Complementi di Algebra 1

APPUNTI DEL CORSO DI ALGEBRA 1 TENUTO
DALLA PROF.SSA DEL CORSO E DAL PROF. LOMBARDO

Gabriel Antonio Videtta
g.videtta1@studenti.unipi.it
Università di Pisa

Leonardo Migliorini
l.migliorini@studenti.unipi.it
Università di Pisa

Anno Accademico 2022-23

Indice

Premessa

Le seguente dispense sono una rielaborazione delle lezioni del corso di Algebra 1 tenuto dalla prof.ssa Del Corso e dal prof. Lombardo nell'anno accademico 2022-23, con alcune aggiunte relative all'anno accademico 2023-24. **Queste dispense non sono state revisionate dai suddetti professori**.

In particolare, queste dispense contengono soltanto gli appunti delle lezioni complementari del prof. Lombardo (per le note delle lezioni della professoressa Del Corso si rimanda agli Appunti di Algebra 1). Gli argomenti sono pressoché ordinati secondo il programma del corso. Chiunque volesse aiutare a migliorare questi appunti può farlo segnalando eventuali errori e/o imprecisioni alle mail dei due autori.

Con il simbolo della stella ($\star$) si classificano le sezioni di queste dispense che sono considerate generalmente opzionali e che sono state inserite per mettere per iscritto la risoluzione di alcuni esercizi proposti dal prof. Lombardo, alcune curiosità affrontate a lezione o alcuni esercizi proposti all'esame orale.

Ringraziamenti

Si ringraziano Diego Monaco, Niccolò Nannicini, Pietro Crovetto, Leonardo Alfani, Daniele Lapadula, Francesco Sorce, Alessandro Moretti, Matteo Gori, Lorenzo Bonetti e **Rubens Martino**.

§1 Gruppi

§1.1 Insiemi di generatori

Definizione 1.1. Dati un gruppo G e un sottinsieme X di G, definiamo il **sottogruppo generato** da X come il più piccolo sottogruppo $\langle X \rangle$ di G contenente X, ovverosia:

$$\langle X \rangle = \bigcap_{\substack{H \leqslant G \\ X \subseteq H}} H$$

Se X è finito e i suoi elementi sono $x_1, \ldots, x_n$, si scrive $\langle x_1, \ldots, x_n \rangle$ per indicare $\langle X \rangle$.

Osservazione 1.2 — La definizione è ben posta dal momento che l'intersezione avviene su una famiglia non vuota di insiemi dacché G è un sottogruppo contenente X. Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi di X.

Si osserva inoltre che se $X = \varnothing$, allora $\langle X \rangle = \{e_G\}$, il sottogruppo banale di G.

La definizione data non dà direttamente informazioni sulla struttura degli elementi di $\langle X \rangle$. Detto X^{-1} l'insieme degli inversi degli elementi di X, caratterizziamo dunque tale sottogruppo tramite la:

Proposizione 1.3

Dati un gruppo G e X sottinsieme non vuoto di G, allora vale che:

$$\langle X \rangle = \{x_1 \cdots x_r \mid r \in \mathbb{N},\, x_i \in X \cup X^{-1}\ \forall 1 \leq i \leq r\}$$

Dimostrazione. Si mostra innanzitutto che l'insieme del secondo membro, indicato con S, è un sottogruppo di G. Preliminarmente, si verifica che S non è vuoto, dal momento che X non lo è. Inoltre ogni elemento di S ammette un inverso, infatti $(x_1 \cdots x_r)^{-1} = x_r^{-1} \cdots x_1^{-1}$ è ancora un elemento di S. Allo stesso modo, il prodotto di elementi di S è ancora un elemento di S. Pertanto S è un sottogruppo di G.

Sia H un sottogruppo di G contenente X. Allora H contiene ogni prodotto finito di $X \cup X^{-1}$, e quindi S. Si conclude dunque che $\langle X \rangle = S$, da cui la tesi. □

Osservazione 1.4 — Si osserva facilmente che un sottogruppo ciclico H di G è un suo sottogruppo per cui esiste $x \in H$ tale per cui $H = \langle x \rangle$.

Definizione 1.5. Sia G un gruppo. Se X è un sottinsieme non vuoto di G tale per cui $G = \langle X \rangle$, allora si dice che X **genera** G, che X è un **insieme di generatori** per G e che gli elementi di X sono **generatori** per G.

§1.2 Gruppi liberi e presentazioni

Definizione 1.6. Si definisce il **gruppo libero** su n generatori il gruppo F_n tale per cui:

$$F_n = \langle x_1, \ldots, x_n \rangle = \{x_{i_1}^{\pm 1} \cdots x_{i_k}^{\pm 1} \mid i_j \in \{1, \ldots, n\},\, k \in \mathbb{N}\}/\sim$$

dove[1] $a \sim b$ se e solo se eliminando le scritture $x_i x_i^{-1}$ o $x_i^{-1} x_i$ da a e b si ottengono in successione gli stessi simboli. L'operazione di questo gruppo è la concatenazione (ossia il prodotto tra x_i e x_j è per definizione $x_i x_j$) e la stringa vuota è per definizione l'identità, indicata con e. Per convenzione si denota $x \cdots x$ ripetuto k volte come x^k e si pone $x^{-k} := (x^{-1})^k$, facendo valere le usuali proprietà delle potenze.

Osservazione 1.7 (Costruzione del gruppo $F(S)$) — In generale, dato un insieme S, si definisce il gruppo libero $F(S)$ come il gruppo libero ottenuto dalle scritture finite di S a meno di equivalenza per $\sim$. Se S è finito e $|S| = n$, allora $F(S) \cong F_n$, dove l'isomorfismo è costruito mandando ordinatamente i generatori di $F(S)$ in $x_1, \ldots, x_n$.

Per i gruppi liberi vale la **proprietà universale**, ossia $\mathrm{Hom}(F_n, G)$ è in bigezione con G^n tramite la mappa che associa un omomorfismo φ alla n-upla $(\varphi(x_1), \ldots, \varphi(x_n))$, la cui inversa associa una n-upla $(g_1, \ldots, g_n)$ ad un unico omomorfismo tale per cui $\varphi(x_i) = g_i$. Questi gruppi, infatti, non presentano alcuna relazione tra i propri generatori, e dunque gli omomorfismi presentati sono sempre ben definiti.

Definizione 1.8. Si dice che un gruppo G ammette una **presentazione** se esiste un insieme S di generatori di G e un sottoinsieme R di $F(S)$ tale per cui:

$$G \cong F(S)/N$$

dove N è il più piccolo sottogruppo normale di $F(S)$ contenente R, ossia la *chiusura normale* di R. In particolare G ammette una *presentazione finita* se S e R sono finiti.

Se G ammette una presentazione, allora esiste un omomorfismo surgettivo $\varphi : F(S) \to G$ tale per cui φ ristretto a S sia l'identità[2] e per cui $\ker \varphi = N$.

In tal caso, è decisamente più facile descrivere gli omomorfismi da G a un qualsiasi altro gruppo H. Infatti, poiché $G \cong F(S)/N$, esiste una bigezione, secondo il Primo Teorema di Omomorfismo, tra $\mathrm{Hom}(G, H)$ e gli omomorfismi di $\mathrm{Hom}(F(S), H)$ tali per cui N sia contenuto nel nucleo; affinché N sia contenuto nel nucleo è però sufficiente vi sia contenuto R, dacché N è la chiusura normale di R. Pertanto R rappresenta in un certo senso un insieme di "relazioni tra i generatori" che devono essere rispettate affinché l'omomorfismo sia ben definito, e così si dice che R è l'insieme dei **relatori** di G. Si scrive allora la presentazione di G come:

$$G \cong F(S)/N = \langle S \mid R \rangle$$

Talvolta per R si scrive un insieme di identità $a_1 = b_1$, sottintendendo che $a_1 b_1^{-1}$ appartiene ad R.

[1] Si verifica facilmente che la relazione $\sim$ è di equivalenza.
[2] A livello astratto S in $F(S)$ è solo una scrittura simbolica, quello che si intende è che si associa al simbolo $s \in S$ l'effettivo elemento s in G.

Esempio 1.9

Si illustrano alcuni esempi di presentazione:

- $\mathbb{Z} \cong \langle x_1 \rangle = F_1$
- $\mathbb{Z}/n\mathbb{Z} \cong \langle x \mid x^n = e \rangle$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle x, y \mid x^2 = y^2 = e, [x, y] = e \rangle$
- $(\mathbb{Z}/2\mathbb{Z})^3 \cong \langle x, y, z \mid x^2 = y^2 = z^2 = e, [x, y] = [y, z] = [z, x] = e \rangle$
- $\mathrm{D}_n \cong \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle$

§1.3 Automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$

Dato p un primo, vogliamo determinare quanti sono gli automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$, un p-gruppo abeliano elementare. Per fare ciò è conveniente osservare che $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ è un campo e che $(\mathbb{Z}/p\mathbb{Z})^n$ è dunque uno spazio vettoriale, dove il prodotto per scalari $\cdot : \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^n$ è tale per cui:

$$(\overline{\lambda}, v) \longmapsto \overline{\lambda} v$$

con $\overline{\lambda} v = \underbrace{v + \ldots + v}_{\tilde{\lambda} \text{ volte}}$ e $\tilde{\lambda}$ un qualsiasi rappresentante di $\overline{\lambda}$.

Tale prodotto è ben definito. Se infatti $\lambda, \lambda' \in \mathbb{Z}$ sono tali per cui $\overline{\lambda} = \overline{\lambda'}$, cioè esiste $k \in \mathbb{Z}$ tale che $\lambda = \lambda' + kp$, allora

$$\overline{\lambda'} v = \underbrace{v + \ldots + v}_{\lambda' \text{ volte}} = \underbrace{v + \ldots + v}_{\lambda + kp \text{ volte}} = \underbrace{v + \ldots + v}_{\lambda \text{ volte}}$$

Per come abbiamo è definito il prodotto per scalari su $(\mathbb{Z}/p\mathbb{Z})^n$, si osserva che per ogni $\varphi \in \operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ vale che $\varphi(\lambda v) = \lambda \varphi(v)$ per ogni $\lambda \in \mathbb{Z}/p\mathbb{Z}$. Pertanto vale la seguente uguaglianza insiemistica

$$\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = \operatorname{GL}((\mathbb{Z}/p\mathbb{Z})^n) = \{\varphi : (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \mid \varphi \text{ isomorfismo di sp. vett.}\}$$

Poiché $\operatorname{GL}((\mathbb{Z}/p\mathbb{Z})^n) \cong \operatorname{GL}_n(\mathbb{Z}/p\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z}) \mid \det M \neq 0\}$, possiamo rappresentare ogni automorfismo di $(\mathbb{Z}/p\mathbb{Z})^n$ con una matrice invertibile di taglia $n \times n$ a coefficienti in $\mathbb{Z}/p\mathbb{Z}$.

Proposizione 1.10
Dato p un primo, allora

$$\left|\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)\right| = \prod_{i=0}^{n-1} (p^n - p^i)$$

Dimostrazione. Osserviamo che un elemento di $\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ deve necessariamente mandare una base di $(\mathbb{Z}/p\mathbb{Z})^n$ in un'altra base, e si determina univocamente in questo modo. Sia $\{v_1, \ldots, v_n\}$ una base di $(\mathbb{Z}/p\mathbb{Z})^n$ e sia $\varphi \in \operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$. Consideriamo $\varphi(v_1)$: $\varphi(v_1)$ può assumere qualsiasi valore non nullo, pertanto abbiamo $(p^n - 1)$ possibilità per la sua immagine. Per quanto riguarda v_2, $\varphi(v_2)$ può assumere qualsiasi valore non nullo che non sia multiplo di $\varphi(v_1)$, e quindi $p^n - p$ valori. Analogamente $\varphi(v_3)$ può assumere qualsiasi valore non nullo che non appartenga a $\operatorname{Span}(\varphi(v_1), \varphi(v_2))$, che consta di p^2 elementi, e così via. Iterando questo ragionamento fino a $\varphi(v_n)$, che può essere scelto in $p^n - p^{n-1}$ modi, si ottiene la tesi. $\square$

§1.4 Gruppo diedrale

§1.4.1 Elementi del gruppo

Definizione 1.11. Dato $n \geq 3$ un numero naturale, si può considerare un poligono regolare di n vertici centrato nell'origine del piano $\mathbb{R}^2$. Si definisce il **gruppo diedrale** su n vertici, detto D_n, come il gruppo delle isometrie[3] di $\mathbb{R}^2$ che fissano il poligono, cioè che mandano i vertici in se stessi. Per $n = 2$, si definisce D_2 come il gruppo delle isometrie che mandano un segmento in se stesso.

Osservazione 1.12 — D_n è un gruppo, in quanto l'applicazione identità che fissa tutti i vertici è un'isometria dal poligono in se stesso, la composizione di isometrie è un'isometria e un'isometria ammette sempre un'inversa[a], che è anch'essa un'isometria.

[a] In particolare, D_n si immerge sempre in $\mathrm{O}(2)$, il gruppo delle matrici ortogonali di taglia 2×2 a coefficienti in $\mathbb{R}$, dal momento che queste rappresentano esattamente le isometrie del piano. Una matrice M di $\mathrm{O}(2)$ è tale per cui $MM^\top = M^\top M = I_2$, e quindi $\det(M) \in \{\pm 1\}$. In particolare M è invertibile, e la sua inversa appartiene ancora a $\mathrm{O}(2)$.

Osservazione 1.13 — Una rotazione di angolo[a] $\frac{2\pi}{n}$ è un elemento di D_n, così come una simmetria rispetto a un asse.

[a] Per convenzione, indichiamo con un angolo positivo una rotazione in senso antiorario e con un angolo negativo una rotazione in senso orario.

Proseguendo con questa intuizione geometrica, indicheremo con r una rotazione di angolo $\frac{2\pi}{n}$ e con s una simmetria rispetto a un qualsiasi asse. Si osserva facilmente che $\mathrm{ord}(r) = n$ e $\mathrm{ord}(s) = 2$.

Definizione 1.14. Data $r \in \mathrm{D}_n$ una rotazione di ordine n, indichiamo con $\mathcal{R}$ il **sottogruppo delle rotazioni** $\langle r \rangle$.

Osservazione 1.15 — Il sottogruppo $\mathcal{R}$ contiene tutte le rotazioni di D_n. Se infatti r' è una rotazione di angolo $\frac{2k\pi}{n}$ con $k \in \mathbb{Z}$, allora $r^k = r'$, e quindi $r' \in \mathcal{R}$.

Inoltre, $\mathcal{R}$ si immerge in $\mathrm{SO}(2)$, il gruppo delle matrici ortogonali speciali, ossia delle matrici ortogonali con determinante 1. Se infatti r è un elemento di $\mathcal{R}$, r è rappresentato da una matrice della seguente forma

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

che ha infatti come determinante $\cos^2(\theta) + \sin^2(\theta) = 1$.

Per determinare come sono fatti gli elementi di D_n, studiamo il sottogruppo $\langle r, s \rangle$. Sicuramente $\langle r, s \rangle$ contiene il sottogruppo $\mathcal{R}$ e tutti gli elementi della forma sr^k, $sr^k s$, $sr^k sr^h$, e così via. Vogliamo mostrare che in effetti D_n è generato da r e s.

[3] In particolare tutte queste isometrie sono lineari, dal momento che devono mappare l'origine in se stessa.

Osservazione 1.16 — Gli elementi della forma r^k e sr^h sono distinti per ogni $h, k \in \mathbb{Z}$. Infatti, presi come elementi di base di $\mathbb{R}^2$ un vettore v_1 che giace sull'asse di simmetria di s e un vettore v_2 perpendicolare ad esso, s si rappresenta in tale base come la matrice

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

e quindi s corrisponde a una matrice di determinante -1. In particolare, $\det : \mathrm{O}(2) \to \{\pm 1\}$ è un omomorfismo di gruppi tale per cui $\ker \det = \mathrm{SO}(2)$, in cui si immerge $\mathcal{R}$. In particolare, per il Primo Teorema di Omomorfismo vale che

$$\mathrm{O}(2) \big/ \mathrm{SO}(2) \cong \{\pm 1\}$$

e quindi esistono solo due classi laterali di $\mathrm{O}(2) \big/ \mathrm{SO}(2)$.

In particolare ogni simmetria della forma sr^k si identifica come elemento di $s\,\mathrm{SO}(2) \neq \mathrm{SO}(2)$. Dal momento allora che $\det(r^k) = 1$ e $\det(sr^h) = -1$, questi elementi sono distinti.

Lemma 1.17

Per ogni rotazione $r \in \mathrm{D}_n$ e per ogni simmetria $s \in \mathrm{D}_n$ vale

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

Dimostrazione. Senza perdita di generalità possiamo supporre che r sia la rotazione di angolo $\frac{2\pi}{n}$ e che s sia la simmetria (rispetto all'asse y) che a ogni punto x del piano associa il punto $-x$. Possiamo rappresentare rispettivamente r e s tramite le matrici

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

Svolgendo esplicitamente il prodotto si ottiene quindi che

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

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

che è la matrice associata alla rotazione di angolo $-\frac{2\pi}{n}$, cioè r^{-1}. $\square$

Proposizione 1.18

Se $n \geq 3$ allora $|\mathrm{D}_n| = 2n$.

Dimostrazione. Indicando con 0, ..., $n-1$ i vettori degli n vertici di un poligono regolare di n lati, notiamo che un elemento $g \in \mathrm{D}_n$ è univocamente determinato da $g(0)$ e $g(1)$, rappresentando questi una base di vettori per $\mathbb{R}^2$. Infatti 0 e 1, per $n \geq 3$, sono linearmente indipendenti. In particolare, fissato $g(0)$, per il quale abbiamo n possibili scelte, abbiamo al massimo due valori per $g(1)$, cioè $g(0)+1$ o $g(0)-1$ (opportunamente normalizzati modulo n). Pertanto possiamo determinare g in al più $2n$ modi, e quindi $|\mathrm{D}_n| \leq 2n$. Ricordando adesso che D_n contiene gli elementi della forma r^k e sr^h al variare di $h, k \in \mathbb{Z}$, mostriamo che questi sono esattamente $2n$, e dunque che generano anche D_n. Gli elementi r^k appartengono al gruppo ciclico $\mathcal{R}$ di ordine n, pertanto sono n elementi distinti, inoltre

$$sr^i = sr^j \iff r^i = r^j \iff i \equiv j \pmod n$$

e dunque anche questi sono n elementi distinti. Poiché gli insiemi $\mathcal{R}$ e $\{sr^h \mid h \in \mathbb{Z}\}$ sono disgiunti (Osservazione 1.16), si ricava che $|\mathrm{D}_n| = 2n$. □

Osservazione 1.19 — Abbiamo mostrato che effettivamente $\mathrm{D}_n = \langle r, s \rangle$, quindi i suoi elementi sono tutti della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$. In particolare gli elementi distinti di D_n sono tutti gli r^k e i sr^h con $1 \leq r, k \leq n-1$, insieme all'identità.

Osservazione 1.20 — Il risultato è valido anche per D_2, ma con motivazioni leggermente differenti. Se consideriamo il segmento nel piano $\mathbb{R}^2$ giacente sulla retta $y = 0$ che congiunge $(1,0)$ e $(-1,0)$, ogni isometria di D_2 è tale per cui e_1 può essere mappato in sé stesso o in $-e_1$, e analogamente può essere mappato anche e_2. Pertanto anche in D_2 vi sono al più $2 \cdot 2 = 4$ isometrie. Dal momento che l'identità, la rotazione di angolo π, la simmetria lungo la retta $y = 0$ e la simmetria lungo $x = 0$ sono isometrie, D_2 contiene quindi esattamente quattro elementi: l'identità e tre elementi di ordine 2. Essendo composto da $4 = 2^2$ elementi e non essendo ciclico, si conclude infine che D_2 è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong V_4$, il gruppo di Klein.

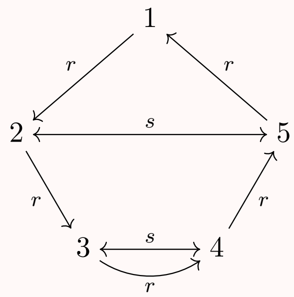
Osservazione 1.21 — Grazie a queste ultime osservazioni, possiamo finalmente svelare un legame tra D_n e $\mathcal{S}_n$. Infatti, D_n è composto dalle isometrie che *permutano* i vertici di un n-agono regolare, e quindi può associarsi iniettivamente a una permutazione di $\mathcal{S}_n$. Formalmente, D_n si immerge in $\mathcal{S}_n$ in modo del tutto naturale. In particolare, poiché $|\mathrm{D}_3| = 2 \cdot 3 = 3! = |\mathcal{S}_3|$ e $n! > 2n$ per $n \geq 4$, D_3 è l'unico gruppo diedrale isomorfo al gruppo simmetrico in cui si immerge, ovverosia $\mathcal{S}_3$.

Esempio 1.22 (Esempio di immersione di D_5 in $\mathcal{S}_5$)

Consideriamo in $\mathcal{S}_5$ gli elementi $\sigma = (1\ 2\ 3\ 4\ 5)$ e $\tau = (2\ 5)(3\ 4)$, e si ponga $H = \langle \sigma, \tau \rangle$. Si osserva che:

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

Questa relazione suggerisce il legame tra H e D_5: non è un caso; come vedremo, dal momento che $\mathrm{ord}(\sigma) = 5$ e $\mathrm{ord}(\tau) = 2$, H soddisfa tutte le relazioni della presentazione di D_5, ed è dunque isomorfo a un suo quoziente. A partire da quest'ultima identità, si ricava che $\langle \sigma, \tau \rangle = \langle \sigma \rangle \cdot \langle \tau \rangle$. Dal momento che $\langle \sigma \rangle \cap \langle \tau \rangle$ è banale, $|H| = |\langle \sigma \rangle| \cdot |\langle \tau \rangle| = 5 \cdot 2 = 10$. Pertanto H è in particolare isomorfo a D_5 stesso. Infatti H rappresenta l'immersione naturale di D_5 in $\mathcal{S}_5$ tale per cui $r \mapsto \sigma$ e $s \mapsto \tau$, come illustra il seguente schema:



§1.4.2 Sottogruppi

Consideriamo un sottogruppo $H \leqslant \mathrm{D}_n$. Distinguiamo il caso in cui $H \subseteq \mathcal{R}$ e il caso in cui $H \not\subseteq \mathcal{R}$. Nel primo caso, se $|H| = d$, vale allora che $d \mid n$ e che H è l'unico sottogruppo di $\mathcal{R}$ di ordine d, essendo $\mathcal{R}$ ciclico. In particolare varrebbe $H = \langle r^{\frac{n}{d}} \rangle$.

Studiamo ora quindi il caso in cui $H \not\subseteq \mathcal{R}$. Innanzitutto si osserva che $\mathcal{R} \trianglelefteq \mathrm{D}_n$ dal momento che $[\mathrm{D}_n : \mathcal{R}] = 2$. Pertanto $\mathrm{D}_n/\mathcal{R}$ è un gruppo, ed essendo composto da due soli elementi è isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

Consideriamo la proiezione al quoziente

$$\pi_{\mathcal{R}} : \mathrm{D}_n \longrightarrow \mathrm{D}_n/\mathcal{R} : g \mapsto g\mathcal{R}$$

Dal momento che $H \not\subseteq \mathcal{R}$, esiste $sr^h \in H$ tale per cui $sr^h \notin \mathcal{R}$, e quindi $\pi_{\mathcal{R}}(sr^h) \neq \mathcal{R}$. In particolare vale allora che $\pi_{\mathcal{R}}(H) \not\subseteq \{\mathcal{R}\}$. Allora, poiché i sottogruppi di $\mathrm{D}_n/\mathcal{R}$ sono solo $\{\mathcal{R}\}$ e $\mathrm{D}_n/\mathcal{R}$, deve valere $\pi_{\mathcal{R}}(H) = \mathrm{D}_n/\mathcal{R}$. Allora, per il Primo Teorema di Omomorfismo, vale che $\ker \pi_{\mathcal{R}|H} = \ker \pi_{\mathcal{R}} \cap H = \mathcal{R} \cap H$ è isomorfo a $\pi_{\mathcal{R}}(H) = \mathrm{D}_n/\mathcal{R} \cong \mathbb{Z}/2\mathbb{Z}$. Da quest'ultima osservazione si ricava quindi che $|H \cap \mathcal{R}| = \frac{1}{2}|H|$.

Dato che $\mathcal{R} \cap H \subseteq \mathcal{R}$, esiste $k \in \mathbb{Z}$ tale per cui $H \cap \mathcal{R} = \langle r^k \rangle$. In particolare $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono entrambi contenuti in H, e così anche $\langle r^k, sr^h \rangle$.

Proposizione 1.23

Dato $H \leqslant \mathrm{D}_n$ un sottogruppo tale per cui $H \not\subseteq \mathcal{R}$, se r è un generatore di $\mathcal{R}$ tale per cui $H \cap \mathcal{R} = \langle r^k \rangle$ e sr^h è una simmetria di H, allora

$$H = \langle r^k \rangle \cdot \langle sr^h \rangle = \{xy \mid x \in \langle r^k \rangle, y \in \langle sr^h \rangle\}$$

Dimostrazione. Per quanto visto sopra vale $|\langle r^k \rangle| = \frac{1}{2}|H|$. Inoltre si osserva facilmente che $\mathrm{ord}(sr^h) = 2$:

$$(sr^h)^2 = sr^h sr^h = (srs)^h r^h = (srs^{-1})^h r^h = r^{-h} r^h = e$$

Pertanto $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Inoltre $\langle sr^h \rangle \subseteq \mathrm{N}_{\mathrm{D}_n}(\langle r^k \rangle)$; infatti per ogni $m \in \mathbb{Z}$ vale che:

$$(sr^h) r^{mk} (sr^h)^{-1} = sr^{h+mk} sr^h = r^{-h-mk} r^h = r^{-mk} \in \langle r^k \rangle$$

Quindi $\langle r^k \rangle \cdot \langle sr^h \rangle$ è effettivamente un sottogruppo di D_n[4]. Poiché $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono contenuti in H, anche $\langle r^k \rangle \cdot \langle sr^h \rangle$ è contenuto in H. Infine si verifica che

$$|\langle r^k \rangle \cdot \langle sr^h \rangle| = \frac{1}{2}|H| \cdot 2 = |H|$$

in quanto $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$[5]. Pertanto i due sottogruppi coincidono. □

Osservazione 1.24 — Per $k \mid n$ e $0 \leq h < k$, i sottogruppi $H_{k,h} = \langle r^k, sr^h \rangle$ e $H = \langle r^k \rangle \cdot \langle sr^h \rangle$ coincidono. Infatti $H_{k,h} \subseteq H$ in quanto r^k, sr^h sono elementi di H; d'altra parte $H \subseteq H_{k,h}$ in quanto $H_{k,h}$ contiene tutti i prodotti finiti delle potenze di r^k e sr^h.

Osservazione 1.25 — Per $k \mid n$ e $0 \leq h < k$, $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$. Infatti $\langle r^k, sr^h \rangle \subseteq \langle r^k, sr^{h+k} \rangle$ in quanto $sr^h = (sr^{h+k}) r^{-k}$ è un elemento del secondo gruppo. Analogamente $\langle r^k, sr^{h+k} \rangle \subseteq \langle r^k, sr^h \rangle$ in quanto $sr^{h+k} = (sr^h) r^k$ è un elemento del primo gruppo.

Teorema 1.26 (Classificazione dei sottogruppi di D_n)
I sottogruppi di D_n sono della forma

(1) $\langle r^k \rangle$ con $k \mid n$,

(2) $\langle r^k, sr^h \rangle$ con $k \mid n$ e $0 \leq h < k$,

con $r \in \mathcal{R}$ e s una simmetria. Inoltre tali sottogruppi sono tutti distinti.

Dimostrazione. La classificazione è sicuramente completa, dal momento che ogni sottogruppo della forma $\langle r^k \rangle$ può ridursi a $\langle r^{k \bmod n} \rangle$, e analogamente $\langle r^k, sr^h \rangle$ è uguale a $\langle r^{k \bmod n}, sr^{h \bmod (k \bmod n)} \rangle$. Consideriamo $H, K \leqslant \mathrm{D}_n$ due sottogruppi, abbiamo tre casi:

- se $H = \langle r^k \rangle$ e $K = \langle r^m \rangle$ con k, $m \mid n$, allora $H = K$ se e solo se $m = k$;
- se $H = \langle r^k \rangle$ e $K = \langle r^m, sr^h \rangle$, allora H e K sono distinti dal momento che sr^h non può appartenere ad H, essendo una rotazione;

[4] Dati H, K sottogruppi di un gruppo G, se $H \subseteq \mathrm{N}_G(K)$, allora $HK = KH$, e quindi HK è un sottogruppo di G.

[5] Si ricorda che se H e K sono sottogruppi finiti di un gruppo G allora vale che $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

- se $H = \langle r^k, sr^h \rangle$ e $K = \langle r^m, sr^l \rangle$, considerando le intersezioni $H \cap \mathcal{R} = \langle r^k \rangle$ e $K \cap \mathcal{R} = \langle r^m \rangle$. Allora, se $H = K$, anche $H \cap \mathcal{R}$ è uguale a $K \cap \mathcal{R}$, e quindi $k = m$. Inoltre, sr^h deve appartenere a $K = \langle r^m, sr^l \rangle = \langle r^m \rangle \langle sr^l \rangle$, e quindi, dacché sr^h è una simmetria, esiste $t \in \mathbb{Z}$ tale per cui

$$sr^h = (r^m)^t sr^l = sr^{-mt+l}$$

da cui ricaviamo che $h \equiv l - mt \pmod{n}$, e quindi $h \equiv l \pmod{m}$; in particolare, se h e l sono minori di m, deve valere $k = l$.

Quindi la classificazione è unica e completa. □

Osservazione 1.27 (Numero di sottogruppi di D_n) — Si contano i sottogruppi di D_n a partire dal teorema precedente. I sottogruppi della forma $\langle r^k \rangle$ con $k \mid n$ sono tanti quanti i divisori di n, e quindi sono[a] $d(n) = \sigma_0(n)$. Scelto $k \mid n$, si considerano anche i sottogruppi della forma $\langle r^k, sr^h \rangle$ con $0 \leq h < k$, che quindi prevedono k scelte per il parametro h. Vi sono dunque $\sum_{k|n} k = \sigma(n) = \sigma_1(n)$ sottogruppi di questa forma. Si conclude dunque che esistono esattamente $d(n) + \sigma(n)$ sottogruppi di D_n.

[a] Con $\sigma_a(n)$ ci si riferisce alla funzione sigma.

Lemma 1.28

Dati un gruppo G e A, B due sottogruppi tali che $A \leqslant B \leqslant G$, se $B \trianglelefteq G$ e A è caratteristico in B allora $A \trianglelefteq G$.

Dimostrazione. Fissato $g \in G$, consideriamo l'omomorfismo di coniugio

$$\varphi_g : G \longrightarrow G : x \longmapsto gxg^{-1}$$

poiché $B \trianglelefteq G$ è ben definita la restrizione $\varphi_{g|B} \in \mathrm{Aut}(B)$[6]. Dal momento che A è un sottogruppo caratteristico di B abbiamo che $\varphi_{g|B}(A) = \varphi_g(A) = A$. Pertanto $A \trianglelefteq G$. □

Corollario 1.29

Ogni sottogruppo di $\mathcal{R}$ è normale in D_n.

Dimostrazione. Siano $\langle r^k \rangle$ un sottogruppo di $\mathcal{R}$ e $\varphi \in \mathrm{Aut}(\mathcal{R})$, allora $\varphi(\langle r^k \rangle) = \langle r^k \rangle$ in quanto φ preserva l'ordine dei sottogruppi e $\langle r^k \rangle$ è l'unico sottogruppo di $\mathcal{R}$ di tale ordine, dacché $\mathcal{R}$ è ciclico. Pertanto $\langle r^k \rangle$ è caratteristico in $\mathcal{R}$. Poiché $\mathcal{R}$ è un sottogruppo normale di D_n, per il Lemma 1.28 abbiamo $\langle r^k \rangle \trianglelefteq \mathrm{D}_n$. □

Osservazione 1.30 — A dire il vero, $\mathcal{R} = \langle r \rangle$ non solo è normale in D_n, ma è anche per $n \geq 3$. Infatti per ogni $\varphi \in \mathrm{Aut}(\mathrm{D}_n)$ allora $\mathrm{ord}(\varphi(r)) = \mathrm{ord}(r) = n$. Se $\varphi(r)$ non appartenesse a $\mathcal{R}$, avremmo $\mathrm{ord}(\varphi(r)) = 2$, assurdo dacché $n \geq 3$.

Questo non è vero per D_2. Sia infatti $\varphi : \mathrm{D}_2 \to \mathrm{D}_2$ l'omomorfismo univocamente determinato da

$$r \mapsto s, \quad s \mapsto r$$

[6] In generale $\varphi_{g|B}$ non è un coniugio di B, poiché g non appartiene necessariamente a B.

Tale omomorfismo è ben definito dal momento che $\varphi(s)\varphi(r)\varphi(s) = rsr = s = s^{-1} = \varphi(r^{-1})$, ed è in particolare un elemento di $\mathrm{Aut}(\mathrm{D}_2)$, dal momento che $\ker\varphi$ è banale. Si osserva inoltre che $\mathrm{Aut}(\mathrm{D}_2) \cong \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathcal{S}_3$.

Corollario 1.31

Per $k \mid n$ e $0 \leq h < k$, il sottogruppo $H_{k,h} = \langle r^k, sr^h \rangle$ è normale in D_n se e solo se $r, s \in \mathrm{N}_{\mathrm{D}_n}(H_{k,h})$.

Dimostrazione.

