{F})$, quindi $a_i \in E' = F$ $\forall i = 1, ..., n$, perché l'estensione è di Galois. Dunque abbiamo scoperto che $f(x) \in F[x]$.
Resta da dimostrare che $f(x)$ è irriducibile in $F[x]$.
Scriviamo $f(x) = f_1(x) f_2(x)$, con $f_1(x), f_2(x) \in F[x]$: se, ad esempio, $f_1(a) = 0$, allora $\forall \gamma \in O$ $f_1(\gamma) = 0$ dunque $f(x) = k f_1(x)$ e quindi $f_2(x)$ è costante. (Dettagli sulle dispense). $\square$

Teorema 2.14.3. *Un'estensione $F \subseteq E$ è di Galois $\Longleftrightarrow$ E è il campo di spezzamento su F di un polinomio $f(x)$ separabile.*

Dimostrazione. $(\Longrightarrow)$ Sia $F \subseteq E$ di Galois, allora $E = F(a_1, ..., a_n)$, perché E è finita.
Ricordiamo che a_i è algebrico su F $\forall i = 1, ..., n$, perché $F(a_i) \subseteq E$ e dunque $[F(a_i) : F]$ è finito $\forall i = 1, ...n$. Per il **Teorema 2.14.2.**, sappiamo che $a_1, ..., a_n$ sono anche separabili.
Per il **Teorema dell'elemento primitivo**, $E = F(\gamma)$, per un certo γ.
Per γ costruiamo il polinomio minimo $f(x)$ come nella dimostrazione del **Teorema 2.14.2.**: sappiamo che $f(x)$ è separabile per costruzione e che tutte le sue radici sono in E. Sia K il campo di spezzamento di $f(x)$ su F. Sappiamo che $E = F(\gamma) \subseteq K \subseteq E \Longrightarrow E = K$.
$(\Longleftarrow)$ Sia E campo di spezzamento su F di un polinomio separabile. $[E:F] < +\infty$.
Studiamo adesso E', il campo fisso di $Aut({}^{E}/_{F})$. Dunque, se $a \in E \setminus F$, per il **Corollario 2.13.4.**, $a \notin E'$, dunque $E' = F \Longrightarrow F \subseteq E$ è di Galois. $\square$

Corollario 2.14.4. *Sia $F \subseteq E$ di Galois e anche $E \subseteq L$ estensione, allora ogni $\psi \in Aut(L/F)$ manda E in E ("**normalità di** E").*

Dimostrazione. E è il campo di spezzamento di un polinomio separabile $f(x) \in F[x]$. (Dettagli sulle dispense). $\square$

Corollario 2.14.5. *Sia $F \subseteq E$ di Galois, allora $|Aut(E/F)| = [E : F]$.*

Dimostrazione.

$$\begin{aligned}[E:F] &\overset{E=F(\gamma)}{=} [F(\gamma):F] \overset{\textbf{Prop. 2.13.2.}}{=} \#\{\phi : F(\gamma) \longrightarrow E \text{ omomorfismo tale che } \phi_{|_F} = Id\} = \\ &= \#\{\phi : E \longrightarrow E \text{ omomorfismo tale che } \phi_{|_F} = Id\} = |Aut(E/F)|\end{aligned}$$

$\square$

Esercizio 42 (10.4.4. delle dispense)**.**
Determinare il polinomio minimo di ζ_5 su $\mathbb{Q}(i)$.

Dimostrazione. ζ_5 è radice di $x^4 + x^3 + x^2 + x + 1$ che è irriducibile in $\mathbb{Q}[x]$.

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

È decisivo sapere se $i \in \mathbb{Q}(\zeta_5)$ o no.
Primo approccio: usiamo che $\cos(72°) = \frac{\sqrt{5}-1}{4}$ e $\sin(72°) = \frac{\sqrt{2\cdot(5+\sqrt{5})}}{4}$.
Secondo approccio: scriviamo $i = a + b\cdot\zeta_5 + c\cdot\zeta_5^2 + d\cdot\zeta_5^3$, con $a, b, c, d \in \mathbb{Q}$, perché $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ è base di $\mathbb{Q}(\zeta_5)$ su $\mathbb{Q}$.
Terzo approccio: notiamo che $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$ è di Galois perché è campo di spezzamento del polinomio separabile $x^4 + x^3 + x^2 + x + 1$. Il gruppo di Galois $Aut(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ ha $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ elementi.
Sia $\begin{array}{cccc}\phi: & \mathbb{Q}(\zeta_5) & \longrightarrow & \mathbb{Q}(\zeta_5) \\ & \zeta_5 & \longmapsto & \zeta_5^2\end{array}$ che lascia fisso $\mathbb{Q}$ ed esiste per un vecchio **Teorema** di Aritmetica.
$\phi \in Aut(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ notiamo che ha ordine 4: $\phi^2(\zeta_5) = \zeta_5^4 = \zeta_5^{-1} \Longrightarrow \phi^4(\zeta_5) = \zeta_5^{16} = \zeta_5$, quindi $\phi^4 = Id$.
Se consideriamo un campo intermedio K, $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\zeta_5)$,

$$Aut(\mathbb{Q}(\zeta_5)/K) < Aut(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

$K \subset \mathbb{Q}(\zeta_5)$ è di Galois o no? Sì, perché è sempre campo di spezzamento di $x^4 + x^3 + x^2 + x + 1$.
Sappiamo allora che $|Aut(\mathbb{Q}(\zeta_5)/K)| = [\mathbb{Q}(\zeta_5) : K] = 2$.
Visto che $Aut(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, allora $Aut(\mathbb{Q}(\zeta_5)/K) = \{Id, \phi^2\}$.
Dato che $K \subset \mathbb{Q}(\zeta_5)$ è di Galois, $\mathbb{Q}(\zeta_5)' = K$ ossia K è il campo fisso di $Id, \phi^2 \Longrightarrow K$ è caratterizzato ed unico.
So che $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$ perché $\zeta_5 + \frac{1}{\zeta_5}$ è radice di $x^2 + x - 1$:

$$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0 \Longrightarrow \frac{1}{\zeta_5} + \frac{1}{\zeta_5^2} + \zeta_5^2 + \zeta_5 + 1 = 0 \Longrightarrow \left(\zeta_5 + \frac{1}{\zeta_5}\right)^2 + \zeta_5 + \frac{1}{\zeta_5} - 1 = 0$$

Le radici di $x^2 + x - 1 = 0$ sono $x_{1,2} = \frac{-1\pm\sqrt{5}}{2}$, perciò $\zeta_5 + \frac{1}{\zeta_5} = \frac{-1\pm\sqrt{5}}{2} \Longrightarrow \sqrt{5} \in \mathbb{Q}(\zeta_5)$.
Dunque $\mathbb{Q}(\sqrt{5})$ è l'unico sottogruppo dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$.
NON può accadere quindi che $i \in \mathbb{Q}(\zeta_5)$ altrimenti avremmo anche $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_5)$ e $\mathbb{Q}(i) \neq \mathbb{Q}(\zeta_5)$ poiché $\mathbb{Q}(i) \nsubseteq \mathbb{R}$ e $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$. $\square$

Esercizio 43. *(comprende il 10.4.8 e il 10.4.9 delle dispense)*
L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *è di Galois? In tal caso calcolare* $Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}})$.

Dimostrazione. Sì, perché $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ è campo di spezzamento del polinomio $(x^2-2)(x^2-3)$.
Sappiamo che $|Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}})| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, perché

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

in quanto $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ ($\nexists a, b \in \mathbb{Q}$ tali che $\sqrt{3} = a + b\sqrt{2}$) e $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ (analogamente).

Consideriamo l'estensione $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dato che $x^2 - 2$ è irriducibile in $\mathbb{Q}(\sqrt{3})[x]$, sappiamo che $\exists \theta : \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \longrightarrow \mathbb{Q}(-\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ isomorfismo tale che $\theta(\sqrt{2}) = -\sqrt{2}$ e $\theta_{|_{\mathbb{Q}(\sqrt{3})}} = Id$.
θ esiste, $\theta \neq Id$ e $\theta \in Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}(\sqrt{3})}) < Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}})$.
Notiamo che $\theta^2 = Id$ e quindi $Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}(\sqrt{3})}) = \{Id, \theta\}$.
Analogamente, costruiamo $\varphi \in Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}(\sqrt{2})})$ tale che $\varphi(\sqrt{3}) = -\sqrt{3}$ e $\varphi_{|_{\mathbb{Q}(\sqrt{2})}} = Id$.
φ esiste, $\varphi \neq Id$ e $\varphi \in Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}(\sqrt{2})}) < Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}})$.
Notiamo che $\varphi^2 = Id$ e quindi $Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}(\sqrt{2})}) = \{Id, \varphi\}$.
Notiamo anche che $\theta \neq \varphi$, allora in $Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}})$ ci sono almeno due elementi distinti di ordine 2 $\Longrightarrow Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$.
Esistono altri campi K tali che $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$?
Si osserva che per un tale K deve valere $[K : \mathbb{Q}] = 2$.
L'estensione $K \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ è di Galois perché $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ è il campo di spezzamento di $(x^2-2)(x^2-3)$ anche su K. Sia G_1 il suo gruppo di Galois: $|G_1| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : K] = 2$.
Inoltre, per definizione, $G_1 < Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}})$ e il campo fisso di G_1 è K perché l'estensione è di Galois. Dunque K è determinato dal sottogruppo G_1.
Dato che in ${}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ esistono 3 sottogruppi di ordine 2, ci possono essere al massimo 3 distinti campi K:
$\mathbb{Q}(\sqrt{2})$ è il campo fissato da $\{Id, \varphi\}$;
$\mathbb{Q}(\sqrt{3})$ è il campo fissato da $\{Id, \theta\}$;
Il terzo sottogruppo è $\{Id, \theta\varphi\}$. Notiamo che se consideriamo $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ vale

$$\theta\varphi(\sqrt{2} \cdot \sqrt{3}) = \theta\big(\sqrt{2}(-\sqrt{3})\big) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}$$

Il campo fissato da $\{Id, \theta\varphi\}$ è quindi $\mathbb{Q}(\sqrt{6})$.

<u>Non ci sono altri campi intermedi!</u>

<u>Nota</u>: $\mathbb{Q}(\sqrt{6}) \neq \mathbb{Q}(\sqrt{2})$: se così non fosse, allora in tale campo avremmo anche $\frac{\sqrt{6}}{\sqrt{2}} = \sqrt{3}$ $\lightning$ per ragioni di grado. Analogamente, $\mathbb{Q}(\sqrt{6}) \neq \mathbb{Q}(\sqrt{3})$. Quindi l'estensione con tutti i suoi sottocampi è

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"'] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Se quindi ci viene chiesto quanto valga il grado $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$, possiamo subito rispondere che è 4, perché $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ e $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \neq \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$, allora deve essere $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.
Se fosse $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2})$, allora in tale campo avremmo anche $\sqrt{2}+\sqrt{3}-\sqrt{2} = \sqrt{3} \Longrightarrow \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ $\lightning$ per ragioni di grado. Oppure vediamo $\mathbb{Q}(\sqrt{2})$ come il campo fisso di $\{Id, \varphi\}$, ma $\varphi(\sqrt{2}+\sqrt{3}) = \sqrt{2}-\sqrt{3}$, allora $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Longrightarrow \mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
Analogamente per $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{6})$. □

Proposizione 2.14.6. *Sia $F \subseteq E$ di Galois e sia $H < Aut(E/F)$ tale che il suo campo fisso $\{a \in E \mid h(a) = a\ \forall h \in H\}$ coincide con F, allora $H = Aut(E/F)$.*

Dimostrazione. $E = F(\delta)$, costruiamo $f(x) = \prod_{\gamma \in O_H} (x-\gamma)$, dove $O_H = \{h(\delta) \mid h \in H\}$. Scopriamo che $f(x) \in F[x]$ e che è irriducibile (analogamente alla dimostrazione del **Teorema 2.14.2.**). Dunque $f(x)$ è il polinomio minimo di δ. $|H| \geq O_H = \deg f(x) = [E:F] = |Aut(E/F)|$, allora deve essere $H = Aut(E/F)$. □

Sia $F \subseteq E$ di Galois. Chiamiamo $\mathcal{C} = \{K \text{ campo} \mid F \subseteq K \subseteq E\}$ e $\mathcal{S} = \{G \mid G < Aut(E/F)\}$ e consideriamo le funzioni $\begin{array}{rccc} i: & \mathcal{C} & \longrightarrow & \mathcal{S} \\ & K & \longmapsto & Aut(E/K) \end{array}$ e $\begin{array}{rccc} j: & \mathcal{S} & \longrightarrow & \mathcal{C} \\ & G & \longmapsto & \{a \in E \mid g(a) = a\ \forall g \in G\} \end{array}$.

Teorema 2.14.7 (Primo teorema di Galois).
Le mappe i e j sono una l'inversa dell'altra.

Dimostrazione. Sia $K \in \mathcal{C}$, $j \circ i(K) = j\big(Aut(E/K)\big) = K$ per definizione di estensione di Galois. Adesso $i \circ j(G) = i\big(j(G)\big) = Aut(E/j(G))$, dove $j(G)$ è un campo. Consideriamo G e notiamo che $G < Aut(E/j(G))$. Per la **Proposizione 2.14.6.**, $G = Aut(E/j(G))$. □

Teorema 2.14.8 (Secondo teorema di Galois).
Sia $F \subseteq E$ di Galois e sia $F \subseteq K \subseteq E$, allora $F \subseteq K$ è di Galois $\Longleftrightarrow Aut(E/K) \lhd Aut(E/F)$. In tal caso $Aut(K/F) \cong Aut(E/F)/Aut(E/K)$.

Dimostrazione. ($\Longrightarrow$) Sia $F \subseteq K$ di Galois e sia $\begin{array}{rccc} \phi: & Aut(E/F) & \longrightarrow & Aut(K/F) \\ & \psi & \longmapsto & \psi_{|K} \end{array}$. Per il **Corollario 2.14.4.**, ϕ è ben definita. Notiamo che ϕ è omomorfismo e $Ker\,\phi = Aut(E/K)$, quindi $Aut(E/K)$ è normale. Resta solo da dimostrare che ϕ è surgettivo.
Sia $\tau: K \longrightarrow K$ tale che $\tau_{|F} = Id$, insomma $\tau \in Aut(K/F)$. Ricordiamo che se $F \subseteq E$ è di Galois, allora E è campo di spezzamento su F di un polinomio $g(x) \in F[x]$ separabile.

$$
\begin{tikzcd}
E \arrow[r, dashed, "T"] & E \\
K \arrow[u, dashed, dash, "\substack{\text{campo di spez-}\\ \text{zamento di } g(x)}"] \arrow[r, "\tau"] & K \arrow[u, dashed, dash, "\tilde{\tau}\left(g(x)\right)=g(x)"']
\end{tikzcd}
$$

$\exists T$ che estende τ per il **Teorema 14.10.** delle dispense di Aritmetica. Dunque $\phi(T) = T_{|K} = \tau$ e ϕ è surgettivo.

($\Longleftarrow$) Studiarla sulle dispense. □

Teorema 2.14.9 (Terzo teorema di Galois).
Sia $F \subseteq E$ estensione di Galois. Se $F \subseteq K \subseteq E$, allora $|Aut(^E/_K)| = [E : K]$ e inoltre $[K : F] =$ indice di $Aut(^E/_K)$ in $Aut(^E/_F)$.

Dimostrazione.

$$|Aut(^E/_F)| \overset{\substack{F \subseteq E \text{ è} \\ \text{di Galois}}}{=} [E : F] \overset{\substack{\textbf{Teorema} \\ \textbf{delle Torri}}}{=} [E : K] \cdot [K : F] \overset{\substack{K \subseteq E \text{ è} \\ \text{di Galois}}}{=} |Aut(^E/_K)| \cdot [K : F]$$

$\square$

Esercizio 44. *Trovare il polinomio minimo di* $\alpha = \sqrt{2 + i\sqrt{2}}$ *e di* $\alpha^2 + 1$.

Dimostrazione. Troviamo facilmente un polinomio che si annulla in α:

$$\alpha^2 = 2 + i\sqrt{2} \Longrightarrow (\alpha^2 - 2)^2 = -2 \Longrightarrow \alpha^4 - 4\alpha^2 + 6 = 0$$

quindi α è radice del polinomio $p(x) = x^4 - 4x^2 + 6$ e notiamo anche che $i\sqrt{2} \in \mathbb{Q}(\alpha)$.
Adesso dobbiamo capire se $p(x)$ è irriducibile e, di conseguenza, proprio il polinomio minimo di α.
$p(x)$ è palesemente irriducibile per Eisenstein con $p = 2$, comunque possiamo dimostrarlo anche nel seguente modo: sia K il campo di spezzamento di $p(x)$ su $\mathbb{Q}$.
Visto che K è il campo di spezzamento di $p(x)$ (che sia o meno irriducibile), l'estensione $\mathbb{Q} \subseteq K$ è di Galois $\Longrightarrow \exists \tau \in Aut({}^{K}/_{\mathbb{Q}})$ tale che $\tau(i\sqrt{2}) \neq i\sqrt{2}$, perciò, dal momento che $x^2 + 2$, il polinomio minimo di $i\sqrt{2}$, ha solo due radici, $\tau(i\sqrt{2}) = -i\sqrt{2}$.
Osserviamo che $\tau(\alpha^2) = 2 - i\sqrt{2}$, quindi $\tau(\alpha) = \pm\sqrt{2 - i\sqrt{2}} = \pm\beta$.
Chi possono essere le radici del polinomio minimo di α?

- $\{\alpha, -\alpha\}$: il termine noto del polinomio sarebbe $-(2 + i\sqrt{2}) \notin \mathbb{Q}$;
- $\{\alpha, \beta\}$: il termine noto del polinomio sarebbe $\sqrt{4 + 2} = \sqrt{6} \notin \mathbb{Q}$;
- $\{\alpha, -\beta\}$: il termine noto del polinomio sarebbe $-\sqrt{6} \notin \mathbb{Q}$;
- $\{\alpha, -\alpha, \beta, -\beta\}$: sono le radici di $p(x)$ che, per esclusione, è il polinomio minimo di α.

