# Esercitazioni di Algebra 1

Francesca Pistolato

19 gennaio 2017

# Indice

Si tratta di appunti (in corso d'opera) presi alle esercitazioni di Algebra 1 tenute dal professor Callegaro nel corso del primo semestre dell'a.a. 2016/2017. Ringrazio Chiara che mi ha prestato i suoi appunti quando ero troppo pigra per andare a lezione e le numerose persone che di volta in volta mi hanno aiutato a decifrare le cose fatte. Se avete correzioni, dubbi o richieste di chiarimenti scrivete a `pistolato[at]mail.dm.unipi.it`

Subito dopo i capitoli allego la descrizione della lezione fornita su UniMap.

Precisazioni: la parte riguardante i gruppi risolubili è mancante. Cercherò di integrarla quanto prima. Inoltre l'esercizio 36 è scritto in modo poco chiaro. Nell'esercizio 50 e risultati seguenti, vi sono alcuni particolari non chiariti.

# Parte I

# Esercitazioni di Teoria dei Gruppi

# Capitolo 1

# Venerdì 30 Settembre

*Descrizione del gruppo diedrale, presentazione, sottogruppi, sottogruppi normali.*

# Capitolo 2

# Venerdì 7 Ottobre

*Cardinalità degli automorfismi del gruppo diedrale. Orbita e centralizzatore di una permutazione: calcolo delle cardinalità in $\mathcal{S}_n$ e in $\mathcal{A}_n$. Casi in cui quella di $\mathcal{S}_n$ si spezza in $\mathcal{A}_n$. Formula di Burnside.*

Formula di Burnside: data un'azione $G \to S(X)$, ci dice che il numero di orbite è

$$\frac{1}{|G|} \cdot \sum_{g \in G} |Fix(g)|$$

# Capitolo 3

# Martedì 11 Ottobre

*Esempi di applicazione della formula di Burnside. Classificazione dei gruppi di ordine minore o uguale a 8. Gruppi di ordine $p^2$. Esercizio circa un gruppo di ordine $2n$ in cui la metà degli elementi ha ordine 2 e l'altra metà forma un sottogruppo.*

**Esercizio 1.** Data una scacchiera di dimensione 3, vogliamo contare le possibili colorazioni delle caselle in bianco o nero a meno di rotazioni e riflessioni della scacchiera in sé.

Contarle a meno di rotazioni/riflessioni significa contarle a meno di azione del diedrale ($\mathcal{D}_4$) sulla scacchiera.
Claim: ne esistono tante quante le orbite di $D_4$ nello spazio di tutte le scacchiere colorate in bianco e nero, che denoteremo $S$, che sappiamo essere isomorfo a $(\mathbb{Z}_2)^9$.

Denotiamo $S^g = Fix(g)$, l'insieme delle scacchiere colorate (colorazioni) invarianti per un dato elemento $g \in D_4$.

Consideriamo la formula di Burnside: il numero delle orbite è $\frac{1}{|G|} \cdot \sum_{g \in G} |S^g|$.

Contiamo, facendoci tutti i disegnini, il numero delle scacchiere che vengono fissate al variare degli elementi di $D_4$:

1. $e$: $S^e = 2^9$
2. 4 riflessioni, lungo asse lato-lato, lungo diagonale vertice-vertice: per ciascuna di queste $S^{r_4} = 2^6$;
3. 2 rotazioni di ordine 4: per ciascuna di queste $S^{\rho_4} = 2^3$;
4. 1 rotazione di ordine 2: $S^{\rho_2} = 2^5$

Quindi il numero di orbite è $\frac{1}{8} \cdot (2^9 + 4 \cdot 2^6 + 2 \cdot 2^3 + 2^5) = 102$.
**Esercizio 2.** Colorazioni dei lati di un ottagono con n colori e cerco quelle $D_8$ invarianti. Credici che lo faccio!

Tanti bei conti che non sto a ripetere... Per formula di Burnside, sono

$$\frac{1}{16} \cdot (n^8 + n^4 + 2 \cdot n^2 + 4 \cdot n + 4 \cdot n^5 + 4 \cdot n^4)$$

**Esercizio 3.** Classificazione dei gruppi $G$ di ordine $\leq 8$.

Quelli con ordine primo e 1 sono banali. Restano da studiare quelli di ordine $4, 6$ e $8$.

**Ordine 4** Claim: $G \cong (\mathbb{Z}_2)^2$ o $G \cong \mathbb{Z}_4$.

In generale sappiamo che, essendo di cardinalità $p^2$, $G$ è abeliano.

Possiamo distinguere due casi:

- $\exists a \in G$ tale che $o(a) = 4$, dunque $G =< a >$, ovvero è ciclico e isomorfo a $\mathbb{Z}_4$;
- $\forall a \in G$ si ha che $o(a) = 2$. Si procede allora in modo diverso. Consideriamo $x \in G$ e denotiamo $N =< x >$. Notiamo che $N \lhd G$ in quanto $G$ abeliano.

  Consideriamo $\pi_N : G \to G/N$. Ora $G/N$ ha ordine 2 ed è isomorfo a $\mathbb{Z}_2$. Il nostro obiettivo è trovare un'inversa $S : G/N \to G$ tale che $\pi \circ S = id_{G/N}$. In generale non è sempre possibile, ma qui abbiamo un gruppo abeliano con tutti gli elementi di ordine 2, un caso abbastanza gestibile.

  La buona definizione di $S$ dipende dalla scelta di un unico elemento: scegliamo $g_1 \in G - N$, dunque tale che $< g_1 N >= G/N$ (fatto dimostrato), infatti così facendo $\pi_N(g_1) = g_1 N$ ha ordine 2 e genera $G/N$. Poniamo $S((gN)^i) = S(g^i N) = (g_1)^i$. É ben definita? Sì, perché tutte le immagini sono uguali.
  In generale vorrei che $S : g^n N \mapsto g_1^n$. Di certo $\pi_N$ su $g_1^n$ fa quello che deve fare. Ne controllo l'ordine: $S : eN = g^2 N \mapsto g^2 = e$.
  Verifichiamo sia un omomorfismo: conticini.

  Dunque $S$ esiste in quanto tutti gli elementi in $G - \{ e \}$ hanno ordine 2. Chiaramente non vale al variare di ogni $h$, qui funziona perché scelgo una unica immagine degli elementi del quoziente.

  Dunque ricapitolando abbiamo in $G$ tramite inclusione $N = i(N) < G$ e tramite sollevamento $S(G/N) < G$. Allora abbiamo anche la

mappa $\phi : N \times G/N \to G$ tale che $(x, gN) \mapsto i(h) \cdot S(gN)$. Verifichiamo sia un omomorfismo di gruppi: lo è in quanto è un omomorfismo sulle componenti.

Claim: abbiamo trovato un isomorfismo. Infatti

$$\begin{aligned} Ker(\phi) &= \left\{ (h, g(N)^i) \in N \times G/N \mid i(h) \cdot S((gN)^i) = e \right\} = \\ &= \left\{ (h, g(N)^i) \mid (g_1)^i = h^{-1} \right\} = \\ &= \{ (e, e) \} \end{aligned}$$

in quanto è chiaro che se $i = 1$, $g_1 \notin N \Rightarrow \forall h \in N$ l'immagine è diversa da $e$; altrimenti se $i = 2$ $(gN)^2 = N \Rightarrow S(N) = e \Rightarrow h^{-1} = e \Rightarrow h = e$, dunque è iniettiva. Allora per cardinalità è anche surgettiva e dunque abbiamo trovato che $N \times G/N \cong G$. Ma allora $G \cong N \times G/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Precisazioni su notazione: prodotto diretto (cartesiano) ha struttura di gruppo con l'operazione componente per componente. Poi vedremo come definirne una diversa (prodotto semidiretto).
**Osservazione 1.** Abbiamo usato prepotentemente il fatto il gruppo è abeliano.

**Ordine 6** Facciamo subito una distinzione.

Supponiamo sia abeliano. Per Cauchy, in $G$ abbiamo un elemento di ordine 2, sia $x$, e anche un elemento di ordine 3, sia $y$: dunque abbiamo anche $H =< x > \cong \mathbb{Z}_2$ e $K =< y > \cong \mathbb{Z}_3$. In quanto abeliano, tali gruppi sono entrambi normali, hanno inoltre intersezione banale e il prodotto delle loro cardinalità è la cardinalità di $G$, dunque $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Supponiamo ora che non sia abeliano. Claim: $G \cong \mathcal{S}_3$. Vogliamo dunque trovare un isomorfismo da $G$ in $\mathcal{S}_3$, o viceversa.

Consideriamo $y \in G$ di ordine 3 e denotiamo $H =< y >$, sappiamo che $H \cong \mathbb{Z}_3$. Con un abuso di notazione identifichiamo $H$ con $\mathbb{Z}_3$ e di conseguenza con $\mathcal{A}_3$.

Immergiamo $H$ in $\mathcal{S}_3$ identificandolo con $\mathcal{A}_3$. Ora $\mathcal{A}_3$ è normale in $\mathcal{S}_3$ in quanto ha indice 2, dunque è ben definita la proiezione al quoziente. Sia $\pi_{\mathcal{A}_3} \mathcal{S}_3 \to \mathcal{S}_3/\mathcal{A}_3 \cong \mathbb{Z}_2$. Come nel caso del gruppo di ordine 4, ora definiamo l'inversa destra di $\pi_{\mathcal{A}_3}$ nel seguente modo: consideriamo un elemento di ordine 2, $\tau\mathcal{A}_3 \in \mathcal{S}_3/\mathcal{A}_3$, che esiste per Cauchy e genera il quoziente: dunque $\tau \notin \mathcal{A}_3$ e ha ordine 2. Poniamo $S(\tau\mathcal{A}_3^i) = x^i$.

Stavolta considero $\mathcal{A}_3 \times \mathbb{Z}_2 \to \mathcal{S}_3$ tale che $(\sigma, [n]) \mapsto \sigma(1\ 2)^n$. Tuttavia non è un omomorfismo.

Abbiamo allora bisogno di un'altra struttura per riuscire a determinare tutti i gruppi di ordine 6.

Ripartiamo. Consideriamo come prima $y \in G$ di ordine 2 e denotiamo $H =< y >$, e $x \in G$ di ordine 3 e denotiamo $N =< x >$. Facciamo agire per coniugio $H \to Aut(N)$ in modo tale che $h \mapsto \phi_h$, dove $\phi_h : n \mapsto hnh^{-1}$.

Tuttavia osserviamo che $Aut(N) \cong {\mathbb{Z}_3}^* \cong \mathbb{Z}_2$. Allora abbiamo solo due automorfismi da poter scegliere e sono univocamente determinati dall'immagine di un generatore di $H$, nel nostro caso $y$. Se $y \tilde{\mapsto} [0]_2$ avremo l'omomorfismo nullo, ovvero tale che $\forall h \in H,\ \forall n \in N$ si ha che $\phi_h(n) = \phi_y^h(n) = id(n) = n$; altrimenti se $y \tilde{\mapsto} [1]_2$ $\phi_y$ sarà un automorfismo di $K$ di ordine 2, ovvero quello che permuta gli elementi nei loro inversi. Se fosse quello nullo i due sottogruppi commuterebbero: dato $h \in H,\ k \in K,\ hk = kh$ in quanto $hk = kh \Leftrightarrow hkh^{-1} = \phi_h k = id(k) = k$. Tuttavia lo escludiamo, in quanto in questo modo si ricadrebbe nell'ipotesi che $G$ è abeliano.

Dunque abbiamo due situazioni:

- o $H$ è normale: ma di nuovo i due sottogruppi commutano e quindi si avrebbe il gruppo abeliano di ordine 6, cioè $G \cong \mathbb{Z}_6$
- o non lo è: abbiamo $G \cong \mathcal{D}_3$ con questa mappa: dato $\rho \in \mathcal{D}_3$ del tipo $\rho = s^\varepsilon r^i$ con $s$ riflessione e $r$ rotazione, $\rho = s^\varepsilon r^i \mapsto h^\varepsilon n^i$.

Questo è un classico modo di procedere.

**Ordine 8** *scritto male* *Useremo i risultati delle proposizioni 1,2 e 3 che alleghiamo sotto.*

Cominciamo la classificazione considerando gli ordini degli elementi di $G$.

Se ve ne sono di ordine 8, allora $G$ è ciclico e isomorfo a $\mathbb{Z}_8$.

Se non ce ne sono, ci chiediamo se abbia elementi di ordine 4. Se la risposta è no, allora tutti gli elementi hanno ordine 1 o 2, allora per proposizione 4 $G \cong (\mathbb{Z}_2)^3$.

Supponiamo allora che vi sia un elemento di ordine 4. Sia questo $n$ e $< n >= N \cong \mathbb{Z}_4$ il sottogruppo di $G$ generato da $n$. Avendo indice 2 è normale.

Ora ci chiediamo se fuori da $N$ ci siano altri elementi di ordine 2. Sappiamo che $N$ ne ha 1, $n^2$.

Se sì, sia $h \notin N$ di ordine 2 e consideriamo il coniugio di $h$ su $N$ che ricordiamo essere normale. Analogamente a quanto fatto nella proposizione 1, $H \cong \mathbb{Z}_2$ e, in quanto $N$ ciclico, $Aut(N) \cong (N)^* \cong (\mathbb{Z}_{\not\varphi})^* \mathbb{Z}_{\varphi(2)} = \mathbb{Z}_4$. Se è quello banale, allora $H$ e $N$ commutano e dunque abbiamo $\mathbb{Z}_4 \times \mathbb{Z}_2$, in quanto possiamo considerare la proiezione al quoziente, l'inversa destra (sollevamento) e blablabla, come fatto nel caso di $|G| = 4$. Altrimenti se è quello non banale, $H$ coniuga ogni elemento di $N$ nel suo inverso e dunque abbiamo $\mathcal{D}_4$: fissa un elemento, scrittura unica e blablabla, come fatto nel caso di $|G| = 6$.

Supponiamo invece che non vi siano elementi di ordine 2 al di fuori di $N$, allora c'è un elemento $h$ di ordine 4 tale che $h \notin N$. Vediamo subito $h^2 \in N$, avendo ordine 2. Allora abbiamo $< n > \triangleleft G$ e $< h > \triangleleft G$. Facciamo agire $H$ su $N$ per coniugio. Ovvero una mappa da $\mathbb{Z}_4 \to Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$. Ne ho dunque due, determinati dall'immagine di un generatore di $H$. Ho altri due casi. Il primo, se è quello banale, $h \mapsto e$, tutto commuta e dico che $(hn)^2 = e$. In quanto abeliano, $(hn)^2 = h^2n^2 = n^4 = e$, ma $hn \notin N$ e ha ordine 2 e commuta con $N$: ma allora sono rientrato nelle ipotesi di $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Secondo, se è quello non banale, troviamo che $o(h) = o(n) = o(hn) = 4$. Definiamoli $h = i,\ n = j,\ hn = k$ e $G = \{ \pm 1, \pm i, \pm j, \pm k \}$ con regole di commutatività tali che ciclano. Questo gruppo è isomorfo a $\mathcal{Q}_8$, i quaternioni.

Abbiamo usato questi risultati:
**Proposizione 1.** *Sia $G$ un gruppo di ordine $2n$. Supponiamo che esattamente la metà degli elementi abbia ordine 2, mentre che l'altra metà formi un sottogruppo $H$ normale. Allora $H$ è abeliano e ha cardinalità dispari.*

*Dimostrazione.* $|H| = n$: $n$ è dispari necessariamente, se non lo fosse, per teorema di Cauchy, conterrebbe elementi di ordine 2, ma contraddirebbe le ipotesi.

Resta da mostrare che $H$ è abeliano. Consideriamo $H \times H$ e contiamo le coppie della forma $(a, a^{-1})$.

Dato $b \notin H$, agiamo con $b$ su $H$ per coniugio in modo non banale, ovvero tale che $\forall h \in H$, $b \diamond h = bhb^{-1} = bhb$. Osserviamo che se agisce non banalmente manda ogni elemento nel suo inverso. Primo, la mappa coniugio ha ordine 2,

ovvero $\forall h \in H$, $b \diamond (b \diamond h) = bb \diamond h = h$. Secondo, $hb \notin H$, allora ha ordine 2 e dunque $hbhb$ ha ordine 2, ovvero $bhb = h^{-1}$, cioè il coniugio manda ogni elemento di $H$ nel suo inverso. Ma da questo si dimostra subito che $H$ è abeliano per proposizione 2. □

**Proposizione 2.** *Se $K$ è un gruppo, $\phi \in Aut(K)$ tale che $\phi(x) = x^{-1}$ allora $K$ è abeliano e viceversa.*

*Dimostrazione.* Se fai conti viene subito. □

**Proposizione 3.** *Sia $G$ un gruppo tale che $\forall x \in G$ $x^2 = e$. Allora $G$ è abeliano.*

*Dimostrazione.* Se fai i conti viene. □

**Proposizione 4.** *Sia $G$ gruppo tale che $|G| = 2^n$, Supponiamo che $\forall x^2 = e$. Allora $G \cong (\mathbb{Z}_2)^n$*

*Dimostrazione.* Jolly: induzione+quozienti sollevati. □

# Capitolo 4

# Venerdì 14 Ottobre

*Il gruppo $\mathcal{Q}_8$ non è un prodotto semidiretto in modo non banale. Classificazione dei gruppi di ordine 12. I gruppi di cardinalità $pq^2$ sono tutti prodotto semidiretto dei loro sottogruppi di Sylow. Classificazione dei gruppi di ordine 30 (da completare).*

Continuiamo la classificazione dei gruppi a partire dal loro ordine. Eravamo arrivati a quelli di ordine 8.

Preliminarmente ricordiamoci alcuni fatti:

Requisiti per struttura di prodotto semidiretto:

1. $H < G$
2. $N \lhd G$
3. $H \cap N = \{ e \}$
4. $HN = G$

allora $G \cong N \rtimes_\phi H$ dove $\phi \in Hom(H, Aut(N))$.

Se $H$ è un gruppo ciclico, ovvero $\exists h \in H$ t.c. $< h >= H$, allora l'omomorfismo $\phi$ è univocamente determinato dall'immagine di $h$, l'immagine di ogni elemento deve avere ordine che divide quello dell'elemento e, se vogliamo un omomorfismo surgettivo, dobbiamo mandare un generatore di $H$ in un generatore di $Aut(N)$.

Tuttavia vi sono gruppi resistenti a questa struttura, ad esempio $\mathcal{Q}_8$, il gruppo dei Quaternioni. Questo è dovuto dal fatto che non vi sono sottogruppi dall'intersezione banale.

Osserviamo che $\forall H < \mathcal{Q}_8$ di ordine 4, questo è isomorfo a $\mathbb{Z}_4$. Prendiamo ora un sottogruppo isomorfo a $\mathbb{Z}_2$.

Possiamo scrivere $\mathcal{Q}_8 \cong \mathbb{Z}_4 \ltimes$ o $\rtimes \mathbb{Z}_2$?
Se fossero entrambi sono normali, il coniugio che mi fornisce il prodotto semidiretto sarebbe banale, ma allora $\mathcal{Q}_8$ sarebbe un prodotto diretto di due gruppi ciclici e dunque abeliano: $\perp$
Allora possiamo supporre $\mathcal{Q}_8 \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2$: ma fuori da ogni sottogruppo di $\mathcal{Q}_8$, a meno di quello banale, non vi è nessun elemento di ordine 2 e questo mi preclude la possibilità di trovare sottogruppo con intersezione banale.

Ma rincuoriamoci: questo è un caso particolare, spesso va tutto bene.

Questo conclude la classificazione dei gruppi di ordine 8.

Riprendiamo la classificazione dei gruppi di ordine fino a 12. Possiamo tralasciare quelli di ordine 11 che, in quanto di ordine primo, sono tutti isomorfi a $\mathbb{Z}_{11}$.

**Ordine 9** Essendo un gruppo di cardinalità $p^2$, sono tutti abeliani e dunque ogni loro sottogruppo è normale, abbiamo o $\mathbb{Z}_9$ o $\mathbb{Z}_3^2$.

**Ordine 10** $10 = 2 \cdot 5$

Per minimalità dell'indice, il 5-Sylow $N_5 \cong \mathbb{Z}_5$ è normale; inoltre l'intersezione con un 2-Sylow è banale per ragioni di ordine degli elementi e $|N_5 N_2| = |G|$. Dunque è ben definito, al variare di $\phi \in Hom(N_2, Aut(N_5))$, il loro prodotto semidiretto: abbiamo o quello diretto $N_5 \times N_2 \cong \mathbb{Z}_{10}$ (se $\phi$ banale) o quello semidiretto proprio $N_5 \rtimes_\phi N_2 \cong D_5$ (se $\phi$ non banale).

**Ordine 12** $12 = 3 \cdot 2^2$.

Classifichiamo i 3-Sylow e i 2-Sylow:
$n_3 = 1,\ 4$ per Sylow 3: nel primo caso siamo contenti, in quanto il 3-Sylow sarebbe normale; nel secondo caso non lo è, ma contando gli elementi di ordine diverso da 3 sarebbe unico il 2-Sylow in quanto 4 3-Sylow danno 8 elementi di ordine 3, per cui restano fuori 4 elementi che necessariamente appartengono a un 2-Sylow di ordine 4, che dunque è unico. Denotiamo $N_3$ un 3-Sylow e $N_2$ un 2-Sylow e consideriamo le seguenti casistiche:

1. se è normale il 3-Sylow, $G \cong N_3 \rtimes_\phi N_2$. Quantifichiamo su $N_2$, che in quanto di ordine 4 può essere isomorfo a

- $N_2 \cong \mathbb{Z}_4$, allora abbiamo $\phi : N_2 \to Aut(N_3) \cong \mathbb{Z}_2$. Allora $\phi$ può essere banale o quello che manda $[1]_4 \mapsto [1]_2$.

  Nel primo caso si ha $G \cong N_3 \times N_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_4$; nel secondo $G \cong N_3 \rtimes_\phi N_2 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

- $N_2 \cong (\mathbb{Z}_2)^2$. In questo caso $Aut(N_2) \cong GL_2(\mathbb{F}_2)$ e ha cardinalità $(2^2-1)(2^2-2) = 6$: infatti possiamo vederli come quelli che permutano i 3 elementi di ordine 2. Abbiamo $\phi : (\mathbb{Z}_2)^2 \to \mathbb{Z}_2$. Quanti sono?

  Di sicuro quello banale che mi produce un prodotto diretto: $G \cong N_3 \times N_2 \cong \mathbb{Z}_3 \times (\mathbb{Z}_2)^2$.

  Se non è banale è surgettivo: allora i possibili nuclei di omomorfismi da $(\mathbb{Z}_2)^2 \twoheadrightarrow \mathbb{Z}_2$ (ovvero tali che $|ker(\phi)| = 2$) sono 3 e sono uguali a meno di permutazioni di $(\mathbb{Z}_2)^2$ in sè. Questi omomorfismi producono allora il prodotto diretto $G \cong N_3 \rtimes_\phi N_2 \cong \mathbb{Z}_3 \rtimes_\phi (\mathbb{Z}_2)^2$.

  Possiamo dire di più: cerchiamo di capire chi sono le immagini di $\phi$. Vederlo in $\mathbb{Z}_2$ è facile, ma in $Aut(\mathbb{Z}_3)$ un po' meno. Dati due generatori indipendenti di $N_2 \cong (\mathbb{Z}_2)^2$, uno genera l'immagine, l'altro il kernel: possiamo assumere che $\phi(([0]_2, [1]_2))$ è l'automorfismo di $\mathbb{Z}_3$ che associa ad ogni elemento il suo inverso, mentre $\phi(([1]_2, [0]_2))$ va nell'identità di $Aut(\mathbb{Z}_3)$; ovvero un generatore di $\mathbb{Z}_2^2$ coniuga, l'altro commuta. Quindi vale che

  $$G \cong (\mathbb{Z}_3 \rtimes \mathbb{Z}_2) \times \mathbb{Z}_2 \cong \mathcal{D}_3 \times \mathbb{Z}_2$$

2. se è normale il 2-Sylow, abbiamo $G \cong N_2 \rtimes_\phi N_3$. Analogamente al punto 1, quantifichiamo su $N_2$, che può essere isomorfo a

   - $N_2 \cong \mathbb{Z}_4$. In questo caso $G \cong \mathbb{Z}_4 \rtimes_\phi \mathbb{Z}_3$ dove $\phi : \mathbb{Z}_3 \to Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$, ovvero un omomorfismo da un gruppo di ordine 3 in uno di ordine 2, cioè solo quello banale e dunque ho un prodotto diretto: $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$, già incontrato nel primo punto di 1.

   - $N_2 \cong (\mathbb{Z}_2)^2$. In questo caso $G \cong \mathbb{Z}_2^2 \rtimes_\phi \mathbb{Z}_3$ e $\phi : \mathbb{Z}_3 \to Aut((\mathbb{Z}_2)^2) \cong \mathcal{S}_3$ (in quanto lo posso vedere come gruppo di permutazioni delle tre coppie di generatori di $(\mathbb{Z}_2)^2$, come sopra). Dove posso mandare $[1]_3$? Di sicuro in un elemento il cui ordine divide 3, o l'identità, o un 3-ciclo, ma allora è

iniettivo e in particolare lascia fissi gli elementi di ordine 2 di $\mathcal{S}_3$ (trasposizioni).

Se $[1]_3$ va nell'identità, abbiamo il prodotto semidiretto banale abeliano: $G \cong N_2 \times N_3 \cong (\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ già incontrato nel secondo punto di 1.