- Se $H_{k,h} \trianglelefteq \mathrm{D}_n$ allora $\mathrm{N}_{\mathrm{D}_n}(H_{k,h}) = \mathrm{D}_n$, e dunque $r, s \in \mathrm{N}_{\mathrm{D}_n}(H_{k,h})$;
- se $r, s \in \mathrm{N}_{\mathrm{D}_n}(H_{k,h})$, dacché il normalizzatore è un sottogruppo di D_n, si osserva che $\mathrm{D}_n = \langle r, s \rangle \subseteq \mathrm{N}_{D_n}(H_{k,h})$, e dunque che $H_{k,h} \trianglelefteq \mathrm{D}_n$.

□

Si calcolano adesso i sottogruppi normali di D_n. Come visto prima, i sottogruppi di $\mathcal{R}$ sono tutti normali. Resta da verificare quali sottogruppi di D_n sono normali tra quelli della forma $\langle r^k, sr^h \rangle$ con $k \mid n$ e $0 \leq h \leq k-1$. Sia H un tale sottogruppo. Allora, per il corollario precedente, H è normale se e solo se $rHr^{-1} = H$ e $sHs^{-1} = H$.

Si verifica facilmente che $rHr^{-1} = r\langle r^k, sr^h \rangle r^{-1} = \langle r^k, rsr^{h-1} \rangle = \langle r^k, sr^{h-2} \rangle$. Quest'ultimo sottogruppo è uguale ad H se e solo se $h - 2 \equiv h \pmod{k}$, e quindi se e solo se $k \mid 2$. Pertanto k è uguale ad 1 o 2. Per $k = 1$, l'unico sottogruppo considerato è $\langle r, s \rangle = \mathrm{D}_n$, che è banalmente normale.

Si considera d'ora in poi il caso $k = 2$. Dal momento che $k \mid n$, questo implica che n sia pari. Pertanto, se n è dispari, non esistono sottogruppi normali che non siano sottogruppi di $\mathcal{R}$ o che non siano D_n stesso. Si applica il coniugio ad H tramite la simmetria s: $sHs^{-1} = s\langle r^2, sr^h \rangle s^{-1} = \langle r^{-2}, s^2r^hs \rangle = \langle r^2, sr^{-h} \rangle$. Quest'ultimo sottogruppo è uguale ad H se e solo se $-h$ è congruo ad h modulo 2, e quindi sempre. Pertanto, per n pari, sono sottogruppi normali anche $\langle r^2, sr \rangle$ e $\langle r^2, s \rangle$.

Si riassume la classificazione dei sottogruppi normali di D_n nella seguente lista:

- se n è dispari, i sottogruppi normali di D_n sono D_n stesso, $\{\mathrm{id}\}$ e i sottogruppi di $\mathcal{R}$,
- se n è dispari, sono sottogruppi normali di D_n i sottogruppi elencati nel caso in cui n sia pari insieme a $\langle r^2, sr \rangle$ e $\langle r^2, s \rangle$.

Osservazione 1.32 — I sottogruppi aggiuntivi che appaiono nel caso in cui n sia pari corrispondono al fatto che in un poligono con un numero pari di lati gli assi di simmetria sono per metà passanti per i lati e metà passanti per i vertici opposti. Al contrario, per un poligono con un numero dispari di lati gli assi di simmetria sono tutti passanti per i lati.

§1.4.3 Classi di coniugio

Consideriamo la classe di coniugio di r^h. Chiaramente ogni elemento di $\mathcal{R}$ commuta con r^h e dunque stabilizza r tramite l'azione di coniugio. Se si considera invece sr^k con $0 \leq k \leq n-1$, allora si verifica che $sr^k r^h (sr^k)^{-1} = sr^k r^h r^{-k} s = sr^h s = r^{-h}$. Pertanto $\mathcal{C}\ell(r^h) = \{r^h, r^{-h}\}$. In particolare $\mathcal{C}\ell(r^h)$ ha sempre due elementi distinti, a meno che $r^h = r^{-h}$. Quest'ultima identità si verifica solo nel caso in cui $r^{2h} = \mathrm{id}$, e quindi se e solo se

$$\frac{n}{(n,h)} = 2$$

da cui si osserva facilmente che n deve essere pari. In tal caso, detto $n = 2m$, vale che

$$\frac{2m}{(2m,h)} = 2 \iff \frac{m}{(2m,h)} = 1 \iff m = (2m,h)$$

e quindi m deve dividere h. Dal momento che $h \leq n-1 = 2m-1$, deve per forza valere $h = m$, e quindi $h = \frac{n}{2}$. Se dunque n è pari, $\mathcal{C}\ell(r^{\frac{n}{2}})$ è composta da un singolo elemento e quindi $r^{\frac{n}{2}}$ appartiene a $\mathrm{Z}(\mathrm{D}_n)$.

Osservazione 1.33 — Se n è pari, $r^{\frac{n}{2}}$ rappresenta la rotazione di 180°, che commuta con ogni isometria del piano. Infatti, nella base canonica di $\mathbb{R}^2$, tale rotazione è rappresentata dalla matrice $-I_2$, che commuta con ogni matrice di $\mathcal{M}_2(\mathbb{R})$.

Consideriamo adesso la classe di coniugio di sr^h. Si verifica facilmente che $r^k sr^h r^{-k} = sr^{h-2k}$ e che $sr^k sr^h sr^k = s^2 r^{h-k} sr^k = sr^{2k-h}$. Pertanto vale che

$$\mathcal{C}\ell(sr^h) = \{sr^{h-2k}, sr^{2k-h} \mid k \in \mathbb{Z}\}$$

I due elementi elencati rappresentano in realtà la stessa sequenza di esponenti, dal momento che $h - 2(h-k) = 2k - h$. Quindi vale che

$$\mathcal{C}\ell(sr^h) = \{sr^{h-2k} \mid k \in \mathbb{Z}\}$$

Osservazione 1.34 — Si studiano le simmetrie di $\mathcal{C}\ell(sr^h)$. La simmetria sr^t appartiene a $\mathcal{C}\ell(sr^h)$ se e solo se $x \in \mathbb{Z}$ tale per cui $sr^{h-2x} = sr^t$ e quindi se e solo se $h - 2x \equiv t \pmod{n}$. Quest'ultima equazione è equivalente a $2x \equiv h - t \pmod{n}$ ed ha soluzione se e solo se $(2,n) \mid h-t$. Se n è dispari, tale equazione ha sempre soluzione, se invece n è pari, $(2,n)$ è uguale a 2 e quindi $sr^t \in \mathcal{C}\ell(sr^h)$ se e solo se t ha la stessa parità di h.

Riassumendo, se n è dispari, $\mathcal{C}\ell(sr^h) = \mathrm{D}_n \setminus \mathcal{R}$ e dunque contiene tutte le simmetrie; se invece n è pari, $\mathcal{C}\ell(sr^h)$ contiene solo le simmetrie sr^t con $t \equiv h \pmod{2}$. Geometricamente questo è equivalente a osservare che, se n è dispari, tutti gli assi di simmetria passano per i vertici (e dunque appartengono alla stessa classe) e che, se n è pari, vi sono due classi di assi di simmetria: quelli passanti solo per i vertici e quelli passanti per il punto medio dei segmenti del poligono regolare considerato.

Osservazione 1.35 — Per $n \geq 3$ si osserva che $\mathcal{C}\ell(sr^h)$ non è mai composto da un singolo elemento, e dunque $sr^h \notin \mathrm{Z}(\mathrm{D}_n)$. Pertanto si conclude facilmente che D_n ha centro banale per $n \geq 3$ dispari e che $\mathrm{Z}(\mathrm{D}_n) = \left\{\mathrm{id}, r^{\frac{n}{2}}\right\}$ per $n \geq 3$ pari.

§1.4.4 Legge di gruppo e omomorfismi

In questa sezione si ricava la presentazione di D_n cercando di descrivere un elemento $s^a r^b$ di D_n come elemento $(a,b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ con una nuova opportuna operazione di gruppo. Infatti vale che

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

e quindi tale operazione di gruppo sarà descritta dalla relazione[7]

$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, (-1)^{a_2} b_1 + b_2)$$

Usando il risultato appena ottenuto si possono descrivere gli omomorfismi da D_n in un qualsiasi gruppo G. Poiché ogni elemento $g \in \mathrm{D}_n$ si scrive come $s^a r^b$, un omomorfismo $\varphi \in \mathrm{Hom}(\mathrm{D}_n, G)$ è chiaramente determinato in modo univoco da $\varphi(r)$ e $\varphi(s)$. Detti $x = \varphi(s)$ e $y = \varphi(r)$, necessariamente $\mathrm{ord}(x) \mid 2$ e $\mathrm{ord}(y) \mid n$, dacché $x^2 = \varphi(s^2) = \varphi(\mathrm{id}) = e_G$ e $y^n = \varphi(r^n) = \varphi(\mathrm{id}) = e_G$. Inoltre deve valere la seguente relazione

$$xyx^{-1} = \varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(srs^{-1}) = \varphi(r^{-1}) = \varphi(r)^{-1} = y^{-1}$$

Mostriamo che effettivamente queste condizioni sono sufficienti affinché un omomorfismo $\varphi : \mathrm{D}_n \to G$ sia ben definito.

Proposizione 1.36
Dati un gruppo G e un'applicazione

$$\varphi : \mathrm{D}_n \longrightarrow G : s^a r^b \longmapsto x^a y^b$$

con x, $y \in G$, allora φ è un omomorfismo se e solo se $x^2 = e_G$, $y^n = e_G$ e $xyx^{-1} = y^{-1}$.

Dimostrazione. Mostriamo che tali condizioni sono sufficienti affinché φ sia un omomorfismo. Poiché $x^m = x^{-m}$ per ogni $m \in \mathbb{Z}$, fissati a_1, a_2, b_1, $b_2 \in \mathbb{Z}$ ricaviamo che

$$\begin{aligned}(x^{a_1} y^{b_1})(x^{a_2} y^{b_2}) &= x^{a_1} x^{a_2} (x^{a_2} y^{b_1} x^{-a_2}) y^{b_2} = x^{a_1+a_2} \varphi_{x^{a_2}}(y^{b_1}) y^{b_2} = \\ &= x^{a_1+a_2} (\varphi(\varphi_{s^{a_2}}(r)))^{b_1} y^{b_2} = x^{a_1+a_2} y^{(-1)^{a_2} b_1} y^{b_2} = x^{a_1+a_2} y^{(-1)^{a_2} b_1 + b_2}\end{aligned}$$

dove con φ_g si indica l'automorfismo di coniugio per g. Allora si verifica facilmente che φ è un omomorfismo. Infatti per ogni h_1, h_2, k_1, $k_2 \in \mathbb{Z}$ vale che

$$\begin{aligned}\varphi((s^{h_1} r^{k_1})(s^{h_2} r^{k_2})) &= \varphi(s^{h_1+h_2} r^{(-1)^{h_2} k_1 + k_2}) = \\ &= x^{h_1+h_2} y^{(-1)^{h_2} k_1 + k_2} = (x^{h_1} y^{k_1})(x^{h_2} y^{k_2}) = \varphi(s^{h_1} r^{h_2}) \varphi(s^{h_2} r^{h_2})\end{aligned}$$

□

[7] Questa operazione è esattamente quella che si ottiene considerando il prodotto semidiretto $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, dove $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ è univocamente determinata dalla relazione $[1] \mapsto -\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$. Più avanti si dimostrerà che in effetti D_n è proprio isomorfo a questo gruppo.

Osservazione 1.37 — Le condizioni $\mathrm{D}_n = \langle r, s\rangle$, $\operatorname{ord}(r) = n$, $\operatorname{ord}(s) = 2$ e $srs^{-1} = r^{-1}$ determinano in modo univoco la struttura astratta di D_n. Pertanto la presentazione desiderata di D_n è la seguente

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

§1.4.5 Automorfismi

Studiamo gli automorfismi di D_n.

Se $n = 2$, $\operatorname{Aut}(\mathrm{D}_2) \cong \operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathcal{S}_3$. Infatti $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \operatorname{Aut}(\mathrm{D}_2)$ e $\operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ è un gruppo non abeliano di ordine $2 \cdot 3 = 6$, e dunque isomorfo a $\mathcal{S}_3$.

Si può visualizzare facilmente l'isomorfismo tra $\operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ e $\mathcal{S}_3$ attraverso il seguente schema:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \leftrightarrow \mathrm{id}, \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \leftrightarrow (1\ 2), \quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \leftrightarrow (2\ 3),$$

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \leftrightarrow (1\ 3), \quad \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} \leftrightarrow (1\ 2\ 3) \quad \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} \leftrightarrow (1\ 3\ 2).$$

Si suppone d'ora in poi che $n \geq 3$.

Sia $\varphi \in \operatorname{Aut}(\mathrm{D}_n)$. Dacché $\mathrm{D}_n = \langle r, s\rangle$, è sufficiente studiare le immagini di r, s per determinare φ in modo univoco. Come già osservato in precedenza, $\varphi(r) \in \mathcal{R}$ dacché $\mathcal{R}$ è caratteristico in D_n. In particolare, affinché φ sia un automorfismo, $\varphi(r) = r^k$ con $(n, k) = 1$, in modo tale da preservare l'ordine di r.

Se n è dispari allora anche $\varphi(s)$ è una simmetria, dacché in tal caso le simmetrie sarebbero gli unici elementi di ordine 2. Se invece n è pari, anche $r^{\frac{n}{2}}$ ha ordine 2. Se tuttavia $\varphi(s)$ fosse uguale a $r^{\frac{n}{2}}$, $\varphi(s)$ apparterrebbe a $\mathcal{R}$, e quindi a $\langle\varphi(r)\rangle$, e dunque esisterebbe $r^k \in \mathcal{R}$ tale per cui $\varphi(r^k) = r^{\frac{n}{2}} = \varphi(s)$, facendo venire meno l'iniettività di φ; dacché però φ è un automorfismo, ciò non è possibile, e dunque $\varphi(s)$ è ancora una simmetria. Pertanto $\varphi(s) = sr^h$ con $0 \leq h \leq n-1$.

Verifichiamo che φ è un omomorfismo. Per la caratterizzazione data in precedenza è sufficiente verificare che $\varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(r)^{-1}$:

$$\varphi(s)\varphi(r)\varphi(s)^{-1} = (sr^h)r^k(sr^h)^{-1} = sr^{h+k}r^{-h}s = sr^ks^{-1} = r^{-k} = \varphi(r)^{-1}$$

Inoltre φ è surgettiva. Infatti vale che

$$\operatorname{im}\varphi \supseteq \langle r^k, sr^h\rangle = \langle r, sr^h\rangle = \langle r, s\rangle = \mathrm{D}_n$$

da cui si conclude che $\operatorname{im}\varphi = \mathrm{D}_n$. Dacché D_n è finito la surgettività di φ ne implica anche la bigettività, e dunque φ è un automorfismo. Gli automorfismi di $\mathrm{D}_n = \langle r, s\rangle$ sono quindi tutti e soli gli omomorfismi da D_n in D_n che mandano r in un generatore di $\mathcal{R}$ – e quindi vi sono $\phi(n)$ scelte per $\varphi(r)$ – e s in un'altra simmetria – dunque vi sono n scelte per $\varphi(s)$. Si conclude dunque che $|\operatorname{Aut}(D_n)| = n \cdot \phi(n)$.

§1.5 Automorfismi di un prodotto diretto

Studiamo il gruppo degli automorfismi di $H \times K$, relazionandolo a quello di H e a quello di K. Chiaramente esiste un'immersione di $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ data dall'omomorfismo ι tale per cui

$$(\varphi_H, \varphi_K) \mapsto \varphi_H \times \varphi_K := [(h,k) \mapsto (\varphi_H(h), \varphi_K(k))]$$

Mostriamo che ι è ben definita e che è effettivamente un omomorfismo iniettivo:

- per ogni $(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, $(h_1, k_1), (h_2, k_2) \in H \times K$ si verifica che

$$\begin{aligned}(\varphi_H \times \varphi_K)((h_1,k_1)(h_2,k_2)) &= (\varphi_H(h_1h_2), \varphi_K(k_1k_2)) = \\ &= (\varphi_H(h_1)\varphi_H(h_2), \varphi_K(k_1)\varphi_K(k_2)) = \\ &= (\varphi_H(h_1), \varphi_K(k_1))(\varphi_H(h_2), \varphi_K(k_2)) = \\ &= ((\varphi_H \times \varphi_K)(h_1,k_1))((\varphi_H \times \varphi_K)(h_2,k_2))\end{aligned}$$

  e quindi $\varphi_H \times \varphi_K$ è un omomorfismo. Inoltre

$$\ker(\varphi_H \times \varphi_K) = \{(h,k) \in H \times K \mid (\varphi_H(h), \varphi_K(k)) = (e_H, e_K)\} = \{(e_H, e_K)\}$$

  quindi si conclude che $\varphi_H \times \varphi_K$ è iniettivo; inoltre se $(h,k) \in H \times K$, $(\varphi_H \times \varphi_K)(\varphi_H^{-1}(h), \varphi_K^{-1}(K)) = (h,k)$, e dunque $\varphi_H \times \varphi_K$ è anche surgettivo, ed è pertanto un automorfismo; quindi ι è ben definita come mappa;

- per ogni $(\varphi_H, \varphi_K), (\psi_H, \psi_K) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(h,k) \in H \times K$ abbiamo

$$\begin{aligned}\iota((\varphi_H, \varphi_K)(\psi_H, \psi_K))(h,k) &= \iota(\varphi_H \circ \psi_H, \varphi_K \circ \psi_K)(h,k) = \\ &= ((\varphi_H \circ \psi_H) \times (\varphi_K \psi_K))(h,k) = (\varphi_H(\psi_H(h)), \varphi_K(\psi_K(k))) = \\ &= (\varphi_H \times \varphi_K)(\psi_H(h), \psi_K(k)) = \\ &= ((\varphi_H \times \varphi_K) \circ (\psi_H \times \psi_K))(h,k) = (\iota(\varphi_H, \varphi_K) \circ \iota(\psi_H, \psi_K))(h,k)\end{aligned}$$

  quindi $\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2)) = \iota(\varphi_1, \varphi_2) \circ \iota(\psi_1, \psi_2)$, da cui si conclude che ι è un omomorfismo;

- ι è iniettiva, infatti

$$\begin{aligned}\ker \iota &= \{(\varphi_H, \varphi_K) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid \iota(\varphi_H, \varphi_K) = \mathrm{id}_{H \times K}\} = \\ &= \{(\varphi_H, \varphi_K) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid (\varphi_H(h), \varphi_K(k)) = (h,k) \ \ \forall (h,k) \in H \times K\} = \\ &= \{(\mathrm{id}_H, \mathrm{id}_K)\}\}\end{aligned}$$

  e dunque il nucleo di ι è banale.

Proposizione 1.38

Dati due gruppi finiti H, K, $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(H \times K)$ se e solo se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono sottogruppi caratteristici di $H \times K$.

Dimostrazione. Sia ι l'immersione da $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ definita come sopra. Se $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(H \times K)$, allora ι deve essere una bigezione essendo un omomorfismo iniettivo (altrimenti $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ sarebbe isomorfo a un sottogruppo proprio di $\mathrm{Aut}(H \times K)$ e un gruppo non può essere isomorfo ad un suo sottogruppo proprio, se finito). Pertanto ogni elemento di $\mathrm{Aut}(H \times K)$ può essere scritto come $\varphi_H \times \varphi_K$ con $\varphi_H \in \mathrm{Aut}(H)$ e $\varphi_K \in \mathrm{Aut}(K)$. Allora abbiamo

$$(\varphi_H \times \varphi_K)(H \times \{e_K\}) = (\varphi_H(H), \varphi_K(\{e_K\})) = H \times \{e_K\}$$

$$(\varphi_H \times \varphi_K)(\{e_H\} \times K) = (\varphi_H(\{e_H\}), \varphi_K(K)) = \{e_H\} \times K$$

e quindi sia $H \times \{e_K\}$ che $\{e_H\} \times K$ sono caratteristici in $H \times K$.

Viceversa, se i due sottogruppi sono caratteristici, dato $\varphi \in \mathrm{Aut}(H \times K)$, si definisce $\varphi_H : H \to H$ in modo tale che $\varphi_H(h) = \pi_H(\varphi(h, e_K))$, dove π_H è la proiezione di $H \times K$ nella prima coordinata (e quindi su H). Analogamente si definisce $\varphi_K : K \to K$ in modo tale che $\varphi_K(k) = \pi_K(\varphi(e_H, k))$, dove stavolta π_K è la proiezione di $H \times K$ nella seconda coordinata (e quindi su K).

Si verifica che φ_H è un automorfismo di H. Sicuramente infatti φ_H è un omomorfismo. Poiché $H \times \{e_K\}$ è caratteristico, $\varphi(H \times \{e_K\}) = H \times \{e_K\}$, e quindi, per ogni $h' \in H$ esiste $h \in H$ tale per cui $\varphi(h, e_K) = (h', e_K)$. Si conclude dunque che $\varphi_H(h) = h'$, e quindi φ_H è surgettivo. Dacché H è finito, la surgettività di φ_H ne implica la bigettività, e quindi $\varphi_H \in \mathrm{Aut}(H)$. Analogamente $\varphi_K \in \mathrm{Aut}(K)$.

Infine, $\iota(\varphi_H, \varphi_K) = \varphi_H \times \varphi_K = \varphi$, dove l'ultima identità è dovuta alla definizione di φ_H e di φ_K. Pertanto ι è surgettiva, ed essendo un'immersione è dunque un isomorfismo, da cui la tesi. $\square$

Esempio 1.39

Consideriamo il gruppo $G = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Osserviamo che il sottogruppo $\{0\} \times \mathbb{Z}/n\mathbb{Z}$ è caratteristico in quanto un automorfismo φ di G deve preservare gli ordini degli elementi, in particolare quello di un generatore. Se infatti la prima coordinata dell'immagine di $(0, \overline{1})$ fosse non nulla, tale elemento avrebbe ordine infinito, e dunque non rispetterebbe l'ordine di $(0, \overline{1})$, che è n. Pertanto $\varphi(\{0\} \times \mathbb{Z}/n\mathbb{Z}) = \varphi(\{0\} \times \langle \overline{1} \rangle) = \langle \varphi(0, \overline{1}) \rangle = \{0\} \times \mathbb{Z}/n\mathbb{Z}$, e quindi il sottogruppo $\{0\} \times \mathbb{Z}/n\mathbb{Z}$ è caratteristico.

Viceversa, si consideri l'immagine (a, b) di $(1, 0)$ tramite φ, dove 1 è preso in quanto generatore di $\mathbb{Z}$. Se φ è surgettivo, necessariamente esiste una coppia $(x, y) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tale per cui $\varphi(x, y) = (1, 0)$. Posti allora $\varphi(1, 0) = (a, b)$ e $\varphi(0, 1) = (0, d)$ con n e d coprimi, ricaviamo che

$$\begin{aligned}\varphi(x, y) = \varphi(x(1, 0) + y(0, 1)) = x\varphi(1, 0) + y\varphi(0, 1) = \\ = x(a, b) + y(0, d) = (xa, xb + yd) = (1, 0)\end{aligned}$$

Pertanto $a \in \mathbb{Z}^*$, e quindi $a \in \{\pm 1\}$.

Posto allora $a = 1$ si verifica che φ è surgettiva. Infatti per ogni $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, scegliendo $x = x_0 a$ e $y \equiv d^{-1}(y_0 - x_0 ab) \pmod n$ si verifica che

$$\varphi(x, y) = (x_0 a^2, x_0 ab + dd^{-1}(y_0 - x_0 ab)) = (x_0, y_0)$$

Infine si mostra che φ è iniettiva per $a = 1$ e b qualsiasi. Infatti $\varphi(x, y) = (0, 0)$ se e solo se

$$\begin{cases} xa = 0 \\ xb + yd \equiv 0 \pmod n \end{cases} \implies \begin{cases} x = 0 \\ yd \equiv 0 \pmod n \end{cases} \implies \begin{cases} x = 0 \\ y \equiv 0 \pmod n \end{cases}$$

dove l'ultima equazione modulare è dovuta al fatto che d è invertibile in $\mathbb{Z}/n\mathbb{Z}$, essendo coprimo con n per ipotesi. Quindi il nucleo di φ è banale, e dunque $\varphi \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. Tuttavia $\varphi(1, 0)$ per $b \not\equiv 0 \pmod n$ non appartiene a $\mathbb{Z} \times \{0\}$, e quindi $\mathbb{Z} \times \{0\}$ non è caratteristico in $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. In questo caso esiste solo un'immersione del gruppo $\mathrm{Aut}(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ dentro a $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ e non una bigezione.

In alcuni casi è facile determinare se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$, a partire dal seguente risultato:

Proposizione 1.40

Dati due gruppi finiti H, K, se $(|H|, |K|) = 1$ allora $H \times \{e_K\}$ e $\{e_H\} \times K$ sono sottogruppi caratteristici di $H \times K$.

Dimostrazione. Posti $n = |H|$, $m = |K|$, consideriamo l'insieme

$$S = \{(h, k) \in H \times K \mid (h, k)^n = (e_H, e_K)\}$$

Mostriamo che $H \times \{e_K\} = S$. Chiaramente $H \times \{e_K\} \subseteq S$ dal momento che tutti gli elementi di $H \times \{e_K\}$ hanno ordine che divide n. D'altra parte, dato $(h, k) \in S$, se $\mathrm{ord}(h, k) \mid n$ allora $\mathrm{ord}(k) \mid n$. Tuttavia $\mathrm{ord}(k)$ divide anche m per il Teorema di Lagrange, e dunque $\mathrm{ord}(k) \mid (n, m) = 1$, da cui si ricava che $k = e_K$ e dunque l'uguaglianza. Con un ragionamento analogo possiamo caratterizzare $\{e_H\} \times K$ come

$$\{e_H\} \times K = \{(h, k) \in H \times K \mid (h, k)^m = (e_H, e_K)\}$$

Poiché un automorfismo di $H \times K$ deve preservare gli ordini degli elementi, per la caratterizzazione data concludiamo che $\varphi(H \times \{e_K\}) \subseteq S = H \times \{e_K\}$, e analogamente che $\varphi(\{e_H\} \times K) \subseteq \{e_H\} \times K$. Pertanto, essendo H e K finiti, i due sottogruppi considerati sono caratteristici. □

Corollario 1.41

Se m, $n \geq 2$ sono interi coprimi allora

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

Dimostrazione. Se m, $n \geq 2$ allora $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$ sono entrambi gruppi finiti. Per il Teorema cinese del resto, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, dacché m e n sono coprimi. Dacché $|\mathbb{Z}/m\mathbb{Z}| = m$ e $|\mathbb{Z}/n\mathbb{Z}| = n$, ancora per la coprimalità tra m e n $\mathbb{Z}/m\mathbb{Z} \times \{0\}$ e $\{0\} \times \mathbb{Z}/n\mathbb{Z}$ sono caratteristici in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Pertanto $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, da cui la tesi. □

Osservazione 1.42 (Teorema cinese del resto per i gruppi moltiplicativi) — Dal momento che $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, il precedente corollario permette di dimostrare il Teorema cinese del resto anche nel caso dei gruppi moltiplicativi di $\mathbb{Z}/n\mathbb{Z}$. Se infatti $(m, n) = 1$ con m, $n \geq 1$, allora:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/mn\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

§1.6 Gruppo derivato e abelianizzazione

Definizione 1.43. Dati un gruppo G e dati x, $y \in G$, si definisce il **commutatore** di x e y l'elemento[8] $[x, y] = xy(yx)^{-1} = xyx^{-1}y^{-1}$. Si definisce inoltre il **sottogruppo derivato** di G, detto anche **sottogruppo dei commutatori** di G, il sottogruppo G' generato da tutti i commutatori di G, ossia

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

Osservazione 1.44 — Si verifica facilmente che $[x, y] = e$ se e solo se x e y commutano, dacché $xy = [x, y]yx$. Vale inoltre che $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$. In un certo senso $[x, y]$ "misura" quanto x e y non commutano.

Proposizione 1.45
Dato un gruppo G, valgono i seguenti fatti:

(1) G' è un sottogruppo caratteristico di G;

(2) dato $N \trianglelefteq G$, ${}^{G}\!/_{N}$ è un gruppo abeliano se e solo se $G' \subseteq N$;

(3) dato A un gruppo abeliano e data $\varphi \in \mathrm{Hom}(G, A)$, allora $G' \subseteq \ker \varphi$.

Dimostrazione. Mostriamo le affermazioni singolarmente:

(1) sia $\varphi \in \mathrm{Aut}(G)$; dati x, $y \in G$ si verifica che

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

da cui $\varphi(G') \subseteq G'$, e quindi la tesi;

(2) se ${}^{G}\!/_{N}$ è abeliano, dati x, $y \in G$, vale che $xyN = yxN$ se e solo se $xy(yx)^{-1} = [x, y] \in N$, e dunque ${}^{G}\!/_{N}$ è abeliano se e solo se $G' \subseteq N$;

(3) dati x, $y \in G$, da prima abbiamo che $\varphi([x, y]) = [\varphi(x), \varphi(y)]$; dacché A è abeliano, $\varphi(x)$ e $\varphi(y)$ commutano, e quindi $[\varphi(x), \varphi(y)] = e_A$; pertanto $[x, y] \in \ker \varphi$, da cui $G' \subseteq \ker \varphi$.

□

Definizione 1.46. Si definisce l'**abelianizzato** G_{ab} di G il gruppo ${}^{G}\!/_{G'}$.

Osservazione 1.47 — In un certo senso la definizione di G_{ab} è suggerita proprio dalla precedente proposizione. Infatti G_{ab} è il "più grande" quoziente di G abeliano: ogni altro quoziente abeliano ${}^{G}\!/_{N}$ è tale per cui $G' \subseteq N$. Pertanto G_{ab} dà una misura di quanto non sia abeliano G; nel peggiore dei casi $G_{\mathrm{ab}} \cong \{e\}$ e dunque G è "enormemente" non abeliano, mentre $G_{\mathrm{ab}} \cong G$ se e solo se $G' = \{e_G\}$, e quindi se e solo se G è già abeliano.

[8] Talvolta in letteratura si definisce $[x, y] = (yx)^{-1}xy = x^{-1}y^{-1}xy$. In tal caso vale che $xy = yx[x, y]$, mentre vengono mantenute tutte le altre proprietà elencate in questa sezione.

Osservazione 1.48 (serie derivata) — Si può reiterare la costruzione del gruppo derivato su G' stesso, ottenendo $(G')'$. Reiterando indefinitivamente questa costruzione per G finito si ottiene la **serie derivata** (o *serie dei derivati*) di G, ossia una sequenza

$$G^{(n)} \triangleleft G^{(n-1)} \triangleleft \cdots \triangleleft G^{(1)} \triangleleft G^{(0)}$$

dove $G^{(0)} = G$, $G^{(i)}$ è l'i-esimo derivato di G e $G^{(k)} = G^{(n)}$ per ogni $k \geq n$. Per il Principio della discesa infinita[a], una tale sequenza esiste sempre dacché il processo di derivazione di G deve terminare in un certo $G^{(n)}$ per poi stabilizzarsi.

Lo studio di questa serie risulta molto utile nello studio della teoria di Galois. Un gruppo si dice infatti **risolubile** se e solo se la sua serie derivata termina nel gruppo banale $\{e\}$.

[a] Infatti la cardinalità dell'i-esimo derivato di G è sempre minore o uguale di quella dell'$i-1$-esimo derivato di G.

Osservazione 1.49 — Dato un gruppo abeliano A, il Primo Teorema di Omomorfismo produce una bigezione naturale tra $\mathrm{Hom}(G, A)$ e $\mathrm{Hom}(G_{\mathrm{ab}}, A)$. Se infatti φ è un omomorfismo di $\mathrm{Hom}(G, A)$, per la proposizione precedente vale che $G' \subseteq \ker \varphi$, e quindi, per il Primo teorema di Omomorfismo, detta $\pi_{G'} : G \to G/G' = G_{\mathrm{ab}}$ la proiezione al quoziente di G su G_{ab}, esiste un'unica $\overline{\varphi} : G_{\mathrm{ab}} \to A$ che fa commutare il seguente diagramma:

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi_{G'}"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\
G_{\mathrm{ab}} \arrow[ur, hook, "\overline{\varphi}"'] &
\end{tikzcd}$$

In particolare $\overline{\varphi}$ è tale per cui $hG' \mapsto \varphi(h)$. Viceversa, dato un omomorfismo $\overline{\varphi} : G_{\mathrm{ab}} \to A$, per il Primo Teorema di Omomorfismo esiste un unico omomorfismo $\varphi : G \to A$ che fa commutare lo stesso diagramma. In particolare vale che $\varphi = \overline{\varphi} \circ \pi_{G'}$. Si conclude quindi che $\mathrm{Hom}(G, A) \leftrightarrow \mathrm{Hom}(G_{\mathrm{ab}}, A)$.

Esempio 1.50

Consideriamo il gruppo $\mathcal{S}_3$. Chiaramente $(\mathcal{S}_3)' \neq \{\mathrm{id}\}$ dal momento che $\mathcal{S}_3$ non è abeliano. Esistono dunque due sole possibilità: $(\mathcal{S}_3)' = \mathcal{S}_3$ oppure $(\mathcal{S}_3)' = \langle(1\ 2\ 3)\rangle = \mathcal{A}_3$[a].

D'altra parte $\mathcal{S}_3 / \langle(1\ 2\ 3)\rangle$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, che è abeliano. Pertanto $(\mathcal{S}_3)'$ è contenuto in $\langle(1\ 2\ 3)\rangle$, e dunque deve necessariamente valere che $(\mathcal{S}_3)' = \langle(1\ 2\ 3)\rangle = \mathcal{A}_3$. Si conclude dunque che $(\mathcal{S}_3) | = | \mathcal{S}_3 / \mathcal{A}_3 \cong \mathbb{Z}/2\mathbb{Z}$ e quindi che $\mathrm{Hom}(\mathcal{S}_3, A) \leftrightarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, A)$ per un gruppo abeliano A.

Vedremo più in generale che $(\mathcal{S}_n)' = \mathcal{A}_n$; per adesso ci limiteremo ad osservare che $(\mathcal{S}_n)'$ deve essere un sottogruppo di $\mathcal{A}_n$, dacché $\mathcal{S}_n / \mathcal{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ è abeliano.