$\alpha^2 + 1$ è radice di $(x - 3)^2 + 2 = x^2 - 6x + 11$ che, essendo di grado 2 e a coefficienti in $\mathbb{Q}$, è necessariamente il suo polinomio minimo. □

Esercizio 45. *Trovare il polinomio minimo di* $\alpha = \sqrt{2 + \sqrt{3}}$ *e il relativo campo di spezzamento.*

Dimostrazione. Troviamo facilmente un polinomio che si annulla in α:

$$\alpha^2 = 2 + \sqrt{3} \Longrightarrow (\alpha^2 - 2)^2 = 3 \Longrightarrow \alpha^4 - 4\alpha^2 + 1 = 0$$

quindi α è radice del polinomio $p(x) = x^4 - 4x^2 + 1$.
Adesso dobbiamo capire se $p(x)$ è irriducibile e, di conseguenza, proprio il polinomio minimo di α.
Come prima, chiamiamo K il campo di spezzamento di $p(x)$ su $\mathbb{Q}$.
Visto che K è il campo di spezzamento di $p(x)$ (che sia o meno irriducibile), l'estensione $\mathbb{Q} \subseteq K$ è di Galois $\Longrightarrow \exists \tau \in Aut({}^{K}/_{\mathbb{Q}})$ tale che $\tau(\sqrt{3}) = -\sqrt{3}$ perciò, come prima, $\tau(\alpha) = \pm\sqrt{2 - \sqrt{3}}$.
Osserviamo che

$$\alpha \cdot \sqrt{2 - \sqrt{3}} = \sqrt{2 + \sqrt{3}} \cdot \sqrt{2 - \sqrt{3}} = 1 \Longrightarrow \sqrt{2 - \sqrt{3}} = \alpha^{-1}$$

Perciò $\mathbb{Q}(\alpha)$ contiene tutte le radici di $p(x)$ e, in particolare, pure $\sqrt{3} \in \mathbb{Q}(\alpha)$.
Notiamo adesso che

$$\left(\alpha + \frac{1}{\alpha}\right)^2 = \alpha^2 + \frac{1}{\alpha^2} + 2 = 2 + \sqrt{3} + 2 - \sqrt{3} + 2 = 6 \Longrightarrow \alpha + \frac{1}{\alpha} = \pm\sqrt{6} \Longrightarrow \sqrt{6} \in \mathbb{Q}(\alpha)$$

$$\begin{tikzcd} \mathbb{Q}(\alpha) \arrow[dd, dash, "4\geq"'] \arrow[dr, dash] & \\ & \mathbb{Q}(\sqrt{3}, \sqrt{6}) \arrow[dl, dash, "4"] \\ \mathbb{Q} & \end{tikzcd} \Longrightarrow \text{visto che } \alpha \text{ ha grado 4 su } \mathbb{Q},\ p(x) \text{ è il suo polinomio minimo}$$

$$\Longrightarrow \mathbb{Q}(\sqrt{3}, \sqrt{6}) = K \text{ è il campo di spezzamento di } p(x).$$

Per essere sicuri di aver fatto bene, vorremmo riuscire a scrivere $\alpha = a + b\sqrt{3} + c\sqrt{6} + d\sqrt{2}$, con $a, b, c, d \in \mathbb{Q}$. Sappiamo anche che $Aut(^{K}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$, perciò consideriamo due suoi generatori:

$$\tau: \begin{array}{ccc} \sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ \sqrt{6} & \longmapsto & -\sqrt{6} \end{array} \qquad \sigma: \begin{array}{ccc} \sqrt{2} & \longmapsto & -\sqrt{2} \\ \sqrt{3} & \longmapsto & \sqrt{3} \\ \sqrt{6} & \longmapsto & -\sqrt{6} \end{array} \qquad \tau\sigma: \begin{array}{ccc} \sqrt{2} & \longmapsto & -\sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ \sqrt{6} & \longmapsto & \sqrt{6} \end{array}$$

Si hanno tre casi:

- $\begin{array}{ccc} \alpha & \longmapsto & -\alpha \\ \sqrt{3} & \longmapsto & \sqrt{3} \\ \sqrt{6} & \longmapsto & -\sqrt{6} \\ \sqrt{2} & \longmapsto & -\sqrt{2} \end{array}$ cioè $\sigma \Longrightarrow \begin{cases} \alpha + \sigma(\alpha) = \alpha - \alpha = 0 \\ \alpha + \sigma(\alpha) = 2a + 2b\sqrt{3} \end{cases} \Longrightarrow a = b = 0;$

- $\begin{array}{ccc} \alpha & \longmapsto & \frac{1}{\alpha} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ \sqrt{6} & \longmapsto & \sqrt{6} \\ \sqrt{2} & \longmapsto & -\sqrt{2} \end{array}$ cioè $\tau\sigma \Longrightarrow \begin{cases} \alpha + \tau\sigma(\alpha) = \alpha + \frac{1}{\alpha} = \pm\sqrt{6} \\ \alpha + \tau\sigma(\alpha) = 2a + 2c\sqrt{6} \end{cases} \Longrightarrow c = \pm\frac{1}{2};$

- $\begin{array}{ccc} \alpha & \longmapsto & -\frac{1}{\alpha} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ \sqrt{6} & \longmapsto & -\sqrt{6} \\ \sqrt{2} & \longmapsto & \sqrt{2} \end{array}$ cioè $\tau \Longrightarrow \begin{cases} \alpha + \tau(\alpha) = \alpha - \frac{1}{\alpha} = \pm\sqrt{2} \\ \alpha + \tau(\alpha) = 2a + 2d\sqrt{2} \end{cases} \Longrightarrow d = \pm\frac{1}{2}.$

Perciò $\alpha = \pm\frac{1}{2}\sqrt{2} \pm \frac{1}{2}\sqrt{6}$, infatti $\alpha^2 = \frac{1}{4}(2 + 6 + 4\sqrt{3}) = 2 + \sqrt{3}$. □

Esercizio 46. *Trovare il campo di spezzamento e il gruppo di Galois di $p(x) = x^4 - 6x^2 + 25$.*

Dimostrazione. Le radici di $p(x)$ sono $x_{1,2,3,4} = \pm\sqrt{3 \pm 4i}$.
Chiamo $\alpha = \sqrt{3 + 4i}$ e $\beta = \sqrt{3 - 4i} \Longrightarrow \alpha\beta = \sqrt{25} = \pm 5 \Longrightarrow \frac{1}{\alpha} = \pm\frac{\sqrt{3-4i}}{5} \Longrightarrow$

$$\left(\alpha + \frac{5}{\alpha}\right)^2 = (\sqrt{3+4i} \pm \sqrt{3-4i})^2 = 3 + 4i + 3 - 4i \pm 10 = \begin{cases} 16 \\ -4 \end{cases}$$

$\alpha + \frac{5}{\alpha} = \pm 4 \Longrightarrow \alpha$ è radice di $x^2 + 4x + 5$ e di $x^2 - 4x + 5$:

$$(x^2 + 4x + 5)(x^2 - 4x + 5) = (x^2 + 5)^2 - 16x^2 = x^4 - 6x^2 + 25 = p(x)$$

$\Longrightarrow p(x)$ non è irriducibile, perciò il suo campo di spezzamento è $\mathbb{Q}(i)$.
Perciò $Aut(^{\mathbb{Q}(i)}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}}$. □

Esercizio 47. *Calcolare il campo di spezzamento e il gruppo di Galois di $x^3 - x + 1$ e di $x^3 - 3x + 1$.*

Dimostrazione. Non hanno radici in $\mathbb{Q} \Longrightarrow$ sono irriducibili su $\mathbb{Q}$ (perché sono di grado 3) $\Longrightarrow$ il grado del campo di spezzamento è 3 o 6 su $\mathbb{Q}$: $Aut(^{K}/_{\mathbb{Q}}) = \begin{cases} S_3 \\ A_3 \end{cases}$

Per distinguere i due casi dobbiamo vedere se nel gruppo di Galois abbiamo un elemento che permuta in maniera dispari le radici. Siano quindi $\alpha_1, \alpha_2, \alpha_3$ le radici del polinomio irriducibile

di grado 3.
Detto $\delta := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, sia $\sigma \in Aut(^K/_{\mathbb{Q}})$, allora

$$\sigma(\delta) = \begin{cases} \delta & \text{se } \sigma \text{ è pari} \\ -\delta & \text{se } \sigma \text{ è dispari} \end{cases}$$

Prendiamo $\Delta = \delta^2$ e notiamo che sicuramente è fissato da $Aut(^K/_{\mathbb{Q}})$:

$$x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \Longrightarrow \Delta = -4a^3 - 27b^2 \in \mathbb{Q}.$$

- Se Δ è un quadrato in $\mathbb{Q} \Longrightarrow \delta \in \mathbb{Q} \Longrightarrow \delta$ è fissato da $Aut(^K/_{\mathbb{Q}})$.
- Se Δ non è un quadrato in $\mathbb{Q} \Longrightarrow \delta \notin \mathbb{Q} \Longrightarrow \delta$ non è fissato da $Aut(^K/_{\mathbb{Q}})$.

Perciò, in conclusione:

- se $p(x) = x^3 - x + 1 \Longrightarrow \Delta = -23 \Longrightarrow Aut(^K/_{\mathbb{Q}}) = S_3$;
- se $p(x) = x^3 - 3x + 1 \Longrightarrow \Delta = 81 = 9^2 \Longrightarrow Aut(^K/_{\mathbb{Q}}) = A_3$.

$\square$

(Se si ha un polinomio $p(x) = ax^3 + bx^2 + cx + d$, dove la somma delle sue radici $\alpha_1 + \alpha_2 + \alpha_3 = b$, lo si può traslare $p(x) \longrightarrow p\left(x + \frac{b}{3}\right)$ che ha la somma delle radici $\alpha_1 + \alpha_2 + \alpha_3 = 0$.)

In generale, se abbiamo un polinomio $p(x) = x^3 + ax + b$ irriducibile su $\mathbb{Q}$, con una radice reale α_1 e due complesse coniugate α_2, α_3, il campo di spezzamento K di $p(x)$ su $\mathbb{Q}$ lo otteniamo aggiungendo a $\mathbb{Q}$ tutte e tre le radici: notiamo che, applicando il coniugio dei numeri complessi al campo di spezzamento, α_1 rimane ferma mentre $\alpha_2 \longleftrightarrow \alpha_3$, perciò $Aut(^K/_{\mathbb{Q}})$ contiene una trasposizione, cioè una permutazione dispari $\Longrightarrow Aut(^K/_{\mathbb{Q}}) \cong S_3$.

Possiamo anche vedere dove si annulla la derivata formale: dato $p(x) = x^3 + ax + b$, $p'(x) = 3x^2 + a$. La derivata si annulla in $x_{1,2} = \pm\sqrt{-\frac{a}{3}}$, perciò calcoliamo

$$p(x_1) = \left(\sqrt{-\frac{a}{3}}\right)^3 + a\sqrt{-\frac{a}{3}} + b \ \text{ e } \ p(x_2) = -\left(\sqrt{-\frac{a}{3}}\right)^3 - a\sqrt{-\frac{a}{3}} + b$$

e anche

$$p(x_1) \cdot p(x_2) = \left(b + a\frac{2}{3}\sqrt{-\frac{a}{3}}\right)\left(b - a\frac{2}{3}\sqrt{-\frac{a}{3}}\right) = b^2 + \frac{4}{27}a^3$$

$p(x)$ ha tre radici reali se e solo se $p(x_1) \cdot p(x_2) < 0$, perciò

$$b^2 + \frac{4}{27}a^3 < 0 \Longleftrightarrow -4a^3 - 27b^2 > 0$$

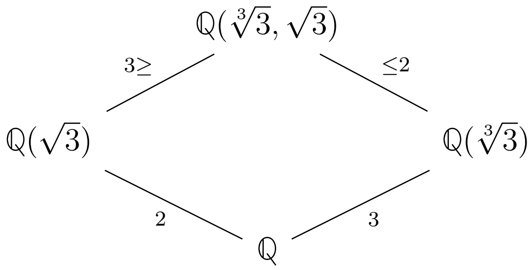
Sia $f(x)$ irriducibile di grado p primo, con $p-2$ radici reali e 2 complesse coniugate.
Sia α radice tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ e K il relativo campo di spezzamento $\Longrightarrow$
$G = Aut(^K/_{\mathbb{Q}}) < S_p$, $p \mid \#G \Longrightarrow G$ contiene un p-ciclo.
Avendo 2 radici complesse coniugate $\Longrightarrow G$ contiene una trasposizione $\Longrightarrow G = S_p$.

Teorema 2.14.10 (fondamentale dell'Algebra).
Ogni polinomio non costante in $\mathbb{C}[x]$ ammette una radice in $\mathbb{C}$.

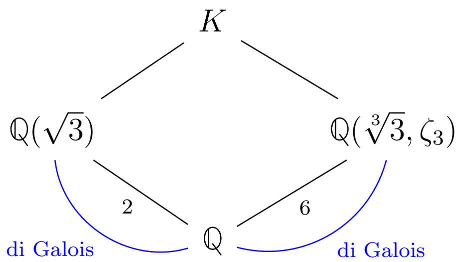
Dimostrazione. Equivale a dire che $\mathbb{C} = \mathbb{R}(i)$ ammette estensioni finite solo di grado 1.
Sia L estensione finita di $\mathbb{C}$, vogliamo quindi dimostrare che $L = \mathbb{C}$.
Osserviamo che $L \subseteq E$ tale che $[E : \mathbb{R}]$ è di Galois.
Infatti, $L = \mathbb{R}(i)(\alpha_1, ..., \alpha_n)$, per il **Teorema dell'elemento primitivo** (notate che $i, \alpha_1, ..., \alpha_n$ sono separabili perché siamo in caratteristica 0), $L = \mathbb{R}(\delta)$. Sia $f(x) \in \mathbb{R}[x]$ il polinomio minimo di δ (in particolare $f(\delta) = 0$). Sia E un campo di spezzamento su $\mathbb{R}$ di $f(x)$ che contiene δ. Dunque $E \supseteq L = \mathbb{R}(\delta) \supseteq \mathbb{R}(i) \supseteq \mathbb{R}$.
Strategia: dimostreremo che $E = \mathbb{R}(i) \implies L = \mathbb{R}(i)$.
Sia $G = Aut(^E/_\mathbb{R})$ gruppo di Galois. $|G| = [E : \mathbb{R}] = [E : \mathbb{R}(i)] \cdot [\mathbb{R}(i) : \mathbb{R}] = 2 \cdot [E : \mathbb{R}(i)]$. Sia N_2 il 2-Sylow di G, $N_2 < G$. Per la corrispondenza di Galois, a N_2 corrisponde un sottocampo $J(N_2) = \{a \in E \,|\, \varphi(a) = a \ \forall \varphi \in N_2\}$ tale che $\mathbb{R} \subseteq J(N_2) \subseteq E$.
Per il **Terzo teorema di Galois**, $[J(N_2) : E] = \underbrace{\text{indice di } N_2 \text{ in } G}_{\text{dispari}}$. Per il **Teorema dell'elemento primitivo**, $J(N_2) = \mathbb{R}(\alpha)$. Sia $g(x)$ il polinomio minimo su $\mathbb{R}$ di α. Dunque $\deg g(x) = [J(N_2) : \mathbb{R}]$ è dispari. Per un noto teorema di Analisi, deve essere $\deg g(x) = 1$, ma allora $\mathbb{R}(\alpha) = \mathbb{R}$, ossia $J(N_2) = \mathbb{R}$, allora, per la corrispondenza di Galois, $N_2 = G$.
Consideriamo $G_1 < G$, con $G_1 = Aut(^E/_{\mathbb{R}(i)})$. $\#G_1 \mid \#G$, dunque $|G_1| = 2^s$.
Se $G_1 = \{e\}$, allora $[E : \mathbb{R}(i)] = |G_1| = 1$ e abbiamo finito.
Se fosse $G_1 \neq \{e\}$, per **Sylow I**, esiste $G_2 < G_1$ tale che $|G_2| = 2^{s-1}$.
Consideriamo il suo campo fisso $J(G_2)$ e osserviamo che $\mathbb{R}(i) \subseteq J(G_2) \subseteq E$, per il **Terzo teorema di Galois**, $[J(G_2) : \mathbb{R}(i)] =$ indice di G_2 in $G_1 = 2$, assurdo, perché sappiamo che non esistono estensioni di grado 2 di $\mathbb{C}$, visto che di un polinomio in $\mathbb{C}[x]$ di grado 2 sappiamo trovare le radici con la ben nota formula risolutiva. $\square$

Esercizio 48. *Sia* $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$*, dimostrare che* $[K : \mathbb{Q}]$ *è di Galois e calcolare* $Aut(^K/_\mathbb{Q})$*. Determinare poi tutti i campi* F *tali che* $\mathbb{Q} \subseteq F \subseteq K$ *tali che* $[F : \mathbb{Q}] = 6$.

Dimostrazione. Osserviamo che il campo di spezzamento di $(x^3 - 3)(x^2 - 3)$ è $\mathbb{Q}(\sqrt[3]{3}, \zeta_3, \sqrt{3})$ e tale campo equivale a K visto che $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Dunque K è campo di spezzamento di un polinomio separabile, quindi $\mathbb{Q} \subseteq K$ è di Galois.
Calcoliamo $[K : \mathbb{Q}]$:



Dato che $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] \leq 6$ ed è diviso sia da 2 che da 3, si ha $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = 6$.
Ora consideriamo $K = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})(i)$ e dunque, per il **Teorema delle Torri**, $[K : \mathbb{Q}] = 12$ $\big(i \notin \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})$ visto che $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) \subseteq \mathbb{R}\big)$.



Notiamo che $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt[3]{3},\zeta_3) = \mathbb{Q}$, infatti, se fosse $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt[3]{3},\zeta_3) = \mathbb{Q}(\sqrt{3})$ (l'unica alternativa per motivi di grado) avremmo $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{3},\zeta_3)$, ossia $K = \mathbb{Q}(\sqrt[3]{3},\zeta_3)$ ma abbiamo già dimostrato che $[K : \mathbb{Q}] = 12 \lightning$.
Costruiamo

$$\begin{array}{rccc} \phi: & Aut(K/F) & \longrightarrow & Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \times Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q}) \\ & \sigma & \longmapsto & (\sigma_{|_{\mathbb{Q}(\sqrt{3})}}, \sigma_{|_{\mathbb{Q}(\sqrt[3]{3},\zeta_3)}}) \end{array}$$

ϕ è ben definita perché $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$ e $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{3},\zeta_3)$ sono di Galois.
ϕ è omomorfismo (verifica immediata).
ϕ è iniettiva, perché se $\sigma_{|_{\mathbb{Q}(\sqrt{3})}} = Id$ e $\sigma_{|_{\mathbb{Q}(\sqrt[3]{3},\zeta_3)}} = Id$, allora $\sigma(\sqrt{3}) = \sqrt{3}$, $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$ e $\sigma(\zeta_3) = \zeta_3$, allora $\sigma = Id$ (σ fissa tutto K).
Per ragioni di cardinalità, ϕ è anche bigettiva, dunque ϕ è isomorfismo.