Altrimenti abbiamo $\phi([1]_3) = (1\ 2\ 3)$ o $(1\ 3\ 2)$ dunque abbiamo due possibili immagini, che tuttavia sappiamo che determinano lo stesso coniugio a meno di permutazione di $\mathbb{Z}_3$ (mandando $[1]_3$ in $[2]_3$). Ma dunque chi sono effettivamente queste permutazioni in $Aut((\mathbb{Z}_2)^2)$? Sono automorfismi di ordine 3 che permutano ciclicamente gli elementi di ordine 2 (che sono 3). Abbiamo allora

$$G \cong N_2 \rtimes_\phi N_3 \cong (\mathbb{Z}_2)^2 \rtimes_\phi \mathbb{Z}_3 \cong \mathcal{A}_4$$

in quanto $\mathcal{A}_4$ non ha elementi di ordine 4, ma solo i 3 2-2-cicli di ordine 2 e i 3-cicli.

Breve recap:

- $\mathbb{Z}_3 \times \mathbb{Z}_4 = \mathbb{Z}_{12}$
- $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$
- $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$
- $\mathbb{Z}_2 \times \mathcal{D}_3 \cong \mathcal{D}_6$
- $\mathcal{A}_4$

Possiamo concludere che sono tutti non isomorfi fra loro portando argomenti quali la presenza di elementi di ordine 4, l'abelianità, la struttura del centro. Lo strumento migliore è guardare chi sono i centri.

**Classifichiamo i gruppi di ordine $p^2q$, con p e q primi distinti.** Preliminarmente abbiamo che i p-Sylow e i q-Sylow hanno intersezione banale e il loro prodotto ha la cardinalità di tutto il gruppo. Per scriverli come prodotto semidiretto resta da verificare che almeno uno dei due sia normale.

Supponiamo che $p < q$. Ripetendo le considerazioni fatte precedentemente, se contiamo gli elementi di ordine $q$, ricaviamo che o è normale il q-Sylow, o il p-Sylow. Se $N_q$ è normale, scriviamo $G \cong N_q \rtimes_\phi N_p$, altrimenti se $N_p$ è normale, $G \cong N_p \rtimes_\phi N_q$. In entrambi i casi bisogna distinguere il caso in cui $N_p \cong \mathbb{Z}_{p^2}$ o $N_p \cong (\mathbb{Z}_p^2)$.

Se supponiamo invece che $p > q$, il p-Sylow ha indice il più piccolo primo che divide l'ordine e quindi è normale.

Dunque tutti i gruppi di tale ordine possono essere espressi come prodotto semidiretto dei due Sylow.

**Classifichiamo i gruppi di ordine 30.** *Per brevità: $N_p$ denota un generico p-Sylow.*

Per Cauchy ci sono elementi di ordine 2, 3 e 5. Consideriamo un elemento $h \in G$ di ordine 5 e sia $< h >= H \cong \mathbb{Z}_5$.

Consideriamone il normalizzatore: $N(H)$ può avere cardinalità 30, 15, 10 o 5 in quanto è un sottogruppo contenente $H$. Possiamo subito scartare 15, in quanto avremmo $n_5 = \frac{|G|}{|N(H)|} = 2$ 5-Sylow, ma non vale che $2 \equiv 1 \ mod \ 5$; 10 per la stessa ragione in quanto si avrebbero 3 5-Sylow. Restano dunque due casi:

1. se ha cardinalità 30, $N(H) = G$, allora $H \lhd G$ e dunque il prodotto diretto con un 3-Sylow è un sottogruppo di ordine 15. Avendo indice 2, un simile sottogruppo è normale e dunque anche il prodotto fra questo e un 2-Sylow è un sottogruppo: $G \cong (N_5 \rtimes N_3) \rtimes N_2$;
2. se ha cardinalità 5, allora $N(H) = H$ e $N_5 = 6$. Questo significa un totale di 24 elementi di ordine 5, in quanto ogni sottogruppo isomorfo a $\mathbb{Z}_5$ ha 4 elementi caratteristici. Avanzano allora 6 elementi. Deduciamo subito che $n_3 = 1$, altrimenti se fossero 4 si avrebbero troppi elementi di ordine 3 (ovvero 8). Perciò abbiamo un unico 3-Sylow che è perciò normale, dunque il prodotto con un 2-Sylow è un sottogruppo, ha ordine 6 e per ragioni di ordine degli elementi, esso è normale, perciò abbiamo $G \cong (N_3 \rtimes N_2) \rtimes N_5$.

Entriamo nel dettaglio:

1. Abbiamo $G \cong (N_5 \rtimes N_3) \rtimes_\tau N_2$ con $N_5 \lhd G$. Come agisce un 3-Sylow su $N_5$? Siccome è equivalente a cercare gli omomorfismi da $\mathbb{Z}_3$ in $\mathbb{Z}_4$, può agire solo banalmente: $N_5 \rtimes N_3 \cong N_5 \times N_3 \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$.

   A questo punto ci resta da trovare gli omomorfismi $\tau : \mathbb{Z}_2 \to Aut(\mathbb{Z}_{15}) \cong Aut(\mathbb{Z}_3) \times Aut(\mathbb{Z}_5) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, ovvero stiamo cercando omomorfismi $\tau : \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_4$. Siccome abbiamo a che fare con un gruppo ciclico, $\tau$ è univocamente determinato dall'immagine di $[1]_2$ che può essere mandato (elenco gli elementi di ordine che divide 2) in: $(0,0),\ (1,0),\ (0,2),\ (1,2)$.

Traduciamo in automorfismi quanto abbiamo trovato:

- $(0,0) \tilde{=} (id_{\mathbb{Z}_3}, id_{\mathbb{Z}_5})$, l'identità su entrambi le componenti, dunque $\tau$ agisce banalmente su tutto $\mathbb{Z}_{15}$: $G \cong \mathbb{Z}_{15} \times \mathbb{Z}_2$;
- $(1,0) \tilde{=} (inv_{\mathbb{Z}_3}, id_{\mathbb{Z}_5})$, l'identità sulla componente di ordine 3 e l'applicazione che manda ogni elemento nel suo inverso di $\mathbb{Z}_5$, dunque $G \cong \mathbb{Z}_5 \times (\mathbb{Z}_3 \rtimes \mathbb{Z}_2) \cong \mathbb{Z}_5 \times D_3$
- $(0,2) \tilde{=} (id_{\mathbb{Z}_3}, inv_{\mathbb{Z}_5})$, abbiamo allora $\mathbb{Z}_3 \times (\mathbb{Z}_5 \rtimes \mathbb{Z}_2) \cong \mathbb{Z}_3 \times D_5$;
- $(1,2) \tilde{=} (inv, inv) \tilde{=} inv_{\mathbb{Z}_{15}}$, abbiamo allora $G \cong D_{15}$.

2. Se il 5-Sylow non è normale, abbiamo che $G \cong (N_3 \rtimes N_2) \rtimes N_5$. Ma $N_3$ è comunque unico, per quanto detto prima, quindi esiste comunque un sottogruppo di ordine 15. Ma allora ricadiamo nelle ipotesi di un sottogruppo di ordine 15 normale in $G$.

Dunque in un gruppo di ordine 30 abbiamo sempre un sottogruppo di ordine 15, per cui possiamo ridurci ai casi trovati nel punto 1.

**Lemma 5.** *$Aut(G \times H) \cong Aut(G) \times Aut(H)$. Quando? Controesempi?*

# Capitolo 5

# Venerdì 21 Ottobre

*Classificazione dei gruppi di ordine 30 (conclusione). Esercizio su gruppi di ordine 255. Sottogruppi caratteristici. Automorfismi di un gruppo ciclico finito. Automorfismi del gruppo diedrale (da completare).*

Iniziamo completando l'esercizio della classificazione dei gruppi di ordine 30. NDR: concluso sopra.

**Definizione 1** (Sottogruppo caratteristico)**.** Se $\forall \phi \in Aut(H)$ $K < H$ è tale che $\phi(K) = K$, $K$ si definisce sottogruppo caratteristico.

**Proposizione 6.** *Se $G$ ha un sottogruppo normale $H$ e $\exists K < H$ caratteristico in $H$, allora $K \lhd G$.*

*Dimostrazione.* Sia $g \in G$ e $\phi_g \in Aut(G)$. Considero $\phi_g|_H : H \to H$. In quanto $K$ caratteristico in H, $\phi_g|_H(K) = K$, ma allora $gKg^{-1} = K$ ed è dunque normale in $G$. □

L'abbiamo usato per dire che il 3-Sylow di un gruppo di ordine 30 è normale, cfr 2.

**Esercizio 4.** Sia $G$ un gruppo di ordine 255, cioè $3 \cdot 5 \cdot 17$.

$N_{17}$ è normale, dunque esiste un sottogruppo di ordine 85. Denotiamo $H$ un simile sottogruppo. Vorremmo dimostrare che $H$ è ciclico, normale e che $G$ è ciclico.

1. Abbiamo detto che $H \cong N_{17} \rtimes N_5$, ma $5 \nmid 17 - 1$, dunque il prodotto semidiretto è banale e dunque $H \cong \mathbb{Z}_{85}$, ciclico;

2. inoltre $H$ ha indice il più piccolo primo che divide l'ordine di $G$, e dunque è normale;
3. siccome $H$ è normale, dato un qualsiasi $N_3$, allora $G \cong H \rtimes_\phi N_3$, con $\phi : N_3 \to Aut(H) \cong Aut(\mathbb{Z}_4) \times Aut(\mathbb{Z}_{16})$, ma non può che immergersi in modo nullo, in quanto non vi sono elementi di ordine 3. Allora $G \cong \mathbb{Z}_{17} \times \mathbb{Z}_5 \times \mathbb{Z}_3$ e dunque è ciclico (stesso ragionamento di 2).

**Esercizio 5.** Sia $n \in \mathbb{N}$, studiamo $Aut(\mathbb{Z}_n)$. Per $n$ primi lo sappiamo fare.

Domanda: sono in generale ciclici? No, si veda l'esercizio precedente.

Ha dei sottogruppi caratteristici? Nell'esempio di prima lo sono i due fattori. Ovvero i p-Sylow di $\mathbb{Z}_n$ sono caratteristici, in quanto sono tutti coniugati fra loro ma in un gruppo abeliano il coniugio è banale, dunque sono unici e caratteristici.

Vogliamo dire che se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, allora $\mathbb{Z}_n \cong \bigtimes_i (\mathbb{Z}_{p_i^{\alpha_i}})$. Infatti essendo normali, posso fare i loro prodotti, e via iterando per induzione dove il passo induttivo è dato dal fatto che

**Proposizione 7.** *Se $G$ gruppo, con $N_1$, $N_2$ normali in $G$ e tali che $N_1 \cap N_2 \lhd G$, allora $N_1 \times N_2 \cong N_1 N_2 \lhd G$.*

*Dimostrazione.* Vale per come è definita l'operazione. □

Possiamo allora dire che

**Osservazione 2.** Un gruppo $G$ abeliano finito è isomorfo al prodotto diretto dei suoi sottogruppi di Sylow.

Inoltre tutti i fattori di $\mathbb{Z}_n \cong \bigtimes_i (\mathbb{Z}_{p_i^{\alpha_i}})$ sono sottogruppi caratteristici.

Allora $Aut(\mathbb{Z}_n) \cong \bigtimes_i Aut((\mathbb{Z}_{p_i^{\alpha_i}}))$.

Abbiamo usato il fatto che

**Proposizione 8.** *Se $G \cong H \times K$ con $H$ e $K$ caratteristici in $G$, vale $Aut(G) \cong Aut(H) \times Aut(K)$*

*Dimostrazione.* Perché ogni fattore deve essere mandato in se stesso in modo indipendente dall'altro fattore e posso creare una bigezione fra i due insiemi. □

Non ci resta che studiare i singoli fattori, ovvero dire chi sono $Aut(\mathbb{Z}_{p_i^{\alpha_i}}) \cong (\mathbb{Z}_{p_i^{\alpha_i}})^*$. In generale non è un gruppo ciclico.

*Da qui in poi conti che non ho avuto voglia di rivedere. Probabilmente sbagliati.*

Ad esempio in $(\mathbb{Z}_8)^*$, tutti gli elementi diversi dall'identità hanno ordine 2 ed è dunque isomorfo a $(\mathbb{Z}_2)^2$. Ovvero

$$(\mathbb{Z}_{2^m})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$$

Di certo $\exists a$ t.c. $a^{2^{m-2}} \equiv 1$, ma tale che non valga $a^{2^{m-3}} \equiv 1$. Ora voglio un elemento di ordine 2, $b$, tale che $b^2 \equiv 1$, ma $b \notin < a >$, ovvero $b \neq a^{2^{m-3}}$.

Proviamo con $b = -1$, mentre $a = 5 = 1 + 2^2$. Vorrei dimostrare che $(1+4)^{2^{m-2}} \equiv 1 \ mod(2^m)$, ma non valga $(1+4)^{2^{m-3}} \equiv 1 \ mod(2^m)$.

Vediamo prima come risulta per un primo diverso da 2: $Aut(\mathbb{Z}_{p^m}) \cong (\mathbb{Z}_p)^* \times \mathbb{Z}_{(p-1)}$. Come prima cerco $a$ e $b$ tali che $b^{p-1} = 1$ ma $b^h \neq 1$ per $h < p-1$ e $a^{p^{n-1}} = 1$ ma $a^{p^{n-2}} \neq 2$. Siccome i due ordini sono coprimi, sono a posto.

Inoltre sappiamo che posso mandare $Aut(\mathbb{Z}_{p^n}) \cong Aut(\mathbb{Z}_p)$ surgettivamente: sia $\tilde{x}$ la classe di $x$ nel dominio, allora tale che $(x, p) = 1$ e dunque $(\tilde{x}, p) = 1$. In soldoni consideri egli stesso, tramite controimmagine.

Quindi per $b$ prenderò un intero tra 1 e $p-1$, ma per questo motivo sarà coprimo anche con $p^n$ e dunque sta negli automorfismi, in quanto $o(x) = p-1$, ma $p-1 \mid o(\tilde{x})$ e dunque contiene un sottogruppo isomorfo a $\mathbb{Z}_{(p-1)}$, in quanto i gruppi ciclici contengono sottogruppi di cardinalità per ciascun divisore.

Sia $a = p+1$, proviamo che $(1+p)^{p^{m-1}} = 1 \ (p^m)$ e $(1+p)^{p^{m-2}} \neq 1 \ (p^m)$.

Per provare che gli ordine moltiplicativi siano proprio quelli che vogliamo, abbiamo bisogno di due risultati:

1. $(1+p^m)^{p^n} \equiv 1 \ (p^{m+n})$
2. $(1+p^m)^{p^{n-1}} \equiv 1 + p^{m+n-1} \ (p^{m+n})$

da questi seguono le congruenze per gli $a$ che abbiamo trovato.

Facciamolo per induzione su $n$. Possiamo subito concludere il passo induttivo, ovvero che se $A \equiv B \ (p^h) \Rightarrow A^p \equiv B^p \ (p^{h+1})$. Segue ovviamente dallo sviluppo col binomio di Newton di $A = B + p^h C$ modulo $p^{h+1}$.

**Esercizio 6.** Cerchiamo gli automorfismi e i sottogruppi caratteristici di questi 3 gruppi:

1. $\mathbb{Z}_2 \times \mathbb{Z}_4$;

2. $(\mathbb{Z}_6)^2$;
3. $(\mathbb{Z}_9)^2$.

**Esercizio 7.** Cerchiamo gli automorfismi di $D_3 \times \mathbb{Z}_3$. Osserviamo che $\mathbb{Z}_3$ è caratteristico in quanto ne è il centro, mentre $D_3$ essendo quello generato dagli elementi di ordine 2, non può che andare in se stesso in quanto gli automorfismi mantengono gli ordini degli elementi.

Dunque $Aut(D_3 \times \mathbb{Z}_3) \cong Aut(D_3) \times Aut(\mathbb{Z}_3) \cong Aut(D_3) \times \mathbb{Z}_2$.

In generale $Aut(D_n)$ ha $n \cdot \phi(n)$ elementi, in quanto lo possiamo vedere come isomorfo a $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. Siccome $\mathbb{Z}_n$ è caratteristico in $D_n$, posso restringere ogni automorfismo di $D_n$ a $\mathbb{Z}_n$, vorrei che questa mappa fosse anche surgettiva su $Aut(\mathbb{Z}_n)$, cioè quello manda la permutazione delle potenze di una rotazione $\sigma$ nella permutazione dell'esponente. Il suo nucleo è $\{ \phi \mid \phi(\sigma) = \sigma \} \cong \mathbb{Z}_n$ e quindi

$$Aut(D_n) \cong \mathbb{Z}_n \rtimes (\mathbb{Z}_n)^*$$

Domanda: come agisce?

# Capitolo 6

# Martedì 25 Ottobre

*Automorfismi del gruppo diedrale $\mathcal{D}_n$ visti come affinità di $\mathbb{Z}_n$. Automorfismi di gruppi abeliani e sottogruppi caratteristici di gruppi abeliani.*

# Capitolo 7

# Venerdì 28 Ottobre

*Dimostrazione della semplicità di $\mathcal{A}_n$ per $n > 5$. Esercizio sui gruppi di ordine pqr. Definizione del sottogruppo dei commutatori e caratterizzazione. Risolubilità di un gruppo finito. Esercizi sul normalizzatore di una permutazione. Suriettività dell'omomorfismo dal normalizzatore di una permutazione $\sigma \in \mathcal{S}_n$ sugli automorfismi del sottogruppo generato da $\sigma$.*

**Esercizio 8.** $\forall n > 5$ $\mathcal{A}_5$ è semplice.

Procediamo per induzione. Come basso base, per $n = 5$ l'abbiamo già stato dimostrato. Al passo induttivo dobbiamo dimostrare che se $\mathcal{A}_{n-1}$ è semplice, allora lo è $\mathcal{A}_n$.

Consideriamo al variare di $i \in \mathbb{N}_n$ $G_i < \mathcal{A}_n$ tale che $G_i = \{ \sigma \in \mathcal{A}_n \mid \sigma(i) = i \}$. Osserviamo che $G_i \cong \mathcal{A}_{n-1}$ e dunque è semplice. Inoltre i $G_i$ sono tutti coniugati, basta prendere il coniugio che manda $i \mapsto j$.

Ora consideriamo $N \lhd G$ e $\forall i \in \mathbb{N}_n$ $N \cap G_i$. Siccome $G_i$ è semplice per ipotesi induttiva , possono succedere due cose:

- o $N \cap G_i = \{ id \}$
- o $N \cap G_i = G_i$

Ora consideriamo $\bigcap_{i \in \mathbb{N}_n} N \cap G_i$. Possono succedere due cose

**Esercizio 9.** Sia $G$ di cardinalità $pqr$ con $p < q < r$. Vogliamo mostrare tre cose:

1. esiste un r-Sylow normale in $G$;
2. esiste $H \lhd G$ tale che $|H| = pq$;

3. se $q \nmid r-1$ allora il q-Sylow è normale.

*Dimostrazione.* 1. Supponiamo per assurdo che $H$, un r-Sylow, non sia normale. Allora $n_r = 1, p, q, pq$: 1 lo escludiamo in quanto stiamo supponendo che non sia normale, $p$ e $q$ anche perché essendo minori di $r$ non può valere $\equiv 1\ (r)$. Dunque abbiamo $pq$ sottogruppi di ordine $r$, per un totale di $(r-1)pq$ elementi di ordine $r$ e dunque i p-Sylow, $N_p$, e q-Sylow, $N_q$, devono spartirsi $pq$ elementi.

Se non fossero entrambi normali, allora $N_p$ ha almeno $q$ coniugati e $N_q$ almeno $r$. Dunque ho almeno $q(p-1)$ elementi di ordine $p$ e $r(q-1)$ elementi di ordine $q$, ma allora avremo che $pq \geq (p-1)q + (q-1)r$ assurdo.

Dunque almeno uno dei due è normale. Supponiamo $N_q \lhd G$, allora $K = N_q \rtimes N_p$ è un sottogruppo di $G$ di cardinalità $pq$, ma questo è normale in quanto non ho abbastanza elementi fuori da $K$per costituire un suo coniugato diverso da lui.

Consideriamo allora $K \rtimes_\tau H$ con $\tau : H \to Aut(K)$. Se $K$ è abeliano i suoi automorfismi hanno cardinalità $(p-1)(q-1)$, se non è abeliano hanno cardinalità $(q-1)q$ (lo dà per esercizio): in entrambi i casi $r$ non lo divide, dunque $\tau$ può essere solo l'omomorfismo banale. Ciò vuol dire che $G \cong H \times K$, ma ciò implica che $H$ è normale. Assurdo.

2. sapendo che $H$ è normale, è ben definito un sottogruppo $H \rtimes L$ con $L$ q-Sylow. Tale sottogruppo ha indice $p$, il più piccolo primo che divide l'ordine di $G$ e dunque è normale

3. se $q \nmid r-1$, il sottogruppo di prima $K = H \rtimes L = H \times L$, ma allora $L$ è unico di un dato ordine, e dunque caratteristico, in $K$ che è normale, perciò è anch'esso normale.

**Definizione 2** (Commutatore)**.** Dato un gruppo $G$ e $x, y \in G$ definiamo commutatore di $x$ e $y$ l'elemento $[x,y] = xyx^{-1}y^{-1}$. Definiamo commutatore di $G$ il gruppo $G' =< [g_1 g_2] \mid g_1, g_2 \in G >$.

Osserviamo che gli elementi di un gruppo commutano sempre, a meno di elementi del commutatore: $xy = [x,y]yx$. Inoltre $\forall h \in G,\ [x,y] \in G'$,

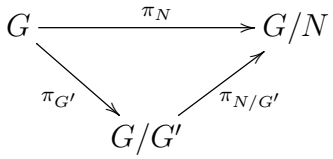
$$\begin{aligned} h[x,y]h^{-1} &= hxyx^{-1}y^{-1}h^{-1} = \\ &= hxh^{-1}hyh^{-1}hx^{-1}h^{-1}hy^{-1}h^{-1} = \\ &= (hxh^{-1})(hyh^{-1})(hx^{-1}h^{-1})(hy^{-1}h^{-1}) = \\ &= (hxh^{-1})(hyh^{-1})(hxh^{-1})^{-1}(hyh^{-1})^{-1} = \end{aligned}$$

$$= [hxh^{-1}, hyh^{-1}] \in G'$$

ovvero $G'$ è invariante per coniugio cioè normale.

Il fatto che a meno di elementi del commutatore gli elementi del gruppo commutino comporta che $G/G'$ è abeliano. In particolare è il più grande quoziente abeliano di $G$. Proviamolo. Sia $N \lhd G$ tale che $G/N$ abeliano. Mostriamo che $N \supseteq G'$.

*Dimostrazione.* Siano $xN, yN \in G/N$. Vale che $xNyN = yNxN \Leftrightarrow xyN = yxN \Leftrightarrow N = (xyN)(yxN)^{-1} = xyN(xy)^{-1}N = xy(yx)^{-1}N = xyx^{-1}y^{-1}N = N \Leftrightarrow [x, y] \in N$. Quindi il seguente diagramma commuta




dunque $G/N \cong G/G' \Big/ N/G'$. Mutatis mutandis, abbiamo dimostrato il terzo teorema di omomorfismo. □

**Definizione 3** (Gruppo risolubile)**.** Un gruppo $G$ si definisce risolubile se $\exists i = 1, \ldots, n$ e $H_i < G$ tali che $\forall i$ si ha $H_{i+1} \lhd H_i$ il cui quoziente è abeliano, con $H_n = G$ e $H_0 = \{ e \}$. In altre parole se $G$ ammette una catena di sottogruppi normali finita con i quozienti abeliani

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{ e \}$$

**Proposizione 9.** *Se $G$ è risolubile, allora lo è con quozienti ciclici.*

*Dimostrazione.* Se $G$ è risolubile, consideriamo una catena

$$G \rhd \ldots \rhd H_i \rhd H_{i+1} \cdots \rhd H_n = \{ e \}$$

con il generico $H_i/H_{i+1}$ abeliano finito. I suoi sottogruppi sono tutti normali, in quanto abeliano. Allora vogliamo mostrare che esiste una catena una catena

$$H_i \rhd N_{1_i} \ldots N_{h_i} \rhd H_{i+1}$$

tale che il generico quoziente $N_{j_i}/N_{j+1_i}$ è ciclico.

In quanto abeliano finito, possiamo supporre esistano $\exists m \in \mathbb{N}$ tali che $H_{i+1}/H_i = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$. Per $j = 1, \ldots, k$ definiamo il sottogruppo $H_{i+1}/H_i > L_{i,j} = \{ e \} \times \ldots \times \{ e \} \times \mathbb{Z}_{m_j} \times \ldots \times \mathbb{Z}_{m_k}$. La catena

è sbagliato. non sto capendo na sega

**Proposizione 10.** *Un gruppo $G$ è risolubile se e solo se è risolubile per commutatori.*

*Dimostrazione.* $\Leftarrow$ è banalmente vero.

$\Rightarrow$ lo dimostriamo per induzione sulla cardinalità di $G$.

Il passo base è banalmente vero. Induttivamente, sia ora vero per un gruppo di cardinalità $< |G|$.

Preliminarmente notiamo che un gruppo è risolubile per commutatori se e solo se il suo derivato è risolubile per commutatori. Infatti se un gruppo $K$ è risolubile per commutatori, sarà ben definita e con quozienti abeliani la catena

$$K > K' > \ldots > ((K')^{\cdots})' = \{ e \}$$

ma allora la catena $K' > \ldots > ((K')^{\cdots})' = \{ e \}$ è una catena di risolubilità per $K'$. Analogamente il viceversa, aggiungendo all'inizio $K$, il cui quoziente $K/K'$ è abeliano per definizione di derivato.