[a] Gli unici sottogruppi normali di $\mathcal{S}_3$ sono infatti $\{\mathrm{id}\}$, $\langle(1\ 2\ 3)\rangle = \mathcal{A}_3$ e $\mathcal{S}_3$.

§1.7 Azioni di gruppo

§1.7.1 Azioni transitive

Definizione 1.51. Siano G un gruppo e X un insieme. Un'azione

$$\varphi : G \to \mathcal{S}(X) : g \mapsto \varphi_g$$

si dice **transitiva** se per ogni x, $y \in X$ esiste $g \in G$ tale che $\varphi_g(x) = y$. Equivalentemente φ è transitiva se $\mathrm{Orb}(x) = X$ per ogni $x \in X$. In tal caso si dice che G **agisce transitivamente** su X tramite φ.

Lemma 1.52

Dato G un gruppo finito e $H \lneq G$ un suo sottogruppo proprio, allora

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

Dimostrazione. Sia $G = \bigcup_{g \in G} gHg^{-1}$. Mostriamo che deve valere necessariamente $H = G$. Osserviamo che tutti gli elementi della forma xHx^{-1} con $x \in g\,\mathrm{N}_G(H)$ con $g \in G$ danno lo stesso contributo[9] nell'unione che produce G. Detto quindi $\mathcal{R}$ un insieme di rappresentanti di ${}^{G}\!/_{\mathrm{N}_G(H)}$, vale ancora che

$$G = \bigcup_{g \in \mathcal{R}} gHg^{-1}$$

Dal momento che $\left|gHg^{-1}\right| = |H|$ per ogni $g \in G$, possiamo stimare la cardinalità di K nel seguente modo:

$$|G| \leq \sum_{g \in \mathcal{R}} \left|gHg^{-1}\right| = \sum_{g \in \mathcal{R}} |H| = [G : \mathrm{N}_G(H)]\,|H| = \frac{|G|}{|\mathrm{N}_G(H)|}\,|H|$$

Inoltre, poiché $H \leqslant \mathrm{N}_G(H)$, $|\mathrm{N}_G(H)| \geq |H|$, e quindi

$$|G| \leq \frac{|G|}{|\mathrm{N}_G(H)|}\,|H| \leq \frac{|G|}{|H|}\,|H| = |G|$$

Se $[G : \mathrm{N}_G(H)]$ non fosse uguale ad 1, vi sarebbero più ripetizione di e nei termini dell'unione, e quindi $|G|$ sarebbe strettamente minore di $\frac{|G|}{|\mathrm{N}_G(H)|}\,|H|$, e dunque anche strettamente minore di $|G|$, assurdo. Pertanto $\mathrm{N}_G(H) = G$, e quindi $H \trianglelefteq G$. Allora, esiste un'unica classe laterale in ${}^{G}\!/_{\mathrm{N}_G(H)}$, e, sceltone come rappresentante e, vale quindi che $G = eHe^{-1} = H$, da cui la tesi. □

Osservazione 1.53 — Si verifica facilmente che $\mathrm{Stab}(g \cdot x) = g\,\mathrm{Stab}(g)g^{-1}$. Infatti vale che:

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

[9] Infatti $xHx^{-1} = yHy^{-1}$ se e solo se $x\,\mathrm{N}_G(H) = y\,\mathrm{N}_G(H)$. Questo è un risultato relativo alla teoria delle azioni di gruppi. Infatti xHX^{-1} e yHy^{-1} sono le immagini dell'azione di x e y sull'elemento H dell'insieme dei sottogruppi di G; affinché le due immagini siano uguali, xy^{-1} deve appartenere allo stabilizzatore di H relativo alla stessa azione, che in questo caso coincide proprio con $\mathrm{N}_G(H)$.

e quindi che:

$$\mathrm{Stab}(g\cdot x) = \{h \in G \mid (g^{-1}hg)\cdot x = x\} = \{h \in G \mid g^{-1}hg \in \mathrm{Stab}(x)\} = g\,\mathrm{Stab}(x)g^{-1}$$

Pertanto gli stabilizzatori relativi a elementi di una stessa orbita sono coniugati, e dunque anche isomorfi.

Proposizione 1.54

Sia G un gruppo e X un insieme. Se

$$\varphi : G \to \mathcal{S}(X) : g \mapsto \varphi_g$$

è un'azione transitiva valgono i seguenti fatti:

(1) tutti gli stabilizzatori sono coniugati tra loro;

(2) se X e G sono finiti e $|X| \geq 2$, allora esiste $g \in G$ che agisce su X senza punti fissi, cioè tale per cui $\varphi_g(x) \neq x$ per ogni $x \in X$.

Dimostrazione. Mostriamo i due fatti singolarmente:

(1) poiché φ è transitiva, esiste un'unica orbita; allora, per l'osservazione precedente, tutti gli stabilizzatori sono coniugati tra loro;

(2) un elemento $g \in G$ con tali proprietà non può essere contenuto nello stabilizzatore di nessun elemento di X e deve essere tale per cui

$$g \in \bigcap_{x \in X} \mathrm{Stab}(x)^{\mathcal{C}}$$

ossia, equivalentemente, esistono g con tale proprietà se

$$\bigcup_{x \in X} \mathrm{Stab}(x) \neq G$$

Per il punto (1), tutti gli stabilizzatori sono coniugati tra loro e quindi, scelto $y \in X$, vale che

$$\bigcup_{x \in X} \mathrm{Stab}(x) = \bigcup_{h \in G} h\,\mathrm{Stab}(y)h^{-1}$$

Per il lemma precedente, tale unione è diversa da G se e solo se $\mathrm{Stab}(y)$ è diverso da G. Se $\mathrm{Stab}(y)$ fosse uguale a G, per il Lemma orbita-stabilizzatore varrebbe che $|X| = 1$, assurdo in quanto $|X| \geq 2$. Pertanto l'unione considerata è diversa da G ed esiste dunque $g \in G$ tale per cui $\varphi_g(x) \neq x$ per ogni $x \in X$.

□

Proposizione 1.55

Dato G un gruppo finito e H un sottogruppo proprio di G, se $[G : H]$ è uguale a p, dove p è il più piccolo primo che divide l'ordine di G, allora H è normale in G.

Dimostrazione. Consideriamo l'azione di G sull'insieme quoziente ${}^{G}\!/_{H}$

$$\psi : G \to \mathcal{S}\left({}^{G}\!/_{H}\right) : g \mapsto \psi_g$$

tale per cui

$$\psi_g : {}^{G}\!/_{H} \to {}^{G}\!/_{H} : g'H \mapsto gg'H$$

Dal momento che $[G : H] = p$, $\mathcal{S}\left({}^{G}\!/_{H}\right) \cong \mathcal{S}_p$, e quindi $|\mathrm{im}\,\psi| \mid p!$. Inoltre, per il Primo Teorema di Omomorfismo, $|\mathrm{im}\,\psi| = \frac{|G|}{|\ker\psi|} \mid |G|$, e quindi $|\mathrm{im}\,\psi| \mid (p!, |G|) = p$.

D'altra parte osserviamo che ψ è un'azione transitiva. Dati infatti g_1, $g_2 \in G$, si verifica che

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

Pertanto, poiché $[G : H] = p > 1$, se $x \in X$, $\mathrm{Stab}(x) \neq G$, e quindi $\ker\psi \neq G$. Allora $|\mathrm{im}\,\psi|$ deve valere esattamente p.

Si osserva che $\ker\psi = \bigcap_{x\in X}\mathrm{Stab}(x)$, e quindi che $\ker\psi \subseteq \mathrm{Stab}(H) = \{g \in G \mid gH = H\} = H$. Dacché allora $[G : H] = p = |\mathrm{im}\,\psi| = [G : \ker\psi]$, vale che $H = \ker\psi$, e dunque H è normale in G. □

§1.7.2 Il Lemma normalizzatore-centralizzatore

Si definisce il centralizzatore di un sottogruppo H in G:

Definizione 1.56. Sia H un sottogruppo di G. Allora si definisce il **centralizzatore** di H il sottogruppo $\mathrm{Z}_G(H) \leqslant G$ così definito:

$$\mathrm{Z}_G(H) = \bigcap_{h\in H} \mathrm{Z}_G(h)$$

ossia come il sottogruppo degli elementi di G che commutano con tutti gli elementi di H.

Osservazione 1.57 — Si osserva che, per $g \in G$, $\mathrm{Z}_G(\langle g\rangle)$ e $\mathrm{Z}_G(g)$ coincidono. Infatti se $k \in G$ commuta con g, k commuta in particolare con ogni sua potenza; viceversa se k commuta con ogni potenza di g, commuta in particolare con g stesso. Se $H \leqslant G$, vale inoltre che $\mathrm{Z}(H) \subseteq \mathrm{Z}_G(H)$, ed in particolare $\mathrm{Z}(H) = H \cap \mathrm{Z}_G(H)$.

Si illustra una relazione fondamentale tra il normalizzatore e il centralizzatore di un sottogruppo H di G:

Proposizione 1.58 (Lemma normalizzatore-centralizzatore)
Sia H un sottogruppo di G. Allora $\mathrm{Z}_G(H)$ è normale in $\mathrm{N}_G(H)$ ed esiste un omomorfismo iniettivo da ${}^{\mathrm{N}_G(H)}\!/_{\mathrm{Z}_G(H)}$ in $\mathrm{Aut}(H)$, ovverosia:

$${}^{\mathrm{N}_G(H)}\!/_{\mathrm{Z}_G(H)} \hookrightarrow \mathrm{Aut}(H)$$

Dimostrazione. Consideriamo l'omomorfismo $\alpha : \mathrm{N}_G(H) \to \mathrm{Inn}(G)$ tale per cui $g \overset{\alpha}{\mapsto} \varphi_g$. Si osserva che per ogni $g \in \mathrm{N}_G(H)$, φ_g può essere ristretto su H dacché $\varphi_g(H) = gHg^{-1} = H$. Inoltre $\varphi_g\big|_H$ è ancora un omomorfismo, ed è in particolare un automorfismo di H, ossia un elemento di $\mathrm{Aut}(H)$.

Si considera pertanto l'omomorfismo $\beta : \mathrm{N}_G(H) \to \mathrm{Aut}(H)$ ottenuto restringendo φ_g su H, ovverosia l'omomorfismo tale per cui $g \overset{\beta}{\mapsto} \varphi_g\big|_H$.

Si studia il nucleo di β. Sia $g \in \ker \beta$, allora $\varphi_g\big|_H = \mathrm{id}_H$, e dunque $ghg^{-1} = h$ per ogni $h \in H$, ovverosia $g \in \mathrm{Z}_G(H)$. Viceversa, per $g \in \mathrm{Z}_G(H)$, $\varphi_g\big|_H$ è l'identità di H, dacché g commuta con ogni elemento di H. Pertanto $\ker \beta = \mathrm{Z}_G(H)$.

Pertanto, $\mathrm{Z}_G(H)$ è normale in $\mathrm{N}_G(H)$ e per il Primo Teorema di Omomorfismo esiste un omomorfismo iniettivo da ${\mathrm{N}_G(H)}\big/{\mathrm{Z}_G(H)}$ in $\mathrm{Aut}(H)$, da cui la tesi. □

Osservazione 1.59 — Non è difficile verificare a mano che $\mathrm{Z}_G(H)$ è normale in $\mathrm{N}_G(H)$. Infatti, se $h \in H$, $z \in \mathrm{Z}_G(H)$ e $n \in \mathrm{N}_G(H)$, allora vale che:

$$[h, nzn^{-1}] = h(nzn^{-1})h^{-1}(nzn^{-1})^{-1} = hnzn^{-1}h^{-1}nz^{-1}n^{-1}$$

e quindi che:

$$[h, nzn^{-1}] = hznn^{-1}h^{-1}nn^{-1}z^{-1} = hzh^{-1}z^{-1} = [h, z] = e$$

da cui si deduce che $nzn^{-1} \in \mathrm{Z}_G(H)$, ovverosia che $\mathrm{Z}_G(H)$ è normale in $\mathrm{N}_G(H)$.

Esercizio 1.60 ($\star$)**.** Sia G un gruppo infinito che non ammette sottogruppi normali di indice finito che non siano banali. Si mostri allora che ogni sottogruppo normale N di G è contenuto in $\mathrm{Z}(G)$, se di cardinalità finita.

Soluzione. Si consideri il gruppo $K := \mathrm{N}_G(H)/\,\mathrm{Z}_G(H)$. Dacché H è normale, vale che $\mathrm{N}_G(H) = G$, e dunque $K = G/\,\mathrm{Z}_G(H)$. Per il Lemma normalizzatore-centralizzatore, esiste un'immersione di K in $\mathrm{Aut}(H)$, che è un gruppo finito, dal momento che H lo è. Pertanto $[G : \mathrm{Z}_G(H)]$ è finito, e quindi, per ipotesi, $\mathrm{Z}_G(H)$ è $\{e_G\}$ o G stesso. Se $\mathrm{Z}_G(H)$ fosse $\{e\}$, G si immergerebbe in $\mathrm{Aut}(H)$, assurdo dal momento che G è un gruppo infinito e $\mathrm{Aut}(H)$ non lo è. Pertanto $\mathrm{Z}_G(H) = G$, ovverosia $H \subseteq \mathrm{Z}(G)$, da cui la tesi. □

§1.7.3 Dimostrazioni alternative del Teorema di Cauchy e del Piccolo Teorema di Fermat

In questa sezione illustriamo una dimostrazione alternativa, che fa uso del concetto di azione, del Teorema di Cauchy e del Piccolo Teorema di Fermat, di cui ricordiamo gli enunciati:

Teorema 1.61 (Teorema di Cauchy)

Dato un gruppo finito G e un numero primo p, se $p \mid |G|$ allora esiste $g \in G$ tale che $\mathrm{ord}(g) = p$.

Teorema 1.62 (Piccolo Teorema di Fermat)

Dato un numero primo p, se $n \in \mathbb{Z}$ è coprimo con p allora $n^{p-1} \equiv 1 \pmod{p}$.

Dati un gruppo G e un numero primo p, consideriamo l'insieme

$$X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \ldots g_p = e\}$$

Osserviamo che $|X| = |G|^{p-1}$: possiamo infatti scegliere liberamente i primi $p-1$ elementi di ogni p-upla, che ne determinano l'ultimo in modo univoco, per l'unicità dell'inverso in un gruppo.

Definiamo ψ come l'azione di $\mathbb{Z}/p\mathbb{Z}$ su X univocamente determinata dalla relazione nel seguente modo:

$$(g_1, \ldots, g_p) \overset{\psi(\overline{1})}{\mapsto} (g_2, \ldots, g_p, g_1)$$

In particolare $\psi(\overline{a})$ "shifta", ossia trasla, di a posizione la p-upla verso sinistra.

Sia $x \in X$. Poiché la cardinalità di $\mathrm{Orb}(x)$ divide l'ordine di $\mathbb{Z}/p\mathbb{Z}$, ossia p, ricaviamo che $|\mathrm{Orb}(x)| \in \{1, p\}$. Se $|\mathrm{Orb}(x)| = 1$, allora x è un elemento della forma $(g, \ldots, g)$ con $g \in G$; ed in particolare deve valere $g^p = e$.

Poniamo $S = \{g \in G \mid \mathrm{ord}(g) = p\}$ e definiamo $\mathcal{R}$ come un insieme di rappresentanti per la relazione di equivalenza indotta dalle orbite di ψ. Dal momento che le orbite degli elementi di X formano una partizione di X stesso, detto $\mathbf{e} := (e, \ldots, e)$, vale che

$$|G|^{p-1} = |X| = \sum_{x \in \mathcal{R}} |\mathrm{Orb}(x)| = 1 + |S| + \sum_{x \in \mathcal{R} \setminus (S \cup \{\mathbf{e}\})} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathrm{Stab}(x)|} = 1 + |S| + |\mathcal{R} \setminus (S \cup \{\mathbf{e}\})|\, p$$

Distinguiamo dunque due casi:

- se $p \mid |G|$, riducendo modulo p l'identità ottenuta si ricava che $|S| \equiv -1 \pmod p$, e dunque $S \neq \varnothing$; pertanto esiste almeno un elemento di ordine p (Teorema di Cauchy);
- se $G = \mathbb{Z}/n\mathbb{Z}$ con p e n coprimi, $\mathbb{Z}/n\mathbb{Z}$ non contiene elementi di ordine p, pertanto $S = \varnothing$; riducendo allora modulo p l'identità ottenuta ricaviamo che $n^{p-1} \equiv 1 \pmod p$ (Piccolo Teorema di Fermat).

Esercizio 1.63. Mostrare che i gruppi di ordine 15 sono ciclici.

Soluzione. Sia G un gruppo di ordine 15. Poiché 5 è un primo che divide $|G|$, per il Teorema di Cauchy esiste $h \in G$ tale per cui $\mathrm{ord}(h) = 5$. Posto $H = \langle h \rangle$, $[G : H] = 3$ è il più piccolo primo che divide $|G|$, e quindi H è un sottogruppo normale di G.

Mostriamo che $H \subseteq \mathrm{Z}(G)$. Questo è equivalente a richiedere che l'omomorfismo

$$\varphi : G \to \mathrm{Aut}(H) : g \mapsto \varphi_g\big|_H$$

dove φ_g è il coniugio per g, abbia come unico elemento dell'immagine id_H. Poiché $H \cong \mathbb{Z}/5\mathbb{Z}$, si ricava facilmente che $\mathrm{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$. D'altra parte $|\varphi|$ divide $(|G|, |\mathrm{Aut}(H)|) = (15, 4) = 1$; pertanto $\mathrm{im}\,\varphi$ è banale, e quindi $H \subseteq \mathrm{Z}(G)$.

Osserviamo che se G è un gruppo abeliano, cioè se $\mathrm{Z}(G) = G$, allora abbiamo che G è ciclico. Posto infatti $k \in G$ un elemento di ordine 3, che esiste in virtù del Teorema di Cauchy, abbiamo che $\mathrm{ord}(hk) = \mathrm{ord}(h)\,\mathrm{ord}(k) = 15$ dacché h e k commutano e hanno ordini coprimi tra loro. Si illustrano adesso due modi per concludere l'esercizio:

(1) se G non fosse abeliano, avremmo necessariamente $\mathrm{Z}(G) = H$, e quindi ${}^{G}\!/_{\mathrm{Z}(G)}$ sarebbe ciclico dal momento che si avrebbe $[G : \mathrm{Z}(G)] = \frac{15}{5} = 3$; però così G sarebbe un gruppo abeliano e dunque $\mathrm{Z}(G)$ sarebbe diverso da H, assurdo; quindi G è abeliano sin da prima, e dunque è anche ciclico;

(2) sia $k \in G$ un elemento di ordine 3; consideriamo il centralizzatore di k

$$\mathrm{Z}_G(k) = \{x \in G \mid xk = kx\}$$

Osserviamo che $k \in \mathrm{Z}_G(k)$ e $\mathrm{Z}(G) \subseteq \mathrm{Z}_G(k)$. Pertanto $h \in H \subseteq \mathrm{Z}(G)$ è un elemento di $\mathrm{Z}_G(k)$. Abbiamo quindi che $\mathrm{ord}(h) \mid |\mathrm{Z}_G(k)|$ e anche che $\mathrm{ord}(k) \mid |\mathrm{Z}_G(k)|$, da cui si ricava che $|\mathrm{Z}_G(k)| = 15$. Allora $\mathrm{Z}_G(k) = \mathrm{Z}(G)$, e quindi $k \in \mathrm{Z}(G)$. Poiché h e k appartengono entrambi a $\mathrm{Z}(G)$, $[3, 5] = 15 \mid |\mathrm{Z}(G)|$, e quindi $\mathrm{Z}(G) = G$, dunque G è abeliano, e quindi ciclico.

□

Osservazione 1.64 — In generale, dati $x, y \in G$, se x e y commutano e $(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$, allora $\mathrm{ord}(xy) = [\mathrm{ord}(x), \mathrm{ord}(y)] = \mathrm{ord}(x)\,\mathrm{ord}(y)$, anche se G non è un gruppo abeliano.

Infatti $\mathrm{ord}(xy) \mid \mathrm{ord}(x)\,\mathrm{ord}(y)$, dal momento che, siccome x e y commutano, vale che $(xy)^{\mathrm{ord}(x)\,\mathrm{ord}(y)} = x^{\mathrm{ord}(x)\,\mathrm{ord}(y)} y^{\mathrm{ord}(x)\,\mathrm{ord}(y)} = e$. Se allora $k = \mathrm{ord}(xy)$, vale che $x^k y^k = e \implies x^k = y^{-k} \in \langle x \rangle \cap \langle y \rangle$. Tuttavia $|\langle x \rangle \cap \langle y \rangle| \mid (|\langle x \rangle|, |\langle y \rangle|) = (\mathrm{ord}(x), \mathrm{ord}(y)) = 1$, e quindi $\langle x \rangle \cap \langle y \rangle = \{e\}$. Pertanto deve valere che $x^k = y^{-k} = e$, e dunque $\mathrm{ord}(x), \mathrm{ord}(y) \mid k$, da cui si deduce che $\mathrm{ord}(xy)$ è esattamente $\mathrm{ord}(x)\,\mathrm{ord}(y)$.

Osservazione 1.65 — Se x e $y \in G$ commutano, non è in generale detto che $\mathrm{ord}(xy) = [\mathrm{ord}(x), \mathrm{ord}(y)]$, benché sicuramente $\mathrm{ord}(xy)$ divida $[\mathrm{ord}(x), \mathrm{ord}(y)]$. Si può comunque dimostrare che esiste $g \in G$ tale per cui $\mathrm{ord}(g) = [\mathrm{ord}(x), \mathrm{ord}(y)]$.

Si ponga $m = \mathrm{ord}(x)$ ed $n = \mathrm{ord}(y)$. Siano $m = \prod_{i=1}^\infty p_i^{m_i}$ ed $n = \prod_{i=1}^\infty p_i^{n_i}$ le due fattorizzazioni in numeri primi di m ed n. Allora $[m, n] = \prod_{i=1}^\infty p_i^{c_i}$, dove si pone $c_i = \max(m_i, n_i)$. Chiaramente esiste un numero finito di i per cui $c_i \neq 0$; per ogni tale i, se $c_i = m_i$, si pone $z_i = x^{m/p_i^{m_i}}$, altrimenti $z_i = y^{n/p_i^{n_i}}$.

Si osserva che tali z_i hanno esattamente ordine $p_i^{c_i}$. Sia allora $g = \prod_{i \mid c_i \neq 0} z_i$. Poiché $\mathrm{ord}(z_i)$ è coprimo con $\mathrm{ord}(z_j)$ per $j \neq i$, g ha come ordine, per la precedente osservazione, esattamente $\prod_{i \mid c_i \neq 0} p_i^{c_i} = \prod_{i=1}^\infty p_i^{c_i} = [m, n]$.

Esercizio 1.66. Dato d un numero dispari, si mostri che ogni gruppo di ordine $2d$ ammette un sottogruppo normale di indice 2.

Soluzione. Consideriamo la rappresentazione regolare a sinistra (*embedding* di Cayley) di G, ossia l'azione

$$\lambda : G \to \mathcal{S}(G) : g \mapsto \lambda_g$$

con

$$\lambda_g : G \to G : x \mapsto gx$$

Dopo aver fissato un isomorfismo $\psi : \mathcal{S}(G) \to S_{2d}$, poniamo $\varphi = \psi \circ \lambda : G \to S_{2d}$. φ è un omomorfismo iniettivo: infatti λ è un'azione fedele e ψ è un isomorfismo. Consideriamo il sottogruppo $H := \varphi^{-1}(\mathcal{A}_{2d})$; mostriamo che il suo indice in G è al più 2. Detta $\pi_{\mathcal{A}_{2d}}$ la proiezione al quoziente di $\mathcal{S}_{2d}$ su ${}^{\mathcal{S}_{2d}}\!/\!_{\mathcal{A}_{2d}} \cong \mathbb{Z}/2\mathbb{Z}$, possiamo caratterizzare H come

$$H = \varphi^{-1}(\mathcal{A}_{2d}) = \{g \in G \mid \varphi(g) \in \mathcal{A}_{2d}\} = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$$

Pertanto H è normale in G, essendo nucleo di un omomorfismo. Per il Primo Teorema di Omomorfismo vale che

$$G/_H = G/_{\ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)} \cong \operatorname{im}(\pi_{\mathcal{A}_{2d}} \circ \varphi) \hookrightarrow \mathbb{Z}/2\mathbb{Z}$$

e quindi $[G : H] \mid 2$.

Si osserva che H ha indice 1 se e solo se $G = H = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$, cioè se e solo se $\varphi(G) \subseteq \mathcal{A}_{2d}$. Mostriamo che esiste tuttavia un elemento di G la cui immagine tramite φ è una permutazione dispari. Poiché $2 \mid |G| = 2d$, per il Teorema di Cauchy esiste $g \in G$ tale per cui $\operatorname{ord}(g) = 2$. Dal momento che φ è un omomorfismo iniettivo abbiamo che $\operatorname{ord}(\varphi(g)) = \operatorname{ord}(g) = 2$; pertanto la permutazione $\varphi(g)$ si decompone in un prodotto di trasposizioni disgiunte.

In particolare la decomposizione di $\varphi(g)$ deve essere la stessa di $\lambda(g)$. Per contare il numero di trasposizioni di $\varphi(g)$ consideriamo l'azione naturale ζ di $\lambda(g)$ su G, ossia $\zeta : \langle \lambda(g) \rangle \to S(G)$ tale per cui

$$\zeta(\lambda(g)) : G \to G,\ h \mapsto \lambda(g)(h) = gh$$

Dal momento che λ è un'azione fedele, $\operatorname{Stab}_\zeta(h)$ è sempre banale per ogni $h \in G$, e quindi, per il Lemma orbita-stabilizzatore, $|\operatorname{Orb}_\zeta(h)| = |\langle \lambda(g) \rangle| = \operatorname{ord}(\lambda(g)) = 2$. Pertanto $\lambda(g)$ si decompone in d trasposizioni, e quindi $\varphi(g) \notin \mathcal{A}_{2d}$. Allora $[G : H] = 2$, da cui la tesi. $\square$

Osservazione 1.67 — In realtà, il sottogruppo di indice 2 in un gruppo di ordine $2d$ con d dispari è unico, e dunque caratteristico. Se infatti H e K sono due sottogruppi di indice 2, sia H che K sono normali in G. Pertanto HK è un sottogruppo di G, e dunque, per il Teorema di Lagrange, vale che:

$$\frac{d^2}{|H \cap K|} = \frac{|H| \cdot |K|}{|H \cap K|} = |HK| \mid |G| = 2d$$

In particolare, dal momento che per il Teorema di Lagrange $|H \cap K|$ divide $|H| = d$, $\frac{d}{|H \cap K|}$ divide 2, e dunque $|H \cap K|$ è uguale a d oppure $d = 2\,|H \cap K|$. Dacché per ipotesi d è dispari, deve per forza valere l'identità $|H \cap K| = d$. Pertanto $H = H \cap K = K$.

Possiamo generalizzare il ragionamento appena impiegato per dimostrare che H ha indice divisore di 2:

Proposizione 1.68

Sia G un gruppo e H un sottogruppo tale per cui $[G : H] = 2$. Se K è un sottogruppo di G, allora $H \cap K$ ha indice 1 o 2 in K.

Dimostrazione. Distinguiamo due casi:

- se $K \subseteq H$ allora $H \cap K = K$, da cui $[K : H \cap K] = 1$;
- se $K \nsubseteq H$, consideriamo la proiezione

$$\pi_H : G \to G/_H, g \mapsto gH$$

Dal momento che ${}^{G}\!/_{H} \cong \mathbb{Z}/2\mathbb{Z}$, gli unici sottogruppi del quoziente sono $\{H\}$ e ${}^{G}\!/_{H}$ stesso; pertanto $\pi_H(K) = {}^{G}\!/_{H}$ (altrimenti si avrebbe $K \subseteq \ker \pi_H = H$). Osserviamo che $\ker \pi_H\big|_K = \ker \pi_H \cap K = H \cap K$, e quindi, per il Primo Teorema di Omomorfismo, vale che

$$ {}^{K}\!/_{H \cap K} = {}^{K}\!/_{\ker \pi_H|_K} \cong \operatorname{im} \pi_H\big|_K = {}^{G}\!/_{H} \cong \mathbb{Z}/2\mathbb{Z} $$

ovverosia $[K : H \cap K] = 2$.

□

Esercizio 1.69 ($\star$)**.** Sia G un gruppo finito. Si dimostri che G è sempre isomorfo a un sottogruppo di $\mathrm{GL}_n(K)$ per un qualche n e per un campo K qualsiasi.

Soluzione. Per il Teorema di Cayley, l'*embedding* di Cayley induce un'immersione α di G in $\mathcal{S}_n$, dove $n = |G|$. Si mostra che a sua volta $\mathcal{S}_n$ si immerge in $\mathrm{GL}_n(K)$ dove K è un campo qualsiasi.

Si ricorda che vi è una corrispondenza naturale tra una permutazione $\sigma \in \mathcal{S}_n$ e la relativa matrice di permutazione[10] P_σ. In particolare $P_{(1\,2)}$ e $P_{(1\,2\,\ldots\,n)}$ generano un sottogruppo di $\mathrm{GL}_n(K)$ isomorfo a $\mathcal{S}_n$. Pertanto esiste un'immersione β di $\mathcal{S}_n$ in $\mathrm{GL}_n(K)$. Si conclude allora che $\beta \circ \alpha$ è l'immersione da G a $\mathrm{GL}_n(K)$ ricercata. □

Approfondimento 1.70 ($\star$) — La scelta del campo K per immergere G in $\mathrm{GL}_n(K)$ può risultare fondamentale per affrontare alcuni problemi. Consideriamo per esempio il problema di trovare un'immersione consona di un p-gruppo G in $\mathrm{GL}_n(K)$.

Se scegliamo $K = \mathbb{Z}/p\mathbb{Z}$, troviamo un'immersione di G in $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Chiamiamo H il sottogruppo isomorfo a K trovato in $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. In particolare, poiché K è un p-gruppo, anche H lo è, e quindi H è contenuto in un determinato p-Sylow di $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Poiché $p^{1+2+\ldots+n-1} = p^{\frac{n(n-1)}{2}} \parallel |\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})|$, come si evince dalla Proposizione 1.10, allora un p-Sylow di $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ ha ordine $p^{\frac{n(n-1)}{2}}$. Un tale p-Sylow è dato dalle matrici triangolari superiori (o inferiori) di $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ con tutti 1 sulla diagonale. Detto P questo sottogruppo, allora H è contenuto in un coniugato di P, dal momento che per il Teorema di Sylow i coniugati dei p-Sylow sono esattamente tutti i p-Sylow. In particolare, tramite una mappa di coniugio di può immergere H in P. Componendo le varie immersioni si dimostra quindi che un p-gruppo G si immerge sempre nel sottogruppo delle matrici triangolari superiori (o inferiori) di $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ con soli 1 sulla diagonale per $n = |G|$.

§1.7.4 Teorema di Poincaré

Illustriamo un teorema che risulterà utile nel futuro nello stabilire se un gruppo ammette sottogruppi normali.

[10] Per ulteriori approfondimenti si rimanda alla relativa pagina su Wikipedia.

Teorema 1.71 (Teorema di Poincaré)
Sia G un gruppo finito e sia $H \leqslant G$ un suo sottogruppo. Se $[G : H] = n$, allora esiste un sottogruppo normale $N \trianglelefteq G$ tale per cui che:

(1) $N \leqslant H \leqslant G$

(2) $n \mid [G : N] \mid n!$

Dimostrazione. La dimostrazione segue in parte lo schema utilizzato precedentemente per dimostrare la Proposizione 1.55. Si consideri l'usuale azione ψ di G su ${}^{G}\!/\!_{H}$ e si ponga $N = \ker \psi$.

(1) $N = \ker \psi$ è l'intersezione di tutti gli stabilizzatori dell'azione, e quindi è in particolare un sottinsieme di $\mathrm{Stab}(H) = H$. Pertanto $N \leqslant H \leqslant G$.

(2) Dal momento che $\ker \psi \leqslant H$, si verifica che $n = [G : H] \mid [G : \ker \psi]$. Dal Primo Teorema di Omomorfismo vale che

$$ {}^{G}\!/\!_{N} = {}^{G}\!/\!_{\ker \psi} \cong \operatorname{im} \psi \hookrightarrow \mathcal{S}_n $$

e quindi $[G : N] \mid |\mathcal{S}_n| = n!$.

Dal momento che N è normale in qualità di nucleo di ψ, N soddisfa i requisiti della tesi, e dunque il teorema è dimostrato. $\square$

Osservazione 1.72 — Se dunque G ha un sottogruppo non banale di indice n e $n! < |G|$ allora G ammette per il Teorema di Poincaré un sottogruppo normale non banale, ed è in particolare non semplice.

§1.8 Gruppo simmetrico e gruppo alterno

§1.8.1 Generatori di $\mathcal{S}_n$ e $\mathcal{A}_n$

Esibiamo alcuni insiemi di generatori per $\mathcal{S}_n$, con $n \geq 2$:

- $I_1 = \{(i\ j) \mid i, j \in \{1, \ldots, n\}, i < j\}$, dal momento che ogni permutazione può essere scritta come prodotto di trasposizione;
- $I_2 = \{(1\ j) \mid j \in \{2, \ldots, n\}\}$, dal momento che per ogni $i < j$ abbiamo
$$(i\ j) = (1\ i)(1\ j)(1\ i)$$
e dunque $\langle I_2 \rangle = \langle I_1 \rangle = \mathcal{S}_n$;
- $I_3 = \{(i\ i+1) \mid i \in \{1, \ldots, n-1\}\}$, infatti per ogni j abbiamo
$$(1\ j) = (j-1\ j)(1\ j-1)(j-1\ j)$$
e quindi $\langle I_3 \rangle = \langle I_2 \rangle = \mathcal{S}_n$;
- $I_4 = \{(1\ 2), (1\ 2\ \ldots\ n)\}$, infatti per ogni i abbiamo
$$(i\ i+1) = (1\ \ldots\ n)^{i-1}(1\ 2)(1\ \ldots\ n)^{1-i}$$
da cui $\langle I_4 \rangle = \langle I_3 \rangle = \mathcal{S}_n$.