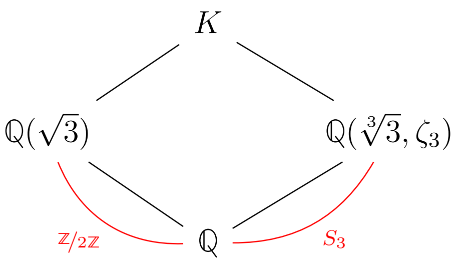
$$Aut(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q})$$

Consideriamo $\tau \in Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q}(\sqrt[3]{3}))$ tale che $\tau(\sqrt[3]{3}) = \sqrt[3]{3}$ e $\tau(\zeta_3) = \zeta_3^2$. τ esiste perché consideriamo il polinomio $x^2 + x + 1$ che è irriducibile su $\mathbb{Q}(\sqrt[3]{3})$ e ζ_3 e ζ_3^2 sono le sue radici.
Usiamo dunque il vecchio teorema di Aritmetica, $\begin{array}{rccc} \tau: & \mathbb{Q}(\sqrt[3]{3})(\zeta_3) & \longrightarrow & \mathbb{Q}(\sqrt[3]{3})(\zeta_3^2) \\ & \zeta_3 & \longmapsto & \zeta_3^2 \end{array}$.
Analogamente consideriamo $\sigma \in Aut(\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q}(\zeta_3))$ tale che $\sigma(\zeta_3) = \zeta_3$ e $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}\zeta_3$ $\big(\sqrt[3]{3}$ e $\sqrt[3]{3}\zeta_3$ sono entrambe radici di $x^3 - 3$ che è irriducibile su $\mathbb{Q}(\zeta_3)\big)$.
τ e σ appartengono anche a $Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q})$.
Notiamo che $\tau^2 = Id$ e $\sigma^3 = Id$ e che $\tau\sigma\tau = \sigma^{-1} \neq \sigma$: infatti,

$$\tau\sigma\tau(\zeta_3) = \tau\sigma(\zeta_3^2) = \tau(\sigma_3^2) = \zeta_3^4 = \zeta_3 \;\text{ e }\; \tau\sigma\tau(\sqrt[3]{3}) = \tau\sigma(\sqrt[3]{3}) = \tau(\sqrt[3]{3}\zeta_3) = \sqrt[3]{3}\zeta_3^2$$

Mentre $\sigma^{-1}(\zeta_3) = \zeta_3$ e $\sigma^{-1}(\sqrt[3]{3}) = \sqrt[3]{3}\zeta_3^2$.
Con questo abbiamo dimostrato che $Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q}) \cong D_3 \cong S_3 \Longrightarrow Aut(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times S_3$.
<u>Alternativa</u>: si osserva che $Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q}) \cong D_3 \cong S_3$ possiamo vederlo come sottogruppo di S_3, infatti prendiamo $X = \{\sqrt[3]{3}, \sqrt[3]{3}\zeta_3, \sqrt[3]{3}\zeta_3^2\}$ e, dato $\sigma \in Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q})$, $\sigma_{|X}$ è una bigezione di X:
$\sigma(X) \subseteq X$, dunque abbiamo un omomorfismo iniettivo $Aut(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q}) \longrightarrow S_3$ e, per ragioni di cardinalità, <u>in questo caso</u> è un isomorfismo.
Parte finale: trovare tutti i sottocampi F, con $\mathbb{Q} \subseteq F \subseteq K$, tali che $[F : Q] = 6$.
Per il **Terzo teorema di Galois**, tali F corrispondono ai sottogruppi di indice 6 di $\mathbb{Z}/2\mathbb{Z} \times S_3 = Aut(K/\mathbb{Q})$, ossia i sottogruppi di ordine 2 generati da

$$\left.\begin{array}{cc} \big(0,(i,j)\big) & 3 \text{ elementi} \\ \big(1,(i,j)\big) & 3 \text{ elementi} \\ (1,e) & 1 \text{ elemento} \end{array}\right\} \text{ci sono dunque 7 sottogruppi di ordine 2} \Longrightarrow \text{ci sono 7 sottocampi.}$$



Esiste dunque $\tilde{\sigma} \in Aut(K/\mathbb{Q})$ tale che $\tilde{\sigma}(\sqrt{3}) = \sqrt{3}$, $\tilde{\sigma}(\zeta_3) = \zeta_3$ e $\tilde{\sigma}(\sqrt[3]{3}) = \sqrt[3]{3}\zeta_3$.
Allo stesso modo, esiste $\tilde{\tau} \in Aut(K/\mathbb{Q})$ tale che $\tilde{\tau}(\sqrt{3}) = \sqrt{3}$, $\tilde{\tau}(\zeta_3) = \zeta_3^2$ e $\tilde{\tau}(\sqrt[3]{3}) = \sqrt[3]{3}$.
Esiste anche $\gamma \in Aut(K/\mathbb{Q})$ tale che $\gamma \leftrightarrow (1,e)$, cioè $\gamma(\sqrt{3}) = -\sqrt{3}$, $\gamma(\zeta_3) = \zeta_3$ e $\gamma(\sqrt[3]{3}) = \sqrt[3]{3}$.

Notiamo che $ord(\gamma) = 2$, $ord(\tilde{\tau}) = 2$ e $ord(\tilde{\sigma}) = 3$.
$\gamma, \tilde{\tau}, \tilde{\sigma}$ generano $Aut({}^{K}/_{\mathbb{Q}})$ visto che le loro immagini generano ${}^{\mathbb{Z}}/_{2\mathbb{Z}} \times S_3$.
Notiamo inoltre che γ, $\tilde{\tau}$, $\tilde{\tau}\tilde{\sigma}$ e $\tilde{\tau}\tilde{\sigma}^2$ e anche $\gamma\tilde{\tau}$, $\gamma\tilde{\tau}\tilde{\sigma}$ e $\gamma\tilde{\tau}\tilde{\sigma}^2$ hanno ordine 2.
Basta dunque trovare, per ognuno di questi elementi, il sottocampo di K da lui fissato $\big($Notazione: $Fix(\cdot)\big)$.

- $Fix(\tilde{\tau}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ che ha grado 6.
- $Fix(\tilde{\tau}\tilde{\sigma}) = ?$ Certamente c'è $\sqrt{3}$, Vediamo ora $\tilde{\tau}\tilde{\sigma}(\sqrt[3]{3}\zeta_3) = \tilde{\tau}(\sqrt[3]{3}\zeta_3^2) = \sqrt[3]{3}\zeta_3^4 = \sqrt[3]{3}\zeta_3 \Longrightarrow \sqrt[3]{3}\zeta_3 \in Fix(\tilde{\tau}\tilde{\sigma}) \Longrightarrow Fix(\tilde{\tau}\tilde{\sigma}) = \mathbb{Q}(\sqrt[3]{3}\zeta_3, \sqrt{3})$ (per ragioni di grado) che ha grado 6.
- $Fix(\gamma\tilde{\tau}) = ?$ Di sicuro c'è $\sqrt[3]{3}$. $\gamma\tilde{\tau} \in Aut({}^{K}/_{\mathbb{Q}(\sqrt[3]{3})})$. L'estensione $\mathbb{Q}(\sqrt[3]{3}) \subseteq K$ ha grado 4. $\{1, \zeta_3, \sqrt{3}, \sqrt{3}\zeta_3\}$ è base di K su $\mathbb{Q}(\sqrt[3]{3})$, perciò $\gamma\tilde{\tau} : K \longrightarrow K$ è anche applicazione $\mathbb{Q}(\sqrt[3]{3})$-lineare. $\gamma\tilde{\tau}$, rispetto alla base fissata in partenza e in arrivo, ha matrice

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

$\big($in cui la prima colonna è data da $\gamma\tilde{\tau}(1)$, la seconda da $\gamma\tilde{\tau}(\zeta_3)$, la terza da $\gamma\tilde{\tau}(\sqrt{3})$ e la quarta da $\gamma\tilde{\tau}(\sqrt{3}\zeta_3)\big) \Longrightarrow$ da questo punto di vista, $Fix(\gamma\tilde{\tau}) = Ker(\gamma\tilde{\tau} - Id) =$

$$= Ker \begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = Span < \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} >= \{a + b(\sqrt{3} + 2\sqrt{3}\zeta_3) \mid a, b \in \mathbb{Q}(\sqrt[3]{3})\}.$$

Perciò $Fix(\gamma\tilde{\tau}) = \mathbb{Q}(\sqrt[3]{3}, \overbrace{\sqrt{3} + 2\sqrt{3}\zeta_3}^{=3i}) = \mathbb{Q}(\sqrt[3]{3}, i)$.

Esercizio 49. *Proseguire e trovare tutti e 7 i campi.*

□

2.15 Polinomi ciclotomici

Definizione 2.15.1. $\phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i)$, *dove α_i sono le radici primitive n-esime di 1.*
Il gruppo moltiplicativo $(\zeta_n) \cong {}^{\mathbb{Z}}/_{n\mathbb{Z}}$.

A priori $\phi_n(x) \in \mathbb{C}[x]$.

$\phi_1(x) = x-1 \quad \phi_2(x) = x+1 \quad \phi_3(x) = x^2+x+1 \quad \phi_4(x) = x^2+1 \quad \phi_5(x) = x^4+x^3+x^2+x+1$

$\phi_6(x) = x^2-x+1 \quad \phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1 \quad \phi_8(x) = x^4+1 \quad \phi_9(x) = x^6+x^3+1$

Osservazione 12. $\prod_{d|n} \phi_d(x) = x^n - 1$.

Teorema 2.15.1. $\forall n \geq 1$ $\phi_n(x) \in \mathbb{Z}[x]$ *ed è irriducibile in $\mathbb{Z}[x]$ (e quindi in $\mathbb{Q}[x]$).*
Inoltre, il campo di spezzamento di $\phi_n(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\zeta_n)$, ha grado $\varphi(n)$ e $Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}}) \cong ({}^{\mathbb{Z}}/_{n\mathbb{Z}})^*$.

Corollario 2.15.2. *Siano n, m coprimi, allora $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ e $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.*

Esempio 13. *$\zeta_4 = i$, $\mathbb{Q}(\zeta_4) \cap \mathbb{Q}(\zeta_5) = \mathbb{Q}$ e $\mathbb{Q}(\zeta_4, \zeta_5) = \mathbb{Q}(\zeta_{20})$.*

Dimostrazione. (**Corollario 2.15.2.**)

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_n,\zeta_m)=\mathbb{Q}(\zeta_{nm}) \arrow[dl, dash, "\varphi(m)"'] \arrow[dr, dash, "\varphi(n)"] \arrow[dd, dash, "\varphi(nm)"'] & \\
\mathbb{Q}(\zeta_n) \arrow[dr, dash, "\varphi(n)"'] & & \mathbb{Q}(\zeta_m) \arrow[dl, dash, "\varphi(m)"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

dove $\varphi(nm) = \varphi(n)\varphi(m)$. Se consideriamo un campo $F = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$ tale che $[\mathbb{Q}(\zeta_n) : F] = d$, con $1 < d \mid \varphi(n) \Longrightarrow \varphi(n) = [\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}(\zeta_m)] \leq d \Longrightarrow d = \varphi(n)$. $\square$

Dimostrazione. (**Teorema 2.15.1.**) Consideriamo il campo di spezzamento di $f(x) = x^n - 1$ su $\mathbb{Q}$: è $\mathbb{Q}(\zeta_n)$. L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ è di Galois, perché $x^n - 1$ è separabile.
Sia $\begin{array}{rccc} \theta: & Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}}) & \longrightarrow & Aut({}^{\mathbb{Z}}/_{n\mathbb{Z}}) \\ & \sigma & \longmapsto & \sigma_{|_{(\zeta_n)}} \end{array}$, dove (ζ_n) è il gruppo ciclico moltiplicativo generato da ζ_n. Visto che $\sigma_| : (\zeta_n) \longrightarrow (\zeta_n)$ e che σ è iniettivo $\Longrightarrow$ σ è bigettivo. σ è in particolare un omomorfismo moltiplicativo, allora $\sigma_| \in Aut\big((\zeta_n)\big)$. Inoltre θ è iniettivo perché se $\sigma_| = Id$, allora $\sigma(\zeta_n) = \zeta_n$ e dunque $\sigma = Id$ in $Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}})$.

Osservazione 13. *Per ora possiamo dunque dire che $|Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}})| \leq \varphi(n)$.*

Lemma 2.15.3. *Siano n un intero positivo, ω una radice primitiva n-esima di 1 e $q(x) \in \mathbb{Z}[x]$ il suo polinomio minimo primitivo, allora $\forall p$ primo tale che $p \nmid n$, ω^p è radice di $q(x)$.*

Dimostrazione. Per il **Lemma di Gauss**, $f(x) = x^n - 1 = q(x)g(x)$, con $q(x), g(x) \in \mathbb{Z}[x]$ primitivi. Dato che il coefficiente direttore di $f(x)$ è 1, posso supporre che i coefficienti direttori di $q(x)$ e $g(x)$ siano entrambi 1 (l'alternativa sarebbe stata entrambi -1). Sappiamo che ω è radice di $q(x)$. ω^p è radice di $x^n - 1$, dunque, se non fosse radice di $q(x)$, dovrebbe essere radice di $g(x)$. Perciò ω è radice di $g(x^p)$, allora $q(x) \mid g(x^p)$ perché $q(x)$ era polinomio minimo di ω. Per il **Lemma di Gauss**, $g(x^p) = q(x)h(x)$, con $h(x) \in \mathbb{Z}[x]$ primitivo, e si osserva che il coefficiente direttivo di $h(x)$ è 1. Proiettiamo la relazione $g(x^p) = q(x)h(x)$ in ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[x]$:

$$\overline{g(x^p)} = \overline{q}(x)\overline{h}(x)$$

(i polinomi sono monici quindi sicuramente non si annullano).
Osserviamo che $\overline{g(x^p)} = \big(\overline{g}(x)\big)^p$, perché in ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[x]$ per ogni polinomio $\gamma(x)$ vale $\gamma(x^p) = \big(\gamma(x)\big)^p$.
Dunque, riassumendo, in ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[x]$ abbiamo $\overline{f}(x) = \overline{q}(x)\overline{g}(x)$ e $\big(\overline{g}(x)\big)^p = \overline{q}(x)\overline{h}(x)$. Quest'ultima ci dice inoltre che una radice di $\overline{q}(x)$ (in una estensione) è anche radice di $\overline{g}(x)$. Da $\overline{f}(x) = \overline{q}(x)\overline{g}(x)$ deduciamo che $\overline{f}(x)$ ha almeno una radice multipla, ma $\overline{f}'(x) = nx^{n-1}$ e ricordiamo che $p \nmid n$, dunque non è il polinomio nullo. Sia b l'inverso di n in ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$: $\overline{f}(x) - b\overline{f}'(x)x = x^n - 1 - x^n = -1$, dunque $MCD(\overline{f}, \overline{f}') = 1$ e questo contraddice il **Criterio della derivata**. $\square$

Sia allora $q(x)$, come sopra, il polinomio minimo primitivo di ζ_n in $\mathbb{Z}[x]$.
Le radici primitive n-esime di 1 sono della forma ζ_n^k, con $MCD(k, n) = 1$.
Sia $k = p_1^{\alpha_1} \cdot ... \cdot p_r^{\alpha_r}$, con $MCD(p_i, n) = 1$ $\forall i = 1, ..., r$.
ζ_n è radice di $q(x)$, $\zeta_n^{p_1}$ è radice di $q(x)$ per il **Lemma 2.15.1.**, $\zeta_n^{p_1^2}$ è radice di $q(x)$ per il **Lemma 2.15.1.** applicato a $\zeta_n^{p_1}$ e così via... $\zeta_n^{p_1^{\alpha_1} \cdot ... \cdot p_r^{\alpha_r}} = \zeta_n^k$ è radice di $q(x)$, quindi $q(x)$ è diviso da tutte le radici n-esime primitive. Dunque $\phi_n(x) \mid q(x)$, ma $\deg q(x) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, ma $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}})|$ perché $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ è di Galois, allora $\deg q(x) = |Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}})| \leq \varphi(n)$ per la disuguaglianza iniziale. Dato che $\phi_n(x) \mid q(x)$, deduciamo che $\deg q(x) = \varphi(n)$.
Poiché $\phi_n(x)$ e $q(x)$ sono monici, segue che $\phi_n(x) = q(x)$.
Tornando all'omomorfismo iniettivo $\theta : Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}}) \longrightarrow Aut({}^{\mathbb{Z}}/_{n\mathbb{Z}})$.
Ora, per ragioni di cardinalità, sappiamo che θ è un isomorfismo $\big($infatti adesso sappiamo che $|Aut({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}})| = \varphi(n)\big)$. $\square$

2.16 Campi finiti

Se ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \subseteq K$, allora K ha grado p^n: gli elementi di K sono tutte e sole le radici di $x^{p^n} - x$. Studiare il **Teorema 14.17.** sulle dispense di Aritmetica.

Osservazione 14. *$\mathbb{F}_{p^n}$ è estensione di Galois di ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, perché è campo di spezzamento di $x^{p^n} - x$ che ha radici tutte distinte ed è dunque separabile.*

Chi è $Aut({}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p})$? Ha n elementi.
Consideriamo l'**omomorfismo di Frobenius** $\mathcal{F} \in Aut({}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p})$. Sappiamo che $\mathcal{F}^n = Id$, quindi se $ord(\mathcal{F}) = n$, allora il gruppo è ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.
$(\mathbb{F}_{p^n})^*$ è ciclico generato da un certo γ: $ord(\gamma) = p^n - 1 \Longrightarrow ord(\mathcal{F}) = n$.
Sappiamo che $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ è di Galois in quanto campo di spezzamento di $x^{p^n} - x$ e sappiamo che $Aut({}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p}) \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ (generato da $\mathcal{F}$).
$\forall d \mid n$ ho in ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ un sottogruppo isomorfo a ${}^{\mathbb{Z}}\!/_{\frac{n}{d}\mathbb{Z}}$ $\big($ossia $(d)\big)$, allora $J\big((d)\big)$ è un sottocampo di $\mathbb{F}_{p^n}$ che ha grado d su $\mathbb{F}_p$, allora tale sottocampo è $\cong \mathbb{F}_{p^d}$. D'altra parte sapevamo già l'anno scorso che se $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$, allora $[K : \mathbb{F}_p] \mid n$.
Conclusione: i sottocampi di $\mathbb{F}_{p^n}$ sono tutti e soli gli $\mathbb{F}_{p^d}$, con $d \mid n$.

2.16.1 Conseguenza sui polinomi

Sia $f(x)$ un polinomio di grado d irriducibile su $\mathbb{F}_p$. ${}^{\mathbb{F}_p[x]}\!/_{\big(f(x)\big)} = K \cong \mathbb{F}_{p^d}$. Sappiamo inoltre che $f(x)$ ha tutte le radici in $\mathbb{F}_{p^d}$. Infatti, sicuramente, in K $f(x)$ ha una radice α.
Sappiamo anche che gli elementi di $K \cong \mathbb{F}_{p^d}$ sono tutte e sole le soluzioni di $x^{p^d} - x = 0$, allora $f(x) \mid x^{p^d} - x$, perché entrambi hanno α come radice e $f(x)$ è il polinomio minimo.
Allora tutte le radici di $f(x)$ sono anche radici di $x^{p^d} - x$ e dunque sono in K.
Per ragioni di grado, K è il campo di spezzamento di $f(x)$. Dato che $f(x)$ era un qualunque irriducibile di grado d, possiamo concludere che $\mathbb{F}_{p^d}$ è il campo di spezzamento di qualunque polinomio irriducibile di grado d su $\mathbb{F}_p$.