Tornando al passo induttivo, sappiamo che se $G'$ è risolubile, allora lo è per commutatori in quanto $|G'| < |G|$ (ipotesi induttiva). Dobbiamo allora provare che $G'$ è risolubile. Consideriamo una catena di risolubilità di $G$

$$G > H_1 > \ldots > H_n = \{ e \}$$

Dato che $G/H_1$ è abeliano, per proprietà del derivato $H_1 \supseteq G'$, allora $G' \cap H_1 = G'$, di conseguenza $G' = G' \cap H_1 \supset G' \cap H_2$ e così via per ogni indice della catena di $G$: allora è ben definita la catena di sottogruppi

$$G' > G' \cap H_2 > \ldots > G' \cap H_n = \{ e \}$$

Proviamo che è una catena di risolubilità, ovvero che i sottogruppi sono normali e che i quozienti sono abeliani.

$G' \cap H_{i+1} \lhd G' \cap H_i$ in quanto $H_{i+1} \lhd H_i$, infatti se $h \in H_{i+1} \cap G'$ e $g \in G' \cap H_i$ allora banalmente $ghg^{-1} \in G'$, ma vale anche che $ghg^{-1} \in H_{i+1}$ per normalità.

Invece il quoziente $G' \cap H_i / G' \cap H_{i+1}$ è abeliano in quanto sottogruppo di $H_i/H_{i+1}$ che sappiamo essere abeliano per ipotesi.

Dunque $G'$ è risolubile, per ipotesi induttiva lo è per commutatori e per l'osservazione preliminare lo è $G$. □

**Esercizio 10.** Sia $\sigma = (1\ 2)(3\ 4) \in \mathcal{S}_6$. Troviamo esplicitamente e via isomorfismo $N_{\mathcal{S}_6}(< \sigma >)$.

Brevemente troviamoci $Z_{\mathcal{S}_6}(\sigma)$. Sappiamo che contiene le potenze dei cicli disgiunti componenti $\sigma$, le permutazioni degli elementi lasciati fissi da $\sigma$ e le permutazione che permutano fra loro i cicli (disgiunti) di pari lunghezza componenti $\sigma$. A meno di alcune verifiche

$$Z_{\mathcal{S}_6}(\sigma) \cong ((< (1\ 2) > \times < (3\ 4) >) \rtimes_{C_{\mathcal{S}_6}} S_{(1\ 2),(3\ 4)}) \times S_{\{5,6\}} \cong ((\mathbb{Z}_2^2) \rtimes \mathbb{Z}_2) \times \mathbb{Z}_2$$

Ora sappiamo che $N(< \sigma >) \cong Z(\sigma) \rtimes Aut(\sigma)$, ma ora $Aut(\sigma) \cong Aut(\mathbb{Z}_2) \cong \{ e \}$ e dunque $N(< \sigma >) = Z(\sigma)$.

**Esercizio 11.** Sia $\sigma = (1\ 2\ 3)(4\ 5\ 6) \in \mathcal{S}_{10}$. Calcoliamo $N(< \sigma >)$.

Al solito, $Z(\sigma) = ((\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2) \times \mathcal{S}_4$. Invece $Aut(< \sigma >) \cong Aut(\mathcal{S}_3) \cong \mathbb{Z}_2$. Dunque

$$N(< \sigma >) \cong Z(\sigma) \rtimes Aut(< \sigma >) \cong (((\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2) \times \mathcal{S}_4) \rtimes \mathbb{Z}_2$$

# Capitolo 8

# Venerdì 4 Novembre

*Normalizzatore di una permutazione come prodotto diretto (ripasso). Esercizi su gruppi di ordine 144 e 168. Descrizione dei 2 e 3-Sylow di $\mathcal{S}_n$ per n piccolo e cenni alla descrizione di un p-Sylow di $\mathcal{S}_n$. Immersioni di $\mathcal{Q}_8$ in $\mathcal{S}_n$: trovare l'n minimo. Equivalenza tra risolubilità e risolubilità per commutatori.*

Abbiamo richiamato il fatto che il normalizzatore di un gruppo ciclico sia isomorfo al centralizzante di un generatore prodotto semidiretto gli automorfismi del gruppo: vista tramite successione $Z(\sigma) \hookrightarrow N(\sigma) \twoheadrightarrow Aut(<\sigma>)$ e inversa destra (sollevamento e dunque omomorfismo) della seconda surgettiva. Basta verificare le ipotesi determinanti lo spezzamento in prodotto semidiretto (conti).

**Esercizio 12.** Costruire un sollevamento iniettivo a partire da un omomorfismo surgettivo.

Dati $A, B$ gruppi tali che $f : A \twoheadrightarrow B$ allora posso definire $g : B \to A$ ponendo $\forall b \in B \ f(g(b)) = b$. L'iniettività consegue necessariamente.

In particolare, sono stati fatti gli esempi delle permutazioni di $\mathcal{S}_n$ $\sigma = (1\ 2\ 3)(4\ 5\ 6)$ e $\sigma' = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8)$. Anche nel secondo caso è piuttosto semplice trovare gli automorfismi, in quanto abbiamo comunque a che fare con un gruppo ciclico contenente due sottogruppi caratteristici (li esibisce esplicitamente, così come le permutazioni che coniugano, basta giocare un po' di più sulle congruenze degli esponenti).

**Esercizio 13.** Un gruppo di cardinalità 144 non è semplice.

Supponiamo non lo sia e facciamo considerazioni sul numero dei 3-Sylow: sono 4 o 16.

Ragioniamo sul fatto che $G$ agisca non banalmente sui 3-Sylow: se sono 4 trovo assurdi sul nucleo dell'azione (non è banale), se sono 16 e hanno intersezione banale abbiamo 12 elementi di ordine diverso da 3, dunque il 2-Sylow è normale. Se sono 16 e non tutti hanno intersezione banale considero l'intersezione di due 3-Sylow, in particolare il suo normalizzatore che ha almeno $9 \cdot k$ con $k \geq 2$ elementi e divide 144. Ragiono per esclusione su $9 \cdot k$: 144 lo escludo altrimenti sarebbe normale, 36 e 72 perché hanno indice troppo piccolo, 18 considerando che uno dei due è normale nell'intersezione per indice.

**Osservazione 3.** Dire che ho n p-Sylow equivale a dire che il normalizzatore di un p-Sylow ha esattamente indice n. Discende immediatamente da Sylow 3.

**Esercizio 14.** Sia $G$ di cardinalità $168 = 2^3 \cdot 3 \cdot 7$ semplice. Richieste:

1. trovare $n_7$
2. dimostrare che esiste un sgr di ordine 21
3. dimostrare che non esiste un sgr di ordine 14

Il primo punto è banale, usando il terzo teorema di Sylow e la semplicità.
Nel secondo punto si riflette sul fatto che, se esiste, è contenuto nel normalizzatore di un 7-Sylow, dunque cerco un elemento di ordine 3 che lo normalizza. Agendo su coniugio e ragionando su come si immerge $\mathbb{Z}_3$ in $\mathcal{S}_8$, osservo che fissa almeno due elementi e si conclude.
Alternativamente osservo che il normalizzatore di un p-Sylow ha indice 8 e che dunque ha cardinalità $3 \cdot 7 = 21$.
Nel terzo punto, suppongo esista, allora esiste un elemento (e un sottogruppo) di ordine 2 nel normalizzatore di un 7-Sylow (in quanto il 7-Sylow sarebbe normale in un sgr di ordine 14). Ma $|N(\text{7-sylow})| = 21$ e dunque trovo un assurdo.

É un esercizio che è stato proposto ad un compito.

**Esercizio 15.** Esploriamo i 2-Sylow di $\mathcal{S}_n$.

In $\mathcal{S}_4$ sono isomorfi a $\mathcal{D}_4$, del tipo $< (1\ 2\ 3\ 4)(2\ 4) >$
In $\mathcal{S}_5$ sono quelli di $\mathcal{S}_4$, per ciascun elemento tenuto fisso. Chi è la loro intersezione? L'identità, altrimenti avrei un sottogruppo normale (l'intersezione di tutti i 2-Sylow) e dunque avrei un assurdo.
In $\mathcal{S}_6$ sono i normalizzatori dei 2-Sylow di $\mathcal{S}_5$, isomorfi a $\mathcal{D}_4 \times \mathbb{Z}_2$.
In $\mathcal{S}_7$ sono quelli di $\mathcal{S}_6$.
In $\mathcal{S}_8$ ho un $\mathcal{D}_4 \times \mathcal{D}_4$ di ordine $2^6$, normale nel 2-Sylow (avente ordine $2^7$),

coniugato dal 4-2-ciclo che permuta i 2 4-cicli dei $\mathcal{D}_4$, scambiando i due termini.

Come sono fatti in generale in $\mathcal{S}_n$? Cfr. Balbo

Da questo osservo anche che $\mathcal{Q}_8$ si immerge in $\mathcal{S}_n$ con $n \geq 8$.

**Esercizio 16.** Esploriamo i 3-Sylow di $\mathcal{S}_n$.

Le cose interessanti arrivando da $\mathcal{S}_9$ in poi, in cui ha 81 elementi. Osserviamo che sono i normalizzatori del prodotto diretto di 3 3-cicli.

Ordunque, come sono fatti in generale i p-Sylow in un generico $\mathcal{S}_n$?

**Esercizio 17.** Sia $G = \mathbb{Z}_4 \times \mathbb{Z}_8$. Chi sono $Aut(G)$? Osservo che lo posso mandare in $End(\mathbb{Z}_2 \times \mathbb{Z}_2)$, in che modo?

Osserviamo che $2G = 2\mathbb{Z}_4 \times 4\mathbb{Z}_8$ è caratteristico in $G$, in quanto sono gli elementi di ordine 2, ovvero il kernel della moltiplicazione per 2 su $G$. Questo mi permette di definire una mappa $\phi' : G/K \to G/K$ a partire da $K$ caratteristico e $\phi : G \to G$ omomorfismo (osserva che un particolare diagramma commuta). Tutto ciò mi serve per trascinare l'omomorfismo DENTRO il quoziente. Allora $G/2G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (sta spezzando!!).

Mostriamo che se $\phi \in Aut(G$, allora $\phi' \in Aut((\mathbb{Z}_2)^2)$ e la mappa che associa $\phi$ a $\phi'$ è un omomorfismo surgettivo.

**Esercizio 18.** Descriviamo gli automorfismi di $\mathcal{Q}_8$.

Richiamiamo la definizione di gruppo risolubile:

**Definizione 4** (Gruppo risolubile)**.** Un gruppo si dice risolubile se boh

Questo equivale a dire che è risolubile per commutatori, ovvero che boh
Il $\Rightarrow$ è immediato.
Il $\Leftarrow$ è un po' meno ovvia: boh

Link to Wikipedia: Gruppi risolubili

# Capitolo 9

# Martedì 8 Novembre

*Automorfismi del gruppo di $\mathcal{Q}_8$. Forma normale di Smith, determinante e indice di un sottogruppo in $\mathbb{Z}^n$. Automorfismi di $\mathbb{Z}_4 \times \mathbb{Z}_8$ e cenni sul gruppo di automorfismi di un p-gruppo abeliano finito.*

**Esercizio 19.** Descriviamo $Aut(\mathcal{Q}_8)$.

Un automorfismo di un gruppo in particolare è una permutazione dei suoi sottogruppi, quindi qui in particolare i 3 sottogruppi generati dagli elementi di ordine di 4 vengono permutati l'uno nell'altro: è quindi ben definito un omomorfismo $\phi : Aut(\mathcal{Q}_8) \to \mathcal{S}_3$. Ci chiediamo se sia iniettivo e/o suriettivo.

Possiamo subito escludere che sia iniettivo in quanto ogni sottogruppo normale (in particolare quelli di ordine 4 in questione) è caratteristico per gli automorfismi interni, ovvero esprimibili come coniugi rispetto a elementi. Dunque $Int(G) \subseteq Ker(\phi)$. Inoltre osserviamo che se $\vartheta \in Ker(\phi)$, allora $\vartheta(i) \in < i >$ e avendo ordine 4 $\vartheta(i) = \pm i$. Per $j$ è analogo, mentre per $k$ è univoco. Dunque abbiamo che $|Ker(\phi)| \leq 4$.
Sappiamo inoltre che $C : \mathcal{Q}_8 \twoheadrightarrow Int(\mathcal{Q}_8)$, il cui kernel è $Z(\mathcal{Q}_8) = \{\ 1,\ -1\ \}$, è surgettiva e dunque

$$Ker(\phi) \supseteq Int(\mathcal{Q}_8) \cong \mathcal{Q}_8/Z(\mathcal{Q}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

in quanto è un sottogruppo di ordine 4 in cui non vi sono elementi di ordine 4 (altrimenti ciclico e $\mathcal{Q}_8$ abeliano). Dunque $|Ker(\phi)| \geq 4$.
Allora $|Ker(\phi)| = 4$ ed è proprio uguale a $Int(\mathcal{Q}_8)$ e dunque isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Vediamo se è surgettivo, ovvero se esistono $S,\, T \in Aut(\mathcal{Q}_8)$ tali che $\mathcal{S}_3 =< \phi(S), \phi(T) >$. Definiamo questi due elementi come segue

$$S = \begin{cases} i \mapsto j \\ j \mapsto i \\ k \mapsto -k \end{cases} \qquad T = \begin{cases} i \mapsto -i \\ j \mapsto k \\ k \mapsto j \end{cases}$$

Identificando i sottogruppi $< i >,\ < j >$ e $< k >$ con gli gli elementi 1, 2 e 3, è immediato verificare che $\phi(S) = (1\ 2)$ e $\phi(T) = (2\ 3)$. Sappiamo che questi due elementi generano tutto $\mathcal{S}_3$, dunque $\phi$ è surgettiva.

Ci chiediamo ora se sia possibile trovare un sollevamento (iniettivo) di $\mathcal{S}_3$ in $Aut(\mathcal{Q}_8)$, ovvero se esista un sottogruppo di $Aut(\mathcal{Q}_8)$ isomorfo a $\mathcal{S}_3$. Dobbiamo fare due cose. La prima è trovare due elementi che di ordine 2 che si comportino come i 2-cicli che generano $\mathcal{S}_3$, la seconda è verificare che tale sottogruppo è realmente isomorfo a $\mathcal{S}_3$, ovvero che ne condivide le regole di commutatività o che è isomorfo a $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

Consideriamo $H =< S,\ T >$, quelli di prima. Di quali elementi è composto? Osserviamo che

- $S^2 = T^2 = id_{Aut(\mathcal{Q}_8)}$;
- $(TS)^3 = id_{Aut(\mathcal{Q}_8)}$ e da questo deriva anche il fatto che $STS = TST$;

e che dunque $< S,\ T >= \left\{\ id_{Aut(\mathcal{Q}_8)},\ S,\ T,\ ST,\ TS,\ STS\ \right\}$. Come cardinalità ci siamo.
Inoltre $< TS > \cong \mathbb{Z}_3$ e $< S > \cong \mathbb{Z}_2$ è tale che $< TS > \cap < S >= \left\{\ id_{Aut(\mathcal{Q}_8)}\ \right\}$ e la cardinalità del prodotto è la cardinalità di $< S,\ T >$. Inoltre $< S >$ agisce su $< S,\ T >$ tramite coniugio in modo non banale, infatti $S(TS)S = ST = STSS = (STS)S = (TST)S = (TS)(TS) = (TS)^{-1}$. Dunque $< S,\ T > \cong \mathcal{S}_3$.

Definiamo allora il sollevamento $\mathfrak{S} : \mathcal{S}_3 \hookrightarrow Aut(\mathcal{Q}_8)$ in modo tale che $Im(\mathfrak{S}) =< T,\ S >$ e che $\phi \circ \mathfrak{S} = id_{\mathcal{S}_3}$.

Possiamo allora ben definire la seguente successione esatta corta

$$\{\ 0\ \} \longrightarrow Ker(\phi) \longrightarrow Aut(\mathcal{Q}_8) \longrightarrow \mathcal{S}_3 \longrightarrow \{\ 0\ \}$$

A questo punto abbiamo che

- $Ker(\phi) \cap H = \{\ 0\ \}$;
- $Ker(\phi) \lhd Aut(\mathcal{Q}_8)$, in quanto kernel di un omomorfismo;

- $|Ker(\phi) \cdot H| = |Aut(\mathcal{Q}_8)|$

e allora $Aut(\mathcal{Q}_8) \cong Ker(\phi) \rtimes_\tau H$.

Studiamolo nel dettaglio. Per quanto detto fino a qui $Aut(\mathcal{Q}_8) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\tau \mathcal{S}_3$ dove $\tau : \mathcal{S}_3 \to Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathcal{S}_3$. Facciamo vedere che nel nostro caso $\tau$ è iniettivo e che dunque, a meno di automorfismi di $\mathcal{S}_3$, vi è un solo coniugio possibile:

- proviamo che $Ker(\tau) \neq H$, ovvero che esiste $\sigma \in H =< S,\ T >$ tale che $\tau(\sigma) \neq id_{Ker(\phi)=id_{Aut(\mathcal{Q}_8)}}$. Basta prendere $\sigma = S$, infatti $\tau(S)(C_i)(i) = S \circ C_i \circ S(i) = -i \neq id_{Aut(\mathcal{Q}_8)}(i)$ e questo mi dice anche che $\tau(S)(C_i) = C_j$;
- proviamo che $Ker(\phi) \neq\!< TS ><\!\lhd H$, ovvero che l'altro sottogruppo normale non banale non può essere kernel, infatti basta prendere $\tau(TS)$: $\tau(TS)(C_i) = (TS) \circ C_i \circ (TS)^{-1} = T(SC_iS^{-1})T^{-1} = TC_jT^{-1}$ tale che $TC_jT(j) = TC_j(k) = T(jkj^{-1}) = T(-k) = -j$, dunque nemmeno questo può essere il kernel.

Necessariamente $Ker(\phi) = \{\ id_H\ \}$ e dunque è iniettiva, cioè un isomorfismo fra $H$ e $Aut(Ker(\phi))$. Tale prodotto semidiretto è inoltre unico, a meno di permutazioni di $\mathcal{S}_3$ (cui sono entrambi isomorfi).

Possiamo concludere dicendo che $Aut(\mathcal{Q}_8) \cong \mathcal{S}_4$. Infatti $S_4 \cong K \rtimes_\lambda \mathcal{S}_3$ con $\lambda$ iniettivo e $K$ il sottogruppo di Klein.

**Esercizio 20.** Contare $|Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)|$.

Iniziamo mettendoci in un caso più generale, ovvero cerchiamo le condizioni per cui è ben definito un elemento di $End(\mathbb{Z}_4 \times \mathbb{Z}_8)$, vedendo ogni endomorfismo come applicazione lineare indotta da una matrice.

Preliminarmente, ci chiediamo quando una matrice $A \in \mathcal{M}(2, \mathbb{Z}_4 \times \mathbb{Z}_8)$ (la prima riga è modulo 4, la seconda modulo 8) induca effettivamente un endomorfismo. Questo avviene se $2 \mid [A]_{2,1}$. Questa condizione è sufficiente anche affinché il prodotto di matrici (e, crediamoci, di endomorfismi) sia ben definito in $\mathcal{M}(2, \mathbb{Z}_4 \times \mathbb{Z}_8)$. Bisogna fare un po' di conti, ma viene.

Consideriamo $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Osserviamo che $r : End(\mathbb{Z}_4 \times \mathbb{Z}_8) \to End(\mathbb{Z}_2 \times \mathbb{Z}_2)$ tale che $A \mapsto [A]_2$ ovvero la matrice con i coefficienti ridotti modulo $p$ è un omomorfismo. $r$ non è surgettivo, in quanto $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ non è immagine di nessuna $A \in End(\mathbb{Z}_4 \times \mathbb{Z}_8)$ in quanto le abbiamo costruite aventi $2 \mid [A]_{2,1}$; tuttavia non è un problema in quanto a noi interessa ragionare su $\rho = r|_{Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)}$.

Consideriamo la seguente successione esatta corta:

$$\{ 0 \} \to Ker(\rho) \hookrightarrow Aut(\mathbb{Z}_4 \times \mathbb{Z}_8) \twoheadrightarrow Im(\rho) \subseteq Aut(\mathbb{Z}_4 \times \mathbb{Z}_8) \to \{ 0 \}$$

Ci dice che $Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)/Ker(\rho) \cong Im(\rho)$ e che dunque, avendo a che fare con gruppi finiti, $|Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)| = |Ker(\rho)| \cdot |Im(\rho)|$.

In $Im(\rho)$ abbiamo solo le matrici $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ e $N = I$ ed è dunque isomorfo a $\mathbb{Z}_2$.

Una matrice $A \in Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)$ sta nel kernel se e solo se $\rho(A) = [A]_p = I$, il che equivale al fatto che $A = A' + 2B$ con $A' = I$ e $B \in Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)$ elementi che alla quarta danno l'identità. Facendo leva su questa condizione, $A$ è determinata dalla scelta di $B \in \mathbb{Z}_4^2 \times \mathbb{Z}_8^2$.

Dunque $|Aut(\mathbb{Z}_4 \times \mathbb{Z}_8)| = 64 \cdot 2 = 128$.

**Esercizio 21.** Proponiamo un esercizio un po' più difficile per generalizzare questo risultato. Si chiede di studiare $Aut(\mathbb{Z}_{p_1^{\varepsilon_1}} \times \ldots \times \mathbb{Z}_{p_k^{\varepsilon_k}})$.

Facciamo presente che una condizione necessaria per la buona definizione di una matrice $A$ (quella che induce un automorfismo) è il fatto che $\forall i > j$ si abbia che $p^{\varepsilon_i - \varepsilon_j} \mid [A]_{i,j}$.

**Esercizio 22** (Difficile)**.** Contare $|Aut(G)|$ con $G$ gruppo abeliano finito.

**Esercizio 23.** Dato $G \cong \mathbb{Z}^n$ e $H < G$ tale che $H \cong \mathbb{Z}^n$, calcolare $[G : H]$.

$H$ è finitamente generato, dunque ammette un insieme finito di generatori $\{ v_1, \ldots, v_n \}$. Consideriamo la matrice composta dai vettori $v_i$ come colonne, la chiamiamo $A$. Ogni matrice a coefficienti in $\mathbb{Z}$ può essere ridotta nella propria forma di Smith, diagonale con gli elementi che si dividono l'un l'altro. Possiamo supporre che $A$ sia già in forma di Smith e che dunque esistano $\gamma_i \in \mathbb{Z}$ tali che $v_i = \gamma_i \cdot e_i$, dove gli $e_i$ sono i vettori della base canonica. Ora $H$ ha rango $n$ in quanto $H \cong \mathbb{Z}^n$ e (rifatti alla dimostrazione della classificazione dei gruppi abeliani fin. gen.) questo mi garantisce che $\forall i \ \gamma_i \neq 0$. A questo punto abbiamo che l'omomorfismo $\pi_H : G \to G/H$ tale che $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n) + H$ è surgettivo e dunque tale che $G/H \cong \mathbb{Z}_{\gamma_1} \times \ldots \times \mathbb{Z}_{\gamma_n}$ e dunque $[G : H] = \gamma_1 \cdot \ldots \cdot \gamma_n$.

É stato fatto un esempio con $G = \mathbb{Z}^2$ e $H = 2\mathbb{Z} \times 13\mathbb{Z}$.

# Ricevimento del pomeriggio

Viene chiesto se la presenza di un omomorfismo non banale tra $N \to Aut(H)$ sia necessaria e sufficiente per dire che $H \rtimes N$ non è isomorfo a un prodotto diretto. Un esempio è l'isomorfismo fra $\mathcal{S}_3 \rtimes \mathbb{Z}_2$ e $\mathcal{S}_3 \times \mathbb{Z}_2$. La riflessione nasce dal fatto che quando si classifica un gruppo a partire dal suo ordine potrei incappare in più di un omomorfismo possibile, ma che producono lo stesso gruppo. Ciò ci dice che bisogna sempre fare l'ultima verifica per eliminare i doppioni cfr. i gruppi di ordine 12, esibendo un isomorfismo. Uno è il lemma di "a meno di automorfismo", altri modi dipendono dal contesto.