Osservazione 1.73 — Quando si tratta il gruppo $\mathcal{S}_n$, bisogna tenere bene a mente che i numeri che si trovano all'interno dei cicli sono soltanto dei simboli. Come $(1\ 2)$ e $(1\ 2\ \ldots\ n)$ generano $\mathcal{S}_n$ per $n \geq 2$, anche $(3\ 4)$ e $(3\ 4\ 1\ 2\ 5\ 6\ \ldots\ n)$ generano lo stesso gruppo, ovverosia non c'è nessuna differenza se si scambia 1 con 3 e 2 con 4. Per lo stesso motivo, se X è un insieme finito di n elementi, $S(X)$ è isomorfo a $\mathcal{S}_n$.

Osservazione 1.74 — In generale non è vero che una trasposizione e un n-ciclo generano $\mathcal{S}_n$. Consideriamo ad esempio $H = \langle \sigma, \rho \rangle \leqslant \mathcal{S}_4$ con $\sigma = (1\ 2\ 3\ 4)$ e $\rho = (2\ 4)$. Allora $\sigma^4 = \rho^2 = 1$ e $\rho\sigma\rho^{-1} = (1\ 4\ 3\ 2) = \sigma^{-1}$. Pertanto H rispetta tutte le condizioni D_4, e dunque sarà isomorfo ad un suo quoziente. D'altra parte $\langle \sigma \rangle \cap \langle \rho \rangle = \{\mathrm{id}\}$ e $\rho \in \mathrm{N}_{\mathcal{S}_4}(\sigma)$, da cui si deduce che $\langle \sigma, \rho \rangle = \langle \sigma \rangle \langle \rho \rangle$ e quindi che $|\langle \sigma, \rho \rangle| = 4 \cdot 2 = 8$. Si può allora concludere che H è isomorfo a D_4.

Se tuttavia n fosse un numero primo, la tesi sarebbe valida, come dimostra il Lemma 3.18.

Esibiamo adesso alcuni insiemi di generatori per $\mathcal{A}_n$ con $n \geq 3$:

- $G_1 = \{(i\ j)(k\ l) \mid i \neq j,\ k \neq l\}$, infatti ogni elemento di $\mathcal{A}_n$ può essere scritto come prodotto di coppie di trasposizioni in quanto permutazione pari;
- $G_2 = \{(i\ j\ k) \mid i, j, k \text{ distinti}\}$, infatti si può dimostrare che $\langle G_2 \rangle = \langle G_1 \rangle$ considerando tre casi:
  - se $\{i, j\} = \{k, l\}$, allora $(i\ j)(k\ l) = \mathrm{id}$ appartiene già a $\langle G_2 \rangle$, essendo l'identità;
  - se $|\{i, j\} \cap \{k, l\}| = 1$, possiamo, senza perdita di generalità, supporre che valga $j = k$; allora, in tal caso, $(i\ j)(k\ l) = (i\ j)(j\ l) = (i\ j\ l) \in G_2$;
  - se $\{i, j\} \cap \{k, l\} = \varnothing$, allora $(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ j\ k)(j\ k\ l) \in \langle G_2 \rangle$.

  Pertanto $\langle G_2 \rangle = \langle G_1 \rangle = \mathcal{A}_n$.

§1.8.2 Significato del coniugio in $\mathcal{S}_n$

Illustriamo inoltre una relazione fondamentale di $\mathcal{S}_n$, che permette di caratterizzarne le classi di coniugio, come già visto negli Appunti di Algebra 1:

Lemma 1.75

Siano σ, $\tau \in \mathcal{S}_n$. Se $\sigma = (x_1 \ \dots \ x_k)$ è un k-ciclo, allora vale che

$$\tau\sigma\tau^{-1} = (\tau(x_1) \ \dots \ \tau(x_k))$$

Dimostrazione. Si verifica facilmente che

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

per ogni $i \in \{1, \dots, k\}$, da cui si deduce facilmente la tesi. □

Osservazione 1.76 — Quest'ultima relazione, relativa al coniugio in $\mathcal{S}_n$, permette di formalizzare l'osservazione fatta in precedenza, secondo cui "$\mathcal{S}_n$ è indipendente dai numeri e tratta solo dei simboli". Infatti il coniugio è la chiave attraverso cui si possono sostituire (in realtà permutare) i simboli di $S(X)$ con X finito. Ad esempio, per dimostrare formalmente che $(3\ 4)$ e $(3\ 4\ 1\ 2\ 5\ 6\ \dots\ n)$ generano $\mathcal{S}_n$, è sufficiente considerare il coniugio per $\sigma = (1\ 3)(2\ 4)$, detto φ_σ. Infatti φ_σ è un automorfismo (interno) di $\mathcal{S}_n$, e dunque vale che:

$$\langle \varphi_\sigma(1\ 2), \varphi_\sigma(1\ 2\ \dots\ n) \rangle = \langle (1\ 2), (1\ 2\ \dots\ n) \rangle = \mathcal{S}_n$$

Dal momento che $\varphi_\sigma(1\ 2) = (3\ 4)$ e $\varphi_\sigma(1\ 2\ \dots\ n) = (3\ 4\ 1\ 2\ 5\ 6\ \dots\ n)$, si è così dimostrato che questi due elementi generano $\mathcal{S}_n$.

Pertanto $\mathrm{Inn}(\mathcal{S}_n)$ si può descrivere intuitivamente come il gruppo di morfismi che permettono di permutare i simboli negli elementi $\mathcal{S}_n$. Non c'è dunque da meravigliarsi se $\mathrm{Inn}(\mathcal{S}_n) \cong \mathcal{S}_n$ per $n \geq 3$, dal momento che, come si è visto, tali morfismi sono delle vere e proprie permutazioni. Infatti $\mathrm{Inn}(\mathcal{S}_n) \cong {}^{\mathcal{S}_n}\!/_{Z(\mathcal{S}_n)} \cong \mathcal{S}_n$.

In realtà, per n diverso da 2 e 6 vale un risultato ancora più forte, ossia $\mathrm{Aut}(\mathcal{S}_n) \cong \mathcal{S}_n$, e dunque *tutti* i morfismi bigettivi di tali $\mathcal{S}_n$ sono esattamente quelli che permutano i simboli, come dimostra il Teorema 1.100.

§1.8.3 Sottogruppi abeliani transitivi di $\mathcal{S}_n$

Definizione 1.77. Un sottogruppo $G \leqslant \mathcal{S}_n$ si dice **transitivo** se l'azione naturale

$$\varphi : G \hookrightarrow \mathcal{S}_n : \sigma \mapsto \sigma$$

indotta da G su $\{1, \dots, n\}$ è transitiva, cioè se per ogni i, $j \in \{1, \dots, n\}$ esiste $\sigma \in G$ tale per cui $\sigma(i) = j$.

Lemma 1.78

Se G è un sottogruppo abeliano e transitivo di $\mathcal{S}_n$, allora[a] $|G| = n$.

[a] A partire da questo lemma si può dimostrare che un'azione fedele e transitiva di un gruppo abeliano è in particolare anche libera, ossia ammette solo stabilizzatori banali.

Dimostrazione. Consideriamo l'azione naturale φ di G su $\{1, \ldots, n\}$. Dal momento che G è transitivo, φ è un'azione transitiva, e dunque tutti i suoi stabilizzatori sono coniugati. Dacché però G è abeliano, gli stabilizzatori non solo sono coniugati, ma coincidono del tutto.

L'azione φ è fedele, e dunque:

$$\ker \varphi = \bigcap_{i=1}^{n} \mathrm{Stab}(i) = \{\mathrm{id}\}$$

Tuttavia, per quanto detto prima, gli stabilizzatori coincidono, e dunque $\bigcap_{i=1}^{n} \mathrm{Stab}(i) = \mathrm{Stab}(1)$, da cui si deduce che $\mathrm{Stab}(1)$ è banale. Allora, per il Lemma orbita-stabilizzatore, vale che $|G| = |\mathrm{Stab}(1)| \cdot |\mathrm{Orb}(1)| = 1 \cdot n = n$, da cui la tesi. □

§1.8.4 Sottogruppi abeliani massimali di $\mathcal{S}_{3m}$ ⋆

Vogliamo studiare i sottogruppi abeliani di $\mathcal{S}_{3m}$, caratterizzando in particolare i suoi sottogruppi abeliani massimali.

Lemma 1.79

Se $a_1, \ldots, a_k$ sono interi positivi tali che $\sum_{i=1}^{k} a_i = 3m$, con $m \geqslant k$ intero, allora $\prod_{i=1}^{k} a_i \leq 3^m$, e vale l'uguaglianza se e solo se $k = m$ e $a_i = 3$ per ogni $i \in \{1, \ldots, k\}$.

Dimostrazione. Senza perdita di generalità, a meno di aumentare k possiamo supporre $a_i \in \{1, 2, 3\}$ per ogni $i \in \{1, \ldots, k\}$, infatti se uno degli a_i è uguale a 4 possiamo sostituirlo con $2 + 2$, se uno degli a_i è uguale a 5 possiamo sostituirlo con $2 + (a_i - 2)$ e così via (queste sostituzioni mantengono inalterato il valore della somma). In particolare abbiamo che $a_i \leqslant 3$ per ogni $i \in \{1, \ldots, n\}$, pertanto

$$\prod_{i=1}^{k} a_i \leq 3^k \leq 3^m$$

inoltre se $k = m$ e tutti gli a_i sono uguali a 3 abbiamo chiaramente

$$\prod_{i=1}^{k} a_i = 3^k = 3^m$$

Viceversa, se il prodotto degli a_i è uguale a 3^m allora necessariamente $k = m$ e $a_i = 3$ per ogni $i \in \{1, \ldots, k\}$ in quanto possiamo supporre $a_i \in \{1, 2, 3\}$ senza perdita di generalità. □

Esercizio 1.80. Posto $n = 3m$, mostrare che la massima cardinalità di un sottogruppo abeliano di $\mathcal{S}_n$ è 3^m e caratterizzare la sua classe di isomorfismo.

Soluzione. Per prima cosa, osserviamo che $\mathcal{S}_n$ contiene sottogruppi abeliani di cardinalità $3m$, ad esempio

$$\langle(1\ 2\ 3)\rangle \cdot \langle(4\ 5\ 6)\rangle \cdot \ldots \cdot \langle(n-2\ n-1\ n)\rangle$$

è un sottogruppo abeliano di $\mathcal{S}_n$ di cardinalità 3^m, essendo isomorfo a

$$\langle(1\ 2\ 3)\rangle \times \langle(4\ 5\ 6)\rangle \times \ldots \times \langle(n-2\ n-1\ n)\rangle$$

Sia G un sottogruppo abeliano di $\mathcal{S}_n$ di ordine massimo, data

$$\psi : G \longrightarrow \mathcal{S}_n : \sigma \longmapsto \sigma$$

l'azione naturale di G su $\{1, \ldots, n\}$ chiamiamo $\Omega_1, \ldots, \Omega_k$ le orbite. Consideriamo le mappe $\varphi_i : G \longrightarrow \mathcal{S}(\Omega_i)$ tali che, data $\sigma \in G$ e fissata $\rho_1 \ldots \rho_k$ una sua decomposizione in cicli disgiunti, $\varphi_i(\sigma) = \rho_i$, poniamo $G_i = \mathrm{Im}\varphi_i = \mathrm{Im}\psi \cap \mathcal{S}(\Omega_i)$. Possiamo quindi costruire l'omomorfismo

$$\varphi : G \longrightarrow G_1 \times \ldots \times G_k : g \longmapsto (\varphi_1(g), \ldots, \varphi_k(g))$$

che è iniettivo in quanto

$$\varphi(\sigma) = id \iff \varphi_i(\sigma) = id_{\mathcal{S}(\Omega_i)} \iff \sigma_{|\Omega_i} = id_{\mathcal{S}(\Omega_i)}$$

per ogni $i \in \{1, \ldots, k\}$, che è equivalente a $\sigma = id_{\mathcal{S}_n}$ dato che le orbite ricoprono $\{1, \ldots, n\}$, da cui $\ker \varphi = \{id_{\mathcal{S}_n}\}$. Osserviamo adesso che ogni G_i è un gruppo abeliano poiché immagine omomorfa di G, che è un gruppo abeliano, inoltre è transitivo sull'orbita Ω_i per costruzione, pertanto per il Lemma 1.54 abbiamo $|G_i| = |\Omega_i|$ per ogni $i \in \{1, \ldots, k\}$. Vale quindi la seguente disuguaglianza, data dall'iniettività di φ

$$|G| \leqslant \prod_{i=1}^{k} |G_i| = \prod_{i=1}^{k} |\Omega_i|$$

D'altra parte

$$3m = \sum_{i=1}^{k} |\Omega_i|$$

pertanto per il Lemma 1.55 abbiamo $|G| \leq 3^m$, ma questa è effettivamente un'uguaglianza in quanto $\mathcal{S}_n$ contiene almeno un sottogruppo abeliano di ordine 3^m e G ha ordine massimo. Sempre per il Lemma 1.55 allora $k = m$ e $|\Omega_i| = 3$ per ogni $i \in \{1, \ldots, k\}$. Abbiamo quindi che φ è un isomorfismo e che $G_1 \times \ldots \times G_k$ è isomorfo a $(\mathbb{Z}/3\mathbb{Z})^k$, pertanto G è isomorfo a $(\mathbb{Z}/3\mathbb{Z})^k$. □

Osservazione 1.81 — Se $a_1, \ldots, a_k$ sono interi tali che

$$3m + 2 = \sum_{i=1}^{k} a_i$$

ragionando come nella dimostrazione del Lemma 1.55 possiamo scrivere

$$3m + 2 = 2 + \sum_{i=1}^{k-1} a_i$$

da cui ricaviamo

$$\prod_{i=1}^{k} a_i \leqslant 2 \cdot 3^m$$

Inoltre questa è un'uguaglianza se e solo se esiste $j \in \{1, \ldots, k\}$ tale che $a_j = 2$, $a_i = 3$ per ogni $i \in \{1, \ldots, k\} \setminus \{j\}$ e $k = m$. Ragionando come sopra otteniamo

$|G| \leqslant 2 \cdot 3^m$, d'altra parte osserviamo che $\mathcal{S}_n$ contiene un sottogruppo abeliano

$$\langle (1\ 2\ 3) \rangle \cdot \ldots \cdot \langle (3m-2\ 3m-1\ 3m) \rangle \cdot \langle (3m+1\ 3m+2) \rangle$$

di ordine $2 \cdot 3^m$ poiché isomorfo a

$$\langle (1\ 2\ 3) \rangle \times \ldots \times \langle (3m-2\ 3m-1\ 3m) \rangle \times \langle (3m+1\ 3m+2) \rangle$$

pertanto $|G| = 2 \cdot 3^m$ e $G \cong (\mathbb{Z}/3\mathbb{Z})^m \times \mathbb{Z}/2\mathbb{Z}$. Se $n = 3m+1$, ragionando in modo simile abbiamo che la somma delle cardinalità delle orbite $\Omega_1, \ldots, \Omega_k$ è $3m+1$ e il loro prodotto è minore o uguale a $4 \times 3^{m-1}$, da cui $|G| \leq 4 \cdot 3^{m-1}$. D'altra parte $\mathcal{S}_n$ contiene almeno due tipi di sottogruppi abeliani di ordine $3m+1$, uno isomorfo a $(\mathbb{Z}/3\mathbb{Z})^{m-1} \times \mathbb{Z}/4\mathbb{Z}$ e uno isomorfo a $(\mathbb{Z}/3\mathbb{Z})^{m-1} \times V_4$, dove

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

è un sottogruppo abeliano non ciclico di $\mathcal{S}_4$, chiamato **gruppo di Klein** (o *Klein 4-group*). Pertanto un sottogruppo abeliano di ordine massimo deve avere una di queste due forme.

Osservazione 1.82 — I sottogruppi di $\mathcal{S}_n$ di questo tipo sono tutti coniugati tra loro, infatti se

$$G = \langle (x_1\ x_2\ x_3) \rangle \cdot \ldots \cdot \langle (x_{n-2}\ x_{n-1}\ x_n) \rangle$$
$$G' = \langle (y_1\ y_2\ y_3) \rangle \cdot \ldots \cdot \langle (y_{n-2}\ y_{n-1}\ y_n) \rangle$$

sono due sottogruppi abeliani di $\mathcal{S}_n$ di ordine massimo (per semplicità supponiamo $n = 3m$, gli altri due casi si studiano in modo analogo) consideriamo $\sigma \in \mathcal{S}_n$ tale che $\sigma(y_i) = x_i$ per ogni $i \in \{1, \ldots, n\}$, è sufficiente mostrare che i generatori delle componenti del prodotto sono tra loro coniugate. Infatti, per il Lemma 1.56 abbiamo

$$\sigma(x_i\ x_{i+1}\ x_{i+2})\sigma^{-1} = (\sigma(x_i)\ \sigma(x_{i+1})\ \sigma(x_{i+2})) = (y_i\ y_{i+1}\ y_{i+2})$$

per ogni $i \in \{1, \ldots, n-2\}$, pertanto G e G' sono coniugati.

§1.8.5 I sottogruppi derivati di $\mathcal{S}_n$ e di $\mathcal{A}_n$

In questa sezione si studiano i gruppi derivati di $\mathcal{S}_n$ e di $\mathcal{A}_n$.

Per $n = 2$, la discussione è del tutto banale. Infatti $\mathcal{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$, e quindi $\mathcal{S}_2' = \{\mathrm{id}\} = \mathcal{A}_2 = \mathcal{A}_2'$.

Sia adesso $n \geq 3$. Siano $\tau_1 = (i\ j)$ e $\tau_2 = (j\ k)$ due trasposizioni di $\mathcal{S}_n$ con i, j e k distinti. Allora vale che:

$$[\tau_1, \tau_2] = (k\ i\ j)^2 = (k\ j\ i).$$

Pertanto, al variare di i, j e k si possono realizzare tutti i 3-cicli di $\mathcal{S}_n$ come commutatore di due trasposizioni. Allora, poiché i 3-cicli generano $\mathcal{A}_n$ per $n \geq 3$, vale che $\mathcal{A}_n \subseteq \mathcal{S}_n'$. Pertanto $\mathcal{S}_n'$ è $\mathcal{A}_n$ o $\mathcal{S}_n$.

Allo stesso tempo, l'omomorfismo sgn ha come codominio un gruppo abeliano e come nucleo $\mathcal{A}_n$. Pertanto $\mathcal{S}_n' \subseteq \ker \operatorname{sgn} = \mathcal{A}_n$. Si conclude dunque che vale:

$$\mathcal{S}_n' = \mathcal{A}_n, \quad \forall n \geq 3.$$

Osservazione 1.83 — Dall'ultimo risultato si può immediatamente dedurre che, se G è un gruppo abeliano, allora gli omomorfismi da $\mathcal{S}_n$ a G sono in bigezione con gli omomorfismi da $(\mathcal{S}_n)_{ab} = \mathcal{S}_n/\mathcal{S}_n' \cong \mathbb{Z}/2\mathbb{Z}$ a G, tramite il Primo teorema di Omomorfismo.

Per $\mathcal{A}_n$, la questione si complica. Infatti, come vedremo, $\mathcal{A}_n$ è molto "non abeliano", ossia, per $n \geq 5$, $\mathcal{A}_n$ e il suo derivato coincidono.

Sia infatti $n \geq 5$. Allora, se $x = (a\ c\ b)$ e $y = (b\ c)(d\ e)$, per a, b, c, d ed e distinti, vale che:

$$[x, y] = (c\ a)(b\ c\ a)(b\ c)(d\ e)^2 = (b\ c\ a),$$

e dunque, al variare di a, b, c, ogni 3-ciclo di $\mathcal{A}_n$ può scriversi come commutatore. Pertanto, poiché i 3-cicli generano ancora $\mathcal{A}_n$, $\mathcal{A}_n \subseteq \mathcal{A}_n' \subseteq \mathcal{A}_n$, e dunque vale che[11]:

$$\mathcal{A}_n' = \mathcal{A}_n, \quad \forall n \geq 5.$$

Per $n = 4$, la situazione è totalmente diversa. Infatti V_4, il gruppo di Klein, è un sottogruppo normale di $\mathcal{A}_4$. In particolare $[\mathcal{A}_4 : V_4] = 3$, e dunque $\mathcal{A}_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$. Dal momento che $\mathbb{Z}/3\mathbb{Z}$ è abeliano, $\mathcal{A}_4' \subseteq V_4$. Inoltre $\mathcal{A}_4'$ non può essere banale dacché $\mathcal{A}_4$ non è abeliano; pertanto esiste una doppia trasposizione σ in $\mathcal{A}_4'$. Dal momento che $\mathcal{A}_4'$ è normale in $\mathcal{A}_4$, $\mathcal{C}\ell_{\mathcal{A}_4}(\sigma) \subseteq \mathcal{A}_4$, e dunque $V_4 \subseteq \mathcal{A}_4$. Si conclude dunque che $\mathcal{A}_4' = V_4$. Per $n = 3$, invece, $\mathcal{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$, e dunque $\mathcal{A}_3'$ è banale.

La classificazione è dunque la seguente:

- se $n \geq 5$, $\mathcal{A}_n' = \mathcal{A}_n$;
- se $n = 4$, $\mathcal{A}_4' = V_4$;
- se $n = 3$, $\mathcal{A}_3' = \{\mathrm{id}\}$.

§1.8.6 Classi di coniugio in $\mathcal{A}_n$

Studiamo le classi di coniugio in $\mathcal{A}_n$. In particolare, fissato $\sigma \in \mathcal{A}_n$, vogliamo determinare una relazione tra $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$ e $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$.

Si osserva innanzitutto che per il Lemma orbita-stabilizzatore vale che:

$$|\mathcal{A}_n| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| \cdot |\mathrm{Z}_{\mathcal{A}_n}(\sigma)|$$

Inoltre $\mathrm{Z}_{\mathcal{A}_n}(\sigma) = \mathrm{Z}_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n$. Pertanto si ricava la seguente identità:

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{|\mathcal{A}_n|}{|\mathrm{Z}_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2}\frac{|\mathcal{S}_n|}{|\mathrm{Z}_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n|}$$

Dal momento che $[\mathcal{S}_n : \mathcal{A}_n] = 2$, per la Proposizione 1.49 $[\mathrm{Z}_{\mathcal{S}_n}(\sigma) : \mathrm{Z}_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n]$ vale 1 se $\mathrm{Z}_{\mathcal{S}_n}(\sigma) \leqslant \mathcal{A}_n$ e 2 altrimenti. Distinguiamo quindi i due casi:

- nel primo caso $|\mathrm{Z}_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n| = |\mathrm{Z}_{\mathcal{S}_n}(\sigma)|$, e quindi $|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)|$;
- nel secondo caso $|\mathrm{Z}_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n| = \frac{1}{2}|\mathrm{Z}_{\mathcal{S}_n}(\sigma)|$, e quindi $|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = |\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)|$, ovverosia $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$ e $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$ coincidono.

[11]Questo risultato diviene totalmente ovvio una volta che si dimostra che $\mathcal{A}_n$ è semplice per $n \geq 5$, come mostra il Teorema 1.91.

Ipotizziamo di essere nel primo caso. Allora possiamo dimostrare che

$$\mathcal{C}\ell_{\mathcal{S}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$$

dove τ è una qualsiasi permutazione dispari di $\mathcal{S}_n$.

Chiaramente $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1}) \subseteq \mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$, dal momento che i coniugati di $\tau\sigma\tau^{-1}$ sono anche coniugati di σ. D'altra parte per ogni $\rho \in \mathcal{S}_n$ si verifica che:

- $\rho\sigma\rho^{-1} \in \mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$, se ρ è pari;
- $\rho\sigma\rho^{-1} = (\rho\tau^{-1})(\tau\sigma\tau^{-1})(\rho\tau^{-1})^{-1} \in \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$, se ρ è dispari.

Quindi si conclude che $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$.

Osservazione 1.84 — Si mostra facilmente che $|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = |\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})|$. Infatti vale che:

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{|\mathcal{A}_n|}{|\mathrm{Z}_{\mathcal{A}_n}(\sigma)|} = \frac{|\mathcal{A}_n|}{|\mathrm{Z}_{\mathcal{A}_n}(\tau\sigma\tau^{-1})|} = |\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})|$$

dove, ricordando che l'unico coniugato di $\mathcal{A}_n$ è $\mathcal{A}_n$ stesso, si osserva che[a]:

$$|\mathrm{Z}_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\mathrm{Z}_{\mathcal{S}_n}(\tau\sigma\tau^{-1}) \cap \mathcal{A}_n| = |\tau\,\mathrm{Z}_{\mathcal{S}_n}(\sigma)\tau^{-1} \cap \mathcal{A}_n|$$

e quindi che:

$$|\mathrm{Z}_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\tau(\mathrm{Z}_{\mathcal{S}_n} \cap \mathcal{A}_n)\tau^{-1}| = |\mathrm{Z}_{\mathcal{A}_n}(\sigma)|$$

[a] L'identità $\mathrm{Z}_{\mathcal{S}_n}(\tau\sigma\tau^{-1}) = \tau\,\mathrm{Z}_{\mathcal{S}_n}(\sigma)\tau^{-1}$ non è altro che un corollario dell'identità $\mathrm{Stab}(g \cdot x) = g\,\mathrm{Stab}(x)g^{-1}$, dove si considera come azione l'azione di coniugio.

Si esclude subito il caso in cui $|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})|$: se così fosse, $\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$ avrebbe tanti elementi quanti $\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})$, e così, per l'osservazione precedente, anche $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$; in tal caso saremmo nel secondo caso descritto precedentemente, mentre per ipotesi avevamo posto di essere nel primo.

Pertanto vale che:

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})| = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)|$$

da cui si ricava che:

$$|\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| + |\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})|$$

Pertanto, per il Principio di Inclusione-Esclusione, l'unione descritta precedentemente è anche disgiunta, come volevamo dimostrare.

Si riassume dunque lo studio della classe di coniugio di $\sigma \in \mathcal{A}_n$ in $\mathcal{A}_n$ stesso:

- se $\mathrm{Z}_{\mathcal{S}_n}(\sigma) \not\subseteq \mathcal{A}_n$, allora le classi di coniugio di σ in $\mathcal{S}_n$ e in $\mathcal{A}_n$ coincidono;
- altrimenti, se τ è una permutazione dispari di $\mathcal{S}_n$, vale che $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$, dove ogni termine dell'unione ha metà degli elementi di $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$.

§1.8.7 Classificazione delle classi di coniugio di $\mathcal{A}_5$ e di $\mathcal{A}_6$

Illustriamo adesso una tabella che conta le cardinalità delle varie classi di coniugio in $\mathcal{S}_5$, che ricordiamo essere esattamente gli insiemi delle permutazioni con la medesima decomposizione in cicli (e dunque le classi di coniugio sono in bigezione con le partizioni di 5).

Partizioni di 5	Cardinalità della classe di coniugio associata
5	$\binom{5}{5}\frac{5!}{5} = 4! = 24$
$4+1$	$\binom{5}{4}\frac{4!}{4} = 30$
$3+2$	$\binom{5}{3}\frac{4!}{4}\binom{2}{2}\frac{2!}{2} = 20$
$3+1+1$	$\binom{5}{3}\frac{3!}{3} = 20$
$2+2+1$	$\frac{1}{2}\binom{5}{2}\frac{2!}{2}\binom{3}{2}\frac{2!}{2} = 15$
$2+1+1+1$	$\binom{5}{2}\frac{2!}{2} = 10$
$1+1+1+1+1$	1

Si osserva che nel calcolo della cardinalità della classe associata alla partizione $2+2+1$ è necessario dividere per 2, dacché contiamo i cicli di stessa lunghezza a meno dell'ordine. Di queste, le permutazioni non banali che appartengono a $\mathcal{A}_5$ sono quelle la cui classe di coniugio è associata alle partizioni 5, $3+1+1$ e $2+2+1$, cioè le permutazioni σ_5, σ_3 e σ_2 aventi una decomposizione in cicli disgiunti della forma

$$\sigma_5 = (a_1\ a_2\ a_3\ a_4\ a_5), \quad \sigma_3 = (b_1\ b_2\ b_3), \quad \sigma_2 = (c_1\ c_2)(d_1\ d_2)$$

Studiamo le classi di coniugio di questi elementi in $\mathcal{A}_5$.

- si mostra che $\mathrm{Z}_{\mathcal{S}_5}(\sigma_5) = \langle (a_1\ a_2\ a_3\ a_4\ a_5) \rangle$, infatti vale che:

  $$|\mathrm{Z}_{\mathcal{S}_5}(\sigma_5)| = \frac{|\mathcal{S}_5|}{|\mathcal{C}\ell_{\mathcal{S}_5}(\sigma_5)|} = \frac{5!}{4!} = 5$$

  Allora $\mathrm{Z}_{\mathcal{S}_5}(\sigma_5)$ contiene solo permutazioni pari. Data dunque una permutazione dispari $\psi \in \mathcal{S}_5$, per quanto visto prima, vale dunque che:

  $$\mathcal{C}\ell_{\mathcal{S}_5}(\sigma_5) = \mathcal{C}\ell_{\mathcal{A}_5}(\sigma_5) \mathbin{\dot\cup} \mathcal{C}\ell_{\mathcal{A}_5}(\psi\sigma_5\psi^{-1})$$

- $\mathrm{Z}_{\mathcal{S}_5}(\sigma_3)$ non è contenuto in $\mathcal{A}_5$ dal momento che una trasposizione ψ disgiunta da σ_3 è una permutazione dispari che appartiene al $\mathrm{Z}_{\mathcal{S}_5}(\sigma_3)$. Pertanto vale che:

  $$\mathcal{C}\ell_{\mathcal{S}_5}(\sigma_3) = \mathcal{C}\ell_{\mathcal{A}_5}(\sigma_3)$$

- anche $\mathrm{Z}_{\mathcal{S}_5}(\sigma_2)$ non è contenuto in $\mathcal{A}_5$, dal momento che $(c_1\ c_2)$ è una permutazione dispari che commuta con σ_2. Infatti $(c_1\ c_2)$ e $(d_1\ d_2)$ commutano in quanto cicli disgiunti e $(c_1\ c_2)$ commuta con se stessa. Pertanto vale ancora che:

  $$\mathcal{C}\ell_{\mathcal{S}_5}(\sigma_2) = \mathcal{C}\ell_{\mathcal{A}_5}(\sigma_2)$$

Adesso possiamo illustrare le cardinalità delle classi di coniugio in $\mathcal{A}_5$:

Rappresentante della classe	Cardinalità della classe	Coincide con la classe in $\mathcal{S}_n$
(1 2 3 4 5)	$\frac{24}{2} = 12$	No
(2 1 3 4 5)	$\frac{24}{2} = 12$	No
(1 2 3)	20	Sì
(1 2)(3 4)	15	Sì
id	1	Sì

Infatti ogni 3-ciclo σ_3, per quanto visto prima, appartiene alla stessa classe di coniugio in $\mathcal{A}_n$, dacché $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma_3) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma_3)$. In particolare $(1\ 2\ 3)$ è un rappresentante di tale classe. Lo stesso discorso vale per le doppie trasposizioni, che hanno come rappresentante $(1\ 2)(3\ 4)$. Per l'identità, le proprietà elencate nella tabella sono del tutto banali da verificare.

Al contrario, vi sono due classi di coniugio possibili per un 5-ciclo, e ognuna di queste classi si ottiene coniugando un rappresentante dell'altra per una permutazione dispari, per quanto visto prima. Pertanto, se $(1\ 2\ 3\ 4\ 5)$ è il rappresentante di una classe, $(1\ 2)(1\ 2\ 3\ 4\ 5)(1\ 2)^{-1} = (2\ 1\ 3\ 4\ 5)$ è rappresentante dell'altra classe. Dal momento che entrambe hanno la stessa cardinalità e partizionano $\mathcal{C}\ell_{\mathcal{S}_n}(1\ 2\ 3\ 4\ 5)$, in particolare hanno cardinalità $\frac{24}{2} = 12$.

Analogamente a quanto fatto per $\mathcal{A}_5$, si possono descrivere le cardinalità delle classi di coniugio di $\mathcal{A}_6$. Innanzitutto contiamo le cardinalità delle classi di coniugio degli elementi di $\mathcal{A}_6$ in $\mathcal{S}_6$:

Partizioni di 6 relative a elementi di $\mathcal{A}_6$	Cardinalità della classe di coniugio associata
$5 + 1$	$\binom{6}{5}\frac{5!}{5} = 144$
$4 + 2$	$\binom{6}{4}\frac{4!}{4}\binom{2}{2}\frac{2!}{2} = 90$
$3 + 3$	$\frac{1}{2}\binom{6}{3}\frac{3!}{3}\binom{3}{3}\frac{3!}{3} = 40$
$3 + 1 + 1 + 1$	$\binom{6}{3}\frac{3!}{3} = 40$
$2 + 2 + 1 + 1$	$\frac{1}{2}\binom{6}{2}\frac{2!}{2}\binom{4}{2}\frac{2!}{2} = 45$
$1 + 1 + 1 + 1 + 1 + 1$	1

Si mostra che, eccetto per quella di un 5-ciclo, tutte le classi di coniugio di $\mathcal{A}_6$ coincidono con quelle di $\mathcal{S}_6$.