Corollario 2.16.1. *Sia $f(x) \in \mathbb{F}_p[x]$ tale che $f(x) = q_1(x) \cdot ... \cdot q_k(x)$, con $q_i(x)$ irriducibile di grado β_i $\forall i = 1, ..., k$, allora il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ è $F_{p^{mcm(\beta_1,...,\beta_k)}}$.*

Dimostrazione. Sia K il campo di spezzamento. Dato che contiene un campo di spezzamento di $q_1(x)$, allora contiene $\mathbb{F}_{p^{\beta_1}}$, dunque $\beta_1 \mid [K : \mathbb{F}_p]$ e così via... dunque $\beta_k \mid [K : \mathbb{F}_p]$ e quindi $mcm(\beta_1, ..., \beta_k) \mid [K : \mathbb{F}_p]$ e viceversa $\mathbb{F}_{p^{mcm(\beta_1,...,\beta_k)}}$ ha questo grado. $\square$

Esercizio 50. *Calcolare il campo di spezzamento e il relativo gruppo di Galois del polinomio irriducibile* $p(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$.

Dimostrazione. $\Delta = a^2 - 4b$ non può essere un quadrato in $\mathbb{Q}$. Se lo fosse, il polinomio t^2+at+b si fattorizzerebbe su $\mathbb{Q}[t]$ e quindi anche $p(x)$ non sarebbe irriducibile su $\mathbb{Q}[x]$.
Chiamiamo ω_1, ω_2 le radici di $t^2 + at + b$ (in cui chiaramente $a = \omega_1 + \omega_2$ e $b = \omega_1\omega_2$).
Se $\sqrt{\Delta} \in \mathbb{Q}$ o se ci mettiamo in $\mathbb{Q}(\sqrt{\Delta})$, abbiamo che

$$t^2 + at + b = (t - \omega_1)(t - \omega_2) \implies x^4 + ax^2 + b = (x^2 - \omega_1)(x^2 - \omega_2)$$

perciò le radici di $p(x)$ sono $\pm\sqrt{\omega_1}$ e $\pm\sqrt{\omega_2}$.
Se $p(x)$ fosse riducibile (prodotto di due fattori di grado 2), potrebbe essere

$$p(x) = (x^2 - \omega_1)(x^2 - \omega_2)$$

$$p(x) = \left[(x - \sqrt{\omega_1})(x - \sqrt{\omega_2})\right]\left[(x + \sqrt{\omega_1})(x + \sqrt{\omega_2})\right]$$
$$p(x) = \left[(x - \sqrt{\omega_1})(x + \sqrt{\omega_2})\right]\left[(x + \sqrt{\omega_1})(x - \sqrt{\omega_2})\right]$$

Chi sono i possibili termini noti dei fattori di grado 2?

$$\omega_1 \text{ e } \omega_2, \qquad \sqrt{\omega_1\omega_2} \text{ e } \sqrt{\omega_1\omega_2}, \qquad -\sqrt{\omega_1\omega_2} \text{ e } -\sqrt{\omega_1\omega_2}$$

Ci chiediamo: $b = \omega_1\omega_2$ è un quadrato in $\mathbb{Q}$?

No $\implies$ sicuramente $p(x)$ è irriducibile su $\mathbb{Q}$.

Sì $\implies$ il solo fatto che Δ non sia un quadrato in $\mathbb{Q}$ non basta come garanzia di irriducibilità. Potremmo quindi avere

$$p(x) = (x^2 + cx + \sqrt{b})(x^2 - cx + \sqrt{b}) \text{ oppure } p(x) = (x^2 + cx - \sqrt{b})(x^2 - cx - \sqrt{b})$$

Perciò $2\sqrt{b}x^2 - c^2x^2 = ax^2 \implies 2\sqrt{b} - a = c^2 \implies 2\sqrt{b} - a$ è un quadrato in $\mathbb{Q}$, oppure $-2\sqrt{b} - c^2 = a \implies -2\sqrt{b} - a = c^2 \implies -2\sqrt{b} - a$ è un quadrato in $\mathbb{Q}$.

La richiesta generale è quindi: $p(x)$ irriducibile $\iff \Delta$ non è un quadrato in $\mathbb{Q}$ e $\big((b$ non è un quadrato in $\mathbb{Q})$ o $(b$ è un quadrato in $\mathbb{Q}$ e $-a \pm 2\sqrt{b}$ non è un quadrato in $\mathbb{Q})\big)$.

Consideriamo adesso il campo $\mathbb{Q}(\sqrt{\Delta})$: notiamo che $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$ visto che Δ non è un quadrato.
b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$?

Sì: si ha $\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{\Delta}) \xrightarrow{2} \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ (Perché $\omega_1 \in \mathbb{Q}(\sqrt{\Delta})$ e $\sqrt{\omega_1}$ è radice di $p(x)$ che è irriducibile di grado 4 perché $[\mathbb{Q}(\sqrt{\omega_1}) : \mathbb{Q}] = 4$.).
$\sqrt{b} \in \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ e $\sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2} \implies \sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}) \implies K = \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ è il campo di spezzamento di $p(x)$ e ha grado 4 su $\mathbb{Q}$.

- b è un quadrato in $\mathbb{Q}$: chi è $G = Aut(K/\mathbb{Q})$?
  $\exists \sigma \in G$ tale che $\sigma(\sqrt{\omega_1}) = -\sqrt{\omega_1} \implies \sigma(\sqrt{\omega_2}) = -\sqrt{\omega_2}$, visto che $\sigma(\sqrt{b}) = \sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2}$ che deve essere fissato perché $\sqrt{b} \in \mathbb{Q}$.
  $\exists \tau \in G$ tale che $\tau(\sqrt{\omega_1}) = \sqrt{\omega_2} \implies \tau(\sqrt{\omega_2}) = \sqrt{\omega_1}$, visto che $\tau(\sqrt{b}) = \sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2}$ che deve essere fissato perché $\sqrt{b} \in \mathbb{Q}$.

$$\begin{tikzcd} \sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"] \arrow[d, leftrightarrow, "\sigma"'] & \sqrt{\omega_2} \arrow[d, leftrightarrow, "\sigma"] \\ -\sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"] & -\sqrt{\omega_2} \end{tikzcd} \implies G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

– b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$ ma non in $\mathbb{Q}$, cioè $b \cdot \Delta$ è un quadrato in $\mathbb{Q}$:
chi è $G = Aut(^K/_{\mathbb{Q}})$?
$\exists \sigma \in G$ tale che $\sigma(\sqrt{\omega_1}) = \sqrt{\omega_2} \Longrightarrow \sigma(\omega_1) = \omega_2$, $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$ e $\sigma(\sqrt{b}) = -\sqrt{b}$, cioè $\sigma(\sqrt{\omega_1}\sqrt{\omega_2}) = -\sqrt{\omega_1}\sqrt{\omega_2} \Longrightarrow \sigma(\sqrt{\omega_2}) = -\sqrt{\omega_1}$.

$$\begin{tikzcd} \sqrt{\omega_1} \arrow[r, mapsto, "\sigma"] & \sqrt{\omega_2} \arrow[d, mapsto, "\sigma"] \\ -\sqrt{\omega_2} \arrow[u, mapsto, "\sigma"] & -\sqrt{\omega_1} \arrow[l, mapsto, "\sigma"'] \end{tikzcd} \Longrightarrow G \cong {}^{\mathbb{Z}}/_{4\mathbb{Z}}.$$

No: Si ha $\mathbb{Q} \overset{2}{\text{———}} \mathbb{Q}(\sqrt{\Delta}) \overset{2}{\text{———}} Q(\sqrt{\Delta}, \sqrt{b}) \overset{1 \text{ o } 2}{\text{———}} \mathbb{Q}(\sqrt{\Delta}, \sqrt{b}, \sqrt{\omega_1})$.
Sicuramente $\sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta}, \sqrt{b}, \sqrt{\omega_1})$ perciò $\mathbb{Q}(\sqrt{\Delta}, \sqrt{b}, \sqrt{\omega_1}) = K$ è il campo di spezzamento di $p(x)$. Chi è $Aut(^K/_{\mathbb{Q}})$?
Visto che $[K : \mathbb{Q}(\sqrt{\Delta}, \sqrt{b})] \in \{1, 2\} \Longrightarrow |G| \in \{4, 8\}$. $\mathbb{Q}(\sqrt{\Delta}) \subseteq K$ è di Galois.
$\exists \sigma \in Aut(^K/_{\mathbb{Q}(\sqrt{\Delta})})$ tale che $\sigma(\sqrt{\omega_1}) = \pm\sqrt{\omega_1}$ e $\sigma(\sqrt{\omega_2}) = \pm\sqrt{\omega_2}$.
Supponiamo che $\sigma(\sqrt{\omega_1}) = -\sqrt{\omega_1} \Longleftrightarrow \sigma(\sqrt{\omega_2}) = -\sqrt{\omega_2} \Longrightarrow \sigma(\sqrt{b}) = \sqrt{b} \Longrightarrow \sqrt{b}$ è fissata da $Aut(^K/_{\mathbb{Q}(\sqrt{\Delta})}) \Longrightarrow \sqrt{b} \in \mathbb{Q}(\sqrt{\Delta})$ $\lightning$ $\Longrightarrow$ deve esistere $\sigma \in Aut(^K/_{\mathbb{Q}(\sqrt{\Delta})})$ tale che $\sigma(\sqrt{\omega_1}) = -\sqrt{\omega_1}$ e $\sigma(\sqrt{\omega_2}) = \sqrt{\omega_2}$ (a meno di scambiare $\omega_1 \longleftrightarrow \omega_2$).

$$\begin{tikzcd} \sqrt{\omega_1} \arrow[dr, leftrightarrow, "\sigma"'] & \sqrt{\omega_2} \\ -\sqrt{\omega_2} \arrow[ur, leftrightarrow, "\sigma"] & -\sqrt{\omega_1} \end{tikzcd}$$

Notiamo ora che $\sqrt{\Delta} \notin \mathbb{Q}(\sqrt{b})$ altrimenti, per questioni di grado, sarebbe $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{b})$.
Dunque $\exists \tau \in Aut(^K/_{\mathbb{Q}(\sqrt{b})})$ tale che $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$, quindi $\tau(\omega_1) = \omega_2$ e si deve avere $\tau(\sqrt{\omega_1}) = \pm\sqrt{\omega_2}$. Supponiamo $\tau(\sqrt{\omega_1}) = \sqrt{\omega_2} \Longrightarrow \tau(\sqrt{\omega_2}) = \sqrt{\omega_1}$.

$$\begin{tikzcd} \sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"] & \sqrt{\omega_2} \\ -\sqrt{\omega_1} \arrow[r, leftrightarrow, "\tau"] & -\sqrt{\omega_2} \end{tikzcd}$$

Notiamo che $ord(\tau\sigma) = 4$ mentre $ord(\tau) = ord(\sigma) = 2$:

$$\begin{tikzcd} \sqrt{\omega_1} \arrow[d, mapsto, "\tau\sigma"'] & \sqrt{\omega_2} \arrow[l, mapsto, "\tau\sigma"'] \\ -\sqrt{\omega_2} \arrow[r, mapsto, "\tau\sigma"] & -\sqrt{\omega_1} \arrow[u, mapsto, "\tau\sigma"'] \end{tikzcd}$$

$\big($analogo se fosse stato $\tau(\sqrt{\omega_1}) = -\sqrt{\omega_2}\big)$.
Dunque, poiché $G < S_4$, deve essere $G \cong D_4$ e $[K : \mathbb{Q}] = 8$.
In $Aut(^K/_{\mathbb{Q}(\sqrt{\Delta})})$ $\sigma : \begin{array}{ccc} \sqrt{\omega_1} & \longmapsto & -\sqrt{\omega_1} \\ \sqrt{\omega_2} & \longmapsto & \sqrt{\omega_2} \end{array}$ $\sigma' : \begin{array}{ccc} \sqrt{\omega_1} & \longmapsto & \sqrt{\omega_1} \\ \sqrt{\omega_2} & \longmapsto & -\sqrt{\omega_2} \end{array}$
In G abbiamo 4 elementi di ordine 4:

$$\begin{tikzcd}
\sqrt{\omega_1} \arrow[r, mapsto, "\lambda"] & \sqrt{\omega_2} \arrow[d, mapsto, "\lambda"] \\
-\sqrt{\omega_2} \arrow[u, mapsto, "\lambda"] & -\sqrt{\omega_1} \arrow[l, mapsto, "\lambda"']
\end{tikzcd}$$

$\Longrightarrow G =< \lambda, \sigma >$.
Nel caso **No**, cerchiamo i sottocampi di K pensandoli in corrispondenza coi sottogruppi di $G = D_4 =< \lambda, \sigma >$:

$< \lambda >$	$< \lambda^2 >$	$< \lambda^2, \sigma >$	$< \lambda^2, \lambda\sigma >$
$\mathbb{Q}(\sqrt{b \cdot \Delta})$	$\mathbb{Q}(\sqrt{\Delta}, \sqrt{b})$	$\mathbb{Q}(\sqrt{\Delta})$	$\mathbb{Q}(\sqrt{b})$
$< \sigma >$	$< \lambda\sigma >$	$< \lambda^2\sigma >$	$< \lambda^3\sigma >$
$\mathbb{Q}(\sqrt{\omega_2}, \sqrt{\Delta})$	$\mathbb{Q}(\sqrt{\omega_1} - \sqrt{\omega_2}, \sqrt{b})$	$\mathbb{Q}(\sqrt{\omega_1}, \sqrt{\Delta})$	$\mathbb{Q}(\sqrt{\omega_1} + \sqrt{\omega_2}, \sqrt{b})$

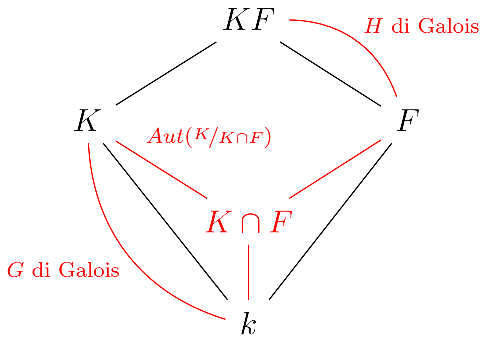
$K = \mathbb{Q}(\zeta_5) \xrightarrow{\ 4\ } \mathbb{Q}$, $Aut(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$. □

Esercizio 51. *Per quali $n \in \mathbb{Z}$ $\sqrt{n} \in K = \mathbb{Q}(\zeta_5)$?*

Dimostrazione. Sicuramente se n è un quadrato in $\mathbb{Z}$, $\sqrt{n} \in K$.
$Aut(K/\mathbb{Q})$ è generato da $\sigma : \zeta_5 \longmapsto \zeta_5^2$.
Chi è $K^{<\sigma^2>}$ (= il campo fissato dal sottogruppo generato da σ^2)?
Sicuramente $\alpha = \zeta_5 + \zeta_5^{-1} = \zeta_5 + \zeta_5^4 \in K^{<\sigma^2>}$. Chi è il polinomio minimo di $\alpha \in K^{<\sigma^2>}$?
$\alpha^2 = \zeta_5^2 + \zeta_5^3 + 2 \Longrightarrow \alpha$ è radice di $x^2 + x - 1$ con $\Delta = 5$, quindi ha radici in $\mathbb{Q}(\sqrt{5})$
$\Longrightarrow K^{<\sigma^2>} = \mathbb{Q}(\sqrt{5}) \Longrightarrow$ se $n = 5m^2$, con $m \in \mathbb{Z}$, $\sqrt{n} \in K$. □

Esercizio 52. *Per quali $n \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_7)$?*
In generale, per quali $n \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_p)$, con p primo?

Esercizio 53. *11.3.9. delle dispense]*
Sia K estensione di Galois di k e sia F estensione di k, allora $F \subseteq KF$ è di Galois e $K \cap F \subseteq K$ è di Galois. Siano $H = Aut(^{KF}/_F)$ e $G = Aut(^K/_k)$. Sia $\begin{array}{cccc} \phi: & H & \longrightarrow & G \\ & \sigma & \longmapsto & \sigma_{|K} \end{array}$*, allora ϕ è isomorfismo tra H e $Aut(^K/_{K\cap F})$.*



$$KF = \left\{ \frac{\text{somma finita di prodotti di elementi di } K \text{ ed elementi di F}}{\text{somma finita} \neq 0 \text{ di prodotti di elementi di } K \text{ ed elementi di F}} \right\}$$

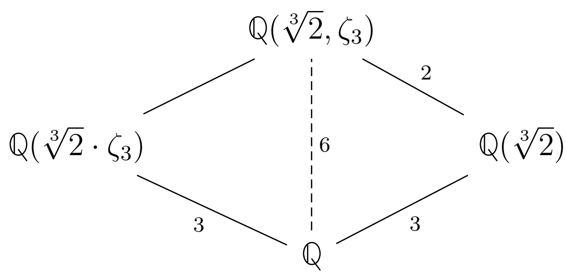
Dimostrazione. Sia $\sigma \in Aut(^{KF}/_F)$, $\sigma_{|K} \in Aut(^K/_k)$ perché $k \subseteq K$ è di Galois. Quindi ϕ è omomorfismo ben definito. Poiché σ fissa F, allora $\sigma_{|K}$ fissa $K \cap F$, quindi $Imm\,\phi \subseteq Aut(^K/_{K\cap F})$.
Chi è $Ker\,\phi$?
Sia $\sigma \in Ker\,\phi$, allora $\sigma_{|K} = Id$, σ fissa F e K, quindi σ fissa tutti gli elementi $\frac{k_1 l_1 + \dots}{k_1' l_1' + \dots \neq 0} \in KF$.
Dunque ϕ è iniettivo.
Sia $\alpha \in K$ un elemento lasciato fisso da tutti gli automorfismi di $Imm\,\phi = \phi(H)$.
Dunque $\forall \alpha \in Aut(^{KF}/_F)$ vale che $\sigma_{|K}(\alpha) = \alpha$, ossia $\sigma(\alpha) = \alpha$.
Poiché $F \subseteq KF$ è di Galois*, $\alpha \in F \implies$ scopriamo che $\alpha \in K \cap F$. Abbiamo dunque dimostrato che il campo fisso di $\phi(H)$ è $K \cap F$. Poiché $K \cap F \subseteq K$ è di Galois, per la **Proposizione 2.14.1.**, vale

$$\phi(H) = Aut(^K/_{K\cap F})$$

*Perché K è campo di spezzamento di un polinomio separabile $f(x) \in k[x]$.
Analogamente, KF è campo di spezzamento di $f(x)$ su F.
Ossia, se $K = k(\gamma_1, \dots, \gamma_r) \implies KF = F(\gamma_1, \dots, \gamma_r)$. □

Corollario 2.16.2. *Siano K, F come sopra, allora $[KF : F] \mid [K : k]$.*

Controesempio: se $k \subseteq K$ non è di Galois:

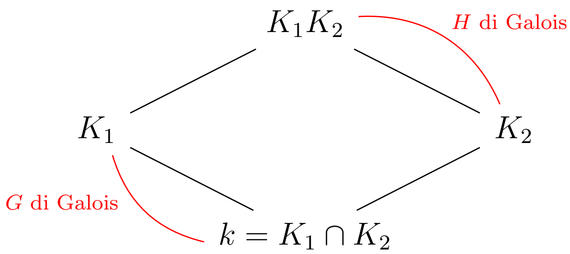


Esercizio 54 (11.3.10. delle dispense)**.**
Se K_1 e K_2 sono estensioni di Galois su k, allora $k \subseteq K_1K_2$ è di Galois.
Inoltre $\theta : Aut(^{K_1K_2}/_k) \longrightarrow Aut(^{K_1}/_k) \times Aut(^{K_2}/_k)$ è omomorfismo iniettivo e, se $K_1 \cap K_2 = k$, allora θ è isomorfismo.