Si chiedono precisazioni sul omomorfismo fra il normalizzatore di un sottogruppo ciclico e il centralizzatore di un generatore semidiretto gli automorfismi del generato. In quanto $C : N(H) \to Aut(H)$ via coniugio è tale che $Ker(C|_{N(H)}) = Z(H)$. In generale non possiamo dire di più, in quanto $C$ non è suriettiva e non è detto che $Im(C)$ si possa sollevare in $N(H)$, potremmo azzardare che se è ciclico sia più fattibile giocando con le controimmagini. Funziona se esiste una controimmagine del generatore di pari ordine. Dunque potrei scrivere che $N(H) \cong H \rtimes Im(C)$.
In $\mathcal{S}_n$, se $H =< \sigma >$ posso sempre farlo e dunque ottengo $N(H) \cong Z(\sigma) \rtimes Aut(H)$ in quanto il secondo termine lo vedo come sottogruppo di $\mathcal{S}_n$ risultato del sollevamento dei generatori di $H$ (non univoco). (sembra fatto apposta per funzionare)

Abbiamo definito $\phi : Aut(\mathbb{Z}_4 \times \mathbb{Z}_8) \to Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Dubbi in merito alla buona definizione di cui abbiamo parlato a lezione. Se sappiamo che $\sigma^n = id$ negli automorfismi, lo continua ad essere negli endomorfismi, che nell'immagine $\sigma'$ che nella riduzione modulo 2. (ripassa le proprietà delle riduzioni modulo p, in particolare quando ho gruppi di cardinalità multipla di un solo primo)

Se avessi $H \rtimes C$ con $C$ ciclico. Consideriamo due diversi omomorfismi $\tau$, tali che le immagini del generatore sono diverse ma di pari ordine. Sono allora isomorfi i due prodotti semidiretti? Un controesempio: $H = \mathbb{Z}_3 \rtimes \mathbb{Z}_7$, $C = \mathbb{Z}_2$. Nemmeno la diversità dell'ordine è sufficiente, si pensi alla prima domanda.
Il dubbio nasce nella classificazione di $G$ di cardinalità 66. Si era arrivati ad avere $G \cong \mathbb{Z}_{33} \to \mathbb{Z}_2$. In questo caso può essere utili calcolare i centri dei due gruppi. Se si ha un prodotto diretto, il centro è $G$; se l'azione è banale solo su $\mathbb{Z}_{10}$ uno è diretto, l'altro no e in questo caso il centro è solo isomorfo a $\mathbb{Z}_{11}$ (ne siamo certi in quanto l'altro elemento è $\mathcal{S}_3$); nel caso in cui agisca

banalmente sono su $\mathbb{Z}_{10}$, si ha $G \cong \mathcal{D}_{11} \times \mathbb{Z}_3$ e $Z(G) \cong \mathbb{Z}_3$; nell'ultimo caso si ha $G \cong \mathcal{D}_{33}$ di centro banale.

Chiarimenti su un esercizio. Si devono trovare gli automorfismi di un gruppo isomorfo a $\mathbb{Z}_q \rtimes \mathbb{Z}_p$ non banale. Gli automorfismi non banali sono $\varphi(q) = q - 1$, ma per un lemma fatto producono prodotti semidiretti tutti isomorfi fra loro. Ora $\mathbb{Z}_q$ è normale, dunque unico e dunque caratteristico, ovvero $\forall a \in \mathbb{Z}_q$ generatore, $\phi(a)$ può andare in un altro generatore, per un totale di $\varphi(q) = q - 1$ scelte. A priori ho $q(p-1)$ elementi di ordine p, quindi ho al più $q(p-1)$ scelte per un generatore, $b$, di $\mathbb{Z}_p$. Sono evidentemente troppe. Guardo come $b$ può agire su $a$: $bab^{-1} = a^m$ con $m$ di ordine $p$ in $\mathbb{Z}_q^*$, siccome la mappa o è banale o iniettività (semplicità di $\mathbb{Z}_p$), $m$ deve avere ordine moltiplicativo esattamente $p$. In generale $\phi(b) = b^h a^k$ con $(h, p) = 1$. Allora il coniugio diventa $\phi(bab^{-1}) = \phi(a)^m \Leftrightarrow b^h a^k a^i a^{-k} b^{-h} = b^h a^i b^{-h} \Leftrightarrow b^h a^i b^{-h} = a^{im^h}$ solo se $h$ è tale che $a^{im} = a^{im^h}$, siccome $i$, $m$ sono fissati. Questo vale se $im \equiv im^h\ (q) \Leftrightarrow m \equiv m^h\ (q) \Leftrightarrow (h, p) = 1$ in quanto $m$ ha ordine $p$. Allora

$$\begin{cases} \phi(b) = ba^k,\ k \in \mathbb{Z}_q \\ \phi(a) = a^i,\ (i, q) = 1 \end{cases}$$

Questo mi dice che $|Aut(G)| = (q-1) \cdot q$.
Allora $\mathbb{Z}_q$ agisce su $\mathbb{Z}_q \rtimes \mathbb{Z}_p$ mandando

$$[1]_q \mapsto \begin{cases} a \mapsto a \\ b \mapsto ba^x \end{cases}$$

che ha evidentemente ordine $q$; invece $\mathbb{Z}_p^*$ agisce in modo tale che

$$[1]_p \mapsto \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \end{cases}$$

Dunque vi sono due sottogruppi isomorfi a $\mathbb{Z}_q$ e a $\mathbb{Z}_p^*$, e anzi

$$Aut(\mathbb{Z}_q \rtimes \mathbb{Z}_p) \cong \mathbb{Z}_q \rtimes \mathbb{Z}_p^*$$

pensato con l'azione "naturale".

I p-Sylow in $\mathcal{S}_n$ con $n \geq p^3$. Vale che

- in $\mathcal{S}_p$, $H_0 \cong \mathbb{Z}_p$
- in $\mathcal{S}_{p^{i+1}}$, $H_i \cong H_i^p \rtimes \mathbb{Z}_p$

In $Aut(\mathbb{Z}_2^3)$, c'è un elemento di ordine 7, chi è? Infatti ha cardinalità $(2^3-2^2)(2^3-2)(2^3-1) = 4\cdot 6\cdot 7$. Tale elemento, possiamo vederlo come se fosse una matrice $A$ è tale che $A^7 = I$, questo è tale che $A^7 - I = A^6+A^5+\ldots+A+I = (A^3+A+I)(A^3+A^2+1) = 0$. Cerchiamo due matrici con quei polinomi caratteristici, il loro prodotto sarà la matrice cercata di ordine 7. La prima è

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Ci segnala il compitino dell'anno scorso. Avrà qualche differenza, più di *stile* che di contenuti. Vediamo il secondo esercizio. Chiede di determinare le coppie di interi positivi $(a,b)$ per cui $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^b}$ contiene un sottogruppo caratteristico di ordine $p$. Un caso gestibile è quando $a < b$ o viceversa, in quanto si considera $p^{b-1}G$. Viceversa se $a = b > 0$, ho molti elementi di ordine $p$, tipo $p^2-1$. Consideriamo un elemento di ordine p, sia $x$, allora $x = (p^{a-1}m', p^{a-1}n')$, con $m',\ n'$ non entrambi multipli di $p$, e il suo generato $< x >= \{\ (p^{a-1}m'c, p^{a-1}n'c) \mid c \in \mathbb{Z}\ \}$. Da qui si fanno un po' di casi. Un controesempio per $a = 2$, dato $x = (m', n')$ con $n' \neq 0$ la completo a base e (se uguale più facile, li scambio) definisco l'automorfismo indotto dalla matrice

$$\begin{pmatrix} m' & 0 \\ n' & 1 \end{pmatrix} \text{ invertibile}$$

che li scambia, dunque non sono caratteristici.
In generale se $x = (p^{a-1}m', p^{a-1}n')$ con $h,\ k$ non entrambi multipli, esisteranno $h,\ k$ tali che

$$det \begin{pmatrix} m' & 0 \\ n' & 1 \end{pmatrix} \neq 0\ (p)$$

ovvero invertibili. Una precisazione è da fare, qui non abbiamo più a che fare con uno spazio vettoriale, anche se vedendo i coefficienti modulo $p^a$ posso vedere che quelle invertibili sono quelle che lo erano già modulo p. Ora il determinante è invertibili modulo $p$. Quindi ora c'è un isomorfismo che mi manda la base canonica in quella che abbiamo costruito, ma allora li posso scambiare e non sono caratteristici.
Un ragionamento analogo poteva partire dalla considerazione che i sottogruppi di cardinalità $p$ sono esattamente $p+1$, fatti in un determinato modo, e osservando che vengono scambiati tutti (siamo sicuri? sì, basta distinguere per casi) dall'isomorfismo tale che

$$\begin{cases} (1,0) \mapsto (1,1) \\ (0,1) \mapsto (1,0) \end{cases}$$

Un modo alternativo è considerare il fatto che la mappa $Aut(\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^b}) \to GL_2(\mathbb{F}_2)$ è surgettiva. Ragioniamo su alcuni ordini e blablabla.

Chiarimenti sulla classificazione dei gruppi di ordine $p^2q$ nel caso in cui $p < q$.

Come sono fatti i $\mathcal{Q}_n$? Guarda su Wikipedia.

# Capitolo 10

# Venerdì 18 Novembre, parte 1

*Presentazione di $\mathcal{S}_n$ tramite un insieme di generatori dato da trasposizioni di elementi consecutivi e relazioni.*

**Esercizio 24** (Presentazione di $\mathcal{S}_n$)**.** Consideriamone due generatori, ad esempio $(1 \ \ldots n)$ e $(1\ 2)$. Tuttavia in questo caso le relazioni sono difficili da esprimere.

Altrimenti consideriamo tutte le trasposizioni $\sigma_i$ tali che $\sigma_i = (i\ i+1)$. Hanno ordine 1, commutano se $|i-j| > 1$ e $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$. Proviamo che bastano.

Sia $\Gamma_n =< s_1, \ldots, s_n \mid s_i^2 = id,\ (s_is_j)^2 = id \ se \ |i-j| > 1,\ (s_is_{i+1})^3 = id >$ una candidata presentazione.

Claim: $\Gamma_n \cong \mathcal{S}_n$. Mostriamolo per induzione.

Per $n = 2$ è banalmente vero.
Induttivamente, assumiamolo per $n$ e proviamolo per $n+1$. Sicuramente abbiamo un omomorfismo suriettivo, che preserva le relazioni $\Gamma_n \to \mathcal{S}_n$ in quanto basta mandare $s_i \mapsto \sigma_i$. Mi basta mostrare che $|\Gamma_n| \leq n!$

Ci serve un risultato preliminare

**Proposizione 11.** *$\mathcal{S}_n$ è generato da trasposizioni successive.*

*Dimostrazione.* Basta osservare che $\sigma_i, \ldots \sigma_n$ generano $\mathcal{S}_{n-1}$ è tutti i prodotti $\alpha\sigma_{n-1}$ al variare di $\alpha \in \mathcal{S}_{n-1}$. In quanto dato $\tau \in \mathcal{S}_n$ se lascia fisso $n$ allora appartiene a $\mathcal{S}_{n-1}$, altrimenti cerco di scriverlo come prodotto di cose. A meno di comporre con elementi di $\mathcal{S}_{n-1}$, $\tau(n) = n-1$ (si vede dai). Supponiamo di

comporlo con $\alpha$, allora $\sigma_{n-1}\alpha\tau(n) = n$ ovvero appartiene a $esse_{n-1}$ e dunque posso esprimerlo come generato di elementi di $\mathcal{S}_{n-1}$ e $\sigma_{n-1}$. □

Allora l'omomorfismo è davvero surgettivo. Resta da provare che $|\Gamma_n| \leq n!$

Osserviamo che dentro esiste un sottogruppo $\Gamma_{n+1}$ generato da $s_1, \ldots, s_n$ ed è quoziente di $\Gamma_n$. Infatti quando ho aggiunto quel generatore, ho aggiunto anche le relazioni che lo coinvolgono. Chiamiamolo $H$ ed è tale che $|H| < minugn!$ in quanto quoziente di $\Gamma_n \cong \mathcal{S}_n$ per ipotesi.

Per concludere, se dimostriamo che $[\Gamma_{n+1} : H] \leq n+1$, dunque $|\Gamma_{n+1} \leq (n+1)!$

Per dimostrarlo ci chiediamo chi sono le classi laterali di $H$ in $\Gamma_{n+1}$. Definiamo $H_n = H$, $H_{n-1} = s_nH$ e $H_{n-2} = s_{n-1}s_nH$ e così via fino a $H_0 = s_1s_2 \ldots s_nH$. Dico che $\{ H_0, \ldots, H_n \}$ sono <u>tutte</u> le classe laterali. Per mostrare che sono tutte basta mostrare che resto in quell'insieme se moltiplico a sinistra per elementi di $\Gamma_{n+1}$, ovvero che moltiplicare a sinistra per $s_i \in \Gamma_{i+1}$ (che tanto generano tutto) produce una permutazione degli indici.

Ora $s_iH_i = s_i(s_{i+1} \ldots s_nH) = H_{i-1}$ e $s_iH_{i+1} = H_i$. Se $j \neq i, i-1$, consideriamo due casi

- sia $j \geq i+1$, allora $s_i$commuta con tutti gli elementi prima di $H$ nella scrittura di $H_j$ e dunque $s_iH_j = s_i(s_{j+1} \ldots s_nH) = (s_{j+1} \ldots s_n)s_iH = s_{j+1} \ldots s_nH = H_j$;
- se $j \leq i-2$, $s_i$ commuta con tutti tranne che con $s_i$ e $s_{i-1}$, dunque ora $s_iH_j = s_i(s_{j+1} \ldots s_{i-1}s_i \ldots s_nH) = (s_{j+1} \ldots)s_is_{i-1}s_i(\ldots s_n)H = (s_{j+1} \ldots)s_{i+1}s_is_{i+1}(\ldots s_n)H$ e ora $s_{i+1}$ scavalca e dunque $= H_j$.

Che siano tutte disgiunte non ci interessa in quanto ci serviva mostrare che fossero al più $n_1$.

# Parte II

# Esercitazioni di Teoria dei Campi e di Galois

# Capitolo 11

# Venerdì 18 Novembre, parte 2

*Polinomio minimo di elementi algebrici su $\mathbb{Q}$. Irriducibilità di polinomi su $\mathbb{Q}$ e su $\mathbb{Q}[i]$.*

**Esercizio 25** (Polinomi irriducibili non separabili a coefficienti in $K$)**.** In un campo a caratteristica 0 non possiamo trovarlo. Dunque mettiamoci in un $K = \mathbb{F}_p(t)$ estensione algebrica finita e non banale di $\mathbb{F}_p$.

Osserviamo che $\mathbb{F}_p(t) = \mathbb{F}_p[t]$, come insieme.

Dato $f(x) = x^p - t \in K[x]$, questo polinomio sicuramente ha derivata nulla e in una qualche estensione ha una radice $\alpha$, dunque tale che $\alpha^p = t$. Possiamo chiederci che molteplicità abbia $\alpha$: consideriamo $x - \alpha$ e $(x-\alpha)^p = x^p - \alpha^p = x^p - t$ in quanto $\alpha$ era radice di $f(x)$, dunque $\alpha$ ha molteplicità $p$. Proviamo che è irriducibile. Lo è in quanto una qualsiasi potenza minore di $p$ di $x - \alpha$ è un polinomio a coefficienti nel campo che contiene $\alpha$:

$$(x-\alpha)^s = \sum_{i=0}^{s} \binom{s}{i} x^{s-i}\alpha^i = x^s + sx^{s-1}\underline{\alpha} + \sum_{i=2}^{s-1} \binom{s}{i} x^{s-i}\alpha^i + \alpha^s$$

Supponiamo $\alpha \in K = \mathbb{F}_p[t]$, allora $\alpha = \frac{a(t)}{b(t)}$ con $a, b \in \mathbb{F}_p[t]$. Ma questo implica $\alpha^p \neq t$, in quanto si avrebbe che $\alpha^p = \frac{a^p(t)}{b^p(t)}$, ovvero $b^p(t) \cdot \alpha^p = t \cdot a^p(t)$ assurdo in quanto il grado del polinomio a sinistra è multiplo di $p$, quello a destra no. Altrimenti detto "perché hanno differenza di gradi multipla di $p$, cosa che è invariante per rappresentazione come quozienti".

Ora ci chiediamo se l'estensione $\mathbb{K}[x]/(f(x))$, che sappiamo essere isomorfa a $K(\alpha)$ campo di spezzamento di $f(x)$, sia separabile. Ce lo chiederemo quando ne avremo la definizione.

**Esercizio 26** (Polinomi minimi)**.** Troviamo il p.m. di $\alpha$ su $\mathbb{Q}$ con $\alpha = \sqrt{2+i\sqrt{2}}$.

Osserviamo che facendo le potenze di $\alpha$ fino alla quarta troviamo che $g(x) = x^4 - 4x^2 + 6$ si annulla in $\alpha$, dunque appartiene all'ideale

$$I = \{\, f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0 \,\}$$

che sappiamo essere generato dal polinomio minimo di $\alpha$ (monico di grado minimo che si annulla in $\alpha$). Ci chiediamo se sia vero che $\alpha$ ha grado 4. Basta provare che è $g(x)$ irriducibile e che perciò genera $I$.

Per rispondere cerchiamone le radici. Sono $\alpha$, $-\alpha$ e $\pm\sqrt{2-i\sqrt{2}}$. Se $g$ fosse riducibile, sarebbe prodotto o di un polinomio di grado 3 e di uno grado 1, con il termine noto uguale a una delle radici di $g(x)$, o sarebbe uguale al prodotto di due polinomi di grado uguale a 2. Tuttavia il primo caso si esclude subito in quanto le sue radici non stanno in $\mathbb{Q}$, il secondo in quanto i polinomi $x-\alpha$, $x+\alpha$, $x-\sqrt{2-i\sqrt{2}}$ e $x+\sqrt{2-i\sqrt{2}}$ comunque vengano moltiplicati a 2 a 2 producono dei polinomi a coefficienti non in $\mathbb{Q}$.

Potevamo anche usare il criterio di Eisenstein, con 2.

**Esercizio 27.** Sia ora $\alpha = 1+\sqrt{3}$. Concludiamo osservando che si annulla in un polinomio di grado 2, grado minimale in quanto $\alpha \notin \mathbb{Q}$, e dunque è il polinomio minimo.

**Esercizio 28.** Sia ora $\alpha = \sqrt{2+\sqrt{3}}$.

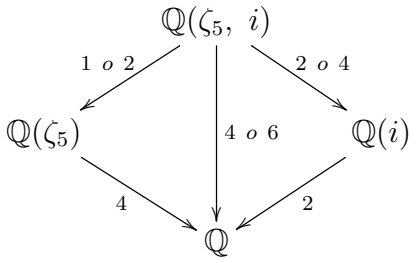
Come prima facendo le potenze, troviamo che si annulla in $g(x) = x^4 - 4x^2 + 1$, polinomio di radici $\pm\sqrt{2\pm\sqrt{3}}$. Ma se faccio il prodotto di coppie di queste quattro radici, questa volta trovo che fa 1. Tuttavia le loro somme danno problemi, in quanto se elevo al quadrato, trovo 6 che non è un quadrato di un elemento di $\mathbb{Q}$.

Altrimenti, ci chiediamo se $\alpha$ possa avere grado 2 su $\mathbb{Q}$. Supponiamo $\alpha$ abbia polinomio minimo di grado 2. Allora $\mathbb{Q}(\alpha)$ ha grado 2. Ma contiene anche $\mathbb{Q}(\sqrt{3})$, cioè $\alpha$ genera $\sqrt{3}$, ma $\frac{(i+\sqrt{3})}{\alpha} = \pm\sqrt{2}$ e dunque $\mathbb{Q}(\alpha)$ contiene anche $\mathbb{Q}(\sqrt{2})$. Ma ora abbiamo che $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2})$ e questo è assurdo in quanto non posso esprimere $\sqrt{3}$ come combinazione lineare di 1 e $\sqrt{2}$, base di $Q(\sqrt{2})$.

Dunque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

**Esercizio 29** (Radici primitive dell'unità)**.** Troviamo il polinomio minimo di $\zeta_5$, radice quinta primitiva dell'unità, su $\mathbb{Q}[i]$.

Osserviamo che si annulla in $\frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$, polinomio irriducibile su $\mathbb{Q}$, in quanto è irriducibile modulo 2. Ora vogliamo riuscire a concludere osservando il diagramma (i numerini sono i gradi)




Mostriamo $[\mathbb{Q}(\zeta_5,\ i) : \mathbb{Q}(\zeta_5)] = 1$.

Lo faremo la prossima lezione.

**Esercizio 30.** Proviamo che $f(x) = x^3 - 3x - 1$ è irriducibile in $\mathbb{Q}[x]$.

Basta osservare che lo è modulo 2.

Lo è anche in $\mathbb{Q}(i)[x]$? Consideriamo $\alpha$ una radice di $f$ e quindi di grado 3 su $\mathbb{Q}$, siccome $i$ ha grado 2, per averle entrambe dovrei avere un estensione di grado multiplo 6, in quanto $2 = [\mathbb{Q}(i) : \mathbb{Q}] \mid [\mathbb{Q}(i, \alpha) : \mathbb{Q}]$ e $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [\mathbb{Q}(i, \alpha) : \mathbb{Q}]$.

Osserviamo che $f$ ha almeno una radice reale, detto meglio o ne ha 3 o ne ha 1 e due complesse coniugate fra loro. Vediamo le due casistiche:

- se ha 3 radici reali $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, ma se è riducibile su $\mathbb{Q}(i)[x]$ allora lo è su $\mathbb{Q}(i)[x] \cap \mathbb{R}[x] = \mathbb{Q}[x]$ che è assurdo;
- se ne ha una reale e due complesse $f(x) = (x - \alpha)(x - \beta)(x - \overline{\beta})$, allora $(x - \alpha) = \frac{f(x)}{(x-\beta)(x-\overline{\beta})} \in \mathbb{Q}(i)[x] \cap \mathbb{R}[x] = \mathbb{Q}[x]$, cioè è riducibile su $\mathbb{Q}[x]$ che è assurdo.

Dunque $f(x)$ è irriducibile anche su $\mathbb{Q}(i)[x]$.

# Capitolo 12

# Mercoledì 23 Novembre

*Grado e isomorfismo di estensioni. Gruppo di Galois del campo di spezzamento di un polinomio di terzo grado. Esempi di gruppo di Galois del campo di spezzamento di un polinomio biquadratico.*

**Esercizio 31** (Radici primitive quinte)**.** Consideriamo $f(x) = x^4 + x^3 + x^2 + x + 1$.

Durante la lezione precedente avevamo detto che è irriducibile su $\mathbb{Q}$, in quanto bastava vederlo modulo 2 in quanto non ha radici mod 2. Infatti l'unico irriducibile di grado 2 su $\mathbb{Z}_2$ è $x^2 + x + 1$ e il suo quadrato è diverso da $f(x)$.

Come dire che è irriducibile su $\mathbb{Q}(i)$? Le sue radici le conosciamo, sono le radici quinte dell'unità: $\zeta_5^i$ per $i = 1, 2, 3, 4$. Sono complesse e a due a due coniugate: $\zeta_5^i = \overline{\zeta_5^{5-i}}$.

Posso scriverlo come prodotto di due polinomi a coefficienti in $\mathbb{Q}(i)$? Osserviamo che $f$ non ha radici in $\mathbb{Q}(i)$ in quanto $\mathbb{Q}(i)$ ha grado 2, mentre $\mathbb{Q}/(f(x))$ (che sappiamo essere isomorfo al cds di $f(x)$), ha grado 4 e non può essere contenuto in un campo di grado 2. Ma quindi se lo fattorizzo, cioè se $f(x)$ fosse riducibile su $\mathbb{Q}(i)$, lo sarebbe come prodotto di due polinomi irriducibili di grado 2 in $\mathbb{Q}(i)$.

Chiediamoci chi è il termine noto di questi polinomi. Sapendo che

$$f(x) = \prod_{i=1}^{4}(x - \zeta_5^i)$$

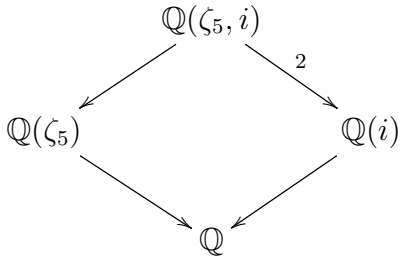
le costanti sono prodotti di due radici primitive dell'unità: $\zeta_5\zeta_5^2 = \zeta_5^3$ etc..., facendo un po' di conti vediamo che l'unico caso in cui i prodotti sono in $\mathbb{Q}(i)$

è accoppiando i coniugati. Allora $g$ avrà radici $\zeta_5^2$ e $\zeta_5^3$ e $h$ avrà le altre due:

$$f(x) = g(x)h(x) = (x^2 + (\zeta_5 + \zeta_5^4)x + 1)(x^2 + (\zeta_5^2 + \zeta_5^3)x + 1)$$

a coefficienti reali. Ma se esistono, allora stanno in $\mathbb{Q}(i) \cap \mathbb{R} = \mathbb{Q}$. Questo produce un assurdo. Dunque $f(x)$ è irriducibile su $\mathbb{Q}(i)$ e dunque $[\mathbb{Q}(i, \zeta_5) : \mathbb{Q}(i)] = 4$.

Un modo alternativo partiva dal considerare il diagramma:




Osserviamo che $\mathbb{Q}(\zeta_5)$ è un'estensione di Galois in quanto campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Chi è $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$? Deve scambiare le radici di $f$ fra loro, sappiamo avere cardinalità 4 (pari al grado) e sappiamo che possiede un elemento di ordine 4: dunque è isomorfo a $\mathbb{Z}_5^* \cong \mathbb{Z}_4$. Sia $\tau : \zeta_5^i \mapsto \zeta_5^{2i}$. Evidentemente $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) =< \tau >$.

Ragioniamo sul diagramma. Se il polinomio fosse riducibile in $\mathbb{Q}(i)$, riuscirei fattorizzare il polinomio in due polinomi di grado 2 non riducibili ulteriormente (per il motivo espresso prima) e dunque le radici avrebbero grado 2 su $\mathbb{Q}(\zeta_5, i)$: quindi avrei un estensione di grado 2 (in alto a destra). Tuttavia le sotto estensioni $\mathbb{Q}(\zeta_5)$ e $\mathbb{Q}(i)$ corrispondono (Corrispondenza di Galois) ai campi fissi di alcuni sottogruppi del gruppo di Galois. Tuttavia i sottogruppi (propri) di $Gal(K/\mathbb{Q})$ hanno ordine 2.