- se σ_5 è un 5-ciclo, allora $|\mathrm{Z}_{\mathcal{S}_6}(\sigma_5)| = \frac{6!}{144} = 5$ per il Lemma orbita-stabilizzatore; pertanto $\mathrm{Z}_{\mathcal{S}_6}(\sigma_5) = \langle \sigma_5 \rangle \subseteq \mathcal{A}_6$;
- se $\sigma_{4,2}$ è un prodotto di un 4-ciclo e di un 2-ciclo, allora σ_4 commuta con la trasposizione che compare nella sua decomposizione, e dunque $\mathrm{Z}_{\mathcal{S}_6}(\sigma_4) \not\subseteq \mathcal{A}_6$; lo stesso discorso si applica a un prodotto $\sigma_{2,2}$ di due 2-cicli;

- se $\sigma_{3,3} = (a_1, a_2, a_3)(b_1, b_2, b_3)$ è prodotto di due 3-cicli, allora, posto:
$$\tau = (a_1, b_1)(a_2, b_2)(a_3, b_3)$$
vale che $\tau\sigma_{3,3}\tau^{-1} = \sigma_{3,3}$, e quindi $\sigma_{3,3}$ e τ commutano; dacché $\tau \notin \mathcal{A}_6$, $\mathrm{Z}_{\mathcal{S}_6}(\sigma_{3,3}) \not\subseteq \mathcal{A}_6$;
- se σ_3 è un 3-ciclo, allora σ_3 commuta con una trasposizione composta da elementi che non compaiono in σ_3, e quindi ancora $\mathrm{Z}_{\mathcal{S}_6}(\sigma_3) \not\subseteq \mathcal{A}_6$.

Si illustrano adesso i numeri degli elementi nelle classi di coniugio di $\mathcal{A}_6$, secondo le stesse ragioni impiegate per costruire la tabella relativa a $\mathcal{A}_5$:

Rappresentante della classe	Cardinalità della classe	Coincide con la classe in $\mathcal{S}_n$
(1 2 3 4 5)	$\frac{144}{2} = 72$	No
(2 1 3 4 5)	$\frac{144}{2} = 72$	No
(1 2 3 4)(5 6)	90	Sì
(1 2 3)(4 5 6)	40	Sì
(1 2 3)	40	Sì
(1 2)(3 4)	45	Sì
id	1	Sì

§1.8.8 Semplicità di $\mathcal{A}_n$ per $n \geq 5$

Si illustra in questa sezione un risultato fondamentale per $\mathcal{A}_n$ con $n \geq 5$, che permetterà successivamente di classificare tutti i sottogruppi normali di $\mathcal{S}_n$.

Definizione 1.85. Un gruppo G non banale si dice **semplice** se i suoi unici sottogruppi normali sono $\{e\}$ e G, ovverosia se i suoi sottogruppi normali sono banali.

Osservazione 1.86 — Gli unici gruppi abeliani finiti semplici sono i gruppi ciclici $\mathbb{Z}/p\mathbb{Z}$ con p numero primo. Se infatti G fosse un gruppo abeliano finito, detto $n = |G|$, se n non fosse primo esisterebbe un suo divisore proprio e non banale k. Inoltre, poiché $k \mid n$, esiste un sottogruppo non banale H di ordine k in G. Dacché G è abeliano, H è normale, e dunque G non è semplice.

Proposizione 1.87

$\mathcal{A}_5$ è semplice.

Dimostrazione. Un sottogruppo è normale se e solo se è unione disgiunta delle classi di coniugio dei suoi elementi. Pertanto la cardinalità di $N \trianglelefteq \mathcal{A}_5$ deve essere somma di alcuni termini nella seconda colonna della tabella costruita precedentemente per le classi di coniugio di $\mathcal{A}_5$, comprendendo sempre 1. D'altra parte $|N|$ deve dividere $|\mathcal{A}_5| = 60$, e quindi vale che:
$$|N| \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$
Si verifica a mano che nessuna tale somma appartiene all'insieme su descritto eccetto che per i casi in cui $|N| = 1$ o $|N| = 60$, da cui si deduce che $N = \{\mathrm{id}\}$ o $N = \mathcal{A}_5$. Pertanto $\mathcal{A}_5$ è semplice. □

Seguendo la stessa traccia si può dimostrare che anche $\mathcal{A}_6$ è semplice, da cui dedurremo successivamente che $\mathcal{A}_n$ è semplice per $n \geq 5$.

Proposizione 1.88

$\mathcal{A}_6$ è semplice.

Dimostrazione. Come prima, un sottogruppo è normale se e solo se è unione disgiunta delle classi di coniugio dei suoi elementi. Quindi la cardinalità di un sottogruppo normale N di $\mathcal{A}_6$ deve essere somma di alcuni termini della seconda colonna della tabella costruita appositamente per le classi di coniugio di $\mathcal{A}_6$, in cui si ammette sempre 1. Inoltre $|N|$ deve dividere $|\mathcal{A}_6| = 360$, e quindi vale che:

$$|N| \in \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360\}$$

Si verifica manualmente che nessuna tale somma appartiene a questo insieme, eccetto che per i casi in cui $|N| = 1$ o $|N| = 360$, da cui si deduce che $N = \{\mathrm{id}\}$ o $N = \mathcal{A}_6$. Si conclude dunque che $\mathcal{A}_6$ è semplice. □

Si illustra adesso un lemma molto utile, che permetterà di dimostrare in modo alternativo la semplicità di $\mathcal{A}_5$:

Lemma 1.89

Sia G un gruppo e N un suo sottogruppo normale di indice finito. Allora N contiene ogni elemento di G il cui ordine è coprimo con $[G : N]$.

Dimostrazione. Sia $n = [G : N]$ e sia $g \in G$ tale per cui $(\mathrm{ord}(g), n) = 1$. Si consideri la proiezione π_N di G su ${}^{G}\!/\!_{N}$. Poiché π_N è un omomorfismo, $\mathrm{ord}(\pi_N(g))$ divide $(\mathrm{ord}(g), n) = 1$. Pertanto $\pi_N(g) = N$, ossia $g \in N$, da cui la tesi. □

Dimostrazione alternativa della Proposizione 1.87. Sia N un sottogruppo normale di $\mathcal{A}_5$. Distinguiamo tre casi, in base a se 2 o 3 dividono $[\mathcal{A}_5 : N]$:

- se $2 \nmid [\mathcal{A}_5 : N]$, per il Lemma 1.89 N contiene tutti gli elementi di $\mathcal{A}_5$ di ordine 2, cioè le doppie trasposizioni, le quali generano $\mathcal{A}_5$, e quindi $N = \mathcal{A}_5$;
- se $3 \nmid [\mathcal{A}_5 : N]$, per il Lemma 1.89 N contiene tutti gli elementi di $\mathcal{A}_5$ di ordine 3, cioè i 3-cicli, che generano $\mathcal{A}_5$, e quindi ancora $N = \mathcal{A}_5$;
- se $6 \mid [\mathcal{A}_5 : N]$, allora $|N| \mid 10$, ma l'unico divisore di 10 che si può ottenere sommando i termini della seconda colonna della tabella delle classi di coniugio di $\mathcal{A}_5$, ammettendo sempre 1, è 1 stesso, e quindi $N = \{\mathrm{id}\}$.

In ogni caso N è $\mathcal{A}_5$ o $\{\mathrm{id}\}$, e dunque $\mathcal{A}_5$ è semplice. □

A partire dal seguente lemma si può poi dimostrare che $\mathcal{A}_n$ è semplice per $n \geq 5$:

Lemma 1.90

Sia H un sottogruppo normale di $\mathcal{A}_n$ con $n \geq 5$. Se H contiene un 3-ciclo, allora H contiene tutti i 3-cicli, e in particolare $H = \mathcal{A}_n$.

Dimostrazione. Sia $\sigma_3 = (a_1\ a_2\ a_3)$ il 3-ciclo contenuto in H. Poiché H è normale, $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma_3) \subseteq H$. Poiché $n \geq 5$, esistono a_4 e a_5 distinti dagli elementi di σ_3, e dunque σ_3 commuta con $\tau = (a_4\ a_5)$, essendo un ciclo distinto. Allora $\mathrm{Z}_{\mathcal{S}_n}(\sigma_3) \not\subseteq \mathcal{A}_n$, e dunque la classe di coniugio di σ_3 in $\mathcal{A}_3$ coincide con quella in $\mathcal{S}_n$. Pertanto vale che:

$$\mathcal{C}\ell_{\mathcal{S}_n}(\sigma_3) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma_3) \subseteq H$$

e dunque, essendo $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma_3)$ l'insieme di tutti i 3-cicli di $\mathcal{S}_n$, H contiene tutti i 3-cicli. In particolare, dacché i 3-cicli generano $\mathcal{A}_n$, $H = \mathcal{A}_n$, da cui la tesi. □

Teorema 1.91

$\mathcal{A}_n$ è semplice per $n \geq 5$.

Dimostrazione. Per $n = 5$ la tesi è garantita dalla Proposizione 1.87. Si procede per induzione per $n \geq 6$. Il passo base è già garantito dalla Proposizione 1.88.

Si assuma ora l'ipotesi induttiva. Sia $H \trianglelefteq \mathcal{A}_{n+1}$ con $n \geq 6$. Consideriamo K_i come il sottogruppo delle permutazioni pari di $\mathcal{A}_{n+1}$ che fissano un i generico, ovverosia:

$$K_i = \{\sigma \in \mathcal{A}_{n+1} \mid \sigma(i) = i\}$$

Questo sottogruppo è naturalmente isomorfo a $\mathcal{A}_n$, allo stesso modo in cui il sottogruppo delle permutazioni di $\mathcal{S}_{n+1}$ che fissano un i generico è isomorfo in modo naturale a $\mathcal{S}_n$.

Dal momento che H è normale, $H \cap K_i$ è normale in $K_i \cong \mathcal{A}_n$, che tuttavia è semplice. Pertanto $H \cap K_i$ è banale o è K_i stesso. Se $H \cap K_i$ è K_i per un qualche i, allora $K_i \subseteq H$, e dunque H contiene un 3-ciclo. Allora, per il Lemma 1.90, H è $\mathcal{A}_n$.

Se invece $H \cap K_i$ è banale per ogni i, si mostra che $H = \{\mathrm{id}\}$. Se infatti H non fosse composto della sola identità, allora si potrebbe supporre per assurdo che esiste $\sigma \in H \setminus \{\mathrm{id}\}$. Poiché $\sigma \neq \mathrm{id}$, esiste $j \neq 1$ tale per cui $\sigma(1) = j$ (altrimenti σ stabilizzerebbe 1 e apparterrebbe a $H \cap K_1$).

Sia τ il 3-ciclo $(j\ k\ l)$, dove j, k, l e 1 sono elementi distinti. Si consideri il commutatore $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$. Si osserva che $[\sigma, \tau]$ appartiene ad H, infatti:

$$[\sigma, \tau] = \underbrace{\sigma}_{\in H} \underbrace{(\tau\sigma^{-1}\tau^{-1})}_{\in H} \in H$$

Detto $\rho = (\sigma\tau\sigma^{-1})$, $[\sigma, \tau]$ è prodotto di due 3-cicli, ovverosia ρ e τ^{-1}, e può dunque contenere nella sua decomposizione al più 6 elementi non fissi.

Poiché $n \geq 6$, $\mathcal{A}_{n+1}$ contiene naturalmente $\mathcal{A}_7$, e quindi $[\sigma, \tau]$ deve ammettere almeno un punto fisso. Poiché però $H \cap K_i$ è banale per ogni i, ciò vuol dire che $[\sigma, \tau]$ è l'identità stessa. Pertanto σ e τ devono commutare.

Tuttavia $(\sigma\tau)(1) = \sigma(1) = j$, mentre $(\tau\sigma)(1) = \tau(j) = k \neq j$. Quindi σ e τ non commutano, assurdo. Pertanto $H = \{\mathrm{id}\}$, da cui si deduce che $\mathcal{A}_{n+1}$ è semplice. Si conclude dunque induttivamente che $\mathcal{A}_n$ è semplice per $n \geq 6$, e dunque che lo è per $n \geq 5$, da cui la tesi. □

Corollario 1.92

L'insieme $X = \{\sigma \in \mathcal{S}_n \mid \sigma \text{ è un 5-ciclo}\}$ genera $\mathcal{A}_n$ per $n \geq 5$.

Dimostrazione. Si osserva che $\langle X \rangle$ è un sottogruppo normale di $\mathcal{A}_n$ che contiene almeno un elemento distinto dall'identità. Allora, per il Teorema 1.91, $\langle X \rangle$ è necessariamente $\mathcal{A}_n$, da cui la tesi. $\square$

Osservazione 1.93 — Vale in generale una tesi più forte di quella del Corollario 1.92, ovverosia, se k è un numero dispari maggiore o uguale di 5, $\mathcal{A}_n$ è generato dai k-cicli per $n \geq k$, con la stessa dimostrazione presentata per il corollario citato.

§1.8.9 Sottogruppi normali di $\mathcal{S}_n$

Lemma 1.94

Per $n \geq 3$ il centro di $\mathcal{S}_n$ è banale, ossia $\mathrm{Z}(\mathcal{S}_n) = \{\mathrm{id}\}$.

Dimostrazione. Sia $\sigma \in \mathrm{Z}(\mathcal{S}_n)$. Si assuma $\sigma \neq \mathrm{id}$. Allora esistono x e y distinti in $\{1, \ldots, n\}$ tali per cui $\sigma(x) = y$. Sia z un elemento di $\{1, \ldots, n\}$ distinto da x e y. Posto $\tau = (y z)$ vale allora che

$$(\tau\sigma)(x) = \tau(y) = z, \quad (\sigma\tau)(x) = \sigma(x) = y$$

Dal momento che $y \neq z$, vale che $\tau\sigma \neq \sigma\tau$, e dunque $\sigma \notin \mathrm{Z}(\mathcal{S}_n)$, assurdo. Pertanto $\sigma = \mathrm{id}$, da cui si deduce che $\mathrm{Z}(\mathcal{S}_n)$ è composto della sola identità. $\square$

Proposizione 1.95

Per $n = 3$ e $n \geq 5$, gli unici sottogruppi normali di $\mathcal{S}_n$ sono $\{\mathrm{id}\}$, $\mathcal{A}_n$ e $\mathcal{S}_n$.

Dimostrazione. Sia N un sottogruppo normale di $\mathcal{S}_n$ e consideriamo $K = N \cap \mathcal{A}_n$. Poiché N è normale in $\mathcal{S}_n$, K è normale in $\mathcal{A}_n$. Si osserva che $\mathcal{A}_n$ è semplice per tutte le scelte di n: se $n \geq 5$, la tesi è garantita dal Teorema 1.91; se $n = 3$, $\mathcal{A}_3$ ha ordine 3, e quindi è ciclico di ordine primo, e in quanto tale è semplice. Pertanto, $K = \{\mathrm{id}\}$ oppure $K = \mathcal{A}_n$. Distinguiamo ora 2 casi:

- se $K = \mathcal{A}_n$, allora $\mathcal{A}_n \leqslant N$: per il Teorema di Corrispondenza i sottogruppi di $\mathcal{S}_n$ contenenti $\mathcal{A}_n$ sono in bigezione con i sottogruppi di $\mathcal{S}_n / \mathcal{A}_n \cong \mathbb{Z}/2\mathbb{Z}$; pertanto le uniche possibilità sono $N = \mathcal{A}_n$ oppure $N = \mathcal{S}_n$;
- se $K = \{\mathrm{id}\}$, dacché $[\mathcal{S}_n : \mathcal{A}_n] = 2$, per la Proposizione 1.68 vale che $[N : K] \in \{1, 2\}$, da cui si deduce che $|N| \leq 2\,|K| = 2$. Se $|N| = 1$, allora $N = \{\mathrm{id}\}$; se invece $|N| = 2$, per il Lemma normalizzatore-centralizzatore, esiste un'immersione tale per cui:
$$\mathrm{N}_{\mathcal{S}_n}(N) / \mathrm{Z}_{\mathcal{S}_n}(N) \hookrightarrow \mathrm{Aut}(N)$$
Poiché $|N| = 2$, abbiamo $N \cong \mathbb{Z}/2\mathbb{Z}$, e quindi pertanto $\mathrm{Aut}(N) \cong (\mathbb{Z}/2\mathbb{Z})^\times$ è di ordine 1. Pertanto l'immersione è un isomorfismo e vale l'identità $\mathrm{N}_{\mathcal{S}_n}(N) = \mathrm{Z}_{\mathcal{S}_n}(N)$. Dal momento che N è normale in $\mathcal{S}_n$, $\mathrm{N}_{\mathcal{S}_n}(N) = \mathcal{S}_n$, e quindi $\mathrm{Z}_{\mathcal{S}_n}(N) = \mathcal{S}_n$, ovverosia $N \subseteq \mathrm{Z}(\mathcal{S}_n)$; tuttavia ciò è assurdo in quanto $|N| = 2$ e $\mathrm{Z}(\mathcal{S}_n) = \{\mathrm{id}\}$ per il Lemma 1.94.

Pertanto N può essere solo $\{\mathrm{id}\}$, $\mathcal{A}_n$ o $\mathcal{S}_n$ stesso, e tutti questi tre sottogruppi sono normali in $\mathcal{S}_n$, da cui la tesi. □

Osservazione 1.96 — L'enunciato è falso per $n = 4$. Infatti $\mathcal{A}_4$ non è semplice e ammette come sottogruppo normale il *gruppo di Klein* V_4, ovverosia:

$$V_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq \mathcal{A}_4$$

Chiaramente V_4 è semplice in $\mathcal{S}_4$, dal momento che V_4 è un sottogruppo che contiene tutte le doppie trasposizioni di $\mathcal{S}_4$. Inoltre, se $\sigma = (1\ 2)(3\ 4)$, $\mathrm{Z}_{\mathcal{S}_4}(\sigma)$ ha ordine 8. Dal momento che 8 non divide $12 = |\mathcal{A}_4|$, $\mathrm{Z}_{\mathcal{S}_4}(\sigma)$ non è contenuto in $\mathcal{A}_4$, e quindi la classe di coniugio di σ in $\mathcal{A}_4$ coincide con quella in $\mathcal{S}_4$. Poiché allora $V_4 = \mathcal{C}\ell_{\mathcal{A}_4}(\mathrm{id}) \cup \mathcal{C}\ell_{\mathcal{A}_4}(\sigma)$, V_4 è normale in $\mathcal{A}_4$.

§1.8.10 Sottogruppi di $\mathcal{S}_n$ isomorfi a $\mathcal{S}_{n-1}$

In precedenza avevamo osservato che $\mathcal{S}_{n-1}$ si immergeva naturalmente in $\mathcal{S}_n$. In questa sezione mostriamo invece un risultato che permette di identificare esattamente tutte le immersioni di $\mathcal{S}_{n-1}$ in $\mathcal{S}_n$, come mostra la:

Proposizione 1.97
Dato un sottogruppo $H \leqslant \mathcal{S}_n$ con $n \geq 5$, se $[\mathcal{S}_n : H] = n$ allora H è isomorfo a $\mathcal{S}_{n-1}$.

Dimostrazione. Si consideri l'azione di moltiplicazione a sinistra di $\mathcal{S}_n$ sull'insieme quoziente ${}^{\mathcal{S}_n}\!/_{H}$, ovverosia l'omomorfismo:

$$\varphi : \mathcal{S}_n \to \mathcal{S}\left({}^{\mathcal{S}_n}\!/_{H}\right) \cong \mathcal{S}_n$$

tale per cui:

$$\varphi(\sigma)(\rho H) = \sigma\rho H, \quad \forall \sigma, \rho \in \mathcal{S}_n$$

Tale azione è chiaramente transitiva dal momento che $\rho H = \rho\sigma^{-1}\sigma H = \varphi(\rho\sigma^{-1})(\sigma H)$. In particolare $\ker\varphi \neq \mathcal{S}_n$ (altrimenti le orbite sarebbero tutte distinte e composte da un unico elemento). Poiché $\ker\varphi$ è un sottogruppo normale di $\mathcal{S}_n$, per la Proposizione 1.95 il nucleo di φ è banale oppure è $\mathcal{A}_n$.

Si esclude il caso in cui $\ker\varphi = \mathcal{A}_n$. Se così fosse, dato $\sigma \in \mathcal{S}_n$, varrebbe che:

$$\mathcal{A}_n = \ker\varphi = \bigcap_{\rho H \in {}^{\mathcal{S}_n}\!/_{H}} \mathrm{Stab}(\rho H) \subseteq \mathrm{Stab}(\sigma) \subseteq \mathcal{S}_n$$

In particolare, per il Teorema di corrispondenza, $\mathrm{Stab}(\rho H)$ è $\mathcal{A}_n$ o $\mathcal{S}_n$. In entrambi i casi, per il Lemma orbita-stabilizzatore varrebbe che:

$$|\mathrm{Orb}(\sigma)| = \frac{|\mathcal{S}_n|}{|\mathrm{Stab}(\sigma)|} \leq \frac{n!}{\frac{n!}{2}} = 2$$

che è assurdo, dal momento che per la transitività di φ vale che $\mathrm{Orb}(\sigma) = {}^{\mathcal{S}_n}\!/_{H}$, che ha, per ipotesi, almeno 5 elementi. Pertanto $\ker\varphi = \{\mathrm{id}\}$, e dunque φ induce un isomorfismo da $\mathcal{S}_n$ a $\mathcal{S}_n$, dacché $\mathcal{S}\left({}^{\mathcal{S}_n}\!/_{H}\right) \cong \mathcal{S}_n$.

Si consideri $\alpha = \varphi\big|_H : H \to \mathcal{S}\left({}^{\mathcal{S}_n}\!/\!_{H}\right) \cong \mathcal{S}_n$, ossia la restrizione di φ ad H. Dal momento che φ è un omomorfismo iniettivo, anche α è iniettivo, ovverosia rappresenta un'azione fedele. Si osserva inoltre che $\mathrm{Stab}(H)$ è esattamente H, e quindi che $\mathrm{Orb}(H) = \{H\}$. In particolare, H fissa sempre H come elemento[12] di ${}^{\mathcal{S}_n}\!/\!_{H} \setminus \{H\}$.

Pertanto, "eliminando" H dall'insieme ${}^{\mathcal{S}_n}\!/\!_{H}$ si induce ancora un'azione fedele, ovverosia l'omomorfismo $\beta : H \to \mathcal{S}\left({}^{\mathcal{S}_n}\!/\!_{H} \setminus \{H\}\right) \cong \mathcal{S}_{n-1}$ tale per cui $\beta(h)(\sigma H) = h\sigma H$ per ogni $h \in H$. Infatti β è ben definito, dacché se valesse $h\sigma H = H$, σ sarebbe un elemento di H, e dunque σH sarebbe H, che non appartiene all'insieme su cui agisce H.

Dunque β è un omomorfismo iniettivo tra H e $\mathcal{S}\left({}^{\mathcal{S}_n}\!/\!_{H} \setminus \{H\}\right)$. Poiché $|H| = (n-1)! = \left|\mathcal{S}\left({}^{\mathcal{S}_n}\!/\!_{H} \setminus \{H\}\right)\right|$, β è in particolare un isomorfismo. Dal momento che $\mathcal{S}({}^{\mathcal{S}_n}\!/\!_{H} \setminus \{H\}) \cong \mathcal{S}_{n-1}$, allora H è isomorfo a $\mathcal{S}_{n-1}$, da cui la tesi. $\square$

Osservazione 1.98 — La tesi della precedente proposizione è ancora valida per $n < 5$. Infatti, per $n = 1$ o $n = 2$, la tesi è del tutto ovvia. Per $n = 3$, i sottogruppi di indice 3 sono i sottogruppi di ordine 2, isomorfi dunque a $\mathbb{Z}/2\mathbb{Z} \cong \mathcal{S}_2$. Per $n = 4$, i sottogruppi di indice 4 sono i suoi sottogruppi di ordine 6; dal momento che in $\mathcal{S}_4$ non esistono elementi di ordine 6, tali sottogruppi non possono essere ciclici, e quindi sono tutti isomorfi a $\mathcal{S}_3$.

§1.8.11 Automorfismi di $\mathcal{S}_n$ per $n \neq 6$ $\star$

In questa sezione si descrive il gruppo degli automorfismi di $\mathcal{S}_n$ per $n \neq 6$. Per $n = 2$, $\mathcal{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$, e dunque $\mathrm{Aut}(\mathcal{S}_2)$ è banale. Si presenta ora un lemma molto importante nello studio degli automorfismi di $\mathcal{S}_n$, che permetterà in seguito di dimostrare che $\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Inn}(\mathcal{S}_n)$ per $n \neq 6$.

Lemma 1.99
Sia φ un automorfismo di $\mathcal{S}_n$ con $n \geq 2$ che manda trasposizioni in trasposizioni. Allora φ è un automorfismo interno di $\mathcal{S}_n$

Dimostrazione. Se $n = 2$, la tesi è banale, e dunque si dimostra la tesi per $n > 2$. Si considerino $\varphi(1\ 2) = (a\ b)$ e $\varphi(1\ 3) = (c\ d)$.

Si mostra che $\{a, b\} \cap \{c, d\}$ è un singoletto. Chiaramente tale intersezione non può avere due elementi, altrimenti $(1\ 2)$ e $(1\ 3)$ avrebbero la stessa immagine tramite φ. Allo stesso modo l'intersezione non può essere vuota, perché altrimenti $\varphi(1\ 2)$ e $\varphi(1\ 3)$ commuterebbero in quanto cicli distinti, mentre $(1\ 2)$ e $(1\ 3)$ non commutano. Pertanto $\{a, b\} \cap \{c, d\}$ è un singoletto, e poniamo, senza perdita di generalità, $a = c$. Si pongono inoltre $a_1 := a$, $a_2 := b$ e $a_3 := d$, in modo tale che $a_2 \neq a_3$.

Si mostra che a_1 è un elemento della trasposizione di $\varphi(1\ k)$ per ogni $3 < k \leq n$. Se infatti a_1 non fosse un elemento di $\varphi(1\ k)$, allora, analogamente a prima, poiché φ è iniettiva e $(1\ k)$ non commuta con $(1\ 2)$, a_2 sarebbe un elemento di $\varphi(1\ k)$. Analogamente

[12] Quest'affermazione rappresenta il punto cruciale di tutta la dimostrazione. Si sta infatti mostrando che, dato un insieme di rappresentanti delle classi laterali di H, H è un gruppo di permutazioni su $\{h_1 H, \ldots, h_{n-1} H, h_n H\} \leftrightarrow \{1, \ldots, n-1, n\}$ che fissa sempre $H \leftrightarrow n$, suggerendo che H è un'immersione naturale di $\mathcal{S}_{n-1}$ in $\mathcal{S}_n$.

lo sarebbe anche a_3, da cui si deduce che $\varphi(1\ k) = (a_2\ a_3)$, dacché $a_2 \neq a_3$. Tuttavia ciò è assurdo, dal momento che:

$$\varphi(1\ k) = (a_2\ a_3) = (a_1\ a_2)(a_1\ a_3)(a_1\ a_2)^{-1} = \varphi(1\ 2)\varphi(1\ 3)\varphi(1\ 2) = \varphi(2\ 3)$$

e quindi $(1\ 2)$ avrebbe la stessa immagine di $(2\ 3)$ tramite φ, pur essendone distinto. Pertanto a_1 è elemento di $\varphi(1\ k)$, che dunque si rappresenta come $(a_1\ a_k)$, con a_k distinto[13] per ogni k.

Sia $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ la permutazione di $\mathcal{S}_n$ tale per cui $k \overset{\sigma}{\mapsto} a_k$. Si mostra che l'azione di coniugio φ_σ coincide con φ sull'insieme dei generatori $\{(1\ k)\}_{2 \leq k \leq n}$ di $\mathcal{S}_n$:

$$\varphi_\sigma(1\ k) = \sigma(1\ k)\sigma^{-1} = (a_1\ a_k) = \varphi(1\ k)$$

Pertanto $\varphi = \varphi_\sigma$ è un automorfismo interno, da cui la tesi. □

Teorema 1.100

Sia $n \neq 6$. Allora $\operatorname{Aut}(\mathcal{S}_n) = \operatorname{Inn}(\mathcal{S}_n)$, ed in particolare, per $n \neq 2$, $\operatorname{Aut}(\mathcal{S}_n)$ è isomorfo a $\mathcal{S}_n$ tramite l'azione di coniugio.

Dimostrazione. Se $n = 1$, la tesi è ovvia. Sia pertanto $n \geq 2$. Sia φ un automorfismo di $\mathcal{S}_n$. Allora φ mappa classi di coniugio a classi di coniugio. In particolare, se T_i è la classe di coniugio dei prodotti di i trasposizioni disgiunte, esiste $j > 0$ tale per cui $\varphi(T_1) = T_j$, dal momento che φ deve mandare tutte le trasposizioni in elementi di ordine 2, e dunque in prodotti di trasposizioni. Si mostra che l'unico j possibile è 2, e dunque che φ manda trasposizioni in trasposizioni.

Si osserva che $|T_j| = \frac{n!}{j! 2^j (n-2j)!}$. Poiché φ è un automorfismo, in particolare φ mantiene le cardinalità degli insiemi e dunque deve valere che:

$$|T_1| = \frac{n!}{1!\,2\,(n-2)!} = \frac{n(n-1)}{2} = \frac{n!}{j!\,2^j\,(n-2j)!} = |T_j|$$

In particolare deve valere che:

$$2^{j-1} = \frac{(n-2)!}{j!(n-2j)!} = \underbrace{\frac{(n-2)!}{(n-j)!}}_{a}\underbrace{\binom{n-j}{j}}_{b} = ab$$

dove il coefficiente binomiale è ben definito dal momento che[14] $n - j \geq j$, e così lo sono anche i fattoriali (infatti $n \geq 2$ e $n \geq 2j > j$).

Se φ non mandasse trasposizioni in trasposizioni, j sarebbe maggiore o uguale di 2, e sia a che b sarebbero degli interi. Per $j = 2$, l'equazione è equivalente a $4 = \binom{n-2}{2} = (n-2)(n-3)$, che non ammette soluzione dal momento che uno dei due fattori è diviso da un primo dispari. Per $j = 3$, l'equazione è la seguente:

$$4 = \frac{(n-2)!}{(n-3)!}\binom{n-3}{3} = (n-2)\binom{n-3}{3}$$

[13] Altrimenti si violerebbe l'iniettività di φ.

[14] Infatti una permutazione di $\mathcal{S}_n$ è costituita da al più j trasposizioni, e quindi devono essere disponibili almeno $2j$ elementi, indi per cui $n \geq 2j \implies n - j \geq j$.

dalla quale si ricava che $n-2$ deve dividere 4, e quindi che n è 3, 4 o 6; si verifica a mano che l'unica soluzione è $n=6$, che, per ipotesi, è escluso: quindi $j =$ non ammette soluzione. Per $j>3$, a è prodotto di due interi consecutivi ed è dunque divisibile per un primo dispari, mentre 2^{j-1} chiaramente non può esserlo; pertanto l'equazione non ammette mai soluzione, da cui si deduce che $j=1$, ossia che φ manda trasposizioni in trasposizioni.

Dal Lemma 1.99 questo vuol dire che φ è un automorfismo interno, e quindi che $\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Inn}(\mathcal{S}_n)$. Per $n \geq 3$ $\mathrm{Z}(\mathcal{S}_n)$ è banale per il Lemma 1.94, da cui si conclude che l'azione di coniugio induce un isomorfismo tra $\mathcal{S}_n$ e $\mathrm{Inn}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$, da cui la tesi. □

Osservazione 1.101 (Gruppi completi) — Un gruppo G si dice **completo** se ha centro banale e se $\mathrm{Aut}(G) \cong G$. Equivalentemente, G è completo se $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ e $\mathrm{Z}(G) = \{e_G\}$. Per il Teorema 1.100 e per il Lemma 1.94, $\mathcal{S}_n$ è completo per $n \neq 2$ e $n \neq 6$.

Osservazione 1.102 (Per $n \neq 2,\ 6$, i sottogruppi di indice n di $\mathcal{S}_n$ sono tra loro coniugati) — Sia H un sottogruppo di $\mathcal{S}_n$ di indice n. Dalla Proposizione 1.97 sappiamo già che H è isomorfo a $\mathcal{S}_{n-1}$. Sia φ l'isomorfismo costruito tra $\mathcal{S}_n$ e $S\left({\mathcal{S}_n}/{H}\right)$ e sia ζ il corrispondente automorfismo di $\mathcal{S}_n$ indotto da φ.

Se n è diverso sia da 2 che da 6, per il Teorema 1.100, ζ è un automorfismo interno, e dunque esiste $\sigma \in \mathcal{S}_n$ tale per cui $\zeta = \varphi_\sigma \in \mathrm{Inn}(\mathcal{S}_n)$. Inoltre H è lo stabilizzatore della classe H secondo l'azione φ, e quindi $\zeta(H)$ fissa un elemento di $\mathcal{S}_n$. Allora $H = \zeta^{-1}(\zeta(H)) = \sigma^{-1}\zeta(H)\sigma$ è coniugato ad uno stabilizzatore, e dunque fissa ancora un elemento di $\mathcal{S}_n$. Poiché l'azione naturale di $\mathcal{S}_n$ su $\{1, \dots, n\}$ è transitiva, tutti i suoi stabilizzatori sono coniugati, e quindi i sottogruppi di $\mathcal{S}_n$ di indice n sono coniugati tra loro.

Approfondimento 1.103 (Automorfismi centrali e *class-preserving* di G ⋆) — Abbiamo appena dimostrato che per $\mathcal{S}_n$, con $n \neq 6$, gli automorfismi devono fissare tutte le sue classi di coniugio, e in particolare devono mandare le trasposizioni nelle trasposizioni. In generale, il sottogruppo di $\mathrm{Aut}(G)$ degli automorfismi che fissano *tutte* le classi di coniugio di G è detto sottogruppo dei ***class-preserving automorphisms***, denotato con $\mathrm{Aut}_c(G)$.

Si può sempre considerare l'azione naturale φ di $\mathrm{Aut}(G)$ sull'insieme $\{C_i\}$ delle classi di coniugio di G, tale per cui a f corrisponde la bigezione $\varphi_f : C_i \mapsto f(C_i)$. In particolare, il nucleo di φ è esattamente $\mathrm{Aut}_c(G)$, che quindi è un sottogruppo normale di $\mathrm{Aut}(G)$.