Dimostrazione. K_1 sia campo di spezzamento di $f_1(x)$ separabile su k e K_2 sia campo di spezzamento di $f_2(x)$ separabile su k, allora $K_1K_2 = k(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$, dove $\alpha_1, \dots, \alpha_r$ sono le radici di $f_1(x)$ e $\beta_1, \dots, \beta_s$ sono le radici di $f_2(x)$. Dunque K_1K_2 è il campo di spezzamento

di $f_1(x)f_2(x)$ che è separabile in quanto prodotto di separabili.
θ omomorfismo iniettivo: è immediato perché se per un $\sigma \in Aut({}^{K_1K_2}/_k)$ vale $\sigma_{|K_1} = Id$ e $\sigma_{|K_2} = Id$, allora $\sigma = Id$ su K_1K_2.

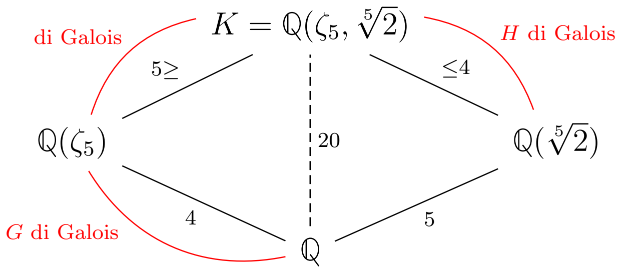
Sia infine $K_1 \cap K_2 = k$:



Per l'**Esercizio** precedente, se $\sigma_1 \in G = Aut({}^{K_1}/_k)$, $\exists \sigma \in Aut({}^{K_1K_2}/_k)$ tale che $\sigma_{|K_1} = \sigma_1$. Ora notiamo che $\theta(\sigma) = (\sigma_{|K_1}, \sigma_{|K_2}) = (\sigma_1, Id)$, allora in $Imm\,\theta$ ho $Aut({}^{K_1}/_k) \times \{Id\}$. Analogamente dimostriamo che in $Imm\,\theta$ ho $\{Id\} \times Aut({}^{K_2}/_k)$. Dunque $Imm\,\theta = Aut({}^{K_1}/_k) \times Aut({}^{K_2}/_k)$. $\square$

Esercizio 55. *Sia K campo di spezzamento su $\mathbb{Q}$ di $x^5 - 2$. Determinare $[K : \mathbb{Q}]$, $Aut({}^{K}/_{\mathbb{Q}})$ e descrivere, se esistono, i sottocampi di K di grado 5 su $\mathbb{Q}$.*

Dimostrazione.



$Aut({}^{\mathbb{Q}(\zeta_5)}/_{\mathbb{Q}}) \cong ({}^{\mathbb{Z}}/_{5\mathbb{Z}})^* \cong {}^{\mathbb{Z}}/_{4\mathbb{Z}}$ è ciclico generato da τ, dove $\tau(\zeta_5) = \zeta_5^2$. Per il primo **Esercizio**, sappiamo che $H \cong G$ e, più precisamente, che esiste $\tilde{\tau} \in H = Aut({}^{K}/_{\mathbb{Q}(\sqrt[5]{2})})$ tale che $\tilde{\tau}_{|\mathbb{Q}(\zeta_5)} = \tau$. In concreto, $\tilde{\tau}(\sqrt[5]{2}) = \sqrt[5]{2}$, $\tilde{\tau}(\zeta_5) = \zeta_5^2$ e $ord(\tilde{\tau}) = 4$. Ora notiamo che $Aut({}^{K}/_{\mathbb{Q}(\zeta_5)})$ è ciclico di ordine 5 ed è generato da σ tale che $\sigma(\zeta_5) = \zeta_5$ e $\sigma(\sqrt[5]{2}) = \sqrt[5]{2} \cdot \zeta_5$.
Dunque in $Aut({}^{K}/_{\mathbb{Q}})$ ho $(\tilde{\tau})$ e (σ). Dato che $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$ è di Galois, $(\sigma) \lhd Aut({}^{K}/_{\mathbb{Q}})$.
Poiché $(\sigma) \cap (\tilde{\tau}) = \{e\}$, segue che $Aut({}^{K}/_{\mathbb{Q}}) = (\sigma)(\tilde{\tau})$, ossia $Aut({}^{K}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{5\mathbb{Z}} \rtimes {}^{\mathbb{Z}}/_{4\mathbb{Z}}$ e, facendo il coniugio, troviamo $\tau\sigma^j\tau^{-1} = \sigma^{2j}$.
Per descrivere i sottocampi di grado 5, cerchiamo i sottogruppi di $Aut({}^{K}/_{\mathbb{Q}})$ di ordine 4. Uno lo conosco: è $H = (\tilde{\tau})$. Non è normale perché $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{2})$ non è di Galois. È un 2-Sylow: $n_2 \equiv 1\,(mod\ 2)$ e $n_2 \mid 5 \implies n_2 = 5$, visto che, non essendo normale, non può essere $n_2 = 1$. Quindi per il **Teorema di Corrispondenza** sappiamo che avremo 5 sottocampi di grado 5 su $\mathbb{Q}$. Uno di essi è $\mathbb{Q}(\sqrt[5]{2})$. Gli altri 2-Sylow sono i coniugati di H:

$$H, \quad \sigma H \sigma^{-1}, \quad \sigma^2 H \sigma^{-2}, \quad \sigma^3 H \sigma^{-3}, \quad \sigma^4 H \sigma^{-4}$$

Sappiamo che $Fix(H) = \mathbb{Q}(\sqrt[5]{2}) = K_0$. Chi è $Fix(\sigma H \sigma^{-1})$? È $\sigma\big(\mathbb{Q}(\sqrt[5]{2})\big) = \mathbb{Q}(\sqrt[5]{2} \cdot \zeta_5) = K_1$. Analogamente, $Fix(\sigma^i H \sigma^{-i}) = \sigma^i\big(\mathbb{Q}(\sqrt[5]{2})\big) = K_i$.

Osservazione 15. *$\forall i \neq j$, $K_i \cap K_j = \mathbb{Q}$.*

$\square$

2.17 Problema inverso di Galois

1) Dato G gruppo finito, esiste un'estensione di campi $F \subseteq K$ di Galois tale che $Aut(^K/_F) \cong G$?
2) Dato G gruppo finito, esiste un'estensione di campi $\mathbb{Q} \subseteq K$ di Galois tale che $Aut(^K/_\mathbb{Q}) \cong G$?
In generale il 2) è un problema aperto.
Studiamo il caso in cui G sia un gruppo abeliano finito.
Come sappiamo, $Aut(^{\mathbb{Q}(\zeta_n)}/_\mathbb{Q}) \cong (^\mathbb{Z}/_{n\mathbb{Z}})^*$, dunque per esempio se volessimo costruire un'estensione $\mathbb{Q} \subseteq K$ tale che $Aut(^K/_\mathbb{Q}) \cong {}^\mathbb{Z}/_{14\mathbb{Z}}$ potremmo considerare $n = 29$:

$$Aut(^{\mathbb{Q}(\zeta_{29})}/_\mathbb{Q}) \cong (^\mathbb{Z}/_{29\mathbb{Z}})^* \cong {}^\mathbb{Z}/_{28\mathbb{Z}}$$

In $^\mathbb{Z}/_{28\mathbb{Z}}$ consideriamo $H = (14)$, $H \lhd {}^\mathbb{Z}/_{28\mathbb{Z}}$, per il **Teorema di corrispondenza di Galois**, il campo fisso di H, ossia $J(H)$ $\big(= Fix(H)\big)$, è tale che $[J(H) : \mathbb{Q}] = 14$, l'estensione $\mathbb{Q} \subseteq J(H)$ è di Galois e $Aut(^{J(H)}/_\mathbb{Q}) \cong {}^{\mathbb{Z}/28\mathbb{Z}}/_H \cong {}^{\mathbb{Z}/28\mathbb{Z}}/_{(14)} \cong {}^\mathbb{Z}/_{14\mathbb{Z}}$.
Cosa ci è servito? Prendere 29, ossia un primo $\equiv 1\,(mod\ 14)$.

> Supponiamo di sapere (forma debole del **Teorema di Dirichlet**) che $\forall n$ intero positivo ci sono infiniti primi della forma $kn+1$.

Sia A gruppo abeliano finito, allora $A \cong {}^\mathbb{Z}/_{d_1\mathbb{Z}} \times ... \times {}^\mathbb{Z}/_{d_s\mathbb{Z}}$, con $d_1 \mid ... \mid d_s$. Per la **Forma debole di Dirichlet**, possiamo prendere $p_1, ...p_s$ primi distinti tali che $p_1 \equiv 1\,(mod\ d_1), ..., p_s \equiv 1\,(mod\ d_s)$.
Consideriamo $n = p_1 \cdot ... \cdot p_s$. $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ è di Galois e

$$Aut(^{\mathbb{Q}(\zeta_n)}/_\mathbb{Q}) \cong Aut(^\mathbb{Z}/_{n\mathbb{Z}}) \cong Aut(^\mathbb{Z}/_{p_1\mathbb{Z}}) \times ... \times Aut(^\mathbb{Z}/_{p_s\mathbb{Z}}) \cong {}^\mathbb{Z}/_{(p_1-1)\mathbb{Z}} \times ... \times {}^\mathbb{Z}/_{(p_s-1)\mathbb{Z}}$$

Prendiamo il sottogruppo $H = (d_1) \times ... \times (d_s) < {}^\mathbb{Z}/_{(p_1-1)\mathbb{Z}} \times ... \times {}^\mathbb{Z}/_{(p_s-1)\mathbb{Z}}$.
Consideriamo $J(H)$: dato che H è normale (il gruppo è abeliano), $\mathbb{Q} \subseteq J(H)$ è di Galois e

$$Aut(^{J(H)}/_\mathbb{Q}) \cong {}^{\mathbb{Z}/(p_1-1)\mathbb{Z} \times ... \times \mathbb{Z}/(p_s-1)\mathbb{Z}}/_{(d_1)\times ... \times (d_s)} \cong {}^\mathbb{Z}/_{d_1\mathbb{Z}} \times ... \times {}^\mathbb{Z}/_{d_s\mathbb{Z}} \cong A$$

1) Dato G gruppo finito, esiste un'estensione di campi $F \subseteq K$ di Galois tale che $Aut(^K/_F) \cong G$?
Sia innanzitutto $G = S_n$. Consideriamo

$$F(x_1, ..., x_n) = \left\{ \frac{g(x_1, ..., x_n)}{h(x_1, ..., x_n)} \middle| g(x_1, ..., x_n) \in F[x_1, ..., x_n] \text{ e } h(x_1, ..., x_n) \in F[x_1, ..., x_n] \setminus \{0\} \right\}$$

S_n agisce su $F(x_1, ..., x_n)$ permutando le variabili.
Detto $\sigma \in S_n$, $\sigma(f+g) = \sigma(f) + \sigma(g)$ e $\sigma(fg) = \sigma(f)\sigma(g)$, dunque $\sigma \in Aut(^{F(x_1,...,x_n)}/_F)$, allora $S_n < Aut(^{F(x_1,...,x_n)}/_F)$.

$$\begin{tikzcd}
F(x_1, ..., x_n) \arrow[d, dash, "\text{di Galois}"] \\
Fix(S_n) \arrow[d, dash] \\
F
\end{tikzcd}$$

Definizione 2.17.1. $Fix(S_n)$ *è il* ***campo delle funzioni razionali simmetriche****.*

Esercizio 56. *Per quali valori di $n \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_7)$?*

Dimostrazione. Sapendo che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$, dobbiamo cercare le sottoestensioni di grado 2, cioè i campi fissi dei sottogruppi del gruppo di Galois che abbiano indice 2. Dal momento che $G = Aut(^{\mathbb{Q}(\zeta_7)}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{6\mathbb{Z}}$, dobbiamo cercare il suo unico sottogruppo di ordine 3 (e quindi indice 2).
G è generato da $\sigma : \zeta_7 \longmapsto \zeta_7^3$, con $ord(\sigma) = 6$, quindi i sottogruppi di G sono generati da σ^3 che, essendo $ord(\sigma^3) = 2$, genera il sottogruppo di ordine 2 e da σ^2 che, essendo $ord(\sigma^2) = 3$, genera il sottogruppo di ordine 3.
Quindi ci concentriamo su $Fix(<\sigma^2>)$, cioè il campo fisso del sottogruppo di ordine 3. Infatti $\sigma^2(\zeta_7) = \zeta_7^2$, $\sigma^2(\zeta_7^2) = \zeta_7^4$ e $\sigma^2(\zeta_7^4) = \zeta_7$ quindi in $Fix(<\sigma^2>)$ abbiamo la loro somma $\zeta_7 + \zeta_7^2 + \zeta_7^4 = \alpha$.

$$\begin{tikzcd}
\mathbb{Q} \arrow[r, dash, "\leq 2"] \arrow[rr, dash, bend left, "6"] \arrow[r, dash, bend right, "2"'] & \mathbb{Q}(\alpha) \subseteq Fix(<\sigma^2>) \arrow[r, dash, "3?"] & \mathbb{Q}(\zeta_7)
\end{tikzcd}$$

$\alpha^2 = \underbrace{\zeta_7^2 + \zeta_7^2 + \zeta_7}_{=\alpha} + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) \Longrightarrow \alpha^2 + \alpha + 2 = 0 \Longrightarrow \alpha$ è radice di $x^2 + x + 2$ che ha $\Delta = -7$
$\Longrightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7}) \Longrightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \Longrightarrow \mathbb{Q}(\alpha) = Fix(<\sigma^2>) \Longrightarrow [\mathbb{Q}(\zeta_7) : \mathbb{Q}(\alpha)] = 3$.
In conclusione, l'unica sottoestensione di $\mathbb{Q}(\zeta_7)$ di grado 2 è $\mathbb{Q}(\alpha)$ perciò gli n possibili sono quelli della forma $n = m^2$ e $n = -7m^2$.
Ora ci chiediamo: chi è l'altra sottoestensione?
Cerchiamo un campo F tale che

$$\begin{tikzcd}
\mathbb{Q}(\zeta_7) \arrow[d, dash, "2"'] \\
F \arrow[d, dash, "3"'] \\
\mathbb{Q}
\end{tikzcd}$$

Proviamo con $F = Fix(<\sigma^3>)$.
Infatti $\sigma^3 : \zeta_7 \longmapsto \zeta_7^{-1}$, quindi consideriamo l'elemento $\beta = \zeta_7 + \zeta_7^{-1}$. Sicuramente $\mathbb{Q}(\beta) \subseteq F$:

$$\begin{tikzcd}
\mathbb{Q}(\zeta_7) \arrow[d, dash, "\geq 2"] \\
\mathbb{Q}(\beta) \subseteq F \arrow[d, dash, "\leq 3"] \\
\mathbb{Q}
\end{tikzcd}$$

Per mostrare che $F = \mathbb{Q}(\beta)$, basta dimostrare che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\beta)] \leq 2$, cioè che ζ_7 ha un polinomio minimo di grado ≤ 2 su $\mathbb{Q}(\beta)$, ma infatti $x^2 - \beta x + 1 \in \mathbb{Q}(\beta)[x]$ ha come radici ζ_7 e ζ_7^{-1}. $\square$

Esercizio 57. *Dato p primo, per quali $n \in \mathbb{Z}$ si ha $\sqrt{n} \in \mathbb{Q}(\zeta_p)$?*

Cerchiamo ora K estensione di Galois di $\mathbb{Q}$ tale che $Aut(^K/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{4\mathbb{Z}}$:

$$Aut(^{\mathbb{Q}(\zeta_{15})}/_{\mathbb{Q}}) \cong ({}^{\mathbb{Z}}/_{15\mathbb{Z}})^* \cong ({}^{\mathbb{Z}}/_{3\mathbb{Z}})^* \times ({}^{\mathbb{Z}}/_{5\mathbb{Z}})^* \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{4\mathbb{Z}}$$

Cerchiamo ora K estensione di Galois di $\mathbb{Q}$ tale che $Aut(K/\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}$:
cerchiamo quindi un primo $p \equiv 1\,(mod\ 8)$, cioè $p = 17$ e consideriamo $Aut(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \cong \mathbb{Z}/16\mathbb{Z}$.
Prendiamo un elemento tale che $\zeta_{17} \longmapsto \zeta_{17}^{-1}$ e consideriamo $\mathbb{Q}(\underbrace{\zeta_{17} + \zeta_{17}^{-1}}_{=\beta})$:

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{17}) \arrow[d, dash, "\leq 2"] \\
\mathbb{Q}(\beta) \arrow[d, dash, "\leq 8"] \\
\mathbb{Q}
\end{tikzcd}$$

lo mostriamo notando che ζ_{17} è radice di $x^2 - \beta x + 1$ e $Aut(\mathbb{Q}(\beta)/\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}$.