Se fosse riducibile, $\mathbb{Q}(i)$ sarebbe il sottocampo di $\mathbb{Q}(\zeta_5, i)$ fissato da un sottogruppo di ordine 2 del gruppo di Galois, ovvero da $< \tau^2 >$ dove $\tau^2 : \zeta_5^i \mapsto \zeta_5^{4i}$.

Sapendo che $\zeta_5 \mapsto \zeta_5^4$ e via di conseguenza gli altri, cerchiamo gli elementi fissati da $\tau^2$. Sono $\zeta_5^2 + \zeta_5^3$ o $\zeta_5 + \zeta_5^4$. Sia $H$ quello che fissa $\alpha = \zeta_5 + \zeta_5^4$, ma il suo polinomio minimo (fai i soliti calcoli elevando le cose al quadrato, alla quarta etc etc) e abbiamo che $\alpha^2 + \alpha = (\sum_{i=1}^{4} \zeta_5^i + 1) + 1$ cioè è radice di

$l(x) = x^2 + x - 1$. Ma allora $\alpha = \frac{-1 \pm \sqrt{5}}{2}$ e quindi $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$ di grado 2. Ma questa è un'estensione reale e dunque $\mathbb{Q}(i)$ non è un campo in cui possiamo spezzare $f(x)$.

**Esercizio 32** (Isomorfismi e uguaglianze fra campi)**.** $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})$?

Un isomorfismo fra campi deve mantenere fisso $\mathbb{Q}$, il campo fondamentale. Tuttavia osserviamo che nel primo 2 ha una radice quadrata, nel secondo no, mentre viceversa per 3. Dunque non sono isomorfi.

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Il contenimento $\supseteq$ è banale. Il viceversa si risolve con qualche calcolo in più.

Ora sia $\alpha = \sqrt{2} + \sqrt{3}$. Osserviamo che $\alpha^2 = 5 + 2\sqrt{6}$, cioè il polinomio minimo di $\alpha$ su $\mathbb{Q}$ non può avere grado 2, ma 4 e quindi $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\alpha)] = 1$.

Mostriamo che

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{ \tau, \tau\sigma, \sigma, id \} \cong \mathbb{Z}_2^2$$

dove $\tau : \sqrt{2} \mapsto -\sqrt{2}$ e $\sigma : \sqrt{3} \mapsto -\sqrt{3}$ e lasciano fisso il resto.

Infatti fra questa estensione e $\mathbb{Q}$ abbiamo (fai diagramma a tre elementi in mezzo):

- $\mathbb{Q}(\sqrt{2})$ di grado 2: è fissato da $< \sigma >$;
- $\mathbb{Q}(\sqrt{3})$ di grado 2: è fissato da $< \tau >$;
- $\mathbb{Q}(\sqrt{6})$ di grado 2: è fissato da $\tau\sigma$; (controlla!)

ovvero ci sono tre sottogruppi di indice 2 nel gruppo di Galois.

Dunque $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2^2$.

**Esercizio 33** (Polinomi di grado 3)**.** Consideriamo $p(x) = x^3 + ax^2 + bx + c$ irriducibile (e dunque senza radici) su $\mathbb{Q}$. Studiamo il gruppo di Galois del suo campo di spezzamento $K$.

Studiamo inizialmente $K$. Mostriamo che può avere grado 3 o 6:

- 3 se una radice è sufficiente a generare tutto $K$;
- 6 se oltre a una radice di grado 3, ho bisogno anche di un'altra radice.

Sicuramente può essere visto come un sottogruppo di $\mathcal{S}_3$, in quanto gli elementi del gruppo di Galois sono automorfismo che permutano le radici di $f(x)$, tante quante il grado di $f(x)$. Allora se ha grado 3, $Gal(K/\mathbb{Q}) \cong \mathbb{Z}_3$, invece se ha grado 6 è proprio $\mathcal{S}_3$. Questo secondo caso avviene quando abbiamo due

radici complesse coniugate, in quanto un elemento di ordine 2 può essere il coniugio.

Denotiamo le tre radici di $p(x)$, $\alpha$, $\beta$, $\gamma$. Sia $\delta = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$. Sta in $K$. Prendiamone il quadrato $\delta^2 = \Delta$.

Osserviamo che se permutiamo le radici, ovvero agiamo su $\delta$ con un automorfismo del gruppo di Galois, allora $\delta \mapsto \pm\delta$ e dunque $\Delta$ è fissato. Quindi sta nel campo fisso di $Gal(K/\mathbb{Q})$, cioè $\Delta \in \mathbb{Q}$.

Ora scriviamo $p(x)$, a meno di traslazione di $x$, come $f(x) = x^3 + ax + b$ con $a, b$ diversi da prima (sostanzialmente sto dicendo che la somma delle radici può essere 0).

Allora $\Delta$ è scrivibile in termini dei coefficienti nuovi $a$ e $b$: $\Delta = -4a^3 - 27b^2$ (basta porre che $b = prodotto$ e $\alpha = somma$ e si fa il conto).

A questo punto se permuto ciclicamente tutte e tre le radici $\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$, abbiamo che $\delta \mapsto \delta$, mentre se ne scambio solo due, $\delta \mapsto -\delta$. In sostanza, $\delta$ è un indicatore della parità/disparità della permutazione con cui sta agendo sull'insieme delle radici e sappiamo che $\delta$ viene fissato da $A_3$.

Ci chiediamo ora se $\Delta$ sia un quadrato ($\square$) in $\mathbb{Q}$, ovvero se esista $q \in \mathbb{Q}$ tale che $q^2 = \Delta$. Se è negativo evidentemente no, né in $\mathbb{Q}$ né in $R$, se è positivo lo è sicuramente in $R$ e in $\mathbb{Q}$ non sempre. Se non lo è su $\mathbb{Q}$, allora possiamo considerare la sotto estensione $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\delta) \subseteq K$.

Se $\Delta\square$ su $\mathbb{Q}$, allora $\delta \in \mathbb{Q}$. Ma questo implica che non ci sono permutazioni dispari nel gruppo di Galois, in quanto manderebbero $\delta \mapsto -\delta$. A questo punto $Gal(K/\mathbb{Q}) \cong A_3 \cong \mathbb{Z}_3$.

Se invece $\Delta$ non è quadrato, allora $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$, e allora per torri di estensione $[K : \mathbb{Q}] = 6$ e quindi $Gal(K/\mathbb{Q}) \cong \mathcal{S}_3$.

In conclusione, se $\sqrt{\Delta} \in \mathbb{Q}$, allora $Gal(K/\mathbb{Q}) \cong \mathbb{Z}_3$, altrimenti a $\mathcal{S}_3$.

Possiamo ricavare delle informazione anche studiando il grafico di $f(x) = x^3 + ax + b$. Ha derivata $f'(x) = 3x^2 + a$ che si annulla in $x_{1,2} = \pm\sqrt{-\frac{a}{3}}$. Ora se $f(x_1)f(x_2) > 0$, allora ho solo una radice reale; se sono discordi, ne ho tre reali.

Il conto da svolgere è $f(x_1)f(x_2) = (roba)(roba_2) = b^2 + roba\ al\ quadrato = b^2 + \frac{4}{27}a^3$.

**Esercizio 34** (Polinomi di grado 4)**.** Consideriamo $f(x) = x^4 - 6x^2 + 25$.

Sappiamo che $Gal(K/\mathbb{Q}) \subseteq \mathcal{S}_4$ (o insomma si immerge iniettivamente).

Poniamo $y = x^2$ e troviamo le radici di $g(y) = y^2 - 6y + 25$, ovvero $y_{1,2} = 3 \pm 4i$. Dunque il suo campo di spezzamento è $\mathbb{Q}(i)$, di grado 2 su $\mathbb{Q}$.

Ora consideriamo l'estensione $K \supseteq \mathbb{Q}(i) \supseteq \mathbb{Q}$ dove in $\mathbb{Q}(i)$ il polinomio si spezza in $(x^2 - 3 - 4i)(x^2 - 3 + 4i)$.

Vediamo se $3 + 4i$ è $\square$ in $\mathbb{Q}(i)$ e se $3 - 4i$ in $\mathbb{Q}(i, \sqrt{3 + 4i})$. Mostriamo che presa l'estensione $\mathbb{Q}(i, \sqrt{3 + 4i}) \supseteq \mathbb{Q}(i)$ non ho bisogno di aggiungere altro.

Se $3 + 4i$ è $\square$, lo è anche il suo coniugato $3 - 4i$. Viceversa, se non lo è non lo è nemmeno il coniugato, infatti sapendo che il prodotto dei due lo è a prescindere, infatti $\alpha\overline{\alpha} = |\alpha|^2$, ci ricaviamo $\overline{\alpha} = \frac{\alpha\overline{\alpha}}{\alpha}$.

Allora mi conviene considerare le estensioni $\mathbb{Q}(i, \sqrt{25}) \supseteq \mathbb{Q}(i)$ e allungo con $\mathbb{Q}(i, \sqrt{25}, \sqrt{\alpha}) \supseteq \mathbb{Q}(i, \sqrt{25}) \supseteq \mathbb{Q}(i)$ prodotte dalle seguenti domande:

- $\Delta$ è quadrato su $\mathbb{Q}$?

  In questo caso no, quindi aggiungo $i$.

- il termine noto è un quadrato in $\mathbb{Q}(i)$? O $\mathbb{Q}$?

  In questo caso sì, quindi $[\mathbb{Q}(i, \sqrt{25}) : \mathbb{Q}(i)] = 1$.

- $\alpha$ è un quadrato in $\mathbb{Q}(i, \sqrt{t.noto})$?

  In questo caso facciamolo mettendo a sistema....otteniamo

$$\begin{cases} y = \frac{2}{x} \\ x^2 = 4 \quad x = \pm 2 \end{cases} \qquad \textit{oppure} \quad \begin{cases} y = \frac{2}{x} \\ x = -1 \ NO \end{cases}$$

  e allora $(2 + i)^2 = \alpha$ e dunque $[K : \mathbb{Q}(i, \sqrt{25})] = 1$

Allora $[K : \mathbb{Q}] = [K : \mathbb{Q}(i, \sqrt{25})] \cdot [\mathbb{Q}(i, \sqrt{25}) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2$.

In generale chi è $Gal(K/\mathbb{Q})$ con $K$ cds di un polinomio di grado 4? Ha al più ordine 8 perché prodotto di tre estensioni di al più grado 2, quindi è contenuto in un 2-Sylow di $\mathcal{S}_4$, cioè $\mathcal{D}_4$.

Un esempio in cui è $\mathbb{Z}_2$ l'abbiamo trovato ora.

Anche $\mathcal{D}_4$ l'abbiamo già visto con Gaiffi.

Sia $f(x) = x^4 + 1 = \frac{x^8 - 1}{(x-1)(x^3 + x^2 + x + 1)}$, ha come radici le radici ottave primitive dell'unità.

Qui $\Delta = -4$, estendiamo con $i$ e lo spezziamo in $(x^2 + i)(x^2 - i)$ con radici $\alpha_1$, $\alpha_3$ e il secondo $\alpha_2$,$\alpha_4$. Il termine noto è un quadrato. Per aggiungere le

radici dei due polinomi ci serve $\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i$, ovvero $\sqrt{2}$. E abbiamo grado 4. e in questo caso $Gal(K/\mathbb{Q}) \cong \mathbb{Z}_2^2$ in quanto possiamo scambiare solo le due radici fra loro e il proprio opposto, in quanto se lascio fissi i coefficienti anche le radici dei polinomi spezzati devono a due a due restare fissi.

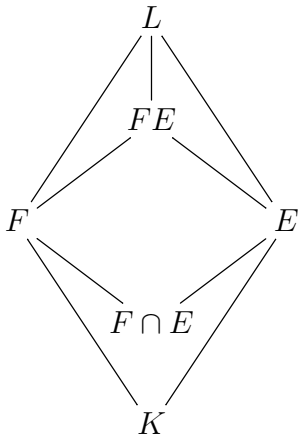
Lo vediamo meglio nella prossima esercitazione.

# Capitolo 13

# Martedì 29 Novembre

*Confronto di un'estensione di Galois con una seconda estensione. Gruppo di Galois della composizione di due estensioni di Galois. Esercizi dalle dispense sul gruppo di Galois di un campo di spezzamento (composizione tra l'estensione ciclotomica con lo radici ottave e una generica estensione quadratica). Gruppo di Galois di un polinomio di grado primo con due sole radici non reali. Gruppo di Galois di un polinomio biquadratico. Irriducibilità del p-esimo polinomio ciclotomico per p primo.*

**Esercizio 35** (Confronti fra estensioni)**.** Dato un campo $K$, una sua generica estensione $F$ e una di Galois $E$, consideriamo un campo $L$ tale che $L \supset E, F$:




In quanto di Galois, $E$ è campo di spezzamento di un polinomio $p(x) \in K[x]$, ma allora lo è anche con i coefficienti in $(F \cap E)[x]$ dunque anche $E/(F \cap E)$ è di Galois. Se ora consideriamo il campo contenente $F$ e le radici di $p(x)$, allora questo diventa il più piccolo campo contenente $F$ e anche $E$, che in

quanto cds è generato dalle radici di tale polinomio: dunque abbiamo che $FE$, che per definizione è il più piccolo campo contenente i due, è un'estensione di Galois su $F$, in quanto cds di $p(x) \in F[x]$.

Proviamo che $Gal(FE/F) \cong Gal(E/(E \cap F))$. Proviamo che

$$\Phi : Gal(FE/F) \to Gal(E/(E \cap F))$$

è un isomorfismo. Sia $\phi \in Ker(\Phi)$, allora $\phi|_E = Id_E$, ma siccome fissa già anche $F$, abbiamo che $\phi = Id_{EF}$, dunque è iniettiva.

Ma se scriviamo, per teorema dell'elemento primitivo, $E$ e $FE$ come estensioni semplici, $\exists \alpha \in E$ tale che

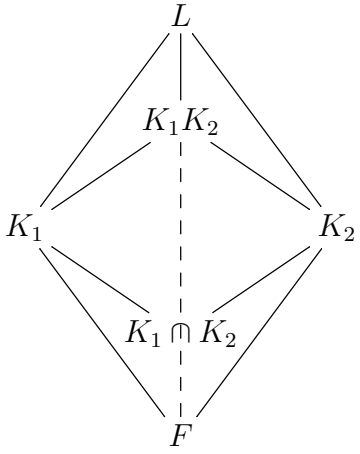
- $E = (E \cap F)(\alpha)$
- $EF = F(\alpha)$

e il modo in cui agisce $\phi$ è ancora più esplicito, in quanto fissa $\alpha \in E$.

É surgettiva in quanto $\forall \phi \in Gal(E/(E \cap F))$ posso sempre considerare la sua estensione che lascia fisso tutto $F$ e dunque $\tilde{\phi} \in Gal(EF/F)$. Dunque sono isomorfi.

**Esercizio 36** (Gruppo di Galois della composizione di due estensioni di Galois)**.** *Questo esercizio è molto poco chiaro, da rivedere*

Ora siano $F$ un campo, $K_1$ e $K_2$ due sue estensioni di Galois. Vogliamo provare che $K_1K_2$ su $F$ è ancora di Galois (quella tratteggiata). Consideriamo il diagramma




Consideriamo l'omomorfismo $\Phi : Gal(K_1K_2/F) \to Gal(K_1/F) \times Gal(K_2/F)$. Proviamo che è un isomorfismo.

Sia $\phi \in Ker(\Phi)$. Allora agisce banalmente sia su $K_1$ che su $K_2$, ma allora anche su tutto $K_1K_2$, cioè $\phi = Id_{K_1K_2}$. Tuttavia è un isomorfismo solo se $K_1 \cap K_2 = F$, in quanto se fosse altrimenti, vi sarebbero automorfismi di $Gal(K_1/F) \times Gal(K_2/F)$ che lasciano fissi elementi fuori da $F$.

Possiamo concludere ugualmente che $K_1K_2/F$ è di Galois:

1. osservando che se $K_1$ è un cds di un polinomio $p_1(x)$ su $F$ e $K_2$ lo è di un $p_2$ sempre su $F$, allora $K_1K_2$ è cds di $p_1p_2$ su $F$, in quanto tale polinomio è ancora separabile;
2. se $K_1/F$ è di Galois, allora $Gal(K_1/F) \lhd Gal(K_1K_2/F)$ e dunque è ben definito il gruppo quoziente

   $$Gal(K_1K_2/F)/Gal(K_1/F) \cong Aut(K_1K_2/K_1) \cong Aut(K_2/(K_1 \cap K_2))$$

   sia per corrispondenza di Galois che per quanto osservato nell'esercizio precedente. Se vale l'ipotesi $K_1 \cap K_2 = F$, allora è anche isomorfo (anzi uguale) a $Aut(K_2/F)$.

**Osservazione 4.** Possiamo concludere che se $p_1$ e $p_2$ sono separabili su $F$, allora lo è anche il loro prodotto? Ci serve che $K_1 \cap K_2 = F$.

Supponiamo che $p_1p_2(x)$ non sia separabile su $F$, allora ha un fattore non separabile, ma di conseguenza tale fattore o divide $p_1$ o $p_2$ per ipotesi aggiuntiva, ma in quanto separabili ho un assurdo.

**Esercizio 37** (Gruppo di Galois di un campo di spezzamento (composizione tra l'estensione ciclotomica con lo radici ottave e una generica estensione quadratica))**.** Al variare di $m \in \mathbb{Z}$, calcoliamo il gruppo di Galois del campo di spezzamento $E$ del polinomio $p(x) = (x^4 + 1)(x^2 - m)$ su $\mathbb{Q}$.

Per prima cosa calcoliamo il gruppo di Galois del primo fattore $(x^4 + 1)$. Ha come radici le potenze della radice ottave dell'unità con esponente coprimo con 8, cioè dispari. Possiamo anche vederlo come polinomio ottenuto da

$$\frac{x^8 - 1}{x^4 - 1}$$

e dunque è evidente quali radici perdo.

Sarebbe interessante disegnare l'ottagono e il quadrato prodotti dai due polinomi e vedere quali vertici restano fuori.

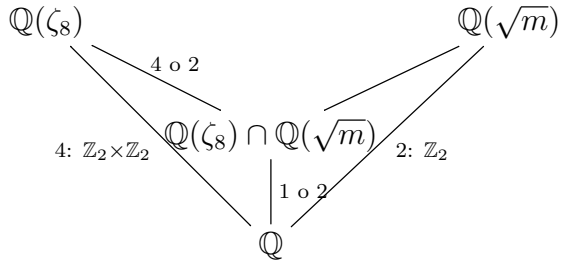
A questo punto le immagini di una radice ottava possono essere tutte le altre con esponente coprimo, dunque $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \mathbb{Z}_8^* \cong \mathbb{Z}_2^2$ e si possono esibire:

- banalmente l'identità;

- per $i = 3, 5, 7$ abbiamo $\phi_i : \zeta_8 \mapsto \zeta_8^i$ che ha ordine 2 per ogni scelta di $i$.

Se $m$ è un quadrato in $\mathbb{Q}$, allora il campo di spezzamento del polinomio $p$ è quello di $x^4 + 1$, che abbiamo appena trovato.

Viceversa, se $m$ non è un quadrato su $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$ abbiamo questa situazione:




Se $[\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 1$, allora $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) = \mathbb{Q}$ e dunque posso applicare quanto visto nell'esercizio precedente.
Se invece $[\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$, allora $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m})$ è una sotto estensione di $\mathbb{Q}(\zeta_8)$ di ordine 2, dunque per il teorema di corrispondenza di Galois possiamo trovarlo cercando i campi fissi dei sottogruppi di indice 2 di $G = Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$.

I sottogruppi di indice 2 in $G$ sono i sottogruppi di ordine 2 e dunque sono tutti e soli i generati degli elementi di ordine 2 che sappiamo essere:

$$\phi_3 : \begin{cases} \zeta_8 \mapsto \zeta_8^3 \\ \zeta_8^3 \mapsto \zeta_8 \\ \zeta_8^5 \mapsto \zeta_8^7 \\ \zeta_8^7 \mapsto \zeta_8^5 \end{cases} , \ \phi_5 : \begin{cases} \zeta_8 \mapsto \zeta_8^5 \\ \zeta_8^3 \mapsto \zeta_8^7 \\ \zeta_8^5 \mapsto \zeta_8 \\ \zeta_8^7 \mapsto \zeta_8^3 \end{cases} , \ \phi_7 : \begin{cases} \zeta_8 \mapsto \zeta_8^7 \\ \zeta_8^3 \mapsto \zeta_8^5 \\ \zeta_8^5 \mapsto \zeta_8^3 \\ \zeta_8^7 \mapsto \zeta_8 \end{cases}$$

Elenchiamo i campi fissi:

- $Fix(< \phi_3 >) = \mathbb{Q}(\zeta_8 + \zeta_8^3, \zeta_8^5 + \zeta_8^7) = \mathbb{Q}(\sqrt{-2}, -\sqrt{-2}) = \mathbb{Q}(\sqrt{-2})$;
- $Fix(< \phi_7 >) = \mathbb{Q}(\zeta_8 + \zeta_8^7, \zeta_8^3 + \zeta_8^5) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$;
- $Fix(< \phi_5 >) = \mathbb{Q}(\zeta_8 + \zeta_8^5, \zeta_8^3 + \zeta_8^7) = \mathbb{Q}$ ma vediamo che questo non ci dà informazioni. Tuttavia osserviamo che anche il loro prodotto resta fisso, cioè $Fix(< \phi_5 >) = \mathbb{Q}(\zeta_8\zeta_8^5, \zeta_8^3\zeta_8^7) = \mathbb{Q}(-i) = \mathbb{Q}(i)$.

Ciò vuol dire che $m$ è quadrato in uno di questi tre sottocampi di $\mathbb{Q}(\zeta_8)$, pur non essendolo su $\mathbb{Q}$.

Allora gli $m$ per cui è vero questo secondo caso sono 2, $-2$ e $-1$.

Ricapitolando abbiamo questi tre casi:

- $m$ è quadrato in $\mathbb{Q}$: $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2^2$;
- $m$ non è quadrato in $\mathbb{Q}$, ma lo è in $\mathbb{Q}(\zeta_8)$, ovvero $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m})$: allora $Gal(E/\mathbb{Q}) = \mathbb{Z}_2^2$;
- $m$ non è un quadrato in $\mathbb{Q}$, né in $\mathbb{Q}(\zeta_8)$, cioè $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) = \mathbb{Q}$: allora $Gal(E/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \times Gal(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \cong \mathbb{Z}_2^3$.

**Esercizio 38** (Gruppo di Galois di un polinomio di grado primo con due sole radici non reali)**.** Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile su $\mathbb{Q}$ di grado $p$ primo.

Supponiamo che $f$ abbia esattamente due radici non reali e denotiamo con $E$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Proviamo che $Gal(E/\mathbb{Q}) \cong \mathcal{S}_p$.

Un'inclusione è ovvia, in quanto gli elementi di $Gal(E/\mathbb{Q})$ inducono permutazioni delle $p$ radici di $f(x)$.

Ora vediamo che $\forall \alpha \in E$ radice di $f(x)$, $\mathbb{Q}(\alpha) \subset E$ e dunque per torri di estensione, $p \mid |Gal(E/\mathbb{Q})|$. Questo implica che c'è un elemento di ordine $p$ nel gruppo di Galois, ovvero un $p$-ciclo. Inoltre contiene anche il coniugio, in quanto scambia fra loro le due radici non reali, che sono coniugate in quanto il polinomio è a coefficiente reali (razionali).

Ma allora in quanto $p$ è primo, tali elementi ti bastano per generare tutte le trasposizioni e di conseguenza tutto $\mathcal{S}_p$. Dunque abbiamo l'inclusione opposta e l'uguaglianza.

**Esercizio 39** (Gruppo di Galois di un polinomio biquadratico)**.** Sia $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ e $E$ il suo campo di spezzamento.

Per quanto detto la scorsa lezione $Gal(E/\mathbb{Q})$ ha al più cardinalità 8, cioè si immerge in $\mathcal{D}_4$.

Consideriamo $y = x^2$ e $g(y) = y^2 + ay + b$. Ha radici $\omega_{1,2} = \frac{-a \pm \sqrt{\Delta}}{2}$ con $\Delta = a^2 - 4b$.

Se $\Delta$ è un quadrato in $\mathbb{Q}$ allora il polinomio è riducibile in due polinomi di grado 2. In questo caso si avrebbe che il campo di spezzamento è il prodotto dei campi di spezzamento dei due polinomi. Se i due polinomi sono entrambi irriducibili e blabla ne esce al più uno $\mathbb{Z}_2^2$. Lo abbiamo già visto.

Supponiamo allora che $\Delta$ non sia un quadrato. Abbiamo la prima estensioncina $\mathbb{Q}(\sqrt{\Delta})$ su $\mathbb{Q}$. In questa estensione possiamo fattorizzare $f(x) = (x^2 - \omega_1)(x^2 - \omega_2)$, dove $\omega_1\omega_2 = b$. Vorremmo fattorizzarlo completamente.

Se $b$ è un quadrato in $\mathbb{Q}(\sqrt{\Delta}) - \mathbb{Q}$, allora $\sqrt{\omega_1\omega_2} = \sqrt{b} \in \mathbb{Q}(\sqrt{\Delta})$, allora in $\mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ posso fattorizzarlo completamente. In questo caso non ho restrizioni sulle immagini di $\sqrt{\omega_1}$ e $\sqrt{\omega_2}$. Osserviamo che questa libertà mi permette di definire un automorfismo di ordine 4:

$$\tau : \begin{cases} \sqrt{\omega_1} \mapsto \sqrt{\omega_2} \\ \sqrt{\omega_2} \mapsto -\sqrt{\omega_1} \end{cases}$$

Dunque sapendo che $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{b})] \cdot [\mathbb{Q}(\sqrt{b}) : \mathbb{Q}(\sqrt{\Delta})] \cdot [\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2 \cdot 1 \cdot 2 = 4$, allora $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_4$.