Inoltre, ogni automorfismo interno è *class-preserving*, e quindi vale che:

$$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}_c(G) \trianglelefteq \mathrm{Aut}(G).$$

Nel caso di $\mathcal{S}_n$ con $n \neq 6$, $\mathrm{Inn}(\mathcal{S}_n)$ e $\mathrm{Aut}(\mathcal{S}_n)$ coincidono, e quindi anche $\mathrm{Aut}_c(\mathcal{S}_n)$ coincide con $\mathrm{Aut}(\mathcal{S}_n)$.

In generale, vi è sempre una proiezione[a] π_H^c da $\mathrm{Aut}_c(G)$ a qualsiasi $\mathrm{Aut}_c(G/H)$, se $H \trianglelefteq G$. Tale proiezione è data dall'associazione ad un automorfismo $\alpha \in \mathrm{Aut}_c(G)$

di un automorfismo $\overline{\alpha} \in \mathrm{Aut}_c(G/H)$ tale per cui:

$$\overline{\alpha}(gH) = \alpha(g)H.$$

Dal momento che $\mathcal{C}\ell(gH) = \mathcal{C}\ell(g)H$, tale automorfismo è infatti ancora *class-preserving.*

Il nucleo della proiezione di $\mathrm{Aut}_c(G)$ su $\mathrm{Aut}_c(G/\,\mathrm{Z}(G))$ è di considerevole importanza, ed è detto sottogruppo degli **automorfismi *class-preserving* centrali**[b], indicato con $\mathrm{Aut}_{c,z}(G)$. Un automorfismo *class-preserving* centrale α è tale se e solo se è *class-preserving* e se $\alpha(g)g^{-1} \in \mathrm{Z}(G)$ per ogni $g \in G$. In particolare, poiché ogni automorfismo *class-preserving* deve fissare ogni elemento del centro (infatti la classe di coniugio di un elemento del centro è composta dall'elemento stesso), se $\alpha \in \mathrm{Aut}_{c,z}(G)$ vale che:

$$\exists z \in \mathrm{Z}(G) \mid \alpha(g) = gz, \quad \alpha^i(g) = gz^i \forall i.$$

[a] La stessa proiezione si può considerare per $\mathrm{Aut}(G)$ su $\mathrm{Aut}(G/H)$, a patto di rimuovere l'ipotesi di conservazione delle classi di coniugio.

[b] Si definiscono invece gli **automorfismi centrali** di $\mathrm{Aut}_c(G)$ come gli automorfismi α per $\alpha(g)g^{-1} \in \mathrm{Z}(G)$; ossia non si richiede in generale che siano *class-preserving.* In altre parole, gli automorfismi centrali sono il nucleo della normale proiezione di $\mathrm{Aut}(G)$ su $\mathrm{Aut}(G/\,\mathrm{Z}(G))$.

In particolare $\mathrm{Aut}_{c,z}(G) = \mathrm{Aut}_c(G) \cap \mathrm{Aut}_z(G)$. Si dimostra facilmente che gli automorfismi centrali sono esattamente gli automorfismi che commutano con gli automorfismi interni, ossia $\mathrm{Aut}_c(G) = Z_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$.

Esercizio 1.104 ($\star$)**.** Sia G un p-gruppo finito. Si dimostri che allora $\mathrm{Aut}_c(G)$ è banale o è anch'esso un p-gruppo.

Soluzione. Sia $|G| = p^n$. Si dimostra la tesi per induzione su n. Se $n = 1$, G è ciclico, e dunque abeliano. Pertanto un automorfismo *class-preserving* deve per forza fissare tutti gli elementi di G, da cui si deduce che $\mathrm{Aut}_c(G)$ è banale.

Si consideri ora il passo induttivo. Se G è abeliano, $\mathrm{Aut}_c(G)$ è banale, come prima. Altrimenti $\mathrm{Z}(G)$ è un p-sottogruppo non banale di G, dal momento che G è un p-gruppo. In tal caso si può considerare la proiezione $\pi^c_{\mathrm{Z}(G)}$ degli automorfismi *class-preserving* di G a quelli di $G/\,\mathrm{Z}(G)$. Per l'ipotesi induttiva $\mathrm{Aut}_c(G/\,\mathrm{Z}(G))$ è banale o un p-gruppo, e quindi anche l'immagine di $\pi^c_{\mathrm{Z}(G)}$ lo è.

Si mostra che il nucleo di $\pi^c_{\mathrm{Z}(G)}$, ossia il sottogruppo degli automorfismi *class-preserving* centrali, è un p-gruppo o è banale. Dato $\alpha \in \mathrm{Aut}_{c,z}(G) = \ker \pi^c_{\mathrm{Z}(G)}$, per ogni $g \in G$ abbiamo osservato precedentemente che esiste un unico $z(g) \in \mathrm{Z}(G)$ in funzione di g tale per cui $\alpha(g) = gz(g)$. In particolare $\alpha^i(g) = gz(g)^i$, e quindi, detto p^k l'ordine di $z(g) \in \mathrm{Z}(G)$, $\alpha^{p^k}(g) = gz(g)^{p^k} = g$.

Se p^t è il minimo comune multiplo degli elementi di $\{\mathrm{ord}(z(g))\}_{g \in G}$, allora $\alpha^{p^t} = \mathrm{id}$, e quindi l'ordine di α è divisore di una potenza di un primo. Pertanto $\mathrm{Aut}_{c,z}(G)$ è un p-sottogruppo di $\mathrm{Aut}_c(G)$ o è banale. Per il Primo Teorema di Omomorfismo si conclude allora che:

$$|\mathrm{Aut}_c(G)| = |\mathrm{Aut}_{c,z}(G)|\,|\mathrm{im}\,\pi^c_{\mathrm{Z}(G)}|,$$

e dunque che anche $\mathrm{Aut}_c(G)$ è un p-gruppo o è il gruppo banale, da cui la conclusione del passo induttivo e la tesi. ☐

§1.8.12 Automorfismi esterni di $\mathcal{S}_6$ ⋆

Abbiamo osservato in precedenza che per $n \neq 6$, ogni automorfismo di $\mathcal{S}_n$ è interno. Il caso $n = 6$ è invece del tutto eccezionale, dal momento che ammette una classe di automorfismi esterni, unici a meno di composizione con un automorfismo interno, come si dimostrerà all'interno di questa sezione.

Innanzitutto si definisce il gruppo degli automorfismi esterni:

Definizione 1.105. Sia G un gruppo. Allora si definisce **gruppo degli automorfismi esterni** di G il gruppo $\operatorname{Out}(G) := \operatorname{Aut}(G)/\operatorname{Inn}(G)$.

In particolare si dice automorfismo esterno di G un suo automorfismo non interno, ossia un automorfismo la cui classe laterale rispetto a $\operatorname{Inn}(G)$ non è $\operatorname{Inn}(G)$ stesso.

Si esibisce per $\mathcal{S}_6$ un automorfismo esterno, e si dimostra in seguito che è unico (ossia che $\operatorname{Out}(\mathcal{S}_6)$ ha ordine 2). Per costruirlo verificheremo l'esistenza di un'immersione di $\mathcal{S}_5$ in $\mathcal{S}_6$ transitiva, ossia verificheremo l'esistenza di un'azione fedele e transitiva di $\mathcal{S}_5$ su 6 oggetti.

Iniziamo osservando che $\mathcal{S}_5$ contiene 6 5-Sylow. Tali sottogruppi hanno infatti ordine 5 e sono dunque ciclici. Dal momento che gli unici elementi di ordine 5 in $\mathcal{S}_5$ sono i 5-cicli, tutti questi sottogruppi contengono $\phi(5) = 4$ 5-cicli, e quindi esistono tanti 5-Sylow quanto vale

$$\frac{1}{\phi(5)}\binom{5}{5}4! = 6$$

Posto $X = \{P_1, \ldots, P_6\}$ l'insieme dei 5-Sylow di $\mathcal{S}_5$, possiamo considerare l'azione di coniugio di $\mathcal{S}_5$ su X, e quindi un omomorfismo $\varphi : \mathcal{S}_5 \to S(X) \cong \mathcal{S}_6$. Per i Teoremi di Sylow, ogni 5-Sylow è coniugato a ogni altro 5-Sylow, e quindi φ è un'azione transitiva.

Si consideri il nucleo di φ. Per la Proposizione 1.95, $\ker\varphi$ è $\mathcal{S}_5$, $\mathcal{A}_5$ o $\{\mathrm{id}\}$. Chiaramente il nucleo non può essere $\mathcal{S}_5$, poiché altrimenti $\operatorname{Stab}(P_1)$ sarebbe anch'esso $\mathcal{S}_5$, e così, per il Lemma orbita-stabilizzatore, $\operatorname{Orb}(P_1)$ avrebbe un singolo elemento, mentre φ è transitiva e $\operatorname{Orb}(P_1) = X$. Allo stesso modo $\ker\varphi$ non può essere $\mathcal{A}_5$. Se così fosse, varrebbe che:

$$\mathcal{A}_n = \ker\varphi = \bigcap_{i=1}^{5} \operatorname{Stab}(P_i) \subseteq \operatorname{Stab}(P_1) \subseteq \mathcal{S}_n$$

In particolare, per il Teorema di corrispondenza, $\operatorname{Stab}(P_1)$ è $\mathcal{A}_n$ o $\mathcal{S}_n$. In entrambi i casi, per il Lemma orbita-stabilizzatore varrebbe che:

$$|\operatorname{Orb}(P_1)| = \frac{|\mathcal{S}_n|}{|\operatorname{Stab}(P_1)|} \leq \frac{n!}{\frac{n!}{2}} = 2$$

che è assurdo, dal momento che per la transitività di φ vale che $\operatorname{Orb}(\sigma) = X$, che ha 5 elementi. Pertanto $\ker\varphi$ è banale, e dunque φ è un'azione fedele. In particolare φ induce un'immersione α di $\mathcal{S}_5$ in $\mathcal{S}_6$, dove $H = \operatorname{im}\alpha$ è transitivo, e dunque non può fissare alcun elemento di $\{1, \ldots, 6\}$.

Consideriamo l'azione ψ di moltiplicazione a sinistra di $\mathcal{S}_6$ su ${}^{\mathcal{S}_6}\!/_{H}$. Come osservato nella dimostrazione della Proposizione 1.97, ψ è un isomorfismo, e dunque induce un automorfismo ζ di $\mathcal{S}_6$, dal momento che $S\left({}^{\mathcal{S}_6}\!/_{H}\right)$ è isomorfo a $\mathcal{S}_6$. Poiché $H \leqslant \mathcal{S}_6$ è esattamente lo stabilizzatore della classe H, $\zeta(H)$ è a sua volta per la sua azione naturale stabilizzatore di un elemento i in $\{1, \ldots, 6\}$.

Se ζ fosse un automorfismo interno di $\mathcal{S}_6$, allora anche ζ^{-1} sarebbe un automorfismo interno, e quindi esisterebbe $\sigma \in \mathcal{S}_6$ tale per cui $\zeta^{-1} = \varphi_\sigma$. Se così fosse, però, varrebbe che:

$$H = \zeta^{-1}(\zeta(H)) = \zeta^{-1}(\operatorname{Stab}(i)) = \sigma \operatorname{Stab}(i)\sigma^{-1} = \operatorname{Stab}(\sigma(i))$$

mentre, come osservato prima, H non può fissare alcun elemento di $\{1, \ldots, 6\}$. Pertanto ζ non è un automorfismo interno, ed è dunque esterno per $\mathcal{S}_6$.

Osservazione 1.106 — Come osservato nella dimostrazione del Teorema 1.100, affinché ζ sia un automorfismo esterno di $\mathcal{S}_6$, ζ deve mappare le trasposizioni alle triple trasposizioni (ossia $\zeta(T_1) = T_3$, l'unica soluzione non banale per $n = 6$).

Pertanto, se α è un altro automorfismo esterno di $\mathcal{S}_6$, $\zeta^{-1}(\alpha(T_1)) = \zeta^{-1}(T_3) = T_1$, e dunque $\zeta^{-1} \circ \alpha$ manda trasposizioni in trasposizioni, da cui si deduce, per il Lemma 1.99, che $\zeta^{-1} \circ \alpha$ è un automorfismo interno di $\mathcal{S}_6$. In particolare ogni automorfismo esterno di $\mathcal{S}_6$ appartiene alla stessa classe laterale di $\operatorname{Inn}(\mathcal{S}_6)$ in $\operatorname{Aut}(\mathcal{S}_6)$. Si conclude dunque che $\operatorname{Out}(\mathcal{S}_6) \cong \mathbb{Z}/2\mathbb{Z}$.

§1.9 Prodotti semidiretti

§1.9.1 Descrizione di $\mathcal{S}_4$ come prodotto semidiretto

Per ogni $n \geq 2$ vale in generale la relazione

$$\mathcal{S}_n \cong \mathcal{A}_n \rtimes \langle (a\ b) \rangle$$

dove $(a\ b)$ è una trasposizione di $\mathcal{S}_n$, vogliamo però dare una decomposizione di $\mathcal{S}_4$ più specifica.
Consideriamo il sottogruppo di Klein $V_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ e $H = \{\sigma \in \mathcal{S}_4 \mid \sigma(4) = 4\}$ lo stabilizzatore di 4 secondo l'azione naturale di $\mathcal{S}_4$ su $\{1, 2, 3, 4\}$, osserviamo che V_4 è normale in $\mathcal{S}_4$ in quanto unione delle classi di coniugio di ogni suo elemento[15] e che H è isomorfo a $\mathcal{S}_3$ (in effetti gli elementi di H sono tutte e sole le permutazioni di 3 elementi). Dato che l'unica permutazione di V_4 che fissa 4 è l'identità abbiamo $V_4 \cap H = \{id\}$, inoltre $V_4 H = \mathcal{S}_4$ in quanto i due insiemi hanno la stessa cardinalità. Possiamo quindi scrivere

$$\mathcal{S}_4 \cong V_4 \rtimes H \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathcal{S}_3$$

con

$$\varphi : \mathcal{S}_3 \longrightarrow \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

Specifichiamo come agisce la mappa φ[16]: consideriamo gli isomorfismi

$$\alpha : V_4 \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : (1\ 2)(3\ 4) \longmapsto (1, 0), (1\ 3)(2\ 4) \longmapsto (0, 1)$$

$$\beta : H \longrightarrow \mathcal{S}_3 : \sigma \longmapsto \sigma_{|\{1,2,3\}}$$

le immagini di φ in $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ corrispondono tramite α e β ai coniugi su V_4 per elementi di H. Vediamo quindi come i generatori $(1\ 2\ 3)$, $(1\ 2)$ di H agiscono per coniugio sui generatori $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ di V_4:

$$(1\ 2\ 3)((1\ 2)(3\ 4))(1\ 3\ 2) = (1\ 4)(2\ 3)$$

$$(1\ 2\ 3)((1\ 3)(2\ 4))(1\ 3\ 2) = (1\ 2)(3\ 4)$$

$$(1\ 2)((1\ 2)(3\ 4))(1\ 2) = (1\ 2)(3\ 4)$$

$$(1\ 2)((1\ 3)(2\ 4))(1\ 2) = (1\ 4)(2\ 3)$$

Pertanto $\varphi((1\ 2\ 3)) = f$ e $\varphi((1\ 2)) = g$, dove f e g sono gli automorfismi di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tali che

$$f : (1, 0) \longmapsto (1, 1), (0, 1) \longmapsto (1, 0)$$

$$g : (1, 0) \longmapsto (1, 0), (0, 1) \longmapsto (1, 1)$$

[15] La classe di coniugio in $\mathcal{S}_4$ di $(1\ 2)(3\ 4)$ è $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

[16] Se descriviamo $\mathcal{S}_4$ come prodotto semidiretto di due sottogruppi questo non è necessario, in quanto tale mappa è sempre il coniugio.

§1.9.2 Automorfismi di D_n

Consideriamo il gruppo

$$G = \{f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \mid \exists a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z} \text{ per cui } f(x) = ax + b \ \forall x \in \mathbb{Z}/n\mathbb{Z}\}$$

delle sostituzioni lineari in $\mathbb{Z}/n\mathbb{Z}$, effettivamente G è un gruppo con l'operazione di composizione. Infatti fissati $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $b \in \mathbb{Z}/n\mathbb{Z}$ e $f \in G$ tali che $f(x) = ax + b$, abbiamo che f^{-1} è tale che $f^{-1}(x) = a^{-1}(x - b)$ (chiaramente G contiene l'applicazione identità ed è chiuso per composizione). Notiamo che un elemento di G è univocamente determinato dalla coppia $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$[17], pertanto G contiene $n\phi(n)$ elementi. In realtà possiamo essere più precisi:

Proposizione 1.107
Il gruppo G definito come sopra è isomorfo a un prodotto semidiretto

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

Dimostrazione. Consideriamo i sottogruppi di G

$$N = \{f \in G \mid f(x) = x + b,\ b \in \mathbb{Z}/n\mathbb{Z}\}$$
$$H = \{f \in G \mid f(x) = ax,\ a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

osserviamo che N e H sono naturalmente isomorfi a $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$ rispettivamente e che $N \cap H = \{id\}$, pertanto $NH = G$ in quanto

$$|NH| = \frac{|N| \cdot |H|}{|N \cap |H|} = |N| \cdot |H| = n\phi(n) = |G|$$

Mostriamo quindi che N è un sottogruppo normale di G: fissati $f \in N$ e $g \in G$ tali che $f(x) = x + t$ e $g(x) = ax + b$, con $b, t \in \mathbb{Z}/n\mathbb{Z}$ e $a \in (\mathbb{Z}/n\mathbb{Z})^*$, abbiamo

$$(g^{-1} \circ f \circ g)(x) = (g^{-1} \circ f)(ax + b) = g^{-1}(ax + b + t) = x + a^{-1}t$$

pertanto $g^{-1} \circ f \circ g \in N$, cioè $N \trianglelefteq G$. Possiamo quindi decomporre G come prodotto semidiretto:

$$G \cong N \rtimes H$$

poiché $N \cong \mathbb{Z}/n\mathbb{Z}$ e $H \cong (\mathbb{Z}/n\mathbb{Z})^*$ abbiamo che G è isomorfo a un prodotto semidiretto

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

□

Rappresentiamo gli elementi di G tramite le coppie $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$ (come insieme, non come gruppo), la composizione in G produce la seguente operazione sulle coppie:

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

pertanto l'omomorfismo che definisce il prodotto semidiretto $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/n\mathbb{Z})^*$ a cui è isomorfo G è

$$\varphi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) : a \longmapsto \varphi_a$$

dove φ_a è l'omomorfismo di moltiplicazione per a

$$\varphi_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : x \longmapsto ax$$

[17] Consideriamo qua solo l'insieme prodotto cartesiano, non la struttura di gruppo data dal prodotto diretto.

Proposizione 1.108

Il gruppo G delle sostituzioni lineari in $\mathbb{Z}/n\mathbb{Z}$ è isomorfo a $\mathrm{Aut}(D_n)$ per $n \geq 3$.

Dimostrazione. Siano $r, s \in D_n$ tali che $\mathrm{ord}(r) = n$, $\mathrm{ord}(s) = 2$, $D_n = \langle r, s\rangle$, consideriamo $\varphi \in Aut(D_n)$. Poiché $\langle r\rangle \cong \mathbb{Z}/n\mathbb{Z}$ è un sottogruppo caratteristico di D_n abbiamo che esistono unici $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $b \in \mathbb{Z}/n\mathbb{Z}$ tali che

$$\varphi(r) = r^a \qquad \varphi(s) = sr^b$$

Consideriamo φ_1, $\varphi_2 \in \mathrm{Aut}(D_n)$ tali che

$$\varphi_i(r) = r^{a_i} \qquad \varphi_i(s) = sr^{b_i}$$

con $a_i \in (\mathbb{Z}/n\mathbb{Z})^*$, $b_i \in \mathbb{Z}/n\mathbb{Z}$ per $i \in \{1, 2\}$, componendo φ_1 con φ_2 otteniamo

$$\varphi_1(\varphi_2(r)) = \varphi_1(r^{a_2}) = r^{a_1 a_2}$$

$$\varphi_1(\varphi_2(s)) = \varphi_1(sr^{b_2}) = sr^{b_1 + a_1 b_2}$$

Pertanto $\mathrm{Aut}(D_n)$ è isomorfo a un quoziente di G in quanto i suoi elementi rispettano la stessa legge di gruppo, d'altra parte $|\mathrm{Aut}(D_n)| = |G|$, pertanto i due gruppi sono proprio isomorfi. □

§1.9.3 Prodotti semidiretti isomorfi

Dati due gruppi, può succedere che il loro prodotto diretto sia isomorfo a un loro prodotto semidiretto non banale.
Consideriamo il gruppo $GL_3(\mathbb{R})$ e $N = SL_3(\mathbb{R}) = \{M \in GL_3(\mathbb{R}) \mid \det M = 1\}$, N è un sottogruppo normale di $GL_3(\mathbb{R})$ in quanto è il nucleo dell'omomorfismo

$$\det : GL_3(\mathbb{R}) \longrightarrow \mathbb{R}^*$$

mostriamo che $GL_3(\mathbb{R}) \cong SL_3(\mathbb{R}) \times \mathbb{R}^*$. Consideriamo il sottogruppo

$$H = \left\{ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R}^* \right\}$$

isomorfo a $\mathbb{R}^*$, abbiamo che:

- $N \cap H = \{Id\}$ in quanto $M = \lambda Id \in N \cap H$ è tale che $\det M = \lambda^3 = 1$, cioè $\lambda = 1$ e quindi $M = Id$;
- H è un sottogruppo normale di $GL_3(\mathbb{R})$, in quanto tutti i suoi elementi sono multipli scalari della matrice identità e quindi commutano con gli elementi di $GL_3(\mathbb{R})$;
- $GL_3(\mathbb{R}) = NH$, infatti per ogni $M \in GL_3(\mathbb{R})$ possiamo scrivere $M = S(\lambda Id)$, dove $\lambda = (\det M)^{\frac{1}{3}}$ e $S = (\det M)^{-\frac{1}{3}} M \in N$.

Possiamo quindi scrivere

$$GL_3(\mathbb{R}) \cong SL_3(\mathbb{R}) \times H \cong SL_3(\mathbb{R}) \times \mathbb{R}^*$$

Consideriamo adesso il sottogruppo di $GL_3(\mathbb{R})$

$$K = \left\{ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R}^* \right\}$$

anch'esso isomorfo a $\mathbb{R}^*$. Ragionando in modo analogo abbiamo $N \cap H = \{Id\}$, inoltre $GL_3(\mathbb{R}) = NK$ in quanto per ogni $M \in GL_3(\mathbb{R})$ possiamo scrivere $M = (MA^{-1})A$ con

$$A = \begin{pmatrix} \det M & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in K, \quad MA^{-1} \in N$$

Possiamo quindi scrivere

$$GL_3(\mathbb{R}) \cong SL_3(\mathbb{R}) \rtimes K$$

Notiamo che l'azione di coniugio di K su $SL_3(\mathbb{R})$ non è banale, in quanto

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \lambda \neq 0, 1$$

quindi il prodotto non è diretto.

È in realtà relativamente semplice costruire prodotti diretti e prodotti semidiretti isomorfi a partire da un gruppo non abeliano, diamo l'esempio di una possibile procedura nella seguente dimostrazione.

Proposizione 1.109

Dato un gruppo G non abeliano, esiste un omomorfismo

$$\varphi : G \longrightarrow \operatorname{Aut}(G)$$

non banale tale che $G \times G \cong G \rtimes_\varphi G$.

Dimostrazione. Consideriamo i sottogruppi $N = G \times \{e\}$, $H = \{(g, g) \mid g \in G\}$, notiamo che N è un sottogruppo normale di $G \times G$. Inoltre $N \cap H = \{e, e\}$ e $NH = G \times G$, in quanto per ogni elemento $(g_1, g_2) \in G \times G$ abbiamo

$$(g_1, g_2) = (g_1 g_2^{-1}, e)(g_2, g_2)$$

con $(g_1 g_2^{-1}, e) \in N$ e $(g_2, g_2) \in H$, pertanto possiamo scrivere $G \times G = N \rtimes_\varphi H$, dove φ è un omomorfismo

$$\varphi : H \longrightarrow \operatorname{Aut}(N)$$

Tale φ è banale se e solo se $\varphi(h) = id$ per ogni $h \in H$, se e solo se $hnh^{-1} = n$ per ogni $h \in H$, per ogni $n \in N$. Questo è equivalente a richiedere

$$(g, g)(h, e)(g^{-1}, g^{-1}) = (ghg^{-1}, e) = (h, e) \ \forall g, h \in G$$

cioè $g \in Z(G)$ per ogni $g \in G$, ma questo è assurdo in quanto G non è abeliano, pertanto φ non è l'omomorfismo banale. Poiché $N \cong H \cong G$ abbiamo quindi

$$G \times G \cong G \rtimes_{\varphi'} G$$

dove

$$\varphi' : G \longrightarrow \operatorname{Aut}(G)$$

è l'omomorfismo non banale corrispondente a φ. □

Vediamo adesso un criterio che stabilisce una condizione sufficiente affinché i prodotti semidiretti di due gruppi siano isomorfi.

Proposizione 1.110 (Criterio di isomorfismo tra prodotti semidiretti)
Siano H, N due gruppi e $\varphi : H \longrightarrow \operatorname{Aut}(N)$ un omomorfismo. Dato $f \in \operatorname{Aut}(H)$ allora $N \rtimes_\varphi H \cong N \rtimes_{\varphi \circ f} H$.

Dimostrazione. Consideriamo l'applicazione

$$\psi : N \rtimes_\varphi H \longrightarrow N \rtimes_{\varphi\circ f} H : (n, h) \longmapsto (n, f^{-1}(h))$$

ψ è una bigezione tra i due insiemi in quanto f è bigettiva, mostriamo che è anche un omomorfismo di gruppi. Per ogni (n_1, h_1), $(n_2, h_2) \in N \rtimes_\varphi H$ abbiamo

$$\begin{aligned}\psi((n_1, h_1)(n_2, h_2)) &= \psi(n_1 \cdot \varphi(h_1)(n_2), h_1h_2) = \\ &= (n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1h_2)) = (n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1)f^{-1}(h_2))\end{aligned}$$

d'altra parte

$$\begin{aligned}&\psi(n_1, h_1)\psi(n_2, h_2) = (n_1, f^{-1}(h_1))(n_2, f^{-1}(h_2)) = \\ &= (n_1 \cdot (\varphi \circ f)(f^{-1}(h_1))(n_2), f^{-1}(h_1)f^{-1}(h_2)) = (n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1)f^{-1}(h_2))\end{aligned}$$

cioè ψ è un omomorfismo, quindi i due gruppi sono isomorfi. □

Esempio 1.111
Abbiamo visto che i prodotti semidiretti della forma $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ con p, q primi tali che $q \mid p - 1$ si suddividono in esattamente due classi di isomorfismo, utilizziamo il risultato appena mostrato per verificare che tutti i prodotti semidiretti non banali sono tra loro isomorfi. Consideriamo un omomorfismo

$$\varphi_a : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z} : 1 \longmapsto a$$

con $\operatorname{ord}(a) = q$ (poiché $\operatorname{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ questo è equivalente a fissare un omomorfismo tra $\mathbb{Z}/q\mathbb{Z}$ e $\operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})$), possiamo scrivere

$$a = k\frac{p-1}{q} \quad k \in \{1, \dots, q-1\}$$

Posto $f_k \in \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$ tale che

$$f_k : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} : x \longmapsto kx$$

con $(k, q) = 1$, possiamo scrivere $\varphi_a = \varphi_{\frac{p-1}{q}} \circ f_k$. Allora i prodotti semidiretti non banali $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_a} \mathbb{Z}/q\mathbb{Z}$ sono tutti isomorfi a tra loro per la Proposizione 1.74.

Vediamo adesso un criterio che fornisce una condizione sufficiente affinché due prodotti semidiretti di p-gruppi non siano isomorfi.

Proposizione 1.112

Siano p, q due primi distinti, G un p-gruppo e H un q-gruppo, consideriamo i prodotti semidiretti

$$X_1 = G \rtimes_{\varphi_1} H \qquad X_2 = G \rtimes_{\varphi_2} H$$

con

$$\varphi_1, \varphi_2 : H \longrightarrow \mathrm{Aut}(G)$$

Se $\ker \varphi_1$ e $\ker \varphi_2$ non sono isomorfi allora X_1 e X_2 non sono isomorfi.

Dimostrazione. Dimostriamo la contronominale, cioè che se X_1 e X_2 sono isomorfi allora $\ker \varphi_1 \cong \ker \varphi_2$.
Sia $f : X_1 \longrightarrow X_2$ un isomorfismo, poniamo $\mathcal{G}_1 = G \rtimes_{\varphi_1} \{e_H\}$, $\mathcal{G}_2 = G \rtimes_{\varphi_2} \{e_H\}$, $\mathcal{H}_1 = \{e_G\} \rtimes_{\varphi_1} H$, $\mathcal{H}_2 = \{e_G\} \rtimes_{\varphi_2} H$. Osserviamo che $f(\mathcal{G}_1) = \mathcal{G}_2$ in quanto $\mathcal{G}_1$ è l'unico p-Sylow di X_1 e $\mathcal{G}_2$ è l'unico p-Sylow di X_2 (infatti $\mathcal{G}_1 \trianglelefteq X_1$ e $\mathcal{G}_2 \trianglelefteq X_2$), mentre $f(\mathcal{H}_1)$ è un q-Sylow di X_2 coniugato a $\mathcal{H}_2$. In particolare esiste $\psi \in \mathrm{Inn}(X_2)$ tale che

$$(\psi \circ f)(\mathcal{G}_1) = \mathcal{G}_2 \qquad (\psi \circ f)(\mathcal{H}_1) = \mathcal{H}_2$$

pertanto, a meno di coniugio, possiamo supporre $f(\mathcal{G}_1) = \mathcal{G}_2$ e $f(\mathcal{H}_1) = \mathcal{H}_2$. Caratterizziamo i nuclei di φ_1, φ_2 in termini di centralizzatori, in particolare scriviamo

$$\begin{aligned} Z_{\mathcal{H}_1}(\mathcal{G}_1) &= \{(e_G, h) \in \mathcal{H}_1 \mid (e_G, h)(g, e_H)(e_G, h)^{-1} = (g, e_H)\ \forall g \in G\} = \\ &= \{(e_G, h) \in \mathcal{H}_1 \mid (\varphi_1(h)(g), h)(e_G, h^{-1}) = (g, e_H)\ \forall g \in G\} = \\ &= \{(e_G, h) \in \mathcal{H}_1 \mid (\varphi_1(h)(g), e_H) = (g, e_H)\ \forall g \in G\} = \\ &= \{(e_G, h) \in \mathcal{H}_1 \mid \varphi_1(h) = id\} = \{e_G\} \rtimes_{\varphi_1} \ker \varphi_1 \end{aligned}$$

e ragionando in modo analogo

$$Z_{\mathcal{H}_2}(\mathcal{G}_2) = \{e_G\} \rtimes_{\varphi_2} \ker \varphi_2$$

Poniamo $\chi = \psi \circ f$, chiaramente $\chi : X_1 \longrightarrow X_2$ è un isomorfismo e $\chi(\mathcal{G}_1) = \mathcal{G}_2$, $\chi(\mathcal{H}_1) = \mathcal{H}_2$ per quanto detto sopra, pertanto

$$\begin{aligned} \{e_G\} \rtimes_{\varphi_2} \ker \varphi_2 &= Z_{\mathcal{H}_2}(\mathcal{G}_2) = Z_{\chi(\mathcal{H}_1)}(\chi(\mathcal{G}_1)) = \\ &= \{\chi(h_1) \mid h_1 \in \mathcal{H}_1, \chi(h_1)\chi(g_1) = \chi(g_1)\chi(h_1)\ \forall g_1 \in \mathcal{G}_1\} = \\ &= \{\chi(h_1) \mid h_1 \in \mathcal{H}_1, \chi(h_1 g_1) = \chi(g_1 h_1)\ \forall g_1 \in \mathcal{G}_1\} = \\ &= \{\chi(h_1) \mid h_1 \in Z_{\mathcal{H}_1}(\mathcal{G}_1)\} = \chi(\{e_G\} \rtimes_{\varphi_1} \ker \varphi_1) \end{aligned}$$

In particolare quindi χ induce un isomorfismo tra $\ker \varphi_2$ e $\ker \varphi_1$. $\square$

§1.10 Classificazione dei gruppi semplici di ordine al più 100

In questa sezione vogliamo classificare tutti i gruppi semplici finiti di ordine al più 100. Innanzitutto, illustriamo alcune osservazioni che ci permetteranno di ridurre lo studio a pochi casi interessanti:

- Gli unici gruppi abeliani semplici sono i gruppi isomorfi a $\mathbb{Z}/p\mathbb{Z}$ con p primo o sono isomorfi al gruppo banale di ordine 1;
- I gruppi di ordine pq con $q > p$ e q, p primi non sono semplici, in quanto possiamo scriverli come prodotto semidiretto di $\mathbb{Z}/q\mathbb{Z}$ e $\mathbb{Z}/p\mathbb{Z}$, e dunque ha un q-Sylow normale (questo esclude gli ordini 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94 e 95);
- I p-gruppi di ordine p^k con $k > 1$ non sono semplici dal momento che hanno centro non banale e il centro è un sottogruppo caratteristico, e dunque è un sottogruppo normale; alternativamente, se $k = 2$, G è abeliano (e dunque è già stato trattato prima), e se $k > 2$, dai Teoremi di Sylow, G contiene un sottogruppo proprio di ordine p^{k-1}, normale dal momento che il suo indice è p, il più piccolo primo che divide $|G|$ (questo esclude gli ordini 4, 8, 9, 16, 25, 27, 32, 49, 64 e 81);
- i gruppi di ordine $2d$ con $d \neq 1$ dispari non sono semplici in quanto contengono un sottogruppo di indice 2, che è normale e non banale, per l'Esercizio 1.66 (questo esclude gli ordini 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 70, 74, 78, 82, 86, 90, 94 e 98);
- I gruppi di ordine $4p$ con $p \geq 5$ primo non sono semplici, dal momento che, per i Teoremi di Sylow, $n_p \mid 4$ e $n_p \equiv 1 \pmod p$ ha come unica soluzione $n_p = 1$, da cui si deduce che il p-Sylow del gruppo è normale (questo esclude gli ordini 20, 28, 44, 52, 68, 76 e 92);
- I gruppi di ordine pq^j con p, q primi e tali per cui $p! < pq^j$, in quanto, per il Teorema di Poincaré, esiste un sottogruppo non banale e normale N di G tale per cui $p \mid |N| \mid p! < pq^j$ e contenuto in un q-Sylow di G (questo esclude gli ordini 12, 18, 24, 48, 50, 54, 75, 96 e 98);
- I gruppi di ordine p^2q^j con p, q primi e tali per cui $(p^2)! < p^2q^j$, per lo stesso motivo per cui si escludono i gruppi di ordine pq^j (questo esclude gli ordini 36 e 100);
- L'unico gruppo alternante semplice di ordine minore o uguale a 100 è $\mathcal{A}_5$, di ordine 60.