Cerchiamo ora K estensione di Galois di $\mathbb{Q}$ tale che $Aut(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$:
proviamo con $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Dobbiamo mostrare che $[K : \mathbb{Q}] = 8$. Intanto

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] \arrow[dd, dash, "4"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

perché $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ dal fatto che $(a + b\sqrt{3})^2 = 2$, con $a, b \in \mathbb{Q} \iff a^2 + 3b^2 + ab\sqrt{3} = 2 \implies ab = 0 \implies a^2 = 2$ oppure $3b^2 = 2$, impossibile perché né 2 né $\frac{2}{3}$ sono quadrati in $\mathbb{Q}$. In generale, $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{m}) \iff nm$ è un quadrato in $\mathbb{Q}$.

$$\begin{tikzcd}
& & & K \arrow[dll, dash, "2"'] \arrow[ddd, dash, "8"] \arrow[ddr, dash, "4"] & \\
& \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & & & \\
\mathbb{Q}(\sqrt{2}) \arrow[drrr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[drr, dash, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[dr, dash, "2"] & & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash, "2"] \\
& & & \mathbb{Q} &
\end{tikzcd}$$

$G = Aut(K/\mathbb{Q})$ è generato da

$$\sigma_1 : \begin{cases} \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} \\ \sqrt{5} \longmapsto \sqrt{5} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto -\sqrt{3} \\ \sqrt{5} \longmapsto \sqrt{5} \end{cases} \qquad \sigma_3 : \begin{cases} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} \\ \sqrt{5} \longmapsto -\sqrt{5} \end{cases}$$

che commutano tra loro e chiaramente $ord(\sigma_1) = ord(\sigma_2) = ord(\sigma_3) = 2$.

Quindi, in conclusione, G ha $8 = [K : \mathbb{Q}]$ elementi su $\mathbb{Q}$: $\sigma : \begin{cases} \sqrt{2} \longmapsto \pm\sqrt{2} \\ \sqrt{3} \longmapsto \pm\sqrt{3} \\ \sqrt{5} \longmapsto \pm\sqrt{5} \end{cases}$.

Esercizio 58. *Calcolare il campo di spezzamento e il relativo gruppo di Galois del polinomio* $p(x) = (x^4 - x^2 + 1)(x^2 - 3)$ *su* $\mathbb{Q}$ *e su* $\mathbb{F}_{13}$.

Dimostrazione. Notiamo che

$$(x^4 - x^2 + 1)(x^4 + x^2 + 1)(x^4 - 1) = x^{12} - 1$$

Visto che $x^4 - 1 = \phi_1(x)\phi_2(x)\phi_4(x)$ e $x^4 + x^2 + 1 = \phi_3(x)\phi_6(x)$, abbiamo che $x^4 - x^2 + 1 = \phi_{12}(x)$. Per studiare quindi il campo di spezzamento di $p(x)$ su $\mathbb{Q}$, studiamo $\mathbb{Q}(\zeta_{12}, \sqrt{3})$:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{12}, \sqrt{3}) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "?"] & \\
\mathbb{Q}(\zeta_{12}) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Proviamo a intersecare $\mathbb{Q}(\zeta_{12})$ e $\mathbb{Q}(\sqrt{3})$, cioè cerchiamo tutte le sottoestensioni non banali di $\mathbb{Q}(\zeta_{12})$ che sono 3 visto che $Aut(^{\mathbb{Q}(\zeta_{12})}/_{\mathbb{Q}}) \cong (^{\mathbb{Z}}/_{12\mathbb{Z}})^* \cong (^{\mathbb{Z}}/_{2\mathbb{Z}})^2$. Poiché

ζ_{12} è radice 12ˆ primitiva di 1
ζ_{12}^3 è radice 4ˆ primitiva di 1
ζ_{12}^4 è radice 3ˆ primitiva di 1

$\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3, \zeta_4)$ in quanto $\zeta_3 \cdot \zeta_4$ è radice 12ˆ primitiva di 1.

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{12}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] \arrow[dd, dash, "4"'] & \\
\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\zeta_4) = \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd} \implies \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\zeta_{12})$$

$\implies \mathbb{Q}(\zeta_{12}, \sqrt{3}) = \mathbb{Q}(\zeta_{12}) \implies [\mathbb{Q}(\zeta_{12}, \sqrt{3}) : \mathbb{Q}] = 4$.
3 è un quadrato in $\mathbb{F}_{13}$ e $x^4 - x^2 + 1$ si fattorizza completamente in $\mathbb{F}_{13} \implies \mathbb{F}_{13}$ è il campo di spezzamento. □

Esercizio 59. *(11.3.5. delle dispense) Calcolare il campo di spezzamento e il relativo gruppo di Galois di $p(x) = x^6 - 2x^4 - 8x^2 + 16$ su $\mathbb{Q}$, $\mathbb{F}_3$ e $\mathbb{F}_9$.*

Dimostrazione. Notiamo che $p(x) = (x^4 - 8)(x^2 - 2)$, perciò consideriamo $\mathbb{Q}(\sqrt{2}, \sqrt[4]{8}, \zeta_4 = i)$ ma $\sqrt{2} = (\sqrt[4]{2})^2$ e $\sqrt[4]{8} = (\sqrt[4]{2})^3$, quindi prendiamo $\mathbb{Q}(\sqrt[4]{2}, i) = K$

$$\begin{tikzcd}
 & K \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] \arrow[dd, dash, "8"] & \\
\mathbb{R} \supseteq \mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \not\subseteq \mathbb{R} \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Gli elementi di $Aut(^K/_{\mathbb{Q}})$ sono del tipo $\begin{cases} \sqrt[4]{2} \longmapsto (i)^a \sqrt[4]{2} \\ i \longmapsto \pm i \end{cases}$, con $a = 0, 1, 2, 3$.
Poiché $|Aut(^K/_{\mathbb{Q}})| = 8$, tutte queste "ipotesi di automorfismi" sono possibili.
Infine, visto che $Aut(^K/_{\mathbb{Q}})$ ha un sottogruppo di ordine 4 e un sottogruppo di ordine 2 non

normale e inoltre $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ non è di Galois, $Aut({}^{K}\!/_{\mathbb{Q}}) \cong D_4$.
Su $\mathbb{F}_3$, $p(x) = (x^2-2)(x^4-2)$. 2 non è un quadrato in $\mathbb{F}_3$, quindi detta α una radice di 2 in una estensione di $\mathbb{F}_3$, il campo di spezzamento di $p(x)$ è $\mathbb{F}_3(\alpha)$, ma quindi $\mathbb{F}_3(\alpha) = \mathbb{F}_9$ visto che $\mathbb{F}_9$ è l'unica estensione di grado 2 su $\mathbb{F}_3$.
Poiché $2^2 \equiv 1$ $(mod\ 3)$, una radice 4ˆ di 2 è 8ˆ di 1. $\mathbb{F}_9^* \cong {}^{\mathbb{Z}}\!/_{8\mathbb{Z}}$, quindi x^8-1 ha come radici gli elementi di $\mathbb{F}_9^* \Longrightarrow Aut({}^{\mathbb{F}_{3^2}}\!/_{\mathbb{F}_3}) \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. □

Esercizio 60. *Calcolare il campo di spezzamento e il relativo gruppo di Galois del polinomio* $f(x) = x^6 - 2$ *su* $\mathbb{Q}$.

Dimostrazione. Chiamiamo E il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ e chiamiamo $G = Aut({}^{E}\!/_{\mathbb{Q}})$.
Consideriamo $E = \mathbb{Q}(\zeta_6, \sqrt[6]{2})$. Notiamo che $\zeta_6^2 - \zeta_6 + 1 = 0$, cioè ζ_6 è radice di $x^2 - x + 1$ che ha $\Delta = -3 \Longrightarrow \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$.

$$
\begin{tikzcd}
 & E \arrow[dl, dash, "6"'] \arrow[dd, dash, "12"] \arrow[dr, dash, "2"] & \\
\mathbb{R} \not\supseteq \mathbb{Q}(\sqrt{-3}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{R} \arrow[dl, dash, "6"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

dove $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ perché $x^6 - 2$ è irriducibile per Eisenstein. Quindi $[E : \mathbb{Q}] = 12$.
G non è abeliano perché $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{2})$ non è di Galois e quindi non tutti i sottogruppi di G sono normali in G.
G contiene un sottogruppo di ordine 6, in quanto se consideriamo il campo $F = \mathbb{Q}(\sqrt{-3})$ e di conseguenza $E = F(\sqrt[6]{2})$, il gruppo $Aut({}^{E}\!/_{F})$ ha 6 elementi determinati univocamente in base a dove mandiamo $\sqrt[6]{2}$, cioè $\sqrt[6]{2} \longmapsto \zeta_6^a \sqrt[6]{2}$, con $a = 0, 1, 2, 3, 4, 5$ (cioè 6 scelte).
E contiene un campo K tale che $\mathbb{Q} \subseteq K$ è di Galois e $Aut({}^{K}\!/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$? □

Esercizio 61. *Siano* $\mathbb{K}$ *campo finito e* α, β *algebrici su* $\mathbb{K}$ *tali che* $[\mathbb{K}(\alpha) : \mathbb{K}] = 5$ *e* $[\mathbb{K}(\beta) : \mathbb{K}] = 4$. *Dimostrare che* $[\mathbb{K}(\alpha\beta) : \mathbb{K}] = 20$.

Dimostrazione. $\mathbb{K} \equiv \mathbb{F}_q$, con q potenza di un primo.

$$\begin{tikzcd}
& \mathbb{K}(\alpha,\beta) \arrow[dl, dash, "4\geq"'] \arrow[dr, dash, "\leq 5"] \arrow[dd, dash, dashed, "20"] & \\
\mathbb{F}_{q^5} \cong \mathbb{K}(\alpha) \arrow[dr, dash, "5"'] & & \mathbb{K}(\beta) \cong \mathbb{F}_{q^4} \arrow[dl, dash, "4"] \\
& \mathbb{K} &
\end{tikzcd}$$

poiché $[\mathbb{K}(\alpha, \beta) : \mathbb{K}] \leq 20$ ed è diviso da 4 e da 5, allora $[\mathbb{K}(\alpha, \beta) : \mathbb{K}] = 20$.
$\mathbb{K} \subseteq \mathbb{K}(\alpha\beta) \subseteq \mathbb{K}(\alpha, \beta)$, dunque il grado $[\mathbb{K}(\alpha\beta) : \mathbb{K}] \in \{1, 2, 4, 5, 10, 20\}$.
Se fosse 1, 2 o 4, allora $\alpha\beta \in \mathbb{F}_{q^4}$ (visto che $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n} \iff d \mid n$), ma $\mathbb{K}(\beta) \cong \mathbb{F}_{q^4}$, dunque in $\mathbb{F}_{q^4}$ troveremmo l'elemento $\frac{\alpha\beta}{\beta} = \alpha$, assurdo perché $[\mathbb{K}(\alpha) : \mathbb{K}] = 5$.
Se invece è 5, 10 o 20, allora $\mathbb{K}(\alpha\beta) \supseteq \mathbb{F}_{p^\alpha} \cong \mathbb{K}(\alpha)$ e quindi $\mathbb{K}(\alpha\beta)$ contiene $\frac{\alpha\beta}{\alpha} = \beta$, allora

$$\begin{tikzcd}
& \mathbb{K}(\alpha\beta) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{K}(\beta) \arrow[dr, dash, "4"'] & & \mathbb{K}(\alpha) \arrow[dl, dash, "5"] \\
& \mathbb{K} &
\end{tikzcd}$$

e dunque, per il solito calcolo dei gradi, vale che $[\mathbb{K}(\alpha\beta) : \mathbb{K}] = 20 \Longrightarrow \mathbb{K}(\alpha, \beta) = \mathbb{K}(\alpha\beta)$. □

Esercizio 62. *Sia* $f(x) \in \mathbb{Q}[x]$ *irriducibile di grado 6. Determinare le possibili fattorizzazioni in* $\mathbb{Q}(\sqrt{2})[x]$.

Dimostrazione. Sia $\alpha \in \mathbb{C}$ una radice di $f(x)$. Ovviamente $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

$$\begin{tikzcd}
& \mathbb{Q}(\alpha,\sqrt{2}) \arrow[dl, dash, "1 \text{ o } 2"'] \arrow[dr, dash, "3 \text{ o } 6"] \arrow[dd, dash, dashed, "6 \text{ o } 12"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "6"'] & & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

$[\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}(\sqrt{2})]$ è il grado del fattore irriducibile di $f(x)$ in $\mathbb{Q}(\sqrt{2})[x]$ che si annulla in α.
Tutto dipende dal fatto che $\sqrt{2} \in \mathbb{Q}(\alpha)$ oppure no. Possono dunque succedere due cose:

- $f(x)$ si spezza in due fattori di grado 3 in $\mathbb{Q}(\sqrt{2})[x]$: $x^6 - 2 = (x^3 + \sqrt{2})(x^3 - \sqrt{2})$;
- $f(x)$ rimane irriducibile in $\mathbb{Q}(\sqrt{2})[x]$: $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
  In $\mathbb{Q}(\zeta_7)$, visto che $Aut(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$, esiste una sottoestensione di grado 2 ed è $\mathbb{Q}(i\sqrt{7})$.
  Quindi $\mathbb{Q}(\sqrt{2}) \nsubseteq \mathbb{Q}(\zeta_7)$, allora $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ è irriducibile in $\mathbb{Q}(\sqrt{2})[x]$.

□

Esercizio 63. *Trovare il campo di spezzamento* K *su* $\mathbb{Q}$ *e il relativo gruppo di Galois del polinomio* $p(x) = x^4 - 2x^2 - 2$.

Dimostrazione. Le radici di $p(x)$ sono $\alpha = \sqrt{1+\sqrt{3}}$, $-\alpha$, $\beta = \sqrt{1-\sqrt{3}}$ e $-\beta$.
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ perché $p(x)$ è irriducibile su $\mathbb{Q}$ per Eisenstein.
$\beta \notin \mathbb{Q}(\alpha)$ visto che $\alpha \in \mathbb{R}$ e $\beta \in \mathbb{C} \setminus \mathbb{R}$. Notiamo che $\alpha^2 = 1 + \sqrt{3} \Longrightarrow \sqrt{3} \in \mathbb{Q}(\alpha)$ e anche che $\beta^2 = 1 - \sqrt{3}$, quindi β è radice di $x^2 - 1 + \sqrt{3} \in \mathbb{Q}(\alpha)[x]$, allora $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$.
Dunque $K = \mathbb{Q}(\alpha, \beta) \Longrightarrow [K : \mathbb{Q}] = 8$.
Notiamo che $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ non è di Galois perché non è preservata dagli elementi di $Aut(K/\mathbb{Q})$.
Quindi $Aut(K/\mathbb{Q})$ non è abeliano perché contiene un sottogruppo non normale. Dato che in Q_8 tutti i sottogruppi sono normali, $Aut(K/\mathbb{Q}) \cong D_4$, vista la classificazione dei gruppi di ordine 8.
Guardiamo più in dettaglio.
Sia c un coniugio in $\mathbb{C}$: $c(\alpha) = \alpha$, $c(-\alpha) = -\alpha$, $c(\beta) = -\beta$ e $c(-\beta) = \beta$. Allora, visto che $\mathbb{Q} \subseteq K$ è di Galois e quindi invariante per c che è automorfismo di $\mathbb{C}$, $c \in Aut(K/\mathbb{Q})$ e ha ordine 2, dunque, per ragioni di grado, $Fix\big((c)\big) = \mathbb{Q}(\alpha)$.
Se calcoliamo $\alpha\beta = \sqrt{1+\sqrt{3}}\sqrt{1-\sqrt{3}} = i\sqrt{2}$, perciò $\mathbb{Q}(i\sqrt{2}) \subseteq K$

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Q}(\alpha\beta, \alpha) = \mathbb{Q}(\alpha, \beta) = K \arrow[dl, "4"'] \arrow[dr] & \\
\mathbb{Q}(i\sqrt{2}) = \mathbb{Q}(\alpha\beta) \arrow[dr, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Un automorfismo $\varphi \in Aut(K/\mathbb{Q}(i\sqrt{2}))$ è determinato da $\varphi(a)$.
$p(x) = x^4 - 2x^2 - 2$ è irriducibile su $\mathbb{Q}(i\sqrt{2})$ perché $[K : \mathbb{Q}(i\sqrt{2})] = 4$.
In $Aut(K/\mathbb{Q}(i\sqrt{2}))$, ricordando che $\alpha\beta$ è fissato da ogni φ,

$$\varphi_1 : \begin{cases} \alpha \longmapsto \alpha \\ \beta \longmapsto \beta \end{cases} \quad \varphi_2 : \begin{cases} \alpha \longmapsto -\alpha \\ \beta \longmapsto -\beta \end{cases} \quad \varphi_3 : \begin{cases} \alpha \longmapsto \beta \\ \beta \longmapsto \alpha \end{cases} \quad \varphi_4 : \begin{cases} \alpha \longmapsto -\beta \\ \beta \longmapsto -\alpha \end{cases}$$

Dunque $ord(\varphi_i) = 2 \ \forall i = 1, 2, 3, 4$.

$$\begin{tikzcd}[arrows=dash]
 & K \arrow[dl, "\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}"'] \arrow[dr, "\mathbb{Z}/2\mathbb{Z} = (c)"] & \\
\mathbb{Q}(i\sqrt{2}) \arrow[dr, "\mathbb{Z}/2\mathbb{Z}"'] & & \mathbb{Q}(\alpha) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd} \Longrightarrow Aut(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Dato che $c\varphi_3 c(\alpha) = c\varphi_3(\alpha) = c(\beta) = -\beta = \varphi_4(\alpha)$, allora $c\varphi_3 c = \varphi_4$. □

Esercizio 64. *Esibire un elemento di ordine 4. (Suggerimento: $c\varphi_3$...)*

Esercizio 65. *Calcolare il campo di spezzamento K su $\mathbb{Q}$ di $x^7 - 2$. Detto $L = K \cap \mathbb{R}$, dire se $\mathbb{Q} \subseteq L$ è di Galois e, se non lo è, determinare la massima estensione di Galois contenuta in L.*

Dimostrazione. Le radici di $x^7 - 2$ sono $\zeta_7^i \sqrt[7]{2}$, con $i = 0, ..., 6$.

$$\begin{tikzcd}[arrows=dash]
 & K \arrow[dl] \arrow[dr] & \\
\mathbb{Q}(\zeta_7) \arrow[dr, "\mathbb{Z}/6\mathbb{Z}"'] & & \mathbb{Q}(\sqrt[7]{2}) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Il coniugio complesso $c \in Aut(^{\mathbb{Q}(\zeta_7)}/_{\mathbb{Q}})$, dunque $Fix\big((c)\big) = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$ ha grado 3 su $\mathbb{Q}$. Dato che $(c) \lhd {}^{\mathbb{Z}}/_{6\mathbb{Z}}$, allora, per il **Teorema di Corrispondenza**, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_7) \cap \mathbb{R} = Fix\big((c)\big)$ è di Galois e $Aut(^{\mathbb{Q}(\zeta_7)\cap\mathbb{R}}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{3\mathbb{Z}}$.
<u>Tentativo</u>: costruiamo $Fix\big((c)\big)\mathbb{Q}(\sqrt[7]{2})$. Per ragioni di grado, $Fix\big((c)\big)\mathbb{Q}(\sqrt[7]{2})$ ha grado 21 su $\mathbb{Q}$:

$$
\begin{tikzcd}[column sep=small]
 & Fix\big((c)\big)\mathbb{Q}(\sqrt[7]{2}) \arrow[dl, dash] \arrow[dd, dash, "21"] \arrow[dr, dash] & \\
Fix\big((c)\big) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\sqrt[7]{2}) \arrow[dl, dash, "7"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Analogamente, per ragioni di grado, abbiamo che $[K : \mathbb{Q}] = 42$. Notiamo che c sta anche in $Aut(^{K}/_{\mathbb{Q}})$.
$L = Fix\big((c)\big)$ (visto come sottocampo di K), allora $[L : \mathbb{Q}] = 21$. Dunque, per ragioni di grado, $L = \big(\mathbb{Q}(\zeta_7) \cap \mathbb{R}\big)\mathbb{Q}(\sqrt[7]{2})$. Infine $\mathbb{Q} \subseteq L$ non è di Galois perché contiene $\sqrt[7]{2}$ ma non $\zeta_7\sqrt[7]{2}$.
Guardiamo le sottoestensioni: certamente $\mathbb{Q}(\zeta_7) \cap \mathbb{R} \subset L$. Se M è la massima (per inclusione) sottoestensione di Galois di L, allora $M \supseteq \mathbb{Q}(\zeta_7)\cap\mathbb{R}$ e dunque $3 \mid [M : \mathbb{Q}] \mid 21$, allora $[M : \mathbb{Q}] = 3$ e $M = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$. $\square$

Esercizio 66. *Trovare il campo di spezzamento su $\mathbb{Q}$ e il relativo gruppo di Galois del polinomio $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 6)$.*
Dimostrare poi che $p(x)$ ha sempre almeno una radice in $\mathbb{F}_p$ $\forall p$ primo.