Se $b$ è un quadrato in $\mathbb{Q}$, allora oltre a quanto già detto vale anche che il prodotto delle due radici deve essere tenuto fisso da ogni elemento di $Gal(E/\mathbb{Q})$ e dunque la scelta dell'immagine di una radice, determina univocamente l'altra. Allora per determinare univocamente un automorfismo del gruppo di Galois cercato mi basta definire l'immagine di $\sqrt{\Delta}$ e di $\sqrt{\omega_1}$. Questo mi produce uno $\mathbb{Z}_2^2$.

Se invece $b$ non è $\square$ in $\mathbb{Q}(\sqrt{\Delta})$, abbiamo che $E = \mathbb{Q}(\sqrt{\Delta}, \sqrt{b}, \sqrt{\omega_1}) = \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}, \sqrt{\omega_2})$ e ha grado 8 su $\mathbb{Q}$. Dunque $Gal(E/\mathbb{Q})$ ha cardinalità 8 e dunque è isomorfo a $\mathcal{D}_4$. Esibiamo esplicitamente l'isomorfismo. Consideriamo gli elementi di $Gal(E/\mathbb{Q})$:

$$\rho : \begin{cases} \sqrt{\omega_1} \mapsto \sqrt{\omega_2} \\ \sqrt{\omega_2} \mapsto -\sqrt{\omega_1} \\ \sqrt{\Delta} \mapsto \sqrt{\Delta} \end{cases} \quad , \; \sigma : \begin{cases} \sqrt{\omega_1} \mapsto -\sqrt{\omega_1} \\ \sqrt{\omega_2} \mapsto \sqrt{\omega_2} \\ \sqrt{\Delta} \mapsto -\sqrt{\Delta} \end{cases}$$

É evidente che $\rho$ ha ordine 4 e $\sigma$ ha ordine 2, inoltre verificano la regola di commutatività del diedrale $\sigma\rho\sigma^{-1} = \rho^{-1}$.

**Esercizio 40** (Irriducibilità del $p$-esimo polinomio ciclotomico per $p$ primo.)**.** Mi sa che ha solo proposto il seguente esercizio: data una radice quinta primitiva dell'unità, $\zeta_5$, calcolare $[\mathbb{Q}(\zeta_5, \sqrt{n}) : \mathbb{Q}]$ al variare di $n \in \mathbb{Z}$.

Fatto: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

# Capitolo 14

# Venerdì 2 Dicembre

*Intersezione di un'estensione ciclotomica e di un'estensione quadratica: esempi con radici quinte e settime. Sotto-estensioni di un'estensione ciclotomica: esempio con le radici settime dell'unità. Esempio di un'estensione di $\mathbb{Q}$ con gruppo di Galois $\mathbb{Z}_8$, esempio con gruppo $\mathcal{Q}_8$. Esercizio sui gruppi di Galois, da un compitino degli anni precedenti.*

**Esercizio 41.** Ci chiediamo quando $\sqrt{n} \in \mathbb{Q}(\zeta_5)$ al variare di $n \in \mathbb{Z}$.

Ciò equivale a chiedersi per quali $n \in \mathbb{Z}$, tale $n$ sia un quadrato in $\mathbb{Q}(\zeta_5)$. Supponiamo non lo sia su $\mathbb{Q}$, allora $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = 2$.

Sappiamo che $Gal(Q(\zeta_5)/Q) \cong \mathbb{Z}_4$, il gruppo moltiplicativo degli invertibili di $\mathbb{Z}_5$. I suoi sottogruppi di indice 2 fissano sottocampi di grado 2, dunque cerchiamo $H \cong \mathbb{Z}_2$ tale che $Fix(H) = \mathbb{Q}(\sqrt{n})$. $Fix(H)$ è un'estensione di Galois perché $H$ è un sottogruppo di un gruppo abeliano, dunque normale. Inoltre sappiamo che è unico ed è dunque unica la sotto estensione di grado 2.

Chi è esplicitamente $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$? É generato da $\tau : \zeta_5 \mapsto \zeta_5^2$.

Dunque il suo quadrato genera l'unico sottogruppo di ordine 2, $H$ ed è $\tau^2 : \zeta_5 \mapsto \zeta_5^4 = \zeta_5^{-1}$.

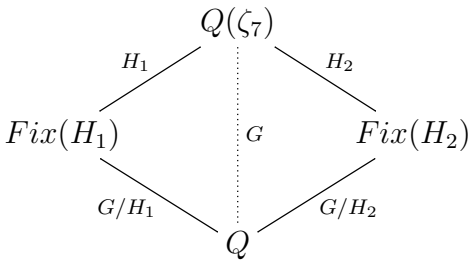
Il sottocampo fissato ha sicuramente grado 2. Osserviamo che contiene $\zeta_5 + \tau^2(\zeta_5) = \zeta_5 + \zeta_5^{-1}$, di grado 2 in quanto annulla il polinomio irriducibile $p(x) = x^2 + x - 1$ e dunque genera una estensione di grado 2 dentro $Fix(H)$. Dunque $Q(\alpha) = Fix(H)$. Esplicitamente $\alpha = \frac{-1 \pm \sqrt{5}}{2}$, quindi $Fix(H) = \mathbb{Q}(\sqrt{5})$.

Ma ora $\sqrt{n} \in \mathbb{Q}(\zeta_5) \Leftrightarrow n$ è un quadrato in $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$, ovvero se $n = (a + b\sqrt{5})^2$ con $a, b \in \mathbb{Q}$. Ovvero $n = a^2 + 5b^2 + 2ab\sqrt{5} \in \mathbb{Q}$, cioè se $5n$ è quadrato in $\mathbb{Q}$.

**Esercizio 42.** Facciamo la stessa cosa in $\mathbb{Q}(\zeta_7)$.

Cerchiamo le sotto estensioni di questo campo. Sappiamo che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ e $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6$, ciclico, dunque abeliano e tale che per ogni $d$ tale che $d \mid 6$ esiste un'unica sotto estensione di Galois di grado $d$ in $\mathbb{Q}(\zeta_7)$.

Individuiamo i sottogruppi isomorfi a $\mathbb{Z}_3$, che chiamiamo $H_1$, e a $\mathbb{Z}_2$, $H_2$, che dunque avranno i seguenti campi fissi: $Fix(H_1)$ tale che $[Fix(H_1) : \mathbb{Q}] = 2$ e $Fix(H_2)$ tale che $[Fix(H_2) : \mathbb{Q}] = 3$. Abbiamo già detto che sono estensioni normali, per abelianità. Inoltre avranno gruppo di Galois isomorfi ai quozienti di $G$ per il sottogruppo di automorfismi che li lasciano fissi.




Un generatori di $G$ è $\tau : \zeta_7 \mapsto \zeta_7^3$.

Allora $H_1 =< \tau^2 >$ e fissa $\alpha = \zeta_7 + \tau^2(\zeta_7) + \tau^4(\zeta_7)$. Dunque $Fix(H_1) \supset \mathbb{Q}(\alpha)$. Cerchiamone il polinomio minimo: vediamo che $\alpha^2 + \alpha + 2 = 0$ e dunque $p(x) = x^2 + x + 2$, di grado 2, dunque abbiamo l'inclusione opposta e l'uguaglianza. Osserviamo che è il campo di spezzamento di $p(x)$, cioè $Fix(H_1) = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(i\sqrt{7})$.

Per il ragionamento fatto prima, $\sqrt{n} \in Q(\zeta_7)$ è un quadrato quando $n$ o $-7n$ è un quadrato in $\mathbb{Q}$.

Sia ora $H_2 =< \tau^3 >$ e cerchiamo $Fix(< \tau^3 >)$. Sappiamo che $\tau^3 : \zeta_7 \mapsto \zeta_7^{-1}$ quindi $Fix(H) \ni \zeta_7 + \zeta_7^{-1} = \beta$. O $\beta \in Q$, o $\beta$ genera tale estensione, in quanto non vi sono estensione intermedie. Allora basta trovare il polinomio minimo di $\beta$ come prima.

Ragioniamo ora in modo diverso: potremmo cercare un polinomio che annulla $\zeta_7$ di grado $\leq 2$ e coefficienti in $Q(\beta)$, ovvero l'estensione che sta "sopra" quella generata da $\beta$.

Vorremmo dimostrare che $[Q(\beta) : Q] = 3$, ma stavolta lo facciamo mostrando che l'estensione sopra ha grado $\leq 2$. Osserviamo che $\zeta_7 - \beta + \zeta_7^{-1} = 0$, ovvero (moltiplicando per $\zeta_7$) $\zeta_7^2 - \zeta_7\beta + 1 = 0$, polinomio in $Q(\beta)$ che annulla $\zeta_7$, di grado voluto.

**Esercizio 43** (Esempio di un campo il cui gruppo di Galois é $\mathbb{Z}_8$)**.** Ricordiamo che è più comodo lavorare con radici dell'unità in quanto campi ciclotomici hanno gruppi di Galois abeliani, i cui sottogruppi sono normali e ciò ci permette subito di individuare sotto estensioni normali.

Osserviamo che $\zeta_{17}$ può andare bene, in quanto ha gruppo di Galois $G \cong \mathbb{Z}_{17}^* \cong \mathbb{Z}_{16}$: dunque basta trovare un suo elemento di ordine 2, che genererà l'unico sottogruppo di indice 8 in $\mathbb{Z}_{16}$, e cercare un elemento da lui fissato che starà nell'unico campo di grado 8 su $\mathbb{Q}$ contenuto in $\mathbb{Q}(\zeta_{17})$.

Dato $\tau \in G$ di ordine 16 e dunque generatore di $G$, sia $K =< \tau^8 >$ di ordine 2 e $K = Fix(H)$, sappiamo che il suo gruppo di Galois è $\cong G/H \cong \mathbb{Z}_8$.

Il generatore di $H$ è $\tau^8 : \zeta_{17} \mapsto \zeta_{17}^{-1}$, ma allora fissa l'elemento $\gamma$ tale che $K \ni \zeta_{17} + \zeta_{17}^{-1} = \gamma$ e sappiamo che ha grado al più l'indice di $H$, cioè 8. In questo caso è più conveniente vedere che $G/\mathbb{Q}(\gamma)$ ha grado $\leq 2$. Infatti $\zeta_{17} - \gamma\zeta_{17} + 1 = 0$, cioè annulla il polinomio $p(x) = x - \gamma x + 1 \in \mathbb{Q}(\gamma)[x]$.

Dunque si ha che $[\mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1}) : \mathbb{Q}] \geq 8$ e dunque vale l'uguaglianza con $Fix(H)$.

Infine osserviamo che $\gamma \in \mathbb{R}$ e dunque quella che abbiamo trovato è un'estensione reale.

**Esercizio 44** (Esempio di un'estensione di campi il cui gruppo di Galois é $\mathcal{Q}_8$)**.** Abbiamo visto che il gruppo di Galois di un'estensione di campi di grado 8 può essere $\mathbb{Z}_2$, $\mathbb{Z}_2^2$, $\mathbb{Z}_4$ o $\mathcal{D}_4$. Ci chiediamo se sia possibile anche ottenere $\mathcal{Q}_8$.

Sappiamo che $\{ \pm 1 \} \lhd \mathcal{Q}_8$. Iniziamo da un campo che ha $\mathbb{Z}_2^2$ come gruppo di Galois: $E = Q(\sqrt{2}, \sqrt{3})$ e consideriamo $L = E(\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)} = \alpha)$. Proviamo che è un'estensione valida.

Sappiamo che $[E : Q] = 4$ e $Gal(E/Q) \cong \mathbb{Z}_2^2$ e ha come generatori

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Ci chiediamo se $L$ sia di Galois su $Q$. $L/E$ lo è in quanto di grado $\leq 2$ e anche $E/Q$, in quanto campo di spezzamento di un polinomio separabile.

Questo mi garantisce che lo è anche l'estensione grande. *Chiarito all'inizio della prossima lezione*

I coniugati di $\alpha$, ovvero gli elementi che possono essere ottenuti come immagini di automorfismi di ordine 2 in $Gal(L/\mathbb{Q})$, sono 8 e questi sono $\alpha_{1,\dots,8} = \pm\sqrt{(\pm\sqrt{2}+2)(\pm\sqrt{3}+3)}$ e implica che $\alpha$ è radice di

$$\prod_{i=1}^{8}(x-\alpha_i) \in \mathbb{Q}[x]$$

I coefficienti sono in $\mathbb{Q}$ in quanto i coefficienti di tale polinomio sono fissati da ogni automorfismo di $Gal(L/\mathbb{Q})$ perché permuta fra loro gli 8 fattori $(x-\alpha_i)$ e dunque il prodotto $p(x)$ è lasciato fisso.

Tuttavia questo ragionamento crea una contraddizione logica. Infatti per conoscere i coniugati di $\alpha$ tramite l'azione di $Gal(L/\mathbb{Q})$ dovremmo conoscere a priori questo gruppo, che è lo scopo di questo ragionamento. Quindi per evitare questa situazione l'unico modo che mi viene in mente è svolgere il conto (per quanto brutto), ma funziona.

Per una dimostrazione rigorosa e più precisa si rimanda al libro, disponibile pdf online, *Teoria delle Equazioni e Teoria di Galois - S. Gabelli.*

Ma ora studiamo il comportamento di $\sigma$. Osserviamo che

$$\begin{aligned}\sigma(\alpha^2) &= \sigma((\sqrt{2}+2)(\sqrt{3}+3)) = \\ &= (-\sqrt{2}+2)(\sqrt{3}+3) \in E\end{aligned}$$

e

$$\begin{aligned}\frac{\sigma(\alpha^2)}{\alpha^2} &= \frac{(-\sqrt{2}+2)(\sqrt{3}+3)}{(\sqrt{2}+2)(\sqrt{3}+3)} = \\ &= \frac{(-\sqrt{2}+2)}{(\sqrt{2}+2)} = \frac{(-\sqrt{2}+2)^2}{2} = (\sqrt{2}-1)^2\end{aligned}$$

cioè un quadrato in $Q(\sqrt{2})$.

Se $\alpha \in E$, cioè se l'estensione $L/E$ fosse banale, allora $\sigma(\alpha) = \pm\alpha(\sqrt{2}-1)$. Dunque $\sigma^2(\alpha) = \alpha(\sqrt{2}-1)\cdot(-\sqrt{2}-1) = -\alpha$, ma $\sigma$ ha ordine 2, dunque l'ipotesi $\alpha \in E$ produce un assurdo.

Dunque $L/Q$ ha grado 8. Vediamo chi è il suo gruppo di Galois.

Siccome $E$ è un'estensione di Galois su $\mathbb{Q}$, il suo gruppo di Galois è un sottogruppo normale di $G$ e dunque $\sigma \in Gal(E/Q) \cong (Gal(L/Q))(Gal(L/E))$.

Quindi esiste $\tilde{\sigma} \in Gal(L/Q)$ (sollevamento) tale che $\tilde{\sigma}|_E = \sigma$. Per il ragionamento di prima abbiamo che $\tilde{\sigma}(\alpha) = \pm\alpha(\sqrt{2}-1)$, dunque $\tilde{\sigma}^2(\alpha) = -\alpha$ dunque $\tilde{\sigma}^2 \neq id$ e inoltre siccome $\tilde{\sigma}^4(\alpha) = \alpha$ si ha che $\tilde{\sigma}^4|_E = Id_E$, cioè $\tilde{\sigma}$ ha ordine 4.

Vale un discorso analogo per $\tau$ e il sollevato $\tilde{\tau}$ in $Gal(L/Q)$ che ha ordine 4.

Ma ora $\tilde{\sigma}\tilde{\tau}(\alpha) = \frac{3-\sqrt{3}}{-\sqrt{6}} \cdot (\sqrt{2}-1) \cdot \alpha$ e $\tilde{\tau}\tilde{\sigma}(\alpha) = \frac{3-\sqrt{3}}{\sqrt{6}} \cdot (\sqrt{2}-1) \cdot \alpha$, e quindi $Gal(L/Q)$ ha due elementi di ordine 4 che non commutano fra loro. L'unico gruppo di ordine 8 è $\mathcal{Q}_8$.

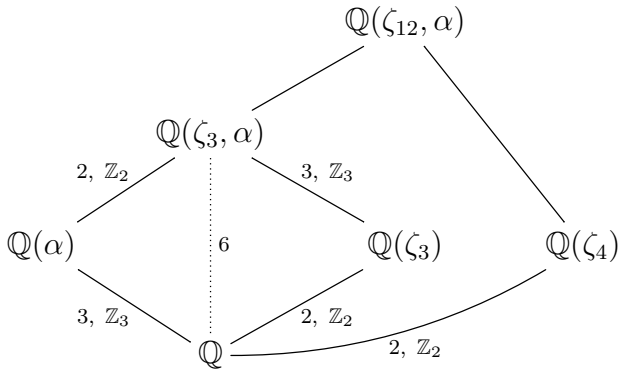
**Esercizio 45** (Proposto)**.** Consideriamo $Q(\zeta_p)$ con $p$ primo. Contiene un'unica estensione $F$ di grado 2 su $Q$. (rifletti su ciclicità del gdg e bla e ordine pari)

Quando, al variare di $p$, $F$ è reale? Cioè $F \subset \mathbb{R}$?

**Esercizio 46.** Sia $L = Q(\zeta_{12}, \alpha)$ con $\alpha = \sqrt[3]{2}$.

Mostriamo che è di Galois e troviamone il grado. Successivamente ne calcoleremo il gruppo di Galois.

Osserviamo che $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_4, \zeta_3)$, dunque possiamo spezzare tale estensione in una composizione delle due:




A questo punto siccome il polinomio minimo di $\alpha = \sqrt[3]{2}$ è $p(x) = x^3 - 2$, con radici $\alpha, \zeta_3\alpha, \zeta_3^2\alpha$ che sappiamo stare tutti in $L$ si ha che $Q(\alpha, \zeta_3)$ è campo di spezzamento di $p(x)$ e dunque è un'estensione di Galois.

Inoltre a destra abbiamo che $\mathbb{Q}(\zeta_4)$ è ancora di Galois per la stessa ragione e dunque anche la loro composizione lo è, in quanto hanno intersezione banale.

Tutti i gradi indicati nel diagramma derivano da risultati noti. Quindi osserviamo che $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 6$ e dunque 6 divide il grado di $L$ su $\mathbb{Q}$.

Ora sappiamo che il gruppo di Galois di $Q(\alpha, \zeta_3)$ è $\mathcal{S}_3$, in quanto non è abeliano perché ha un sottogruppo non normale determinato dall'esistenza del sottocampo $Q(\alpha, \zeta_3)/Q(\zeta_3)$ che non è un'estensione di Galois.

Ma se è $\mathcal{S}_3$, il sottogruppo di indice 2 è unico, e dunque abbiamo un'unica sotto estensione di grado 2 in $\mathbb{Q}(\zeta_3, \alpha)$ cioè $Q(\zeta_3)$ su $Q$.

Dunque se $\mathbb{Q}(\zeta_4)$ intersecasse $\mathbb{Q}(\zeta_3, \alpha)$ in maniera non banale avremmo che $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\zeta_3)$ per unicità di tale estensione, ma questo è assurdo, dunque l'intersezione dei due campi $Q(\zeta_3, \alpha)$ e $Q(\zeta_4)$ è banale.

Quindi per quanto osservato la scorsa lezione, $Gal(L/\mathbb{Q}) = Gal(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \cong \mathcal{S}_3 \times Gal(\mathbb{Q}(\zeta_2)/\mathbb{Q})$.

Se ne esplicitino i generatori.

# Capitolo 15

# Martedì 6 Dicembre

*Sotto-estensione quadratica di un'estensione ciclotomica con le radici p-esime dell'unità, per p primo. Esercizi su estensioni biquadratiche. Se un polinomio è risolubile per radicali, allora il suo campo di spezzamento ha gruppo di Galois risolubile.*

**Esercizio 47** (Precisazioni su quanto fatto con $\mathcal{Q}_8$.)**.** Perché l'estensione grande è necessariamente di Galois?

Non lo è perché lo sono i due "pezzi". Propone un controesempio con le estensioni successive $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt[4]{2})$.

Il punto è che, dato $\alpha = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}$, le altre radici del suo polinomio minimo sono i suoi coniugati $\alpha_{1,\dots,8}$ elencati nella scorsa lezione e quindi se $\alpha'$ è uno di questi, abbiamo che $\frac{\alpha}{\alpha'} = \frac{\sqrt{\sqrt{2}+2}}{\sqrt{-\sqrt{2}+2}} = \frac{\sqrt{2}+2}{\sqrt{2}} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ o una cosa simile. E dunque il campo più grande contiene tutti i coniugati di $\alpha$, cioè tutte le radici del suo polinomio minimo.

**Esercizio 48** (Sotto estensione quadratica di un'estensione ciclotomica con le radici $p$-esime dell'unità, per $p$ primo, esercizio proposto la scorsa lezione)**.** Sappiamo che se prendiamo $K = \mathbb{Q}(\zeta_n)$, $K/\mathbb{Q}$ è una estensione di Galois con gruppo di Galois isomorfo a $(\mathbb{Z}_n)^*$. Per $n$ primo il gruppo di Galois è ciclico e quindi contiene un unico sottogruppo $N$ di indice 2 e dunque $Fix(N)$ è l'unica sotto estensione di grado 2 su $\mathbb{Q}$.

Chi è $N$? Per determinarlo basta trovare in $K$ un elemento di grado 2 su $\mathbb{Q}$.

Introduciamo una notazione: in $(\mathbb{Z}_p)^*$ i quadrati modulo $p$ sono esattamente la metà, ovvero gli elementi del sottogruppo di indice 2 di cardinalità $\frac{p-1}{2}$.
Introduciamo il simbolo di Dirichlet $\left(\frac{i}{p}\right) = \begin{cases} 1 \; se \; i \; \square \; (p) \\ -1 \; se \; i \; non \; \square \; (p) \end{cases}$.

Sia $S = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta_p^i$. Ora studiamo $S^2$.

$$S^2 = \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)\zeta_p^{i+j} =$$

Osserviamo che se $i$ e $j$ sono due quadrati, anche $ij$ lo è: allora $\left(\frac{i}{p}\right)\left(\frac{j}{p}\right) = \left(\frac{ij}{p}\right)$

(Non sono molto convinta...se sono entrambi non quadrati? Mi sa che ho capito male)

$$= \sum_{i,j=1}^{p-1} \left(\frac{ij}{p}\right)\zeta_{i+j} =$$

Ora poniamo $j = ik$

$$= \sum_{k=1}^{p-1}\sum_{i=1}^{p-1} \left(\frac{i^2k}{p}\right)\zeta_p^{i+ik} =$$

Ma ora $i^2k$ è un quadrato se e solo se lo è $k$, quindi

$$= \sum_{k=1}^{p-1}\sum_{i=1}^{p-1} \left(\frac{k}{p}\right)\zeta_p^{(k+1)i} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\sum_{i=1}^{p-1}\zeta_p^{(k+1)i} =$$

Ora possiamo fare delle considerazioni a seconda di chi è $k$: se $p \mid k+1$ (cosa che succede solo nel $p-1$-esimo termine), la sommatoria in $i$ è uguale a $1 \cdot (p-1)$; altrimenti è la somma di tutte le radici dell'unità tranne la $p$-esima, cioè 1 e dunque è uguale a $-1$ in quanto la somma di tutte le radici dell'unità è uguale a 0 (usato altre volte).

Quindi isolando il $p-1$-esimo termine della prima sommatoria si ha che

$$= -\sum_{k=1}^{p-2} \left(\frac{k}{p}\right) + \left(\frac{-1}{p}\right) \cdot (p-1) = -\sum_{i=1}^{p-2} \left(\frac{k}{p}\right) + \left(\frac{p-1}{p}\right) \cdot (p-1) =$$

e distribuendo il secondo fattore del secondo addendo abbiamo che

$$= -\sum_{k=1}^{p-2} (\frac{k}{p}) + (\frac{-1}{p}) \cdot (p)$$

Ma ora la prima sommatoria è una somma di 1 e $-1$, ma l'insieme dei quadrati e dei non quadrati hanno la stessa cardinalità e quindi il primo fattore è nullo. Dunque

$$S^2 = (\frac{-1}{p}) \cdot p = \begin{cases} p \ se \ -1 \ \square \ (p) \\ -p \ se \ -1 \ non \ \square \ (p) \end{cases}$$

Ma se $-1$ è $\square$ $(p)$, cioè se $p \equiv 1$ $(4)$ allora $Fix(N) = \mathbb{Q}(\sqrt{p})$; altrimenti se $p \equiv 3$ $(p)$ $Fix(N) = \mathbb{Q}(i\sqrt{p})$.

Decidere (corso di Aritmetica) se $-1$ è un quadrato modulo $p$ dipende solo dalla classe di congruenza di $p$ modulo 4 (per $p$ dispari).

**Esercizio 49** (Esercizi su estensioni biquadratiche)**.** Sia $f(x) = x^4 - 4x^2 + 6$.

Troviamo le sotto-estensioni di grado 2 del suo campo di spezzamento di grado 2 su $\mathbb{Q}$ e successivamente il gruppo di Galois del campo di spezzamento su $\mathbb{Q}$.