A partire da queste osservazioni, ci riduciamo a studiare i gruppi di ordine 40, 45, 56, 60, 63, 72, 80, 84, 88 e 99. Tutti questi casi, escludendo 56, 60, 72 e 80, ammettono, per almeno un primo, un unico sottogruppo di Sylow, che dunque è normale.

Studiamo quindi i gruppi di ordine 56, 72 e 80, per poi studiare alla fine i gruppi di ordine 60.

$\underline{|G| = 56 = 2^3 \cdot 7}$: poiché $n_7 \equiv 1 \pmod 7$ e $n_7 \mid 56$ abbiamo $n_7 \in \{1, 8\}$. Se $n_7 = 1$ allora G contiene un unico 7-Sylow, chè è quindi un sottogruppo proprio normale di G. Se $n_7 = 8$ allora G contiene $6 \cdot 8 = 48$ elementi di ordine 7 (dato che i 7-Sylow di G sono isomorfi a $\mathbb{Z}/7\mathbb{Z}$) pertanto i restanti 7 elementi non banali devono essere contenuti in un unico 2-Sylow, che è quindi normale. In entrambi i casi G non è semplice.

$\underline{|G| = 72 = 2^3 \cdot 3^2}$: dalle condizioni

$$\begin{cases} n_2 \equiv 1 \pmod 2 \\ n_2 \mid 72 \end{cases} \qquad \begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 72 \end{cases}$$

otteniamo $n_2 \in \{1, 3, 9\}$ e $n_3 \in \{1, 4\}$, distinguiamo quindi due casi.

- Se $n_3 = 1$ allora G contiene un unico 3-Sylow, che è quindi un sottogruppo normale non banale di G, cioè G non è semplice;

- se $n_3 = 4$, siano Q_1, Q_2, Q_3, Q_4 i 3-Sylow di G e $X = \{Q_1, Q_2, Q_3, Q_4\}$, consideriamo l'azione di coniugio di G su X

$$\varphi : G \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_4$$

poiché i 3-Sylow di G sono tutti coniugati tale azione è transitiva. Mostriamo che $\ker \varphi$ è un sottogruppo di G non banale. Se $\ker \varphi = \{e\}$ allora φ sarebbe un omomorfismo iniettivo, che è assurdo in quanto l'ordine di G non divide l'ordine di $\mathcal{S}(X) \cong \mathcal{S}_4$. D'altra parte se fosse $\ker \varphi = G$ allora φ sarebbe l'azione banale, che è assurdo in quanto φ è transitiva e $|X| > 1$ (alternativamente, se φ fosse l'azione banale allora i 3-Sylow di G sarebbero tutti normali). Pertanto $\ker \varphi$ è un sottogruppo normale non banale di G, cioè G non è semplice.

$\underline{|G| = 80 = 2^4 \cdot 5}$: dalle condizioni

$$\begin{cases} n_2 \equiv 1 \pmod 2 \\ n_2 \mid 80 \end{cases} \qquad \begin{cases} n_5 \equiv 1 \pmod 5 \\ n_5 \mid 80 \end{cases}$$

otteniamo $n_2 \in \{1, 5\}$ e $n_5 \in \{1, 16\}$, distinguiamo quindi due casi.

- Se $n_5 = 1$ allora G contiene un unico 5-Sylow, che è quindi un sottogruppo normale non banale di G, cioè G non è semplice;

- se $n_5 = 16$ allora G contiene $4 \cdot 16 = 64$ elementi di ordine 5 (dato che i 5-Sylow di G sono isomorfi a $\mathbb{Z}/5\mathbb{Z}$), pertanto i restanti 15 elementi devono essere contenuti in un unico 2-Sylow, che è quindi normale. Allora G non è semplice.
Alternativamente, consideriamo P_2 un 2-Sylow e l'azione di moltiplicazione a sinistra di G sull'insieme quoziente ${}^{G}\!/_{P_2}$

$$\varphi : G \longrightarrow \mathcal{S}\left({}^{G}\!/_{P_2}\right) \cong \mathcal{S}_5$$

Poiché $|G| \nmid |\mathcal{S}_5|$ abbiamo $\ker \varphi \neq \{e\}$, d'altra parte $\ker \varphi \neq G$ in quanto φ è un'azione transitiva (per ogni $x, y \in G$ vale $\varphi(xy^{-1})(yP_2) = xy^{-1}yP_2 = xP_2$). Quindi $\ker \varphi$ è un sottogruppo normale di G non banale, cioè G non è semplice.

Rimangono da studiare i gruppi di ordine 60, vogliamo dimostrare che $\mathcal{A}_5$ è l'unico sottogruppo semplice di tale ordine (a meno di isomorfismo).

Lemma 1.113
$\mathcal{A}_5$ contiene esattamente 5 2-Sylow.

Dimostrazione. Sia X l'insieme dei 2-Sylow di $\mathcal{A}_5$, consideriamo l'azione di coniugio di $\mathcal{A}_5$ su X

$$\varphi : \mathcal{A}_5 \longrightarrow \mathcal{S}(X)$$

poiché i 2-Sylow di $\mathcal{A}_5$ sono tutti coniugati e $\mathcal{A}_5$ è semplice tale azione è transitiva, in particolare X è composto da un'unica orbita. Fissato P un 2-Sylow abbiamo

$$n_2 = |\operatorname{Orb}(P)| = \frac{|\mathcal{A}_5|}{|N_{\mathcal{A}_5}(P)|}$$

Scegliamo $P = \{id, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$ una copia di V_4 in $\mathcal{A}_5$, il normalizzatore di P in $\mathcal{A}_5$ contiene necessariamente il sottogruppo

$$\operatorname{Stab}(5) = \{\sigma \in \mathcal{A}_5 \mid \sigma(5) = 5\} \cong \mathcal{A}_4 \text{[18]}$$

in quanto V_4 è un sottogruppo normale di $\mathcal{A}_4$, quindi $|N_{\mathcal{A}_5}(P)| \in \{12, 60\}$. D'altra parte $|N_{\mathcal{A}_5}(P)| \neq 60$, altrimenti $\mathcal{A}_5$ conterrebbe un unico 2-Sylow, che sarebbe quindi un sottogruppo normale non banale, che è assurdo in quanto $\mathcal{A}_5$ è semplice. Allora $|N_{\mathcal{A}_5}(P)| = 12$, cioè $n_2 = 5$. □

Proposizione 1.114

Se G è un gruppo semplice di ordine 60 allora è isomorfo a $\mathcal{A}_5$.

Dimostrazione. Dalle condizioni

$$\begin{cases} n_2 \equiv 1 \pmod 2 \\ n_2 \mid 60 \end{cases} \qquad \begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 60 \end{cases} \qquad \begin{cases} n_5 \equiv 1 \pmod 5 \\ n_5 \mid 60 \end{cases}$$

otteniamo $n_2 \in \{1, 3, 5, 15\}$, $n_3 = \{1, 4, 10\}$, $n_5 = \{1, 6\}$. Poiché G è semplice, n_2, n_3 e n_5 sono tutti diversi da 1, altrimenti G conterrebbe un sottogruppo caratteristico, quindi normale, non banale. Distinguiamo tre casi:

- supponiamo per assurdo $n_2 = 3$, posto X l'insieme dei 2-Sylow di G consideriamo l'azione di coniugio di G su X

  $$\varphi : G \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_3$$

  poiché i 2-Sylow sono tutti coniugati e G è semplice tale azione è transitiva, pertanto $\ker \varphi \neq G$. Allora $\ker \varphi = \{e\}$ in quanto $\ker \varphi \lhd G$, ma questo è assurdo dato che $|G| > |\mathcal{S}_3|$;

- supponiamo $n_2 = 5$, posto X l'insieme dei 2-Sylow di G consideriamo l'azione di coniugio di G su X

  $$\varphi : G \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_5$$

  argomentando come sopra si ha che tale azione è transitiva, pertanto $\ker \varphi \neq G$. Allora $\ker \varphi = \{e\}$ in quanto $\ker \varphi \lhd G$, cioè φ è un omomorfismo iniettivo e G è isomorfo a un sottogruppo $H \leqslant \mathcal{S}_5$ di indice 2. Consideriamo l'intersezione $H \cap \mathcal{A}_5$, per la Proposizione 1.49 allora $[\mathcal{A}_5 : H \cap \mathcal{A}_5] \in \{1, 2\}$. D'altra parte se fosse 2 allora $H \cap \mathcal{A}_5$ sarebbe un sottogruppo normale di $\mathcal{A}_5$ non banale, che è assurdo, pertanto l'indice di H è 1, cioè $H = \mathcal{A}_5$. Quindi G è isomorfo a $\mathcal{A}_5$;

[18] Qua stiamo considerando l'azione naturale di $\mathcal{A}_5$ sull'insieme $\{1, 2, 3, 4, 5\}$.

- supponiamo per assurdo $n_2 = 15$, notiamo che due 2-Sylow distinti di G si intersecano banalmente o in un sottogruppo isomorfo a $\mathbb{Z}/2\mathbb{Z}$[19]. Se tutti i 2-Sylow di G si intersecassero banalmente allora la loro unione conterrebbe $1 + 3 \cdot 15 = 46$ elementi, poiché l'unione dei 5-Sylow di G contribuisce con $4 \cdot 6 = 24$ elementi di ordine 5, ma allora G non conterrebbe elementi di ordine 3, che è assurdo. Siano quindi S_1 e $\mathcal{S}_2$ 2-Sylow distinti di G tali che $H = S_1 \cap \mathcal{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$, consideriamo il normalizzatore $N_G(H)$. Osserviamo che S_1 e $\mathcal{S}_2$ sono sottogruppi di $N_G(H)$ in quanto, essendo abeliani, H è un sottogruppo normale di entrambi, pertanto $|N_G(H)| > 4$. D'altra parte poiché tale ordine deve dividere 60 abbiamo $|N_G(H)| \in \{12, 20\}$, infatti se fosse uguale a 60 H sarebbe un sottogruppo normale non banale di G, che non è possibile in quanto G è semplice. Inoltre $|N_G(H)| \neq 20$ in quanto si avrebbe $[G : N_G(H)] = 3$, allora per il Teorema 1.50 G conterrebbe un sottogruppo normale non banale di indice al più 3!, che è assurdo. Abbiamo quindi $|N_G(H)| = 12$, consideriamo l'azione di moltiplicazione a sinistra di G sull'insieme quoziente ${}^{G}\!/\!_{N_G(H)}$

$$\varphi : G \longrightarrow \mathcal{S}\left({}^{G}\!/\!_{N_G(H)}\right) \cong \mathcal{S}_5$$

argomentando come sopra si ha che tale azione è transitiva, pertanto $\ker\varphi \neq G$. Allora $\ker\varphi = \{e\}$ in quanto $\ker\varphi \triangleleft G$, cioè φ è un omomorfismo iniettivo e si mostra come sopra che $G \cong \mathcal{A}_5$, ma questo è assurdo in quanto $\mathcal{A}_5$ contiene 5 2-Sylow.

□

[19] Questo perché la massima potenza di 2 che divide 60 è 4, pertanto un 2-Sylow di G è isomorfo a $\mathbb{Z}/4\mathbb{Z}$ oppure a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

§1.11 Studio di $\mathrm{SL}_2(\mathbb{F}_3)$ $\star$

Consideriamo il gruppo $\mathrm{GL}_2(\mathbb{F}_3)$, ricordiamo che il determinante è un omomorfismo di gruppi surgettivo

$$\det : \mathrm{GL}_2(\mathbb{F}_3) \longrightarrow \mathbb{F}_3^*$$

e che il suo nucleo è il gruppo $\mathrm{SL}_2(\mathbb{F}_3) = \{M \in \mathrm{GL}_2(\mathbb{F}_3) \mid \det M = 1\}$, che è quindi un sottogruppo normale di $\mathrm{GL}_2(\mathbb{F}_3)$. Inoltre, poiché $\mathbb{F}_3^* \cong \mathbb{Z}/2\mathbb{Z}$ abbiamo che $\mathrm{SL}_2(\mathbb{F}_3)$ ha indice 2 in $\mathrm{GL}_2(\mathbb{F}_3)$, pertanto $|\mathrm{SL}_2(\mathbb{F}_3)| = 24$ in quanto $|\mathrm{GL}_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 48$.

Consideriamo quindi il gruppo $S = \mathrm{SL}_2(\mathbb{F}_3)$, dalle condizioni

$$\begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 24 \end{cases}$$

otteniamo $n_3 \in \{1, 4\}$, notiamo però che S non può contenere un unico 3-Sylow in quanto questi sono isomorfi a $\mathbb{Z}/3\mathbb{Z}$ e le matrici

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

hanno ordine 3 e i gruppi che generano sono distinti. In particolare S contiene almeno 2 3-Sylow, pertanto ne contiene esattamente 4. Calcoliamo il centro di S imponendo la commutazione sulle matrici appena esibite. Dall'equazione

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

otteniamo

$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

da cui $c = 0$ e $a = d$. In modo analogo dall'equazione

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

otteniamo

$$\begin{pmatrix} a & b \\ a & a+b \end{pmatrix} = \begin{pmatrix} a+b & b \\ a & a \end{pmatrix}$$

da cui $b = 0$, pertanto un generico elemento del centro è della forma $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ d'altra parte il suo determinante deve essere uguale a 1, quindi $Z(S) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$.
Utilizziamo questo fatto per determinare la classe di isomorfismo del normalizzatore di un 3-Sylow di S.
Fissiamo P un 3-Sylow, poiché $n_3 = [S : N_S(P)]$ abbiamo

$$|N_S(P)| = \frac{|S|}{n_3} = 6$$

inoltre $Z(S)$ e P sono sottogruppi di $N_S(P)$. Notiamo che $N_S(P)$ contiene un elemento di ordine 3 e un elemento di ordine 2 che commutano, ad esempio il generatore di P e il generatore di $Z(S)$, pertanto contiene un elemento di ordine 6, il loro prodotto, da cui $N_S(P) = PZ(S) \cong \mathbb{Z}/6\mathbb{Z}$.

Posto X l'insieme dei 3-Sylow di S, consideriamo l'azione transitiva di coniugio di S su X

$$\Phi : S \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_4$$

il nucleo di Φ è

$$\begin{aligned}\ker \Phi = \{g \in S \mid gPg^{-1} = P \ \forall P \in X\} &= \\ = \{g \in S \mid g \in N_S(P) \ \forall P \in X\} &= \\ = \bigcap_{P \in X} N_S(P) = \bigcap_{P \in X} PZ(S) &= Z(S)\end{aligned}$$

dove l'ultima uguaglianza è giustificata dal fatto che i 3-Sylow di S si intersecano banalmente. Per il Primo Teorema di Omomorfismo otteniamo che $\mathrm{Im}\Phi \cong {}^{S}\!/_{Z(S)}$, che ha cardinalità 12. D'altra parte A$_4$ è l'unico sottogruppo di $\mathcal{S}_4$ con 12 elementi, pertanto ${}^{S}\!/_{Z(S)} \cong \mathcal{A}_4$, sfruttiamo questo fatto per studiare i 2-Sylow di S. Per il Teorema di Corrispondenza i sottogruppi di S contenenti $Z(S)$ sono in bigezione con i sottogruppi di $\mathcal{A}_4$, e tale bigezione preserva l'indice e la normalità dei sottogruppi. Poiché V_4 è l'unico 2-Sylow di $\mathcal{A}_4$ abbiamo che S contiene un unico 2-Sylow di indice 3, cioè di cardinalità 8, chiamiamo J tale sottogruppo. J contiene le matrici

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ [20]

entrambe di ordine 4, inoltre

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

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

pertanto $ij = -ji$. Quindi J è un gruppo di ordine 8 che contiene due elementi di ordine 4 che anticommutano, in particolare ha la seguente presentazione

$$J = \langle i, j \mid i^4 = j^4 = 1, i^2 = -1, ij = -ji \rangle$$

quindi è isomorfo a Q_8. Osserviamo che il sottogruppo derivato S' è contenuto in J in quanto il quoziente ${}^{S}\!/_{J}$ è abeliano (in particolare è isomorfo a $\mathbb{Z}/3\mathbb{Z}$), mostriamo che effettivamente vale l'uguaglianza. Sicuramente S' non è il sottogruppo formato dalla sola identità in quanto S non è abeliano, inoltre S' deve necessariamente contenere un elemento di ordine 2 in quanto sottogruppo non banale di J, quindi $Z(S) \subseteq S'$[21]. Inoltre $Z(S) \neq S'$ in quanto il quoziente è isomorfo a $\mathcal{A}_4$, pertanto S' ha ordine 4 oppure 8, cioè $[S : S'] \in \{3, 6\}$. Consideriamo l'omomorfismo surgettivo

$$\varphi : S \longrightarrow \mathcal{A}_4$$

dato dalla composizione della proiezione su ${}^{S}\!/_{Z(S)}$ con l'isomorfismo tra il quoziente e $\mathcal{A}_4$, per il Teorema di Corrispondenza $\varphi(S')$ è un sottogruppo normale di $\mathcal{A}_4$ con $[\mathcal{A}_4 : \varphi(S')] = [S : S']$. D'altra parte un sottogruppo di indice 6 di $\mathcal{A}_4$ è della forma $\{id, (a\ b)(c\ d)\}$ con $(a\ b)$ e $(c\ d)$ trasposizioni disgiunte, che non è normale in $\mathcal{A}_4$, pertanto $\varphi(S')$ ha indice 3 e quindi S' ha ordine 8, da cui $S' = J$.

[20] Il determinante di questa matrice è -2, che è uguale a 1 in $\mathbb{F}_3$

[21] Infatti l'unico elemento di ordine 2 di S è $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

§2 Anelli

A meno di ulteriori specificazioni, gli anelli che tratteremo saranno sempre anelli commutativi con identità.

§2.1 Interpolazione polinomiale tramite il TCR

Mostriamo il seguente enunciato di interpolazione utilizzando il Teorema Cinese del Resto.

Proposizione 2.1

Siano $a_1, \ldots, a_n \in \mathbb{Q}$ valori distinti e $b_1, \ldots, b_n \in \mathbb{Q}$, allora esiste un unico polinomio $p(x) \in \mathbb{Q}[x]$ di grado al più $n-1$ tale che $p(a_i) = b_i$ per ogni $i \in \{1, \ldots, n\}$.

Dimostrazione. Posto $I_i = (x - a_i)$ per $i \in \{1, \ldots, n\}$, osserviamo che $I_i + I_j = \mathbb{Q}[x]$ per $i \neq j$, infatti $a_i - a_j \in I_i + I_j$, che è un elemento invertibile di $\mathbb{Q}[x]$. Per il Teorema Cinese del Resto abbiamo quindi

$$\frac{\mathbb{Q}[x]}{I_1 \ldots I_n} \cong \mathbb{Q}[x]/I_1 \times \ldots \times \mathbb{Q}[x]/I_n$$

tramite l'isomorfismo

$$\Phi : \frac{\mathbb{Q}[x]}{I_1 \ldots I_n} \longrightarrow \mathbb{Q}[x]/I_1 \times \ldots \times \mathbb{Q}[x]/I_n : \overline{p(x)} \longmapsto (p(x) + I_1, \ldots, p(x) + I_n)$$

abbiamo inoltre che $\mathbb{Q}[x]/I_i \cong \mathbb{Q}$ per ogni $i \in \{1, \ldots, n\}$ tramite l'isomorfismo

$$\Psi : \mathbb{Q}[x]/I_i \longrightarrow \mathbb{Q} : p(x) + I_i \longmapsto p(a_i)$$

La composizione di questi due risulta in un isomorfismo

$$\Psi \circ \Phi : \frac{\mathbb{Q}[x]}{I_1 \ldots I_n} \longrightarrow \mathbb{Q}^n : \overline{p(x)} \longmapsto (p(a_1), \ldots, p(a_n))$$

in particolare per ogni n-upla di razionali $(b_1, \ldots, b_n)$ esiste un unico[22] polinomio $p \in \mathbb{Q}[x]$ con $\deg p \leq n-1$ tale che $p(a_i) = b_i$ per ogni $i \in \{1, \ldots, n\}$. □

Osservazione 2.2 — Con la dimostrazione data l'enunciato è vero su ogni campo con almeno n elementi distinti. Più in generale è vero in ogni anello con almeno n elementi distinti a patto di scegliere $a_1, \ldots, a_n$ tali che $a_i - a_j$ sia invertibile per ogni $i \neq j$.

[22] L'unicità deriva dal fatto che gli elementi di $\frac{\mathbb{Q}[x]}{I_1 \ldots I_n}$ possono essere rappresentati in modo unico da polinomi a coefficienti razionali di grado al più $n-1$.

§2.2 Localizzazione di $\mathbb{Z}$ rispetto a un ideale primo

Premessa — Tutta la teoria sviluppata in questa sezione è ancora valida sostituendo a $\mathbb{Z}$ un generico PID R. Per motivi didattici si è preferito discutere solamente il caso di $\mathbb{Z}$. Si invita ciononostante il lettore a riflettere con gli stessi argomenti nel caso più generale e a discutere il caso in cui R è solo un UFD.

Sia $P = (p)$ un ideale primo non nullo di $\mathbb{Z}$. Consideriamo l'insieme $S = \mathbb{Z} \setminus P$ e mostriamo che S è in effetti una parte moltiplicativa di $\mathbb{Z}$:

- $0 \notin S$ dal momento che $0 \in P$;
- $1 \in S$ in quanto 1 non può appartenere a P (altrimenti P non sarebbe un ideale proprio),
- per ogni x, $y \in S$, $xy \in S$: se così non fosse, xy apparterrebbe a P, e dunque uno tra x e y non potrebbe appartenere a S dacché P è un ideale primo.

Pertanto si può considerare l'anello delle frazioni $S^{-1}\mathbb{Z}$, detto $\mathbb{Z}_P$. Si mostra facilmente che $S^{-1}P = \mathbb{Z}_P \setminus (\mathbb{Z}_P)^*$.

Infatti per quanto visto nella teoria degli anelli delle frazioni vale che:

$$(\mathbb{Z}_P)^* = \left\{ \frac{m}{n} \in \mathbb{Z}_P \mid \exists\, t \in \mathbb{Z} \mid mt \in S \right\},$$

ovverosia un elemento $\frac{m}{n}$ è invertibile se e solo se esiste un $t \in \mathbb{Z}$ per cui mt non appartiene a P. Tuttavia, poiché P è primo, questo è equivalente a richiedere che m non sia un elemento di P, ossia che $p \nmid m$. Pertanto vale che:

$$(\mathbb{Z}_P)^* = \left\{ \frac{m}{n} \in \mathbb{Z}_P \mid m, n \in S \right\} = S^{-1}S,$$

e dunque che $S^{-1}P = \mathbb{Z}_P \setminus (\mathbb{Z}_P)^*$.

Osservazione 2.3 ($S^{-1}P$ è l'unico ideale massimale di $\mathbb{Z}_P$) **—** Consideriamo un ideale I di $\mathbb{Z}_P$ tale per cui $S^{-1}P \subseteq I$. Allora I o è $S^{-1}P$ o contiene un elemento di $\mathbb{Z}_P$ che non appartiene a $S^{-1}P$. Per quanto appena visto, un tale elemento è invertibile, e quindi I sarebbe esattamente $\mathbb{Z}_P$. Pertanto $S^{-1}P$ è un ideale massimale di $\mathbb{Z}_P$.

Si mostra che tale ideale è l'unico ideale massimale di $\mathbb{Z}_P$. Se I è un ideale massimale, allora I non può contenere un invertibile (altrimenti si avrebbe $I = \mathbb{Z}_P$). si avrebbe $I = \mathbb{Z}_P$. Pertanto I è contenuto in $\mathbb{Z}_P \setminus (\mathbb{Z}_P)^* = S^{-1}P$, da cui si deduce che $\mathbb{Z}_P = S^{-1}P$.

Per quanto visto, $\mathbb{Z}_P$ è dunque in qualche modo "speciale" dal punto di vista teorico, dal momento che lo studio dei suoi ideali massimali è decisamente semplificato. Pertanto si dice che $\mathbb{Z}_P$ è un **anello locale** e che è in particolare il **localizzato** di $\mathbb{Z}$ rispetto all'ideale primo P.

Gli ideali di $\mathbb{Z}_P$ sono tutti della forma $S^{-1}(m)$ con $(m) \subseteq \mathbb{Z}$ ideale. Vale inoltre che:

$$S^{-1}(m) = \left\{ \frac{mk}{s} \;\middle|\; k \in \mathbb{Z}, s \in S \right\} = \left\{ m\frac{k}{s} \;\middle|\; \frac{k}{s} \in S^{-1}\mathbb{Z} \right\} = (m)S^{-1}\mathbb{Z}$$

È noto che ogni ideale di un anello di frazioni è indotto da un ideale dell'anello di base. In particolare la mappa $I \mapsto S^{-1}I$ è surgettiva negli ideali di $S^{-1}A$ per una qualche parte moltiplicativa S e qualche anello.

Nel caso di un PID, come $\mathbb{Z}$, e di una localizzazione rispetto a un ideale primo, si può rafforzare la corrispondenza tra gli ideali dei due anelli. Infatti, se (m) ed (n) sono ideali di $\mathbb{Z}$, allora vale che:

$$S^{-1}(m) = S^{-1}(n) \iff \exists u \in (S^{-1}\mathbb{Z})^* \mid m = un \iff \frac{m}{n} \in (S^{-1}\mathbb{Z})^*,$$

ossia i due ideali coincidono se la frazione $\frac{m}{n}$, che corrisponde in modo naturale a un elemento di $\mathrm{Q}(\mathbb{Z}) = (\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z} \cong \mathbb{Q}$, appartiene a $S^{-1}\mathbb{Z}$ ed è invertibile.

Si ricorda inoltre che sussiste la seguente bigezione:

$$\{\text{ideali primi di } S^{-1}\mathbb{Z}\} \leftrightarrow \{\text{ideali primi } P \subseteq \mathbb{Z} \mid P \cap S = \varnothing\}$$

dove a un ideale P di $\mathbb{Z}$ si fa corrispondere $S^{-1}P$ in $\mathbb{Z}_P$. Da questa corrispondenza si verifica immediatamente che gli unici ideali primi di $\mathbb{Z}_P$ sono $S^{-1}(0)$ e $S^{-1}P$.

Osservazione 2.4 (Localizzazione rispetto a $P = (2)$) — Consideriamo il localizzato di $\mathbb{Z}$ rispetto all'ideale $P = (2)$, ossia $\mathbb{Z}_{(2)} = S^{-1}\mathbb{Z}$ con $S = \mathbb{Z} \setminus (2)$. Il suo ideale massimale è $S^{-1}(2)$, ossia:

$$S^{-1}(2) = (2)\mathbb{Z}_{(2)} = \left\{ 2\frac{m}{n} \;\middle|\; m, n \in \mathbb{Z}, 2 \nmid n \right\}$$

In particolare gli elementi invertibili di $S^{-1}\mathbb{Z}$ sono le frazioni in cui sia nominatore che denominatore sono dispari. Pertanto due ideali $(m) = (n)$ corrispondono allo stesso ideale in $S^{-1}\mathbb{Z}$ se e solo se $\frac{m}{n}$, ridotta ai minimi termini, ha numeratore e denominatore dispari, ovverosia, equivalentemente, se m ed n sono divisi esattamente dalla stessa potenza di 2 (ossia se $\nu_2(m) = \nu_2(n)$, dove ν_2 indica la valutazione 2-adica; per esempio, $S^{-1}(3) = S^{-1}(1)$, dacché $2^0 \parallel 1$ e $2^0 \parallel 3$). Pertanto gli unici ideali di $S^{-1}\mathbb{Z}$ sono (0) e quelli della forma $S^{-1}(2^k)$ con $k \in \mathbb{N}$, mentre gli ideali primi sono soltanto $S^{-1}(0)$ e $S^{-1}(2)$.

§2.3 Ideali primi e massimali di $\mathbb{Z}[x]$

Si illustra un lemma preliminare che ci permetterà successivamente di classificare gli ideali di $\mathbb{Z}[x]$:

Lemma 2.5

Se $A \subseteq R$ sono due anelli e $P \subseteq R$ è un ideale primo di R, allora $P \cap A$ è un ideale primo di A.

Dimostrazione. Chiaramente $P \cap A$ è un ideale di A. Uno dei modi per verificarlo è considerare l'omomorfismo di inclusione naturale da A in R ed osservare che $P \cap A$ è esattamente la controimmagine di P tramite questa mappa.

Se allora xy appartiene a $P \cap A$ con x e $y \in A$, allora uno tra x e y deve appartenere a P, essendo P primo in R. Pertanto uno tra x e y deve appartenere a $P \cap A$, e dunque $P \cap A$ è primo in A. $\square$

Consideriamo un ideale primo P di $\mathbb{Z}[x]$. Per[23] il Lemma 2.5 $P \cap \mathbb{Z}$ è un ideale primo di $\mathbb{Z}$, e dunque è (0) o è generato da un primo $p \in \mathbb{Z}$.

$\boxed{P \cap \mathbb{Z} = (p)}$ Ipotizziamo di essere nel caso in cui $P \cap \mathbb{Z} = (p)$. Allora $(p) \subseteq P$, e dunque, per il Teorema di Corrispondenza, P corrisponde all'ideale primo $P' := P/p\mathbb{Z}[x]$ di $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$. Se P' è l'ideale nullo, allora $P = (p)$, che è dunque primo, ma non massimale (infatti (0) non è massimale in $\mathbb{Z}_p[x]$).

Se invece P' non è nullo, poiché $\mathbb{Z}_p[x]$ è un PID (e in particolare, anche un dominio euclideo), P' è massimale oltre che primo, e dunque è generato da un polinomio irriducibile $\overline{f(x)} \in \mathbb{Z}_p[x]$. Allora a P' corrisponde $P = (p) + (f(x)) = (p, f(x))$, che è dunque massimale anche in $\mathbb{Z}[x]$.

Pertanto gli ideali primi di $\mathbb{Z}[x]$ contenenti un ideale primo (p) di $\mathbb{Z}$ sono:

- (p) stesso, che non è massimale,
- $(p, f(x))$ con $f(x)$ irriducibile in $\mathbb{Z}_p[x]$, che è massimale.

$\boxed{P \cap \mathbb{Z} = (0)}$ Supponiamo adesso che P sia un ideale primo di $\mathbb{Z}[x]$ tale per cui $P \cap \mathbb{Z} = (0)$. Si ricorda che $S = \mathbb{Z} \setminus \{0\}$ è una parte moltiplicativa di $\mathbb{Z}$ (e quindi a maggior ragione di $\mathbb{Z}[x]$) e si osserva che $S^{-1}\mathbb{Z}[x] \cong \mathbb{Q}[x]$. Inoltre gli ideali primi di $\mathbb{Q}[x]$ corrispondono agli ideali primi I di $\mathbb{Z}[x]$ tali per cui $I \cap S = \varnothing$, come, per l'appunto, P. Pertanto P corrisponde a un ideale primo di $\mathbb{Q}[x]$, che, essendo un PID, dispone di (0) e degli ideali generati da irriducibili come unici suoi ideali primi. Se $S^{-1}P = (0)$, allora P era già (0) in partenza; se invece $S^{-1}P$ era non nullo, $S^{-1}P = (f(x))$ con $f(x)$ irriducibile su $\mathbb{Q}[x]$.

Se $g(x)$ è un associato di $f(x)$ a coefficienti interi[24], allora $S^{-1}P = (g(x))S^{-1}\mathbb{Z}[x] = S^{-1}(g(x))$, e dunque $P = (g(x))$.

[23] In realtà $\mathbb{Z}$ non è esattamente un sottoinsieme di $\mathbb{Z}[x]$, ma ciononostante vi ci immerge in modo del tutto naturale ($\mathbb{Z}[x]$ estende in questo senso $\mathbb{Z}$). Continueremo dunque a usare il simbolo $\mathbb{Z}$ per l'identificazione naturale di $\mathbb{Z}$ in $\mathbb{Z}[x]$.

[24] Tale $g(x)$ esiste sempre: è sufficiente moltiplicare $f(x)$ per il minimo comune multiplo dei denominatori dei suoi coefficienti.

Osservazione 2.6 ($(f(x))$ non è massimale in $\mathbb{Z}[x]$) — Mostriamo che gli ideali della forma $(f(x))$ non sono massimali in $\mathbb{Z}[x]$. Sia $a \in \mathbb{Z}$ tale per cui $f(a)$ sia divisibile da un primo p. Consideriamo i due omomorfismi φ e ψ tali per cui:

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]/(p)\mathbb{Z}[x] \cong \mathbb{Z}_p[x], g(x) \mapsto \overline{g(x)},$$

$$\psi : \mathbb{Z}[x]/(p)\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}, \overline{g(x)} \mapsto g(a).$$

Per ipotesi, $(\psi \circ \varphi)(f(x)) = \overline{f(a)} \equiv 0$, dunque $f(x) \in \ker(\psi \circ \varphi)$. Inoltre $(\psi \circ \varphi)(p) = \overline{p} \equiv 0$, da cui si deduce che $p \in \ker(\psi \circ \varphi)$. Dal momento che $\ker(\psi \circ \varphi)$ è diverso da $\mathbb{Z}[x]$ e che $I = (f(x)) \subseteq \ker(\psi \circ \varphi)$, allora, se I fosse massimale, si avrebbe l'uguaglianza $I = \ker(\psi \circ \varphi)$. Pertanto p apparterrebbe a I, assurdo.