Dimostrazione. Prendiamo $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, sappiamo che $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ e anche che $Aut(^{\mathbb{Q}(\sqrt{2},\sqrt{3})}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$.
Per dimostrare che $p(x)$ ha sempre almeno una radice in $\mathbb{F}_p$ $\forall p$ primo, basta dimostrare che se né 2 né 3 sono quadrati in $\mathbb{F}_p$, allora 6 è un quadrato in $\mathbb{F}_p$.
Sicuramente $2, 3 \in \mathbb{F}_p^*$ che è ciclico e di ordine $p-1$. Sia $\square = \{x \in \mathbb{F}_p^* \big| \exists y \in \mathbb{F}_p^* \text{ tale che } x = y^2\}$, quindi se $G = {}^{\mathbb{Z}}/_{m\mathbb{Z}} \implies \square = 2 \cdot {}^{\mathbb{Z}}/_{m\mathbb{Z}}$ e, se m è pari (come nel nostro caso), abbiamo che ${}^{G}/_{\square} \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}}$, cioè il gruppo che distingue i *quadrati* ($\leftrightarrow 1$) dai *non quadrati* ($\leftrightarrow -1$) in cui un *non quadrato* moltiplicato per un *non quadrato* dà un *quadrato*. $\square$

Esercizio 67. *Trovare il campo di spezzamento su $\mathbb{F}_5$ e il relativo gruppo di Galois del polinomio $p(x) = x^7 - 2$.*

Dimostrazione. Notiamo che $2 \equiv (-2)^7 \,(mod\ 5) \implies p(x) = x^7 - (-2)^7$, perciò, per avere il campo di spezzamento di $p(x)$ dobbiamo avere le radici 7^e di 1, cioè dobbiamo andare in un'estensione $\mathbb{F}_{5^k}$ in cui $\mathbb{F}_{5^k}^*$ contiene elementi di ordine $7 \implies 7 \mid 5^k - 1$. Chi è $ord_7(5)$? $5^2 \equiv 4 \,(mod\ 7)$, $5^3 \equiv -1 \,(mod\ 7) \implies 5^6 \equiv 1 \,(mod\ 7) \implies 7 \mid 5^6 - 1 \implies K = \mathbb{F}_{5^6}$ con $[K : \mathbb{F}_5] = 6 \implies Aut(^{K}/_{\mathbb{F}_5}) \cong {}^{\mathbb{Z}}/_{6\mathbb{Z}}$. $\square$

Esercizio 68. *Trovare il campo di spezzamento su $\mathbb{Q}$ e il relativo gruppo di Galois del polinomio $p(x) = (x^3 - 3)(x^4 - 3)$.*

Dimostrazione. Prendiamo $\mathbb{Q}(\sqrt[3]{3}, \zeta_3, \sqrt[4]{3}, \zeta_4) = K$.

$$\begin{tikzcd}
& K \arrow[dl, dash, "4"'] \arrow[dr, dash, "3"] \arrow[dd, dash, "12"] & \\
L_1 = \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \arrow[dr, dash, "3"] \arrow[ddr, dash, "6"'] & & \mathbb{Q}(\sqrt[4]{3}, \zeta_4) = L_2 \arrow[dl, dash, "4"'] \arrow[ddl, dash, "8"] \\
& L_1 \cap L_2 \arrow[d, dash, "2"] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Chi è $L_1 \cap L_2$? Notiamo che $[L_1 \cap L_2 : \mathbb{Q}] \in \{1, 2\}$ e che $i\sqrt{3} \in L_2 \implies \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3) \implies [L_1 \cap L_2 : \mathbb{Q}] = 2 \implies [K : \mathbb{Q}] = 24$ perché $L_1 \cap L_2 \subseteq L_1$ e $L_1 \cap L_2 \subseteq L_2$ sono di Galois.

Dimostrare che in $Aut(^{K}/_{\mathbb{Q}})$ esiste un elemento che fissa i e $\sqrt[3]{3}$ ma manda $\sqrt[4]{3}$ in $i\sqrt[4]{3}$
$\exists \sigma \in Aut(^{K}/_{\mathbb{Q}})$ tale che $\sigma(i) = i$, $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$ e $\sigma(\sqrt[4]{3}) = i\sqrt[4]{3}$. Notiamo che

$$\mathbb{Q} \overset{12}{\rule{2em}{0.4pt}} \mathbb{Q}(\sqrt[12]{3}) = \mathbb{Q}(\sqrt[3]{3}, \sqrt[4]{3}) \overset{2}{\rule{2em}{0.4pt}} K = \mathbb{Q}(\sqrt[12]{3}, i)$$

Dunque gli elementi di $Aut(^{K}/_{\mathbb{Q}})$ sono del tipo $\begin{cases} \sqrt[12]{3} \longmapsto \zeta_{12}^a \sqrt[12]{3} \\ i \longmapsto \pm i \end{cases}$ con $a \in {}^{\mathbb{Z}}/_{12\mathbb{Z}}$.

Perciò vediamo che σ corrisponde all'elemento $\begin{cases} \sqrt[12]{3} \longmapsto -i \sqrt[12]{3} \\ i \longmapsto i \end{cases}$ perché $\sigma(\sqrt[4]{3}) = i\sqrt[4]{3}$,

$\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$ e quindi $\sigma\left(\frac{\sqrt[3]{3}}{\sqrt[4]{3}}\right) = -i\frac{\sqrt[3]{3}}{\sqrt[4]{3}}$.

Descrivere le sottoestensioni di K di grado 4 su $\mathbb{Q}$.
Sia $L \subseteq \mathbb{Q}$ tale che $[L : \mathbb{Q}] = 4 \implies [L \cap L_2, \mathbb{Q}] \in \{1, 2, 4\}$.

Se fosse $[L \cap L_2 : \mathbb{Q}] = 2$, avrei $[LL_2 : \mathbb{Q}] = [LL_2 : L_2] \cdot [L_2 : \mathbb{Q}] = 16$, ma $LL_2 \subseteq K$ che ha grado $[K : \mathbb{Q}] = 24$ e $16 \nmid 24$ ↯
Se fosse $[L \cap L_2 : \mathbb{Q}] = 1$, avremmo $[LL_2 : L] = 8$ e $[L : \mathbb{Q}] = 4 \implies [LL_2 : \mathbb{Q}] = 32$, ma $LL_2 \subseteq K$ che ha grado $[K : \mathbb{Q}] = 24$ e $32 \nmid 24$ ↯ $\implies L \subset L_2$.
Quindi in realtà stiamo cercando le sottoestensioni di $L_2 = \mathbb{Q}(\sqrt[4]{3}, i)$ di grado 4 su $\mathbb{Q}$.
L_2 è il campo di spezzamento di $x^4 - 3 \implies Aut({}^{L_2}/_{\mathbb{Q}}) < S_4$, inoltre sappiamo che $|Aut({}^{L_2}/_{\mathbb{Q}})| = 8 \implies Aut({}^{L_2}/_{\mathbb{Q}}) \cong D_4$ che ha 5 elementi di ordine 2 (= sottogruppi di indice 4).

$$D_4 =< \rho : \begin{cases} \sqrt[4]{3} \longmapsto \sqrt[4]{3} i \\ i \longmapsto i \end{cases} \quad , \sigma : \begin{cases} \sqrt[4]{3} \longmapsto \sqrt[4]{3} \\ i \longmapsto -i \end{cases} \quad >$$

$$\begin{tikzcd}
 & \sqrt[4]{3} \arrow[dr, mapsto, "\rho"] & \\
-i\sqrt[4]{3} \arrow[ur, mapsto, "\rho"] \arrow[rr, leftrightarrow, "\sigma"] & & i\sqrt[4]{3} \arrow[dl, mapsto, "\rho"] \\
 & -\sqrt[4]{3} \arrow[ul, mapsto, "\rho"] &
\end{tikzcd}$$

Notiamo che $Fix(\rho^2) = \mathbb{Q}(i, \sqrt{3})$, $Fix(\sigma) = \mathbb{Q}(\sqrt[4]{3})$, $Fix(\rho^2\sigma) = \mathbb{Q}(i\sqrt[4]{3})$, $Fix(\rho\sigma) = \mathbb{Q}\big((1 + i)\sqrt[4]{3}\big)$ e $Fix(\rho^3\sigma) = \mathbb{Q}\big((1 - i)\sqrt[4]{3}\big)$.

Esercizio 69. *Cosa possiamo dire dell'estensione $\mathbb{C}(t) \subseteq \mathbb{C}(x)$, dove $t = x^3 + x^{-3}$?*

$$\mathbb{C}(t) = \mathbb{C}(x^3 + x^{-3}) \overset{2}{\text{———}} \mathbb{C}(x^3) \overset{3}{\text{———}} \mathbb{C}(x)$$

Il polinomio minimo di x su $\mathbb{C}(x^3)$ è $z^3 - x^3 \in \mathbb{C}(x^3)[z]$ che è irriducibile in $\mathbb{C}[x^3][z]$.
Il polinomio $z^2 - tz + 1 \in \mathbb{C}(t)[z]$ ha come radici x^3 e x^{-3}, ma $x^3 \notin \mathbb{C}[t] = \mathbb{C}[x^3 + x^{-3}]$.
L'estensione $\mathbb{C}(x^3) \subseteq \mathbb{C}(x)$ è di Galois.
$z^6 - tz^3 + 1$ è il polinomio minimo di x in $\mathbb{C}(t)[z]$ e le radici sono del tipo $x\zeta_3^a$ e $x^{-1}\zeta_3^a$, con $a \in {}^{\mathbb{Z}}/_{3\mathbb{Z}} \implies \mathbb{C}(t) \subseteq \mathbb{C}(x)$ è di Galois di grado 6.
Un elemento $\sigma \in Aut({}^{\mathbb{C}(x)}/_{\mathbb{C}(t)})$ è determinato da $\sigma(x) = \zeta_3^a x^{\pm 1}$:
se $\sigma_1(x) = x^{-1}$ e $\sigma_2(x) = \zeta_3 x$, allora $\sigma_1\sigma_2(x) = \zeta_3 x^{-1}$ e $\sigma_2\sigma_1(x) = \zeta_3^2 x^{-1} \implies Aut({}^{\mathbb{C}(x)}/_{\mathbb{C}(t)})$ non è abeliano $\implies Aut({}^{\mathbb{C}(x)}/_{\mathbb{C}(t)}) \cong S_3$.
Chi sono le sottoestensioni proprie?

$$Fix(\sigma_2) = \mathbb{C}(x^3) \text{ ha grado 2 su } \mathbb{C}(t)$$
$$\mathbb{C}(t) \overset{3}{\text{———}} \mathbb{C}(x + x^{-1}) \subseteq Fix(\sigma_1) \overset{2}{\text{———}} \mathbb{C}(x)$$
$$\mathbb{C}(t) \overset{3}{\text{———}} \mathbb{C}(x + \zeta_3 x^{-1}) \subseteq Fix(\sigma_1\sigma_2) \overset{2}{\text{———}} \mathbb{C}(x)$$
$$\mathbb{C}(t) \overset{3}{\text{———}} \mathbb{C}(x + \zeta_3^2 x^{-1}) \subseteq Fix(\sigma_1\sigma_2^2) \overset{2}{\text{———}} \mathbb{C}(x)$$

□

Esercizio 70. *Per quali valori di $n \in \mathbb{Z}$ $\sqrt{n} \in \mathbb{Q}(\zeta_p)$?*

Dimostrazione. Sappiamo che $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ è di Galois e che $Aut({}^{\mathbb{Q}(\zeta_p)}/_{\mathbb{Q}}) \cong ({}^{\mathbb{Z}}/_{p\mathbb{Z}})^* \cong {}^{\mathbb{Z}}/_{(p-1)\mathbb{Z}}$, dunque $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. $\mathbb{Q}(\zeta_p)$ contiene un'unica sottoestensione di grado 2 su $\mathbb{Q}$ che corrisponde al campo fisso dell'unico sottogruppo H di indice 2 su $\mathbb{F}_p^*$.

$$\alpha = \sum_{i \,\square\, \text{in } ({}^{\mathbb{Z}}/_{p\mathbb{Z}})^*} \zeta_p^i = \sum_{\zeta_p^i \,\square\, \text{in } \mathbb{F}_p^*} \zeta_p^i$$

Sappiamo anche però che

$$\sum_{i=0}^{p-1} \zeta_p^i = 0 = 1 + \sum_{i \,\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^*} \zeta_p^i + \sum_{i \,\not\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^*} \zeta_p^i$$

Prendiamo

$$s = \sum_{i \,\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^*} \zeta_p^i - \sum_{i \,\not\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^*} \zeta_p^i$$

che è invariante per H.

$$s = \sum_{i \in (\mathbb{Z}/p\mathbb{Z})^*} \varepsilon_p(i) \zeta_p^i \text{ dove } \varepsilon_p(i) = \begin{cases} 1 & i \,\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^* \\ -1 & i \,\not\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^* \end{cases}$$

$$s^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \varepsilon_p(i) \varepsilon_p(j) \zeta_p^{i+j}$$

ma, visto che in $(\mathbb{Z}/p\mathbb{Z})^*$ $\begin{array}{l} \square \cdot \square = \square \\ \not\square \cdot \not\square = \square \\ \square \cdot \not\square = \not\square \end{array}$, cioè guardo tutto in $(\mathbb{Z}/p\mathbb{Z})^*/\text{quadrati} \cong \mathbb{Z}/2\mathbb{Z}$, abbiamo che

$$s^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \varepsilon_p(ij) \zeta_p^{i+j} \overset{j=ik}{=} \sum_{i=1}^{p-1} \sum_{k=1}^{p-1} \varepsilon_p(i^2 k) \zeta_p^{i+ik} = \sum_{i=1}^{p-1} \sum_{k=1}^{p-1} \varepsilon_p(k) \zeta_p^{i(k+1)} =$$

$$= \sum_{k=1}^{p-2} \underbrace{\sum_{i=1}^{p-1} \varepsilon_p(k) \zeta_p^{i(k+1)}}_{\substack{= -\varepsilon_p(k), \text{ perché} \\ \sum_{i=1}^{p-1} \zeta_p^i = -1}} + (p-1)\varepsilon_p(-1) = - \sum_{k=1}^{p-2} \varepsilon_p(k) + (p-1)\varepsilon_p(-1) =$$

$$= \underbrace{- \sum_{k=1}^{p-1} \varepsilon_p(k)}_{\substack{= 0 \text{ perché} \\ \#\square = \#\not\square}} + p\varepsilon_p(-1) \Longrightarrow s^2 = p\varepsilon_p(-1) = \begin{cases} p & \text{se } -1 \text{ è } \square \text{ in } (\mathbb{Z}/p\mathbb{Z})^* \\ -p & \text{se } -1 \text{ è } \not\square \text{ in } (\mathbb{Z}/p\mathbb{Z})^* \end{cases}$$

ma, -1 è $\square$ in $(\mathbb{Z}/p\mathbb{Z})^* \iff 4 \mid p-1$, dunque $n = m^2$ o $n = m^2\sqrt{p}$, con $m \in \mathbb{Z}$,
e -1 è $\not\square$ in $(\mathbb{Z}/p\mathbb{Z})^* \iff 4 \mid p+1$, dunque $n = m^2$ o $n = m^2\sqrt{-p}$, con $m \in \mathbb{Z}$. $\square$

Grado	Polinomio	Radici
1	$f(x) = ax + b$	$x = -\frac{b}{a}$
2	$f(x) = ax^2 + bx + c$	$x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$
3	$f(x) = x^3 + ax + b$	$x = \zeta_3^i \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{a^3}{27} + \frac{b^2}{4}}} + \zeta_3^{-i} \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{a^3}{27} + \frac{b^2}{4}}}$
4	$f(x)$	*formula risolutiva*
≥ 5	$f(x)$	non esiste una formula risolutiva

Teorema 2.17.1 (di Dedekind).
Dati K un campo e $\sigma_1, ..., \sigma_n \in Aut(K)$ tutti distinti, se $\underbrace{\sum_{i=1}^{n} a_i\sigma_i}_{K\longrightarrow K} = 0$, *con* $a_i \in K$ $\forall i = 1, ..., n$, *allora* $a_i = 0$ $\forall i = 1, ..., n$.

Dimostrazione. Per induzione su $n \geq 1$.
Passo base: $n = 1$ ovvio.
Passo induttivo: $n > 1$, sia $\sum_{i=1}^{n} a_i\sigma_i(x) = 0$ $\forall x \in K$. Visto che $\sigma_1 \neq \sigma_2 \Longrightarrow \exists u \in K$ tale che $\sigma_1(u) \neq \sigma_2(u)$. Possiamo scrivere $\sum_{i=1}^{n} a_i\sigma_i(ux) = 0$ $\forall x \in K$, cioè $\forall x \in K$

$$\sum_{i=1}^{n} a_i\sigma_i(u)\sigma_i(x) = 0 \tag{2.1}$$

e anche

$$\sum_{i=1}^{n} a_i\sigma_1(u)\sigma_i(x) = 0 \tag{2.2}$$

Notiamo adesso che

$$(2.1) - (2.2) = \sum_{i=2}^{n} a_i'\sigma_i(x) = 0, \text{ con } a_i' = a_i\big(\sigma_i(u) - \sigma_1(u)\big) \ \forall i = 2, ..., n$$

Per ipotesi induttiva $a_i' = 0$ $\forall i = 2, ..., n$, ma quindi, poiché $\sigma_1(u) \neq \sigma_2(u)$, $a_2 = 0 \Longrightarrow \sum_{\substack{i=1 \\ i\neq 2}}^{n} a_i\sigma_i(x) = 0$ $\forall x \in K \Longrightarrow a_i = 0$ $\forall i = 1, ..., n$. $\square$

Proposizione 2.17.2. *Sia F un campo contenente ζ_n (= radice n-esima primitiva di 1):*

a) Se $E = F(\alpha)$, con $\alpha^n \in F$, allora $F \subseteq E$ è di Galois e $Aut(E/F)$ è ciclico.

b) Se $F \subseteq E$ è di Galois e $Aut(E/F) \cong \mathbb{Z}/n\mathbb{Z}$, allora $E = F(\alpha)$ con $\alpha^n \in F$ (per α opportuno).