La prima possiamo rispondere anche senza calcolare esplicitamente il suo campo di spezzamento. Penso che alcune siano le radici del polinomio associato $g(y) = y^2 - 4y + 6$ con $y = x^2$.

**Esercizio 50** (Metodi per trovare radici di polinomi, risolubilità per radicali)**.** Sia $F$ un campo a caratteristica 0 e un polinomio $p(x) \in F[x]$. Vorremmo trovare le radici, e scriverle. Ma l'unica operazione che potremmo fare è quella di estrarre radici.

Se fosse possibile scriverle in questo modo, allora il polinomio si dice *risolubile per radicali*. Più precisamente

**Definizione 5** (Risolubile per radicali)**.** Un polinomio $f(x) \in F[x]$ con $F$ campo, si dice *risolubile per radicali* se il campo di spezzamento $K$ su $F$ è tale che una successione di estensioni di $F$

$$F = F_0 \subset F_1 = F_0(\alpha_1) \subset \ldots \subset F_{n+1} = F_n(\alpha_{n+1}) = L$$

tali che $K \subset L$ e esistono $h_1, \ldots, h_{n+1} \in \mathbb{N}$ tali che $\forall \alpha_i$ si ha che $\alpha_i^{h_i} \in F_{i-1}$.

**Osservazione 5.** Supponiamo che un dato polinomio sia risolubile per radicali. Possiamo supporre che il campo di partenza contenga le radici dell'unità:

in quanto aggiungere radici dell'unità vuol dire comunque fare un'estensione per radicali.

Dunque se $F$ non contiene le radici $m$-esime di 1 e $p(x)$ è risolubile per radicali su $F$, allora $p(x)$ è risolubile per radicali in $F(\zeta_m)$. Viceversa, se $p(x)$ è risolubile per radicali su $F(\zeta_m)$, allora $p(x)$ è risolubile per radicali su $F$ in quanto mi basta aggiungere $F \subset F(\zeta_m)$ all'inizio.

**Osservazione 6.** Se $p(x)$ è risolubile per radicali su $F$, allora posso supporre che, data la catena di risoluzioni

$$F_0 \subset F_1 = F_0(\alpha_1) \subset \ldots \subset F_{n+1} = F_n(\alpha_{n+1}) = L \supset K,$$

$L$ sia di Galois su $F$.

In generale non sarebbe vero, ma in questo caso posso ricorrere a un'estensione per radicali più lunga. Ovvero sia $F_0 \subset F_1 = F_0(\alpha_1)$ con $\alpha_1^{h_1} = a_0 \in F_0$ per qualche $h_1$ e $g_1(x)$ il polinomio minimo di $\alpha_1$. Sappiamo che $g_1(x) \mid x^{h_1} - a_0$ e siano $\alpha_{1,1}, \ldots, \alpha_{1,s}$ le altre radici di $g_1(x)$. Ma ora

$$F_0 \subset F_1 = F_0(\alpha_1) \subset F_0(\alpha_1, \alpha_{1,1}) \subset F_0(\alpha_1, \alpha_{1,1}, \alpha_{1,2}) \ldots \subset F_0(\alpha_1, \ldots, \alpha_{1,s})$$

Ognuna di queste estensioni è per radicali e l'ultima è il campo di spezzamento di $g_1(x)$ su $F_0$.

Iteriamo con $g_2(x)$ polinomio minimo di $\alpha_2$ e anche qui aggiungiamo le sue radici una alla volta. Ma ora posso dire che $\alpha_2^{h_2} = a_1$ appartenga non solo ad $F_1$, ma piuttosto $\overline{F_1} = F_0(\alpha_1, \ldots, \alpha_{1,s})$ e quindi devo ripartire da dove mi ero fermata con $\alpha_1$:

$$F_0(\alpha_1, \ldots, \alpha_{1,s}) \subset F_0(\alpha_1, \ldots, \alpha_{1,s}, \alpha_2) = \overline{F}_1(\alpha_2) \subset \overline{F}_1(\alpha_2, \alpha_{2,1} \ldots, \alpha_{2,t})$$

che è un'estensione di Galois in quanto campo di spezzamento di $g_2(x)$ su $F_1$. (Non mi convince)

Sono state fatte delle considerazioni su come agiscono gli elementi dei gruppi di Galois di queste estensioni. Sinceramente non le ho capite. Le chiederò.

**Teorema 12.** *Se $p(x) \in F[x]$ è un polinomio risolubile per radicali, allora $K$, il suo campo di spezzamento su $F$, è tale che il gruppo di Galois $Gal(K/F)$ è un gruppo risolubile.*

*Dimostrazione.* L'idea è quella di sfruttare il fatto che siccome tutte le sotto-estensioni sono di Galois, queste produrranno una catena di sottogruppi normali dentro il gruppo di Galois con quozienti a due a due abeliani e

dunque per definizione un gruppo di Galois risolubile. Inoltre sappiamo che questo sarebbe equivalente a dire che è risolubile per commutatori.

Vediamo i dettagli con alcuni lemmi.

Ad esempio questo teorema ci dice che se un polinomio ha come gruppo di Galois $\mathcal{S}_5$ o $\mathcal{S}_n$ con $n \geq 5$, che sappiamo non essere risolubile, allora $p(x)$ non ha una formula per radicali delle sue radici.

Per dimostrare il teorema abbiamo bisogno di alcuni fatti:

**Proposizione 13.** *Un sottogruppo di un gruppo risolubile è risolubile.*

*Dimostrazione.* Data una catena di risolubilità di un gruppo $G$, basta considerare la catena prodotta dalle intersezioni con $H$ degli elementi della catena di $G$. □

**Proposizione 14.** *Quozienti di gruppi risolubili sono risolubili.*

*Dimostrazione.* Se mandiamo $\phi : G \twoheadrightarrow H$ con un omomorfismo surgettivo e consideriamo la catena di $G$, osserviamo che le immagini degli elementi della catena di $G$ producono una catena in $H$ e che $H_i/H_{i+1} = \overline{\phi}(G_i/G_{i+1})$ ancora abeliano in quanto immagine di un gruppo abeliano. Dunque una catena di risolubilità per $H$. □

In alternativa, potevamo farlo per commutatori e proiettarli surgettivamente su $H$: le immagini saranno i commutatori di $H$.

Quindi ora sapendo che per ipotesi il polinomio è risolubile per radicali, esplicito la catena prodotta dai radicali che ho aggiunto in successione aggiungendo all'inizio una radice dell'unità:

$$F \subset F(\zeta_m) \subset F(\zeta_m, \alpha_1) \subset \ldots \subset F(\zeta_m, \alpha_1, \ldots, \alpha_m) = L$$

Sappiamo che $L$ è di Galois su $F$ per quanto detto nell'osservazione 6 e che per definizione contiene $K$, campo di spezzamento di $p(x)$.

Per concludere abbiamo bisogno del seguente lemma

**Lemma 15.** *Se $F$ contiene $\zeta_n$ e $F \ni a \neq 0$ e abbiamo $K$ cds di $x^n - a$, allora*

1. *$K = F(\mu)$ con $\mu$ radice di $x^n - a$;*
2. *$Gal(K/F)$ è abeliano.*

*Dimostrazione.* Se $\mu$ è radice di $x^n - a$, le radici del polinomio sono $\mu$, $\mu\zeta_n$,..., $\mu\zeta_n^{n-1}$ che sappiamo generare tutto il campo di spezzamento $K$. Sappiamo che $Gal(K/F)$ è determinato da dove mando $\mu$. Possiamo definire un omomorfismo $\tau : Gal(K/F) \to \mathbb{Z}_n$ nel seguente modo: se $\sigma \in Gal(K/F)$, si avrà che $\sigma(\mu) = \mu\zeta_n^{i(\sigma)}$ e allora poniamo $\tau(\sigma) = i(\sigma)$. Si può dimostrare che è ben definito ed è iniettivo. Ma ora osserviamo che gli elementi di $Gal(K/F)$ commutano fra loro, in quanto dato $\sigma'(\mu) = \mu\zeta_n^{i(\sigma')}$ abbiamo che $(\sigma\sigma')(\mu) = \mu\zeta_n^{i(\sigma\sigma')} = \mu\zeta_n^{i(\sigma)i(\sigma')} = \mu\zeta_n^{i(\sigma')i(\sigma)} = (\sigma'\sigma)(\mu)$.

Quindi $Gal(K/F)$ è sottogruppo di $\mathbb{Z}_n$ e quindi abeliano. □

Dunque data la solita catena per radicali, abbiamo che $G = Gal(L/F)$ è risolubile in quanto posso considerare la catena prodotta dai suoi sottogruppi $Gal(L/F_1)$, $Gal(L/F_2)$, ... fino a $Gal(L/F_n) = \{ id \}$.

Ora se supponiamo di avere le radici dell'unità, ogni volta che aggiungiamo una radice per il lemma precedente ci troviamo in un campo di spezzamento sul campo precedente e applicare il lemma: dunque $F_i$ è una estensione di Galois di $F_{i-1}$, ma allora $Gal(F_i/F_{i-1}) \cong Gal(L/F_{i-1})/Gal(L/F_i)$, quoziente di gruppi risolubili e dunque risolubile.

Ma quindi $Gal(L/F)$ è risolubile e di conseguenza lo è $Gal(K/F)$ in quanto isomorfo a un quoziente di gruppi risolubili, ovvero a $Gal(L/F)/Gal(L/K)$. □

Nella lezione seguente dimostreremo il viceversa, ovvero che se $Gal(K/F)$ è risolubile, allora il polinomio è risolubile per radicali.

# Capitolo 16

# Venerdì 9 Dicembre

*Un campo di spezzamento con gruppo di Galois risolubile è risolubile per radicali. Esercizi con estensioni biquadratiche. Campo di spezzamento, sotto estensioni reali e corrispondenza di Galois per $x^7 - 2$.*

Continuiamo quanto enunciato alla fine della scorsa lezione. Ricordiamoci che stiamo lavorando su campi a caratteristica 0.

**Teorema 16.** *Se $K$ è il campo di spezzamento su $F$ di un polinomio a coefficienti in $F$ e $Gal(K/F)$ è risolubile, allora il polinomio è risolubile per radicali.*

*Dimostrazione.* Abbiamo bisogno di un risultato preliminare:

**Lemma 17.** *Siano $\sigma_1, \ldots, \sigma_n$ elementi distinti in $Gal(K/F)$. Allora sono linearmente indipendenti su $K$, ovvero non posso scrivere una combinazione $\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n = 0$ con $\lambda_i$ non tutti nulli.*

*Dimostrazione.* Ricordiamo che le funzioni a valori in un campo, in questo caso $K$, sono uno spazio vettoriale su $K$. Vogliamo provare che non esiste una combinazione lineare non banale (cioè con i coefficienti non tutti nulli) nulla, ovvero non esistono $\lambda_i \in K$ non tutti nulli tali che

$$\lambda_1\sigma_1 + \ldots \lambda_n\sigma_n = 0$$

Consideriamo per assurdo una combinazione lineare di lunghezza minima: per ottenerla supponiamo semplicemente di aver già eliminato i coefficienti nulli. Siano $\lambda_1, \ldots, \lambda_m$ i coefficienti che restano.

Possiamo escludere il caso in cui $m = 1$, in quanto un solo automorfismo del campo non può essere nullo in quanto invertibile.

Stiamo supponendo che $\sigma_1 \neq \sigma_2$, cioè $\exists c \in K$ tale che $\sigma_1(c) \neq \sigma_2(c)$. Consideriamo $ac \in K$, in quanto la combinazione è nulla si avrà

$$\lambda_1\sigma_1(ac) + \ldots + \lambda_m\sigma_m(ac) = 0$$

e per proprietà degli omomorfismi

$$= \lambda_1(\sigma_1(a)\sigma_1(c)) + \ldots + \lambda_m(\sigma_m(a)\sigma_m(c)) = 0$$

Supponendo $\sigma_1(c) \neq 0$, abbiamo anche che

$$\begin{aligned} &= \sigma_1(c)(\lambda_1\sigma_1(a) + \ldots + \lambda_m\sigma_m(a)) = \\ &= \lambda_1(\sigma_1(c)\sigma_1(a)) + \ldots + \lambda_m(\sigma_1(c)\sigma_m(a)) = 0 \end{aligned}$$

ma ora sottraendo le due espressione termine a termine otteniamo che il primo termine si elide e quindi resta

$$\lambda_2(\sigma_2(c) - \sigma_1(c))\sigma_2(a) + \ldots + \lambda_m(\sigma_m(c) - \sigma_1(c))\sigma_m(a) = 0$$

è una combinazione lineare non banale nulla di lunghezza minore, e ciò provoca un assurdo.

□

Torniamo alla dimostrazione del teorema. Volevamo provare che se $K$ è il campo di spezzamento di $p(x) \in F[x]$ su $F$ e $Gal(K/F)$ è risolubile, allora $p(x)$ è risolubile per radicali. Anche qui supponiamo, come detto nell'osservazione 5 di avere già le radici dell'unità.

Sia $G = Gal(K/F)$, in quanto risolubile esiste una catena di sottogruppi di $G$ $H_i$ tali che

$$\{ e \} = H_n \lhd H_{n-1} \lhd \ldots \lhd H_1 \lhd H_0 = G$$

e $H_{i-1}/H_i$ è ciclico.

Per corrispondenza di Galois sappiamo che questa produce in $K$ una catena di sotto-estensioni di Galois, ovvero i campi lasciati fissi dai sottogruppi (normali) della catena ovvero

$$K = Fix(\{ e \}) \supset Fix(H_{n-1}) \supset \ldots \supset Fix(H_1) \supset Fix(G) = F$$

Denotiamo $F_i = Fix(H_i)$, quindi sapendo che $Gal(K/F_i) = H_i$ e che$H_{i-1}/H_i$ è ciclico, risulta che $Gal(K/F_{i-1})/Gal(K/F_i)$ è ciclico. Ma questo per teorema

di corrispondenza di Galois è isomorfo a $Gal(F_{i-1}/F_i)$ che di conseguenza è ciclico.

Dobbiamo solo dimostrare che ciascuna di queste estensioni possa essere fatta per radicali, ovvero che esiste $\omega \in K$ e $n \in \mathbb{N}$ tale che $\omega^n \in F$ e $K = F(\omega)$.

Sia $E$ un generico $F_i$. Proviamo che tale affermazione è vera se $Gal(K/E)$ è ciclico.

Sia $Gal(K/E) = \mathbb{Z}_n$ e $\zeta = \zeta_n \in E$. Sia $\sigma \in Gal(K/E)$ un suo generatore. In quanto generatore di ordine $n$, sappiamo che $id, \sigma, \dots \sigma^{n-1}$ sono elementi distinti del gruppo di Galois, dunque per il lemma sono linearmente indipendenti:

$$id_K + \zeta^{-1}\sigma + \zeta^{-2}\sigma^2 + \ldots + \zeta^{-n+1}\sigma^{n-1} \neq 0$$

dunque $\exists \beta \in K$ tale che

$$\begin{aligned}(id_K + \zeta^{-1}\sigma + \zeta^{-2}\sigma^2 + \ldots + \zeta_{-n+1}\sigma^{n-1})(\beta) = \\ =\beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \ldots + \zeta_{-n+1}\sigma^{n-1}(\beta) = \alpha \neq 0\end{aligned}$$

Osserviamo che

$$\begin{aligned}\sigma(\alpha) &= \sigma(\beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \ldots + \zeta^{-n+1}\sigma^{n-1}(\beta)) = \\ &= \sigma(\beta) + \zeta^{-1}\sigma^2(\beta) + \ldots + \zeta^{-n+2}\sigma^{n-1}(\beta) + \zeta^{-n+1}\beta = \\ &= \zeta^{-n+1}\beta + \sigma(\beta) + \zeta^{-1}\sigma^2(\beta) + \ldots + \zeta^{-n+2}\sigma^{n-1}(\beta) = \\ &= \zeta(\beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \ldots + \zeta^{-n+1}\sigma^{n-1}(\beta)) = \zeta\alpha\end{aligned}$$

ma allora i coniugati di $\alpha$ sono $\alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha$, cioè elementi distinti e dunque il polinomio minimo di $\alpha$ non può che avere grado $\geq n$. Ma $\alpha \in K$ e $[K : E] = n$, dunque $K = E(\alpha)$.

Resta da vedere che $\alpha^n \in E$. In quanto il prodotto dei suoi coniugati $\alpha \cdot \sigma(\alpha) \cdot \ldots \cdot \sigma^{n-1}(\alpha)$ è invariante per $\sigma$ appartiene a $F$ e in particolare è uguale a $\zeta^{0+1+2+\ldots+n-1}\alpha$. L'esponente è uguale $\binom{n}{2}$ ed è multiplo di $n$ se suppongo $n$ primo. Se è multiplo di $n$, la produttoria dei coniugati di $\alpha$ è proprio uguale ad $\alpha$.

Ma che sia primo lo posso supporre in quanto ho la libertà di spezzare in quozienti non solo ciclici, ma di ordine primo.

Penso che il ragionamento fatto sull'ordine e i coniugati di $\alpha$ sia utile per l'esercizio aggiuntivo 14.0.30. □

**Esercizio 51** (Esercizi con estensioni biquadratiche (proposto la scorsa lezione))**.** Sia $f(x) = x^4 - 4x^2 + 6$.

Troviamo le sotto-estensioni quadratiche di grado 2 su $\mathbb{Q}$ e il gruppo di Galois del suo campo di spezzamento su $\mathbb{Q}$. Sia $K$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Sappiamo (per quanto fatto le scorse lezioni) che per ottenere il campo di spezzamento dobbiamo fare le seguenti estensioni successive: data $\omega$ una radice di $f(x)$,

$$K = \mathbb{Q}(\sqrt{\Delta}, \sqrt{termine\ noto}, \sqrt{\omega})$$

in questo caso particolare

$$\mathbb{Q}(\sqrt{-2}, \sqrt{6}, \sqrt{2 + \sqrt{-2}})$$

Ora $[\mathbb{Q}(\sqrt{-2}, \sqrt{6}) : \mathbb{Q}] = 4$ ed è un'estensione di Galois, in quanto campo di spezzamento di $(x^2 + 2)(x^2 - 6)$. Inoltre possiamo subito dire che ha gruppo di Galois isomorfo a $\mathbb{Z}_2^2$, in quanto $K$ contiene due estensioni di grado 2 distinte. Ma allora questo vuol dire che $\mathbb{Q}(\sqrt{-2}) \neq \mathbb{Q}(\sqrt{6})$, infatti una è una sotto-estensione reale, l'altra no; potevamo affermarlo anche osservando che nella prima $-2$ (o $+2$ se vogliamo ricondurci al caso di due sotto-estensioni reali) è un quadrato, mentre in $\mathbb{Q}(\sqrt{6})$ non lo è.

*Da qui in poi mi sono un po' addormentata*

Ora cerchiamo un po' a mano gli elementi del gruppi di Galois e i relativi campi fissi.

Inizialmente studiamo $Gal(\mathbb{Q}(\sqrt{-2}, \sqrt{6})/\mathbb{Q})$: sappiamo che vi sono 3 sotto-campi di grado 2, corrispondenti ai sottogruppi di $\mathbb{Z}_2^2$ di indice 2. Esplicitiamoli, sono

$$\sigma_1 : \begin{cases} \sqrt{-2} \mapsto -\sqrt{-2} \\ \sqrt{6} \mapsto \sqrt{6} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{-2} \mapsto \sqrt{-2} \\ \sqrt{6} \mapsto -\sqrt{6} \end{cases} \qquad \sigma_1\sigma_2 : \begin{cases} \sqrt{-2} \mapsto -\sqrt{-2} \\ \sqrt{6} \mapsto -\sqrt{6} \end{cases}$$

Vediamo subito che $Fix(< \sigma_1 >) = \mathbb{Q}(\sqrt{6})$, $Fix(< \sigma_2 >) = \mathbb{Q}(\sqrt{-2})$ e $Fix(< \sigma_1\sigma_2 >) = \mathbb{Q}(\sqrt{-3})$.

Ora cerchiamoli in $D_4$. Qual è il modo più semplice per trovarli? Lui suggerisce di osservare che sono normali, hanno un quoziente di ordine 2 e dunque abeliano ciclico e quindi posso passare per il quoziente dei commutatori cercando omomorfismi surgettivi $D_4/[D_4, D_4] \mapsto \mathbb{Z}_2$.

Ma osserviamo che i commutatori di $D_4$ sono o l'identità (se commuto due rotazioni) o le rotazioni di ordine pari (se commuto una rotazione e una riflessione o due riflessioni distinte), dunque sono isomorfi a $\mathbb{Z}_2^2$ e i modi per fare un omomorfismo non nullo su $\mathbb{Z}_2$ sono 3 e li abbiamo già trovati.

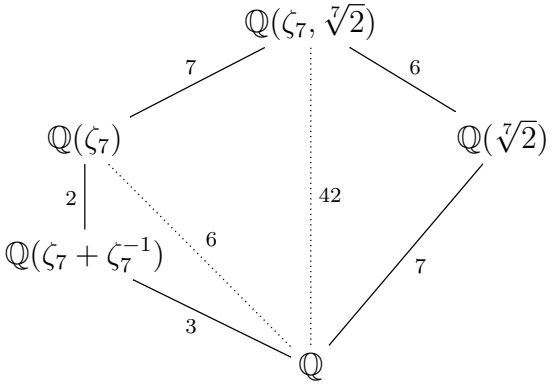
Ora chiediamoci se $\alpha = \sqrt{\omega} \in \mathbb{Q}(\sqrt{-2}, \sqrt{6})$. Vediamo se è scrivibile come combinazione lineare di una base di $\mathbb{Q}(\sqrt{-2}, \sqrt{6})$, ovvero $\alpha = a + b\sqrt{-2} + c\sqrt{6} + d\sqrt{-3}$. Potrebbero essere dei conti poco gestibili.

Un metodo alternativo è osservare che $\alpha^2 = \omega$ è fissato da $\sigma_2$. Tuttavia se $\alpha \in \mathbb{Q}(\sqrt{-2}, \sqrt{6})$, $\sigma_2(\alpha) = \pm\alpha$. Osservando gli autospazi di $\sigma_2$, $\alpha$ vive o in quello relativo a 1 o in quello relativo a $-1$, cioè o in $< 1, \sqrt{-2} >$ o in $< \sqrt{-6}, \sqrt{3} >$ (sono una base di autovettori). E dunque ho spezzato il problema in due più facili.

**Esercizio 52** (Campo di spezzamento, sotto estensioni reali e corrispondenza di Galois per $x^7 - 2$ (13.2.10))**.** Trovare il cds $K$ di $f(x) = x^7 - 2$, il grado di $K \cap \mathbb{R}$ su $\mathbb{Q}$, dire se è di Galois e in caso negativo indicare il massimo sottocampo di $K \cap \mathbb{R}$ di Galois su $\mathbb{Q}$.

Sappiamo che $K = \mathbb{Q}(\sqrt[7]{2}, \zeta_7)$ in quanto le radici di $f$ sono i prodotti fra $\sqrt[7]{2}$ e le potenze successive di $\zeta_7$. Sappiamo che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ e che $[\mathbb{Q}(\sqrt[7]{2}) : \mathbb{Q}] = 7$, inoltre in quanto coprimi hanno intersezione banale e dunque $[K : \mathbb{Q}] = 42$; dunque $G = Gal(K/\mathbb{Q})$ ha ordine 42. Sappiamo inoltre che $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ è normale e quindi $G$ ha un sottogruppo normale di ordine 7 (il 7-Sylow). C'è inoltre un sottogruppo di ordine 6, tuttavia non normale in quanto è gruppo che lascia fisso un'estensione non normale ($\mathbb{Q}(\sqrt[7]{2})$).

Troviamo sotto-estensioni di $K$ normali su $\mathbb{Q}(\sqrt[7]{2})$ ma non su $\mathbb{Q}$. Sfruttiamo quelle di $\mathbb{Q}(\zeta_7)$, che sono entrambe non normali su $\mathbb{Q}$




Ora per cardinalità $Gal(K/\mathbb{Q}(\zeta_7)) \cong \mathbb{Z}_7$.

Ora studiamo $K \cap \mathbb{R}$. É il campo fisso rispetto al coniugio. La sotto-estensione individuata di $\mathbb{Q}(\zeta_7)$, cioè $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, è invariante per coniugio e dunque reale e inoltre ha grado 3 su $\mathbb{Q}$ in quanto quella superiore ha grado 2, infatti il polinomio minimo di $\zeta_7$ su $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ ha grado 2. Abbiamo allora provato che $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \subset K \cap \mathbb{R}$.

Ma inoltre $K \cap \mathbb{R} \supset \mathbb{Q}(\sqrt[7]{2})$ e dunque l'intersezione ha almeno grado 21. La disuguaglianza inversa viene dal fatto che essendo diverso da tutto $K$, non può essere maggiore di 21 e dividere 42.

Non è di Galois, in quanto contiene $\sqrt[7]{2}$, ma non tutte le radici del suo polinomio minimo. Dunque ci chiediamo chi sia il suo più grande sottocampo di Galois su $\mathbb{Q}$. Evidentemente non può contenere $\sqrt[7]{2}$.

Sappiamo che il gruppo di Galois di $K$ su $\mathbb{Q}$ ha 42 elementi: esplicitiamoli al variare di $i$ e $j$

$$\tau_{i,j} = \begin{cases} \sqrt[7]{2} \mapsto \zeta_7^i \sqrt[7]{2} \\ \zeta_7 \mapsto \zeta_7^j \end{cases}$$

Ovvero $G = Gal(K/\mathbb{Q}) \cong \mathbb{Z}_7 \rtimes (\mathbb{Z}_7)^* \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_6$, infatti $< \tau_{i,1} > \cong \mathbb{Z}_7$ e $< \tau_{1,j} > \cong \mathbb{Z}_6$.