Dimostrazione. a) Prendiamo $\sigma \in Aut(E/F)$ tale che $\sigma(\alpha) = \zeta_n^i\alpha$, poiché $\alpha^n \in F$.
Dunque possiamo prendere $\begin{array}{rccl} \varphi: & Aut(E/F) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \cong <\zeta_n> \subset F^* \\ & \sigma & \longmapsto & \frac{\sigma(\alpha)}{\alpha} = \zeta_n^i \end{array}$.
φ è omomorfismo ed è iniettivo $\Longrightarrow Aut(E/F) < \mathbb{Z}/n\mathbb{Z}$, quindi $Aut(E/F)$ è ciclico.
b) Sia σ che genera $G = Aut(E/F) \cong \mathbb{Z}/n\mathbb{Z}$.

Prendiamo $\zeta_n \in F$ e cerchiamo $\alpha \in E^*$ tale che $\sigma(\alpha) = \zeta_n \alpha$ da cui $\alpha^n \in F$ (perché è fissato da σ) e, poiché α ha n coniugati distinti, $[F(\alpha) : F] = n \Longrightarrow F(\alpha) = E$.
$\sum\limits_{i=0}^{n-1} \zeta_n^{-i} \sigma^i \neq 0 \Longrightarrow$ per il **Teorema di Dedekind**, $\exists \gamma \in E$ tale che $\alpha = \sum\limits_{i=0}^{n-1} \zeta_n^{-i} \sigma^i(\gamma) \neq 0 \Longrightarrow$ $\sigma(\alpha) = \zeta_n \alpha$, perché $\sigma(\alpha) = \sum\limits_{i=0}^{n-1} \zeta_n^{-i} \sigma^{i+1}(\gamma) \overset{j=i+1}{=} \sum\limits_{j=1}^{n} \zeta_n^{-j+1} \sigma^j(\gamma) = \zeta_n \sum\limits_{j=0}^{n} \zeta_n^{-j} \sigma^j(\gamma) = \zeta_n \alpha$. $\square$

Teorema 2.17.3. *Sia F un campo di caratteristica 0. Il polinomio $f(x) \in F[x]$ è **risolubile per radicali** $\Longleftrightarrow$ il gruppo di Galois G del suo campo di spezzamento è risolubile (cioè $G = G_0 \rhd G_1 \rhd ... \rhd G_n = \{e\}$, con ${}^{G_i}/_{G_{i+1}}$ abeliano finito $\forall i = 0, ..., n-1$).*

Esercizio 71. *Se ${}^{G_i}/_{G_{i+1}}$ è abeliano finito, allora possiamo trovare $G_i = H_0 \rhd H_1 \rhd ... \rhd H_m = G_{i+1}$ con ${}^{H_i}/_{H_{i+1}}$ ciclico $\forall i = 0, ..., n-1$.*

Dimostrazione. $(\Longleftarrow)$ Prendiamo $f \in F[x]$ con gruppo di Galois del campo di spezzamento G risolubile. Siano $F' = F(\zeta_n)$, con $n = (\deg f)!$, E campo di spezzamento di f su F ed E' campo di spezzamento di f su F'.

$$\begin{tikzcd}
 & E' \arrow[dl, dash, "\text{di Galois}"'] \arrow[dr, dash] & \\
F' \arrow[dr, dash] & & E \arrow[dl, dash, "\text{di Galois}"] \\
 & F &
\end{tikzcd}$$

$G' = Aut({}^{E'}/_{F'}) \hookrightarrow G = Aut({}^{E}/_{F})$, quindi $G' < G$ e G è risolubile $\Longrightarrow G'$ è risolubile.

Esercizio 72. *Il sottogruppo di un risolubile è risolubile. Il quoziente di risolubili è risolubile.*

$\Longrightarrow \exists G' = G_0 \rhd ... \rhd G_m = \{e\}$ con quozienti ${}^{G_i}/_{G_{i+1}}$ ciclici.
Passando ai campi fissi, chiamiamo $F_i = Fix(G_i) \subset E'$, le inclusioni si rovesciano:

$$F \subset F(\zeta_n) = F' = F_0 \subset F_1 \subset ... \subset F_m = E'$$

Sappiamo che ${}^{F_i}/_{F_{i+1}}$ è un'estensione di Galois con gruppo di Galois ciclico $\forall i = 0, ..., m-1$.
Dunque $F_i = F_{i-1}(\alpha_i)$, con $\alpha_i^{r_i} \in F_{i-1}$ e $r_i = [F_i : F_{i-1}]$, cioè $F_i = F_{i-1}(\sqrt[r_i]{\beta_i})$, con $\beta_i \in F_{i-1}$.
$(\Longrightarrow)$ Vogliamo mostrare che $G = Aut({}^{E}/_{F})$ (dove E è il campo di spezzamento di f) è risolubile.
Basta mostrare che G è quoziente di risolubili.
Abbiamo $F = F_0 \subset F_1 \subset ... \subset F_m \supset E$, con $F_i = F_{i-1}(\alpha_i)$ e $\alpha_i^{r_i} \in F_{i-1}$. Prendiamo $F_m = F(\gamma)$, con γ elemento primitivo. Sia $g(x)$ il polinomio minimo di γ su F.
Sia K il campo di spezzamento di $g(x) \cdot (x^n - 1)$, con $n = (\deg f)!$.
$\tilde{G} = Aut({}^{K}/_{F})$, $F_m(\zeta_n) \subset K$ e $F \subseteq K$ è di Galois. Sia $\tilde{E}$ il più piccolo campo tale che $F_m(\zeta_n) \subset \tilde{E} \subset K$ ed $F \subseteq \tilde{E}$ di Galois. $\tilde{E}$ è il più piccolo campo contenente $\sigma\big(F_m(\zeta_n)\big)$ al variare di $\sigma \in \tilde{G}$, quindi $\tilde{E}$ è generato da ζ_n e $\sigma(\alpha_i)$, con $\sigma \in \tilde{G}$ e $i = 1, ..., m$.

$$F \subset F(\zeta_n) \subset F(\zeta_n, \alpha_1) \subset F(\zeta_n, \alpha_1, \alpha_2) \subset ... \subset F(\zeta_n, \alpha_1, ..., \alpha_m) \subset F(\zeta_n, \alpha_1, ..., \alpha_m, \sigma(\alpha_1)) \subset ...$$

Cioè ho una catena finita del tipo

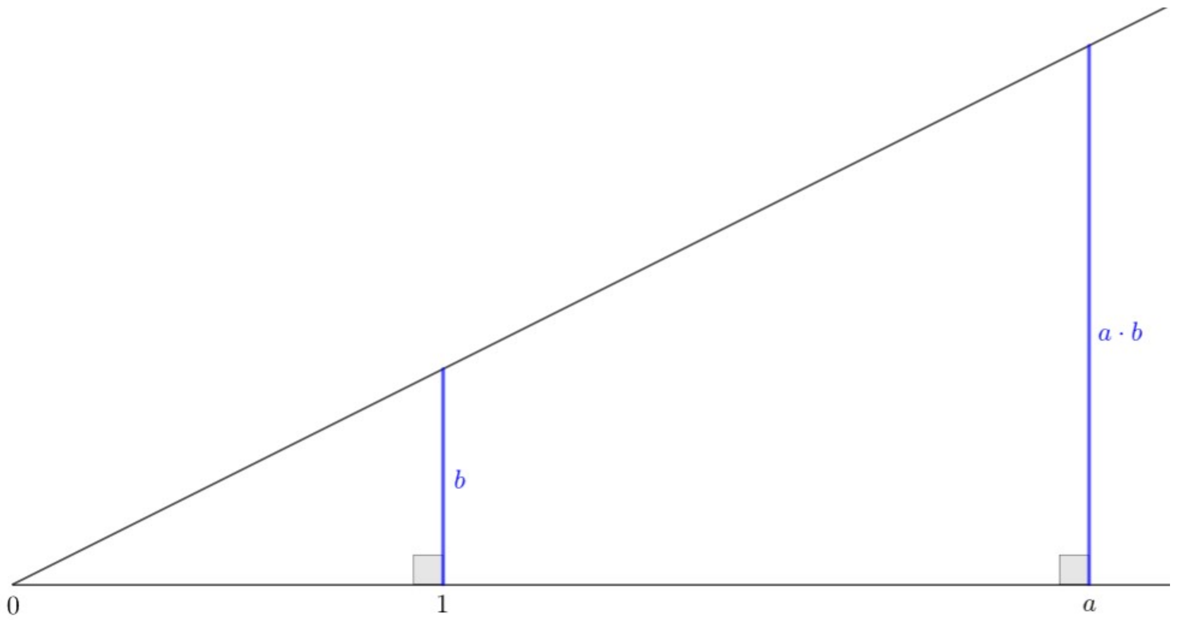
$$F' \subset F'' \subset ... \subset \tilde{E}$$

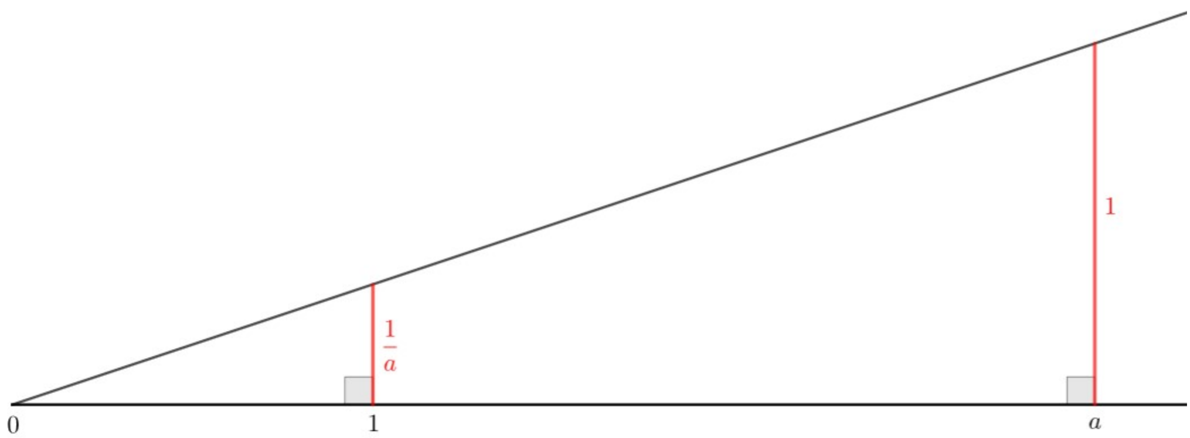
in cui tutte le estensioni sono del tipo F'' ottenuto da F' (cioè il precedente) aggiungendo una radice r-esima (per un certo r) $\Longrightarrow$ tutte le estensioni successive nella catena di estensione di campi sono cicliche (eccetto al più $F \subset F(\zeta_n)$ che è abeliana) $\Longrightarrow Aut({}^{\tilde{E}}/_{F})$ è un gruppo risolubile e $G = Aut({}^{E}/_{F})$ è un suo quoziente. $\square$

Possiamo però scrivere un polinomio f irriducibile con 2 radici $\notin \mathbb{R}$, 3 radici $\in \mathbb{R}$ e con $\deg f = 5$ $\Longrightarrow Aut({}^{cds(f)}/_{\mathbb{Q}}) \cong S_5$ che non è risolubile.

2.18 Riga e Compasso

Fare disegni con riga e compasso *significa* saper disegnare una retta, fissare due punti detti "0" e "1" su di essa e di conseguenza tutti gli altri necessari;
significa che dati due punti distinti, siamo capaci di tracciare l'unica retta passante per entrambi;
significa saper tracciare la circonferenza di centro un punto dato e raggio una lunghezza data. Inoltre *significa* che ogni volta che otteniamo dei punti nuovi (magari tramite intersezioni) possiamo usarli per disegnare ulteriori figure e oggetti.
Significa saper fare moltiplicazioni e divisioni:



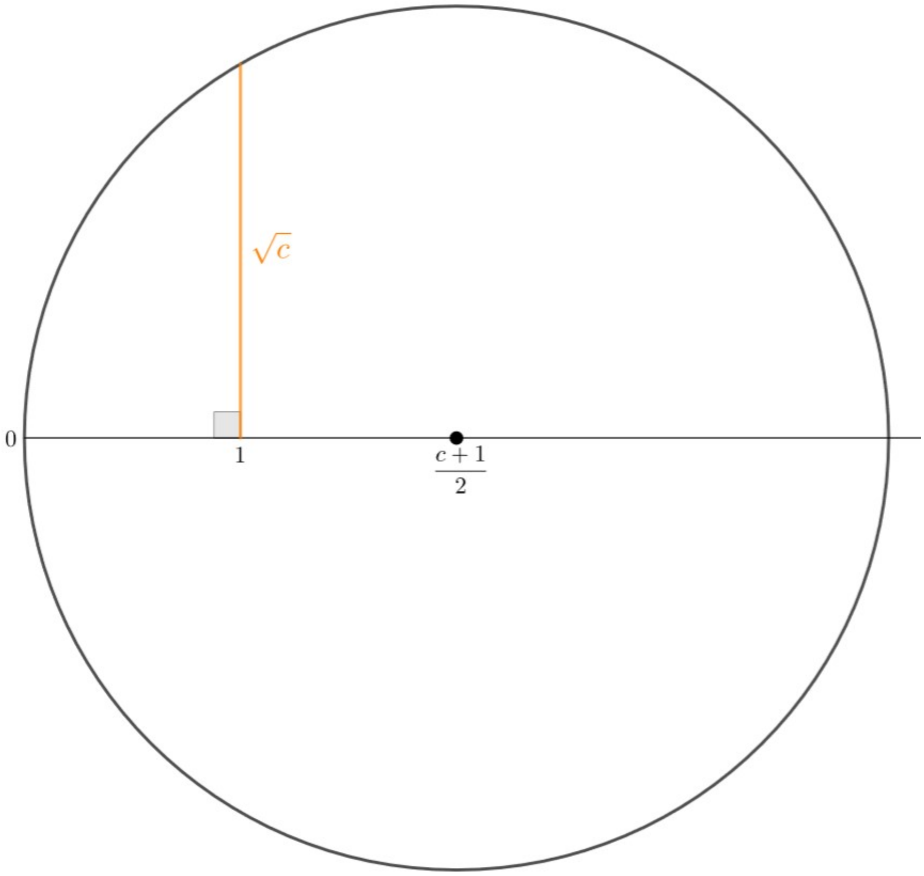


Se usiamo i punti di $F \times F$, con $F \subseteq \mathbb{R}$, per scrivere le equazioni di una retta e di una circonferenza, le coordinate dei loro punti di intersezione stanno in un'estensione quadratica di F.
Stessa cosa, se intersechiamo due circonferenze con centri in $F \times F$ e ciascuna passante per un punto di $F \times F$, le coordinate dei loro punti di intersezione stanno in un'estensione quadratica di F.

Teorema 2.18.1. *a) I numeri costruibili formano un campo.*

b) α *è costruibile* $\iff \alpha \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_r})$, *con* $a_i \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_{i-1}})$ $\forall i > 0$.

Significa saper calcolare la radice quadrata di un numero dato:



Corollario 2.18.2. *$\alpha \in \mathbb{R}$ è costruibile $\Longrightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ per n opportuno.*

Corollario 2.18.3. *Dato un cubo, non possiamo costruirne uno di volume doppio.*

Dimostrazione. Per assurdo, dovremmo risolvere $x^3 - 2 = 0$ su $\mathbb{Z}$. $\square$

Corollario 2.18.4. *Dato un angolo generico, non possiamo dividerlo in tre parti uguali.*

Dimostrazione. Ricordiamo che $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$.
Se per esempio prendiamo $3\theta = \frac{\pi}{3}$, abbiamo $\cos(3\theta) = \frac{1}{2}$ e poniamo $x = \cos(\theta) \Longrightarrow 8x^3 - 6x - 1 = 0$ che è impossibile su $\mathbb{Q}$ perché le radici dovrebbero essere della forma $\pm\frac{1}{a}$ con $a = 1, 2, 4, 8$. $\square$

2.18.1 Poligoni regolari

Per costruire un n-agono regolare, $n \geq 3$, ci serve $\cos\left(\frac{2\pi}{n}\right) = \frac{e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}}}{2} = \frac{\zeta_n + \zeta_n^{-1}}{2}$, con $\zeta_n \notin \mathbb{R}$.

$$\begin{tikzcd} \mathbb{Q} \arrow[r, dash, "\frac{\varphi(n)}{2}"] \arrow[rr, dash, bend right, "\varphi(n)"'] & \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \arrow[r, dash, "2"] & \mathbb{Q}(\zeta_n) \end{tikzcd}$$

perché $x = \zeta_n$ risolve $x^2 - 2\cos\left(\frac{2\pi}{n}\right)x + 1 = 0$

Proposizione 2.18.5. *Un p-agono regolare è costruibile solo se $p = 2^n + 1$ (**Primi di Fermat**).*

Proposizione 2.18.6. *Un n-agono regolare è costruibile solo se $n = 2^k p_1 \cdot ... \cdot p_s$, con p_i primi di Fermat distinti $\forall i = 1, ..., s$.*

Dimostrazione. $\left[\mathbb{Q}\Big(\cos\left(\frac{2\pi}{n}\right)\Big) : \mathbb{Q}\right] = \frac{\varphi(n)}{2} = 2^m$, $\left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\Big(\cos\left(\frac{2\pi}{n}\right)\Big)\right] = 2$, quindi consideriamo $G = Aut(^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}})$ che è abeliano di ordine 2^{m+1}. Dunque $\exists G = G_0 > G_1 > ... > G_{m+1} = \{e\}$ tali che $[G_i, G_{i+1}] = 2 \forall i \implies [Fix(G_{i+1}) : Fix(G_i)] = 2$ ed è quadratica. L'estensione

$$\left[Fix(G_i) \cap \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : Fix(G_{i+1}) \cap \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] = \begin{cases} 1 \\ 2 \end{cases}$$

è quadratica reale $\implies$ si ottiene estendendo con una radice $\implies \mathbb{Q}\Big(\cos\left(\frac{2\pi}{n}\right)\Big)$ è costruibile. $\square$