Cerchiamo un sottogruppo normale di $G$ che contenga il coniugio, il cui campo fisso sarà quello reale cercato. Vediamo che il coniugio è proprio $\tau_{1,-1}$. Ma il più piccolo sottogruppo normale di $G$ contenente $\tau_{0,-1}$ deve contenere anche i suoi coniugati che sono al variare di $i, j$ gli elementi

$$\tau_{i,j} \circ \tau_{0,-1} \circ \tau_{i,j^{-1}} = \tau_{i,j} \circ \tau_{0,-1} \circ \tau_{-i,\frac{1}{j}} = \tau_{2i,-1}$$

e dunque sono gli elementi di $< \tau_{i,0} > \times < \tau_{0,-1} >$ che è isomorfo a $\mathbb{Z}_1 4$ e dunque ha almeno $2 \cdot 7$ elementi e quindi in totale ha indice al massimo 3, e quindi produce una sotto-estensione di grado al più 3 che abbiamo già trovato: $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

**Esercizio 53.** Ci lascia per casa la conclusione dell'esercizio precedente e cercare i sottocampi di grado 2 del campo di spezzamento su $\mathbb{Q}$ di $(x^7 - 2)(x^2 + 7)$. Inoltre mostrare che $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$ è di Galois su $\mathbb{Q}$, trovarne il gruppo di Galois e le sotto-estensioni normali.

# Capitolo 17

# Martedì 13 Dicembre

*Chiusura algebrica di un campo finito e cenni sul suo gruppo di automorfismi. Esercizi su estensioni di Galois, sottocampi e corrispondenza di Galois.*

Richiamiamo alcune cose fatte l'anno scorso sui campi finiti.

**Proposizione 18.** *Per ogni $p$ primo e per ogni $n \in \mathbb{N}$ esiste un unico campo di cardinalità $p^n$, cioè $\mathbb{F}_{p^n}$ e questo è il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$ e i suoi elementi sono tutti e soli le radici distinte di tale polinomio.*

*Ogni campo finito è isomorfo a un certo $\mathbb{F}_{p^n}$.*

I gruppi di automorfismi di questi campi sono particolari. Sappiamo inoltre che

**Proposizione 19.** *Se prendiamo $m$, $n \geq 1$ tali che $n \mid m$, allora $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$.*

Ora vorremmo studiare $Aut(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$. Definiamo un particolare automorfismo:

**Definizione 6** (Morfismo di Frobenius)**.** Se $K$ è un campo a caratteristica $p$, definiamo *morfismo di Frobenius* $\phi : K \to K$ tale che $x \mapsto x^p$.

L'anno scorso abbiamo anche dimostrato che

**Proposizione 20.** *Se $K$ è finito, il morfismo appena definito è un automorfismo di $K$. Altrimenti è solamente un omomorfismo iniettivo.*

Proviamo ora un risultato importante, ovvero che

**Proposizione 21.** *Dato $K = \mathbb{F}_{p^n}$, $Aut(\mathbb{F}_{p^n}/\mathbb{F}_p) =< \phi >$ ed è ciclico di ordine $n$.*

*Dimostrazione.* Troviamo l'ordine di $\phi$. Sicuramente $\phi^n : x \mapsto x^{p^n} = x$ e quindi $\phi^n = Id_{\mathbb{F}_{p^n}}$ e l'ordine di $\phi$ divide $n$. Se per assurdo fosse uguale a $d < n$, allora $x^{p^d} = x \ \forall x \in \mathbb{F}_{p^n}$, ma questo non è possibile con $d < n$ perché questa equazione ha al più $p^d$ soluzioni. □

**Corollario 22.** *Se $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, allora $\mathbb{F}_{p^n}$ è il sottocampo fissato da $\phi^n$.*

Infatti sappiamo che $\mathbb{F}_{p^n}$ è una sotto-estensione di Galois di $\mathbb{F}_{p^m}$ e dunque è ben definito il suo gruppo di Galois, che è $Gal(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) \cong < \phi^{\frac{m}{n}} > \cong \mathbb{Z}_{\frac{m}{n}}$.

Ora vorremmo costruire un campo a caratteristica $p$ più grande in cui tutti i polinomi siano fattorizzabili, ovvero algebricamente chiuso.

Se $f(x) \in \mathbb{F}_p[x]$ è un polinomio irriducibile di grado $n$, sappiamo che una sua radice è contenuta in $\mathbb{F}_{p^n}$.

Osserviamo che vale $\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^{3!}} \subset \mathbb{F}_{p^{4!}} \subset \ldots$. Allora definiamo

$$\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^{n!}}$$

**Proposizione 23.** *$\overline{\mathbb{F}}_p$ è un campo algebricamente chiuso di caratteristica $p$. Inoltre $\forall n \in \mathbb{N}$ vale che $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$.*

*Dimostrazione.* Definiamo la somma e il prodotto di una coppia di suoi elementi come la somma e il prodotto di tale coppia visti come elementi del più piccolo campo che li contiene entrambi. Così dimostro anche che la caratteristica è $p$.

Prendiamo ora un polinomio $p(x) \in \overline{\mathbb{F}}_p[x]$, siccome ha un numero finito di coefficienti possiamo sempre considerare il minimo campo in $\overline{\mathbb{F}}_p$ che li contiene tutti: sia $\mathbb{F}_{p^{n!}}$. Ora il campo di spezzamento di $p(x)$ su $\mathbb{F}_{p^{n!}}$ è una sua estensione finita e quindi è contenuto in un certo $\mathbb{F}_{p^{N!}}$. Ma allora $p$ si spezza anche in $\overline{\mathbb{F}}_p$.

$\forall n \in \mathbb{N}$ vale che $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$ in quanto $\forall n$ si ha che $n \mid n!$ e dunque $\mathbb{F}_p^n \subset \mathbb{F}_{p^{n!}} \subset \overline{\mathbb{F}}_p$.

In particolare osserviamo che la chiusura algebrica di un campo finito è numerabile, in quanto è unione numerabile di campi finiti. □

Studiamo i suoi automorfismi. Notiamo che $\forall n \in \mathbb{N}$ sappiamo prima che $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$ e dunque che ogni automorfismo di $\overline{\mathbb{F}}_p$ può essere ristretto a uno di $\mathbb{F}_{p^n}$, ovvero esiste un omomorfismo surgettivo

$$\rho_n : G = Aut(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to Aut(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$$

Sappiamo che $\phi$, l'automorfismo di Frobenius appartiene a $G$ e dunque può essere ristretto ad ogni $\mathbb{Z}_n$ tramite $\rho_n$.

Allora viene naturale definire $\rho = \prod_{n\in\mathbb{N}} \rho_n : G \to \prod_{n\in\mathbb{N}} \mathbb{Z}_n$.

**Proposizione 24.** *Tale mappa è un omomorfismo iniettivo, ma non necessariamente surgettivo.*

*Dimostrazione.* Studiamo $Ker(\rho)$. Se $\sigma \in G$ è tale che $\sigma \neq id$, allora esisterà $x \in \overline{\mathbb{F}}_p$ tale che $\sigma(x) \neq x$. Ma allora $\exists n \in \mathbb{N}$ tale che $x \in \mathbb{F}_{p^{n!}}$ e quindi $[\rho_n(\sigma)](x) \neq x = Id(x)$ e dunque $\sigma \notin Ker(\rho)$.

Se consideriamo $\rho_n : G \to Aut(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$ e $\rho_m : G \to Aut(\mathbb{F}_{p^m}/\mathbb{F}_p) \cong \mathbb{Z}_m$ con $m \mid n$, allora esiste ed è ben definita la restrizione da $\mathbb{Z}_n \to \mathbb{Z}_m$ che mi manda il morfismo di Frobenius di $\mathbb{Z}_n$ $\phi_n \mapsto \phi_m$, quello di $\mathbb{Z}_m$ che sappiamo essere i generatori di questi gruppi (di Galois).

A questo punto abbiamo che gli elementi dell'immagine di $\rho$ sono delle successioni $(\sigma_n)_{n\in\mathbb{N}}$ tali che se $m \mid n$ allora esiste una mappa tale che $\sigma_n \mapsto \sigma_m$ ed è proprio la restrizione di $\sigma_n$ a $\mathbb{F}_{p^m}$.

Proviamo che non è surgettiva, ma prima abbiamo bisogno di definire alcune strutture:

**Definizione 7** (Insieme diretto)**.** Sia $(I, \prec)$ un insieme parzialmente ordinato. Diciamo che è *diretto* se $\forall n, m \in I$ $\exists j \in I$ tale che $n \prec j$ e $m \prec j$.

Un esempio sono gli interi $\mathbb{Z}$ con la relazione $n \prec m$ se e solo se $m \mid n$.

**Definizione 8** (Sistema inverso)**.** Supponiamo di avere una famiglia di gruppi $\{ G_i \}_{i\in I}$ e $\{ \phi_{i,j} \}_{i,j\in I, i\prec j}$ tale che $\phi_{i,j} \in Hom(G_j, G_i)$.

Se quando $i \prec j \prec k$, si ha che $\phi_{i,j} \circ \phi_{j,k} = \phi_{i,k}$ e $\phi_{i,i} = Id_{G_i}$, allora $\{ G_i, \phi_{i,j} \}_{i,j\in I, i\prec j}$ si dice *sistema inverso.*

**Definizione 9** (Limite inverso)**.** Se $I$ è un insieme diretto e $\{ G_i, \phi_{ij} \}$ è un sistema inverso su $I$, allora definiamo *limite inverso* di $\{ G_i, \phi_{i,j} \}$, l'insieme

$$D = \left\{ (y_i) \in \prod_{i\in I} G_i \mid \phi_{i,j}(y_j) = y_i \ \forall i, j \in I \right\}$$

Questo descrive in modo un po' più generale la nostra situazione:

$$Aut(\overline{\mathbb{F}}_p) = G \xrightarrow{\rho} \prod \mathbb{Z}_n = \prod Aut(\mathbb{F}_{p^n})$$

Si ha che $Im(\rho) \subset D$ limite inverso di $\{\, \mathbb{Z}_n \,\}$: denotiamolo $\varprojlim \mathbb{Z}_n$. Ma vale anche il viceversa, infatti se $(\sigma_n) \in \varprojlim \mathbb{Z}_n$, allora $(\sigma_n)$ definisce $\forall n$ un elemento di $Aut(\mathbb{F}_{p^n}/\mathbb{F}_p)$ e se $n \mid m$ $\sigma_m$ si restringe a $\sigma_n$. Ma quindi questo elemento definisce un automorfismo dell'unione di $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$.

Ma ora $\varprojlim \mathbb{Z}_n \cong Aut(\overline{\mathbb{F}}_p)$, che è contenuto strettamente, ovvero $\rho$ non è surgettiva, in $\prod Aut(\mathbb{F}_{p^n}/\mathbb{F}_p)$ infatti in quest'ultimo gruppo vi sono anche le successioni che non rispettano le proprietà della restrizione. □

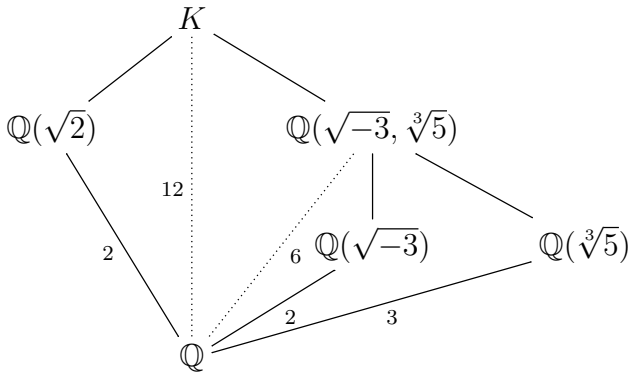
Facciamo ora alcuni esercizi.

**Esercizio 54.** Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$.

Proviamo che è di Galois su $\mathbb{Q}$, troviamone il gruppo di Galois e le sotto-estensioni normali.

$K$ sarà sicuramente contenuto nel campo di spezzamento di $f(x) = (x^3 - 5)(x^2 - 2)(x^2 + 3)$. Ma vediamo che abbiamo già in $K$ tutte le sue radici, infatti $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, è tale che $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

Allora $K$ è di Galois, in quanto campo di spezzamento di $f(x)$.




Costruiamo il diagramma partendo dalle due estensioni quadratiche, e poi quella di grado 3. Quest'ultima non è di Galois, ma $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ lo è ed è di grado 6 per fatti noti. Osserviamo che $[K : \mathbb{Q}] = 12$ in quanto $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5}) = \mathbb{Q}$:

Concludiamolo studiando il gruppo di Galois di $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ su $\mathbb{Q}$. Ha ordine 6 e sappiamo che ha una sotto-estensione non normale, dunque non abeliano, quindi è $\mathcal{S}_3$. Ma allora ha un unico sottogruppo di indice 2, quindi un'unica sotto-estensione di grado 2 su $\mathbb{Q}$, cioè il campo fisso di tale sottogruppo. É

allora quella che avevamo già trovato $\mathbb{Q}(\sqrt{-3})$. Quindi l'intersezione può avere grado 1 o 2 su $\mathbb{Q}$. Se avesse grado 2, allora $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ e dunque sarebbe uguale a $\mathbb{Q}(\sqrt{-3})$, ma questo è assurdo. Dunque può avere solo grado 1, cioè l'intersezione è solo $\mathbb{Q}$.

Inoltre per cose viste nelle lezioni precedenti

$$Gal(K/\mathbb{Q}) \cong Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times Gal(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathcal{S}_3$$

Troviamone dei generatori espliciti.

Il primo $\mathbb{Z}_2 \times \{ Id \}$ è generato da

$$\tau : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \zeta_3 \mapsto \zeta_3 \end{cases}$$

Il secondo gruppo $\{ Id \} \times \mathcal{S}_3$ è generato da

$$\sigma : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{5} \mapsto \zeta_3 \sqrt[3]{5} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \quad \text{e } \rho : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \zeta_3 \mapsto \zeta_3^{-1} \end{cases}$$

Osserviamo che è importante definire gli automorfismi su TUTTI i generatori del campo.

Osserviamo che sono corretti in quanto hanno i campi fissi che ci aspettiamo.

Chi sono ora le sotto-estensioni di $K$? Cerchiamo i sottogruppi normali di $\mathbb{Z}_2 \times \mathcal{S}_3$. Ordiniamoli:

1. Di ordine 1, abbiamo l'identità $\{ Id \} \times \{ Id \}$;
2. Di ordine 2, abbiamo solo $\mathbb{Z}_2 \times \{ Id \}$;
3. Di ordine 3, abbiamo solo $\{ Id \} \times A_3$, unico in quanto 3-Sylow normale;
4. Di ordine 6, vanno bene $\{ Id \} \times \mathcal{S}_3$ e $\mathbb{Z}_2 \times A_3$. Osserviamo che cercare tale sottogruppo equivale a contare i kernel di omomorfismi surgettivi su $\mathbb{Z}_2$ e da questo emerge che ce n'è un terzo: $< \tau\rho, \sigma > \cong \mathcal{S}_3$. In sostanza emerge che $\{ Id \} \times \mathcal{S}_3$ non è un sottogruppo caratteristico.
5. Di ordine 12, tutto.

I relativi campi fissati sono:

1. $K$;
2. $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$;
3. $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$;
4. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-6})$;
5. $\mathbb{Q}$.

**Esercizio 55.** Prendiamo il campo di spezzamento di $x^8-2$ su $\mathbb{Q}$, chiamiamolo $K$.

Cerchiamone il gruppo di Galois $G$, i generatori e la cardinalità. Inoltre mostriamo che $G$ contiene due elementi

$$\theta : \begin{cases} \alpha \mapsto \zeta\alpha \\ ß \mapsto i \end{cases} \quad \text{e } \sigma : \begin{cases} \alpha \mapsto \alpha \\ i \mapsto -i \end{cases}$$

Troviamo i campi fissi dei generati di $\theta$, $\theta^2$, $\theta^4$ e $\sigma$ e il campo fisso di $< \theta^4, \sigma >$.

Dire se $K = \mathbb{Q}(\sqrt[8]{2}, \zeta_8)$.

# Capitolo 18

# Venerdì 16 Dicembre, parte 1

*Descrizione UniMap*

**Esercizio 56.** Sia $K$ un campo finito e $\alpha$, $\beta$ elementi algebrici su $K$ di grado rispettivamente 5 e 4. Ci chiediamo che grado abbia $\alpha\beta$.

Supponiamo $K = \mathbb{F}_q$ con $q = p^a$.

Allora $K(\alpha)$ ha $q^5$ elementi e ha come elementi tutte e sole le radici di $x^{q^5} = x$; mentre $K(\beta)$ ha $q^4$ elementi che sono tutte e sole le radici di $x^{q^4} = x$.

Osserviamo che $\alpha\beta \in K(\alpha, \beta)$ di grado 20 (per torri di estensioni) e quindi starà in un campo intermedio fra $K$ e $K(\alpha, \beta)$ di grado su $K$ che divide 20: $1, 2, 4, 5, 10, 20$.

Se stesse in un'estensione di grado 4, allora starebbe in $K(\beta) = \mathbb{F}_{q^4}$, ma allora $\alpha \in K(\beta)$. Assurdo per gradi, e analogamente escludiamo 5. (Controlla l'unicità a partire dal gruppo di Galois)

$\alpha\beta \in \mathbb{F}_{q^{10}}$? Contiene $\beta$, ma allora anche $\alpha$. Ancora assurdo.

Dunque $K(\alpha\beta) = K(\alpha, \beta)$ di grado 20 su $K$.

Osserviamo che questa tesi si estende a quando i gradi di $\alpha$ e $\beta$ sono coprimi.

**Esercizio 57** (Costruzioni con riga e compasso)**.** Come si interseca una retta con una circonferenza in $\mathbb{Q}^2$? Ovvero le soluzioni di

$$\begin{cases} x^2 + y^2 = 1 \\ x - y = 0 \end{cases}$$

non ce ne sono chiaramente.

Se estendessimo?

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ fx + gy + h = 0 \end{cases}$$

Per avere delle radici qui mi serve un'estensione di grado 2.

Se invece cerchiamo l'intersezione di due circonferenze, osserviamo che se sottraiamo la prima alla seconda ritorniamo al secondo caso

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + fx + gy + h = 0 \end{cases}$$

e troviamo le soluzioni in $\mathbb{Q}(\Delta)^2$

Usando riga e compasso possiamo fare tutte le estensioni quadratiche. Tradotto vuol dire che se abbiamo un campo $F$ a caratteristica 0 e in $F^2$ interseco due circonferenze, due rette (questa a dire il vero già c'è in $F^2$), o retta e circonferenza, i punti di intersezione sono contenuti in un'estensione di grado 2.

Dunque, a meno di iterare, un'estensione di grado complessivo $2^n$.

Se ora consideriamo seno e coseno di particolare angoli, vediamo in che estensioni finiamo.

Sia $\alpha = cos(20°)$. Sappiamo che sviluppando

$$(cos(\vartheta) + isin(\vartheta))^3$$

otteniamo che $cos(3\vartheta) = cos^3(\vartheta) - 3(1 - cos^2(\vartheta))cos(\vartheta)$ e dunque nel nostro caso

$$\frac{1}{2} = cos(60°) = 4cos^3(\vartheta) - 3cos(\vartheta)$$

ovvero $\alpha$ risolve $x^3 - 3x - \frac{1}{2}$ polinomio irriducibile su $\mathbb{Q}$ di grado 3 e dunque non può stare in nessuno dei campi trovati col procedimento di prima, mediante riga e compasso.

Tradotto, non posso trisecare con riga e compasso un angolo.

Analogamente se volessi fare un $n$-agono regolare con $n$ primo, avremmo bisogno del seno e del coseno di $\vartheta = \frac{360}{n}$, ma allora con $i$ avrei la radice $n$-esima dell'unità. Siccome $i$ ha grado pari, l'estensione ha grado $n - 1$, ma allora riesco a costruire l'$n$-agono solo se $n - 1$ è una potenza di 2, ovvero se $n$ è un primo di Fermat.

# Parte III

# Complementi

# Capitolo 19

# Venerdì 16 Dicembre, parte 2

Spiegazione ultimo capitolo dispense Gaiffi.

Consideriamo $\mathbb{P}(K)$ lo spazio proiettivo di dimensione 1 con l'usuale relazione vista a $G2$.

Sia $K$ un campo finito, dunque sarà di cardinalità $p$ e $\mathbb{P}(\mathbb{F}_p)$ avrà cardinalità $p+1$, elenchiamo i suoi elementi. (vedi dispense)

Dentro il prodotto cartesiano finito di un insieme finito $X^n$, gode di una notazione particolare lo spazio di quelle costituite da elementi tutti distinti: lo definiamo *spazio delle configurazioni* e lo denotiamo

$$Conf_n(X)$$

Consideriamo $Conf_n(\mathbb{P}(K))$.

Se la cardinalità di $\mathbb{P}(K)$ è minore di $n$ evidentemente non posso costituire tale insieme, dunque $Conf_n(K) = \emptyset$, altrimenti se è uguale a $n$ ha proprio $n!$ elementi.

Questo spazio si rivela abbastanza adatto a subire l'azione di $\mathcal{S}_n$, che ne permuta le coordinate. Tuttavia nello spazio proiettivo, possiamo far agire non $\mathcal{S}_n$, ma $PGL(K)$ ovvero le proiettività di $K$ cioè le trasformazioni del proiettivo indotte da $K^2 \to K^2$ invertibile, che passa al proiettivo: sia $\phi \in GL_2(K)$

$$\begin{array}{ccc} K^2 - \{0\} & \xrightarrow{\phi} & K^2 - \{0\} \\ \downarrow & & \downarrow \\ \mathbb{P}(K) & \xrightarrow{\overline{\phi}} & \mathbb{P}(K) \end{array}$$

**Proposizione 25.** *Una proiettività $\mathbb{P}(K) \to \mathbb{P}(K)$ è univocamente determinata una volta fissate le immagine di* 0, 1 *e* $\infty$.

*Dimostrazione.* Vogliamo dire che fissati $P_1$,$P_2$ e $P_3 \in \mathbb{P}(K)$ esiste un'unica $\phi \in PGL(K)$ tale che $\phi(0) = P_1$, $\phi(1) = P_2$ e $\phi(P_3) = \infty$.

Tutto questo per studiare questo particolare quoziente:

$$\mathcal{M}_n(K) = Conf_n(\mathbb{P}(K))/PGL(K)$$

cioè $p-upla \sim p-upla$ se e solo se $\exists \phi \in PGL(K)$ tale $\phi(p-upla) = p-upla$.

Sfruttando la proposizione 25, contiamone la cardinalità. Possiamo infatti considerare per ciascuna classe un rappresentante del tipo $(0, 1, \ldots, \infty)$ infatti esiste sicuramente una proiettività che mi manda in una cosa del genere ogni altro rappresentante.

L'azione di $\mathcal{S}_6$ su $Conf_6(\mathbb{P}(\mathbb{F}_5))$ preserva le classi di equivalenza della relazione rispetto a $PGL(\mathbb{F}_5)$ e quindi induce un'azione sul quoziente $\mathcal{M}_n(K)$. Verifichiamolo: basta vedere che $\forall P = (p_1, p_2, \ldots, p_n)$, $\phi \in PGL(K)$ e $\sigma \in \mathcal{S}_6$ e verifichiamo che $\sigma(\phi(P)) = \phi(\sigma(P))$ e dunque $\mathcal{S}_6$ preserva le classi di equivalenza.

Abbiamo una azione $\vartheta : \mathcal{S}_6 \to Big(\mathcal{M}_n(K)) = \mathcal{S}_6$.

Rielenchiamo gli elementi di $\mathcal{M}_n(K)$, ovvero le orbite: siano $L_1$, ..., $L_6$.

Osserviamo che

$$(3\ 4) \begin{cases} L_1 \mapsto L_2 \\ L_2 \mapsto L_1 \\ L_3 \mapsto L_4 \\ L_4 \mapsto L_3 \\ L_5 \mapsto L_6 \\ L_6 \mapsto L_5 \end{cases}$$

ovvero $\vartheta : (3\ 4) = (1\ 2)(3\ 4)(5\ 6) \in \mathcal{S}_6 = Big(\mathcal{M}_n(K))$ cioè abbiamo trovato un omomorfismo di gruppi che ha mandato un 2-ciclo nel prodotto di 3 2-cicli.

Inoltre $\vartheta$ è iniettivo, infatti $Ker(\theta) \cap A_6$ o è uguale a $A_6$, o $\{ Id \}$. Se fosse $A_6$, o lo contenesse allora l'immagine avrebbe al più 2 elementi. Ma osserviamo che $Id$, (3 4) e (4 5) hanno immagini diverse e non sono nel nucleo, dunque ha intersezione banale. Supponiamo contenga una permutazione dispari, il cui quadrato essendo pari sta in $A_6$ e dunque nell'intersezione che è l'identità. Allora $\sigma$ è un 2-ciclo o un 3-2-ciclo. Blabla.

Quindi è bigettivo ed esterno in quanto non preserva la decomposizione in cicli (manda un 2-ciclo nel prodotto di 3 2-cicli).

Dunque si può provare che tutti gli automorfismi esterni sono del tipo

$$\left\{ \vartheta^i \phi \mid \phi \in Int(\mathcal{S}_6),\ i = 0, 1 \right\}$$