Si riassume allora la classificazione degli ideali primi e massimali di $\mathbb{Z}[x]$:

- (0) è un ideale primo non massimale,
- (p), con $p \in \mathbb{Z}$ primo, è primo non massimale,
- $(p, f(x))$, con $p \in \mathbb{Z}$ primo e $\overline{f(x)}$ irriducibile in $\mathbb{Z}_p[x]$, è primo e massimale,
- $(f(x))$, con $f(x)$ irriducibile in $\mathbb{Z}[x]$, è primo non massimale.

Mostriamo che gli ideali primi di quest'ultimo tipo non sono massimali. Se $P = (f(x))$ con $f(x)$ irriducibile fosse massimale in $\mathbb{Z}[x]$, potre

§2.4 Corollari sui domini a ideali principali

Si riassumono in questa sezione alcuni risultati interessanti riguardanti i PID, ovverosia i domini a ideali principali.

Proposizione 2.7

Sia A un PID, ogni ideale primo diverso da (0) di A è un ideale massimale.

Dimostrazione. Sia $P = (p)$ un ideale primo non nullo. Sia M un ideale tale per cui:

$$P \subseteq M \subseteq A$$

Poiché A è un PID, $M = (m)$ per un qualche $m \in A$. Dal momento che $P = (p) \subseteq (m) = M$, allora m divide p, e quindi, dacché p è in particolare anche irriducibile, o m è un'unità, e dunque $M = A$, o m è un associato di p, e dunque $M = P$. Pertanto M è massimale. □

Dimostrazione alternativa. Sia M un ideale di A. Allora $M = (p)$ con p primo in A, dacché A è un PID. Inoltre, sempre perché A è un PID, p è in particolare irriducibile. Pertanto $A/(p)$ è un campo[25], e dunque (p) è massimale. □

Corollario 2.8

Se A è un PID, B è un dominio di integrità e $\varphi : A \longrightarrow B$ è un omomorfismo surgettivo, allora φ è un isomorfismo oppure B è un campo.

Dimostrazione. Dal momento che $A/\ker\varphi \cong B$ è un dominio, $\ker\varphi$ è un ideale primo. Se $\ker\varphi = (0)$, allora φ è un isomorfismo; altrimenti $\ker\varphi$ è massimale per la Proposizione 2.7, e dunque $B \cong A/\ker\varphi$ è un campo. □

Esempio 2.9

Un classico esempio di omomorfismo di questo tipo è l'omomorfismo che descrive la caratteristica di un dominio di integrità B, ossia l'omomorfismo $\varphi : \mathbb{Z} \to B$ univocamente determinato dall'identità $\varphi(1) = 1_B$. In tal caso $\operatorname{char} B$ è definito come il generatore non negativo di $\ker\varphi$, e, per il corollario appena dimostrato, o è 0, o è p. In particolare, se $\operatorname{char} B$ è primo, sicuramente B è un campo.

Corollario 2.10

Se C è un anello, allora $C[x]$ è un PID se e solo se C è un campo.

Dimostrazione. Se C è un campo, allora si verifica facilmente che $C[x]$ è un PID, dal momento che è un dominio euclideo.

Se invece $C[x]$ è un PID, dall'immersione naturale $C \hookrightarrow C[x]$ ricaviamo che C è un dominio di integrità. Pertanto l'ideale (x) è primo in $C[x]$, dacché $C[x]/(x) \cong C$ è un dominio. Poiché $(x) \neq (0)$, (x) è massimale, e dunque $C \cong C[x]/(x)$ è un campo. □

[25]Se a è un elemento irriducibile di un PID A, allora $A/(a)$ è un campo. Infatti, $A/(a)$ è un dominio di integrità dacché a è primo (in un PID i primi e gli irriducibili coincidono), e inoltre l'inverso di un elemento $b + (a)$ con $b \notin (a)$ è dato dall'identità di Bezout che si ricava dall'identità $(a, b) = (1)$.

§2.5 Operazioni tra ideali

Sia A un anello commutativo con identità. Allora sono ben definite le seguenti operazioni su due ideali I e J:

- $I \cap J = \{k \in A \mid k \in I, k \in J\}$, l'**intersezione** tra I e J,
- $I + J = (I, J) = \{i + j \mid i \in I, j \in J\}$, ovverosia la **somma** tra I e J,
- $IJ = (\{ij \mid i \in I, j \in J\})$, ossia il **prodotto** tra I e J, che si ricorda non essere un'estensione di I (anzi, $IJ \subseteq I,\ J$, e quindi $IJ \subseteq I \cap J$),
- $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} \text{ per cui } x^n \in I\}$, detto il **radicale** di I in A,
- $(I : J) = \{x \in A \mid xJ \subseteq I\}$, il cosiddetto **quoziente** (o *colon*) tra ideali.

Proposizione 2.11

Se A è un anello commutativo con identità e I e $J \subseteq A$ sono due suoi ideali, allora vale che:

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

Dimostrazione. Dal momento che $IJ \subseteq I \cap J$, allora $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. Sia ora $a \in \sqrt{I \cap J}$. Per ipotesi esiste $n \in \mathbb{N}$ tale per cui $a^n \in I \cap J$. Allora vale che:

$$a^{2n} = \underbrace{a^n}_{\in I} \cdot \underbrace{a^n}_{\in J} \in IJ$$

e dunque $a \in \sqrt{IJ}$, da cui si conclude che $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$.

Poiché $I \cap J \subseteq I,\ J$, allora $\sqrt{I \cap J} \subseteq \sqrt{I},\ \sqrt{J}$, e dunque $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Se $a \in \sqrt{I} \cap \sqrt{J}$, allora esistono m, $n \in \mathbb{N}$ tali per cui $a^m \in I$ e $a^n \in J$. In particolare $a^{m+n} = a^m a^n$ appartiene ad IJ, e quindi $I \cap J$; pertanto $a \in \sqrt{I \cap J}$. Si conclude dunque che $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$, da cui la tesi. □

Proposizione 2.12

Dato A un anello commutativo con identità, allora

$$\sqrt{(0)} = \bigcap_{\substack{P \subseteq A \\ P \text{ ideale primo}}} P$$

Dimostrazione. Sia X l'intersezione di tutti gli ideali primi di A. Se $x \in \sqrt{(0)}$ allora esiste $n \in \mathbb{N}$ tale che $x^n = 0$, procediamo per induzione su n. Se $n = 1$ allora $x = 0$, quindi x è contenuto in tutti gli ideali di A, in particolare in quelli primi. Se $n > 1$, supponiamo che se $x^{n-1} \in X$ allora $x \in X$. Per ogni ideale primo P, poiché $x^n = 0$ si ha che x^n è contenuto nella loro intersezione, da cui almeno uno tra x e x^{n-1} è un elemento di X. Se $x^{n-1} \in X$ allora $x \in X$ per ipotesi induttiva, pertanto $\sqrt{(0)} \subseteq X$. Viceversa, mostriamo che se $x \notin \sqrt{(0)}$ allora esiste un ideale primo P tale che $x \notin P$. Consideriamo l'insieme

$$\mathcal{F} = \{I \subseteq A \mid I \text{ ideale}, x^n \notin I\ \forall n \in \mathbb{N}\}$$

notiamo che $\mathcal{F}$ è non vuoto in quanto contiene l'ideale nullo. Posta $\mathscr{C} = \{I_i\}$ una catena di ideali tali che $I_i \subseteq I_{i+1}$, sia

$$\mathcal{I} = \bigcup I_i$$

Per costruzione $\mathcal{I}$ è un maggiorante per $\mathscr{C}$ in quanto ogni I_i è contenuto in $\mathcal{I}$, inoltre $\mathcal{I}$ è un ideale di A dato che $I_i \subseteq I_{i+1}$. L'ideale $\mathcal{I}$ è un elemento di $\mathcal{F}$, infatti se le potenze di x non sono elementi degli ideali di $\mathcal{F}$, a maggior ragione non sono contenute in $\mathcal{I}$. Pertanto ogni catena $\mathscr{C}$ di $\mathcal{F}$ ammette un maggiorante in $\mathscr{C}$, pertanto per il Lemma di Zorn esiste un ideale M massimale in $\mathcal{F}$. Mostriamo che M è un ideale primo di A. Siano $a, b \in A$ tali che $ab \in M$, supponiamo per assurdo $a \notin M$ e $b \notin M$, allora M è contenuto strettamente negli ideali $(M, a), (M, b)$. Poiché M è massimale in $\mathcal{F}$, esistono $h, k \in \mathbb{N}$ tali che $x^k \in (M, a)$ e $x^h \in (M, b)$, da cui

$$x^{h+k} \in (M, a)(M, b) \subseteq M$$

che è assurdo in quanto M è un elemento di $\mathcal{F}$. Pertanto M è un ideale primo di A che non contiene nessuna potenza di x, da cui segue la tesi. □

Corollario 2.13

Dati A un anello commutativo con identità e $I \subseteq A$ un ideale, allora

$$\sqrt{I} = \bigcap_{\substack{P \supseteq I \\ P \subseteq A \text{ ideale primo}}} P$$

Dimostrazione. Consideriamo l'omomorfismo di proiezione

$$\pi : A \longrightarrow {}^{A}\!/_{I}$$

osserviamo che $\sqrt{I} = \pi^{-1}(\sqrt{(0)})$, dove $\sqrt{(0)}$ è il radicale di 0 in ${}^{A}\!/_{I}$. Per la Proposizione 2.9 abbiamo

$$\sqrt{I} = \pi^{-1}(\sqrt{(0)}) = \pi^{-1}\left(\bigcap_{\substack{P \subseteq {}^{A}\!/_{I} \\ P \text{ ideale primo}}} P \right) = \bigcap_{\substack{P \supseteq I \\ P \subseteq A \text{ ideale primo}}} P$$

□

Grazie a questo risultato, possiamo classificare gli elementi invertibili degli anelli di polinomi.

Proposizione 2.14

Se A è un anello commutativo con identità allora

$$A[x]^* = \left\{ p(x) = \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_0 \in A^*, a_i \in \sqrt{0} \ \forall i \in \{1, \ldots, n\} \right\}$$

Dimostrazione. Sia X l'insieme definito come sopra. Consideriamo $p(x) = \sum_{i=0}^{n} a_i x^i$ un elemento di X, poiché $a_0 \in A^*$ possiamo scrivere

$$a_0^{-1} p(x) = 1 + \sum_{i=1}^{n} a_i' x^i \qquad a_i' = \frac{a_i}{a_0} \ \forall i \in \{1, \dots, n\}$$

poniamo $t = -\sum_{i=1}^{n} a_i' x^i$. Notiamo che t è nilpotente in quanto tutti i coefficienti a_i' sono nilpotenti e l'insieme dei nilpotenti è un ideale. Fissiamo $m \in \mathbb{N}$ tale che $t^m = 0$, dalla fattorizzazione

$$1 - t^m = (1 - t) \left(\sum_{i=0}^{m-1} t^i \right)$$

otteniamo

$$1 = a_0^{-1} p(x) \left(\sum_{i=0}^{m-1} t^i \right)$$

in particolare $p(x) \in A[x]^*$ e quindi $X \subseteq A[x]^*$.

Viceversa, siano $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ un elemento di $A[x]^*$ e $g(x) = f(x)^{-1}$, allora $f(x)g(x) = 1$. Notiamo che $\alpha_0 \in A^*$, infatti valutando i due polinomi in 0 abbiamo

$$f(0)g(0) = a_0 g(0) = 1$$

Sia $P \subsetneq A$ un ideale primo, $P[x]$ è un ideale primo di $A[x]$, riduciamo l'espressione $f(x)g(x)$ modulo $P[x]$ tramite l'omomorfismo di proiezione

$$\pi : A[x] \longrightarrow {}^{A}\!/\!_{P}[x] \cong {}^{A[x]}\!/\!_{P[x]}$$

Abbiamo $\pi(f(x))\pi(g(x)) = \pi(1)$, cioè $\pi(f(x))$ è invertibile in ${}^{A}\!/\!_{P}[x]$, da cui otteniamo $\pi(f(x)) \in ({}^{A}\!/\!_{P})^*$ in quanto ${}^{A}\!/\!_{P}$ è un dominio di integrità. Allora abbiamo $a_i \in P$ per ogni $i \in \{1, \dots, n\}$, in particolare tali coefficienti sono contenuti nell'intersezione di tutti gli ideali primi di A per l'arbitrarietà di P, sono quindi nilpotenti per la Proposizione 2.9. Vale quindi l'inclusione $A[x]^* \subseteq X$, da cui l'uguaglianza. □

Proposizione 2.15

Siano A un anello commutativo con identità e $I, J, K \subseteq A$ ideali. Valgono i seguenti fatti:

(1) se $I + J + K = A$ allora $I^n + J^n + K^n = A$ per ogni $n \geq 1$;

(2) se $I + J = J + K = I + K = A$ allora $IJ + JK + IK = A$.

Dimostrazione. Mostriamo i due fatti separatamente:

(1) poiché $I + J + K = A$ esistono $i \in I, j \in J, k \in K$ tali che $i + j + k = 1$. Consideriamo la potenza

$$(i + j + k)^N = \sum_{x+y+z=N} \binom{N}{x, y, z} i^x j^y k^z$$ [26]

[26] Ricordiamo che $\binom{N}{x, y, z} = \frac{N!}{x!\, y!\, z!}$.

Se $N \geq 3n$ osserviamo che $\max x, y, z \geq n$ per ogni $x, y, z \in \mathbb{N}$ tali che $x+y+z = N$, pertanto scegliendo N in questo modo abbiamo che $(i+j+k)^N = 1$ è un elemento di $I^n + J^n + K^n$, quindi l'ideale coincide con A;

(2) dalle ipotesi esistono $i_1, i_2 \in I, j_1, j_2 \in J, k_1, k_2 \in K$ tali che

$$i_1 + j_1 = 1 \qquad j_2 + k_1 = 1 \qquad i_2 + k_2 = 1$$

Per la proprietà di assorbimento degli ideali IJ, JK, IK, svolgendo i calcoli si ha

$$1 = (i_1 + j_1)(j_2 + k_1)(i_2 + k_2) \in IJ + JK + IK$$

□

Osservazione 2.16 (Un quoziente non banale di $\mathbb{Q}[x,y]$ isomorfo a $\mathbb{Q}$) — Consideriamo l'omomorfismo $\varphi : \mathbb{Q}[x,y] \to \mathbb{Q}$ che associa a $f(x,y)$ la valutazione $f(1,1)$. Chiaramente sia $x-1$ che $y-1$ appartengono al nucleo di φ, e dunque vale che $(x-1, y-1) \subseteq \ker \varphi$.

Siano $\alpha : \mathbb{Q}[x,y] \to \mathbb{Q}[x]$ e $\beta : \mathbb{Q}[x] \to \mathbb{Q}$ due omomorfismi intermedi per φ tali per cui $f(x,y) \overset{\alpha}{\mapsto} f(x,1)$ e $p(x) \overset{\beta}{\mapsto} p(1)$. Allora $\varphi = \beta \circ \alpha$, e dunque α e β fanno commutare il seguente diagramma:

$$\begin{tikzcd}
\mathbb{Q}[x,y] \arrow[r, "\varphi"'] \arrow[d, "\alpha"] & \mathbb{Q} \\
\mathbb{Q}[x] \arrow[ur, "\beta"] &
\end{tikzcd}$$

In particolare vale che $\ker \beta = (x-1)$.

Studiamo adesso $\ker \alpha$. Chiaramente $y - 1 \in \ker \alpha$, e dunque $(y-1) \subseteq \ker \alpha$. Mostriamo che vale esattamente l'uguaglianza. Se $f(x,y) \in \ker \alpha$, allora $f(x,y)$ può identificarsi come polinomio $p(y)$ a coefficienti in $\mathbb{Q}[x]$, che, essendo un dominio euclideo, è in particolare un UFD.

Dal momento che $f(x,y) \in \ker \alpha$, vale che $p(1) = 0$, e dunque $y-1$ divide p in $\mathbb{Q}(x)[y]$ per il Teorema di Ruffini. Tuttavia $y-1$ è un elemento primitivo di $\mathbb{Q}[x][y] \cong \mathbb{Q}[x,y]$, e dunque $y-1$ divide p anche in $\mathbb{Q}[x][y]$ per il Lemma di Gauss. Pertanto $y-1$ divide $f \equiv p$, e quindi $\ker \alpha = (y-1)$.

Poiché il diagramma commuta, vale che:

$$\ker \varphi = \ker(\beta \circ \alpha) = \{f(x,y) \in \mathbb{Q}[x,y] \mid \alpha(f(x,y)) \in \ker \beta\} = \alpha^{-1}(\ker \beta)$$

Pertanto $\ker \varphi = \alpha^{-1}((x-1)) = (x-1) + \underbrace{(y-1)}_{=\ker \alpha} = (x-1, y-1)$.

Allora, per il Primo Teorema di Omomorfismo vale che:

$$\frac{\mathbb{Q}[x,y]}{(x-1, y-1)} \cong \mathbb{Q}$$

e poiché $\mathbb{Q}$ è un campo, si deduce anche $(x-1, y-1)$ è un ideale primo e massimale di $\mathbb{Q}[x, y]$.

Osservazione 2.17 (Un quoziente non banale di $\mathbb{Q}[x, y]$ isomorfo a $\mathbb{Q}[x]$) — Consideriamo l'omomorfismo $\varphi : \mathbb{Q}[x, y] \to \mathbb{Q}[x]$ che associa a $f(x, y)$ la valutazione $f(x, x)$. Chiaramente $(x-y)$ è contenuto in $\ker\varphi$.

Mostriamo che anche $\ker\varphi$ è contenuto in $(x-y)$. Sia $f(x, y) \in \ker\varphi$. Allora vale che:

$$f(x,y) = \sum_{i,j} a_{ij}x^i y^j = \sum_{i,j} a_{ij}x^i(y^j - x^j + x^j) = \underbrace{\sum_{i,j} a_{ij}x^{i+j}}_{=0} + \sum_{i,j} a_{ij}x^i(y^j - x^j)$$

dove la prima somma è nulla dal momento che $f(x, x) = 0$. Pertanto, dacché $y - x \mid y^j - x^j$, $f(x, y)$ è divisibile per $y - x$, e dunque $\ker\varphi \subseteq (x - y)$.

Alternativamente f può essere visto come un polinomio $p(y)$ a coefficienti in $\mathbb{Q}[x]$, che è un UFD. Dal momento che $f \in \ker\varphi$, allora $p(x) = 0$, e dunque p è diviso, per il Teorema di Ruffini, da $x - y$ in $\mathbb{Q}(x)[y]$. Tuttavia $x - y$ è primitivo in $\mathbb{Q}[x]$, e dunque p è diviso da $x - y$ anche in $\mathbb{Q}[x][y] \cong \mathbb{Q}[x, y]$ per il Lemma di Gauss. Pertanto $f \equiv p$ è divisibile per $x - y$, da cui si conclude che $\ker\varphi = (x - y)$.

Per il Primo Teorema di Omomorfismo allora vale che:

$$\frac{\mathbb{Q}[x, y]}{(x - y)} \cong \mathbb{Q}[x]$$

Dal momento che $\mathbb{Q}[x]$ è un dominio, ma non un campo, $(x - y)$ è un ideale primo non massimale di $\mathbb{Q}[x, y]$.

§2.6 Interi di Gauss

Consideriamo l'anello degli Interi di Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, abbiamo visto che $\mathbb{Z}[i]$ è un dominio euclideo e la sua funzione grado è

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N} : a + ib \longmapsto a^2 + b^2$$

che chiamiamo **norma**. Notiamo che questa norma è il quadrato dell'usuale norma complessa, pertanto è una funzione moltiplicativa.

§2.6.1 Elementi primi

Lemma 2.18
Il gruppo degli elementi invertibili di $\mathbb{Z}[i]$ è $\{1, -1, i, -i\}$.

Dimostrazione. Chiaramente $\{1, -1, i, -i\} \subseteq \mathbb{Z}[i]^*$, mostriamo quindi l'altra inclusione. Sia $a + ib \in \mathbb{Z}[i]^*$, allora esistono $c, d \in \mathbb{Z}$ tali che $(a + ib)(c + id) = 1$, passando alle norme otteniamo l'equazione

$$(a^2 + b^2)(c^2 + d^2) = 1$$

da cui ricaviamo $a^2 + b^2 = c^2 + d^2 = 1$, quindi $a + bi \in \{1, -1, i, -i\}$. □

Lemma 2.19
Dato $p \in \mathbb{Z}$ un primo, se $p \equiv 3 \pmod 4$ allora p è irriducibile in $\mathbb{Z}[i]$.

Dimostrazione. Supponiamo per assurdo che p non sia irriducibile in $\mathbb{Z}[i]$, scriviamo quindi la fattorizzazione

$$p = (a + ib)(c + id)$$

con entrambi i fattori non invertibili, passando alle norme otteniamo l'equazione

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

Poiché gli elementi invertibili di $\mathbb{Z}[i]$ coincidono con gli elementi di norma 1, abbiamo $a^2 + b^2 = c^2 + d^2 = p$. Quindi

$$a^2 + b^2 = p \equiv 3 \pmod 4$$

ma questo è assurdo in quanto gli unici quadrati in $\mathbb{Z}/4\mathbb{Z}$ sono 0 e 1. □

Lemma 2.20
Dato $a + ib \in \mathbb{Z}[i]$, se $N(a + ib)$ è primo in $\mathbb{Z}$ allora $a + ib$ è irriducibile in $\mathbb{Z}[i]$.

Dimostrazione. Fattorizziamo $a + ib$ come

$$a + ib = (c + id)(e + if)$$

passando alle norme otteniamo l'equazione

$$a^2 + b^2 = (c^2 + d^2)(e^2 + f^2)$$

Dato che $a^2 + b^2$ è primo in $\mathbb{Z}$ (quindi irriducibile in $\mathbb{Z}$) abbiamo che almeno uno dei due fattori ha norma 1, cioè è invertibile e quindi $a + ib$ è irriducibile in $\mathbb{Z}[i]$. □

Lemma 2.21

Valgono i seguenti fatti:

(1) $1+i$ è irriducibile in $\mathbb{Z}[i]$;

(2) $(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = (1-i)^2\mathbb{Z}[i]$;

(3) $\dfrac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{F}_2$;

Dimostrazione. Mostriamo i tre fatti separatamente:

(1) poiché $N(1+i) = 2$, per il Lemma 2.14 abbiamo che $1+i$ è irriducibile in $\mathbb{Z}[i]$;

(2) Notiamo che $2 = -i(1+i)^2 = i(1-i)^2$, pertanto

$$(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = (1-i)^2\mathbb{Z}[i]$$

(3) Consideriamo l'isomorfismo

$$\varphi : \mathbb{Z}[i] \longrightarrow \frac{\mathbb{Z}[x]}{(x^2+1)} : a+bi \longmapsto \overline{a+bx}$$

tramite φ abbiamo

$$\frac{\mathbb{Z}[i]}{(1+i)} \cong \frac{\mathbb{Z}[x]}{(x^2+1, 1+x)}$$

Notiamo che 2 è un elemento dell'ideale $(x^2+1, 1+x)$, in quanto possiamo scrivere

$$2 = x^2 + 1 - x(x+1) + x + 1$$

Pertanto

$$\frac{\mathbb{Z}[i]}{(i+1)} \cong \frac{\mathbb{Z}[x]}{(2, 1+x)} \cong \frac{\mathbb{Z}[x]\big/(2)}{(2,1+x)\big/(2)} \cong \frac{\mathbb{F}_2[x]}{(1+x)} \cong \mathbb{F}_2$$

$\square$

Lemma 2.22

Sia $p \in \mathbb{Z}$ un primo, se $p \equiv 1 \pmod 4$ allora $p = (a+bi)(a-bi)$ con $a+bi, a-bi \in \mathbb{Z}[i]$ primi e non associati.

Dimostrazione. Poiché $p \equiv 1 \pmod 4$ esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \pmod p$, da cui $p \mid x^2+1$. Fattorizziamo x^2+1 in $\mathbb{Z}[i]$ come

$$x^2 + 1 = (x+i)(x-i)$$

notiamo che $p \nmid x+i$ e $p \nmid x-i$, pertanto p non è primo in $\mathbb{Z}[i]$. In particolare possiamo scrivere

$$p = (a+bi)(c+di)$$

con $a+bi, c+di \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$. Passando alle norme abbiamo

$$p^2 = (a^2+b^2)(c^2+d^2)$$

da cui $a^2 + b^2 = c^2 + d^2 = p$ in quanto nessuno dei due fattori è invertibile. Abbiamo quindi

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

notiamo che $a + bi$ e $a - bi$ sono primi in $\mathbb{Z}[i]$ in quanto la loro norma è un primo di $\mathbb{Z}$. Supponiamo per assurdo che esista $u \in \mathbb{Z}[i]^*$ tale che $a + bi = u(a - bi)$, distinguiamo i vari casi:

- se $u = 1$ allora $a + bi = a - bi$, da cui $b = 0$ e quindi $p = a^2$, che è assurdo in quanto p è irriducibile in $\mathbb{Z}$;
- se $u = -1$ allora $a + bi = -a + bi$, da cui $a = 0$ e quindi $p = b^2$, che è assurdo in quanto p è irriducibile in $\mathbb{Z}$;
- se $u = i$ allora $a + bi = ai + b$, da cui $a = b$ e quindi $p = 2a^2$, che è assurdo in quanto p è dispari;
- se $u = -i$ allora $a + bi = -ai - b$, da cui $a = -b$ e quindi $p = 2a^2$, che è assurdo in quanto p è dispari.

Pertanto $a + bi$ e $a - bi$ sono primi di $\mathbb{Z}[i]$ non associati. □

Proposizione 2.23

Gli elementi primi di $\mathbb{Z}[i]$ sono, a meno di associati, tutti e soli gli elementi della forma

- $1 + i$;
- i primi p di $\mathbb{Z}$ tali che $p \equiv 3 \pmod 4$;
- $a + bi, a - bi \in \mathbb{Z}[i]$ tali che $a^2 + b^2 = p$ è un primo di $\mathbb{Z}$ con $p \equiv 1 \pmod 4$.

Dimostrazione. Per quanto visto nei lemmi precedenti sappiamo che gli elementi della forma descritta sopra sono tutti primi di $\mathbb{Z}[i]$, vediamo che effettivamente non ne esistono altri.
Sia $a + bi \in \mathbb{Z}[i]$ un primo, fattorizziamo in primi di $\mathbb{Z}$ la norma di $a + bi$

$$a^2 + b^2 = \prod_{j=1}^{k} p_j^{e_j}$$

Poiché $a + bi \mid a^2 + b^2$ in $\mathbb{Z}[i]$, poiché primo si ha che esiste $j_0 \in \{1, \dots, k\}$ tale che $a + bi \mid p_{j_0}$, distinguiamo tre casi:

- se $p_{j_0} \equiv 3 \pmod 4$ allora p_{j_0} è irriducibile in $\mathbb{Z}[i]$, pertanto $a + bi$ è associato a p_{j_0};
- se $p_{j_0} \equiv 1 \pmod 4$ allora si fattorizza in $\mathbb{Z}[i]$ come
$$p_{j_0} = (c + di)(c - di)$$
con $c + di, c - di$ primi, quindi irriducibili, di $\mathbb{Z}[i]$ non associati, pertanto $a + bi$ è associato a uno dei due;
- se $p_{j_0} = 2$ allora $a + bi \mid -i(1 + i)^2$. Poiché $a + bi$ non è invertibile si ha $a + bi \mid 1 + i$, cioè $a + bi$ è associato a $1 + i$.

□

§2.6.2 Quozienti di $\mathbb{Z}[i]$

Abbiamo visto che $\dfrac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{F}_2$, vogliamo determinare le classi di isomorfismo degli altri quozienti di $\mathbb{Z}[i]$ per ideali primi. Osserviamo che tali quozienti sono campi, infatti in un PID tutti gli ideali primi non nulli sono ideali massimali, pertanto il quoziente per un ideale primo produce un campo. In alternativa possiamo notare che tali quozienti sono dei domini finiti, quindi dei campi.

Proposizione 2.24

Sia $p \in \mathbb{Z}$ un primo dispari:

(1) se $p \equiv 3 \pmod 4$ allora $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$;

(2) se $p \equiv 1 \pmod 4$ e $p = (a+bi)(a-bi)$ è la sua fattorizzazione in primi di $\mathbb{Z}[i]$ allora $\dfrac{\mathbb{Z}[i]}{(a+bi)} \cong \mathbb{F}_p$.

Dimostrazione. Mostriamo i due fatti separatamente:

(1) possiamo identificare in modo univoco gli elementi di $\mathbb{Z}[i]/(p)$ con i resti della divisione per p, cioè con l'insieme

$$\{a + bi \mid 0 \leq a \leq p-1, 0 \leq b \leq p-1\}$$

che contiene p^2 elementi. Poiché il quoziente è un campo di cardinalità p^2 si ha

$$\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$$

(2) poiché p è un elemento dell'ideale $(a+bi)$, per il Secondo Teorema di Omomorfismo abbiamo

$$\frac{\mathbb{Z}[i]}{(a+bi)} \cong \frac{\mathbb{Z}[i]/(p)}{(a+bi)/(p)}$$

Consideriamo solo la struttura di gruppo additivo, il quoziente $\mathbb{Z}[i]/(p)$ è isomorfo, come gruppo, all'insieme dei resti

$$\{a + bi \mid 0 \leq a \leq p-1, 0 \leq b \leq p-1\}$$

che è isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Osserviamo che il quoziente $(a+bi)/(p)$ ha cardinalità 1, p, oppure p^2 in quanto, come gruppo, è isomorfo a un sottogruppo di $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Questa non può essere 1 in quanto altrimenti si avrebbe l'identità

$$(a+bi) = ((a+bi)(a-bi))$$

che non è vera in quanto $a+bi$ e $a-bi$ non sono associati. D'altra parte se fosse p^2 allora avremmo

$$\frac{\mathbb{Z}[i]/(p)}{(a+bi)/(p)} = \{\overline{0}\}$$

che sarebbe assurdo in quanto $a+bi$ non è invertibile. Pertanto abbiamo l'isomorfismo di gruppi

$$\frac{\mathbb{Z}[i]}{(a+bi)} \cong \frac{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z}$$

Pertanto il quoziente è un anello di cardinalità p, da cui necessariamente

$$\frac{\mathbb{Z}[i]}{(a+bi)} \cong \mathbb{F}_p$$

□

Osservazione 2.25 — Se $p \equiv 1 \pmod 4$, gli anelli $\mathbb{Z}[i]/(p)$ e $\mathbb{F}_p \times \mathbb{F}_p$ sono isomorfi tramite un isomorfismo diverso da quello visto nella dimostrazione. Fattorizziamo in primi $p = (a+bi)(a-bi)$, poiché $\mathbb{Z}[i]$ è un PID gli ideali $(a+bi), (a-bi)$ sono massimali, quindi $(a+bi)+(a-bi) = \mathbb{Z}[i]$. Per il Teorema Cinese del Resto allora

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[i]}{(a+bi)(a-bi)} \cong \frac{\mathbb{Z}[i]}{(a+bi)} \times \frac{\mathbb{Z}[i]}{(a-bi)} \cong \mathbb{F}_p \times \mathbb{F}_p$$

Osservazione 2.26 — Abbiamo mostrato anche che la cardinalità del quoziente $\mathbb{Z}[i]/(\alpha)$ con α un primo di $\mathbb{Z}[i]$ è uguale a $N(\alpha)$.

Lemma 2.27
Siano A un PID e $I \subseteq A$ un ideale. Se il quoziente A/I è finito allora vale

$$\left|A/I^n\right| = \left|A/I\right|^n \text{ [a]}$$

[a] Con I^n intendiamo il prodotto dell'ideale I con se stesso ripetuto n volte.

Dimostrazione. Sia $I = (p)$, mostriamo la tesi per induzione su n. Consideriamo l'omomorfismo di anelli

$$\varphi : A \longrightarrow A : a \longmapsto ap$$

e la proiezione al quoziente

$$\pi : A \longrightarrow A/I^2 : a \longmapsto a + I^2$$

Il nucleo della loro composizione è

$$\ker \pi \circ \varphi = \{a \in A \mid pa \in I^2 = (p^2)\} = \{a \in A \mid a = pb, b \in A\} = I$$

e l'immagine è

$$\pi(\varphi(A)) = \pi(pA) = \pi(I) = I/I^2$$

Per il Primo Teorema di Omomorfismo allora

$$A/I \cong I/I^2$$

pertanto

$$A/I \cong \frac{A/I^2}{I/I^2}$$

da cui ricaviamo

$$\left|A/I\right| = \left|\frac{A/I^2}{I/I^2}\right| = \left|\frac{A/I^2}{A/I}\right| = \frac{\left|A/I^2\right|}{\left|A/I\right|}$$

Quindi abbiamo la tesi per $n = 2$:

$$\left|A/I^2\right| = \left|A/I\right|^2$$

Per $n > 2$, supponiamo che la tesi sia valida per $n-1$. Consideriamo gli omomorfismi

$$\varphi : A \longrightarrow A : a \longmapsto p^{n-1}a$$

$$\pi : A \longrightarrow A/I^n : a \longmapsto a + I^n$$

Il nucleo e l'immagine della loro composizione sono

$$\ker \pi \circ \varphi = \{a \in A \mid p^{n-1}a \in I^n = (p^n)\} = I$$

$$\pi(\varphi(A)) = \pi(p^{n-1}A) = \pi(I^{n-1}) = I^{n-1}/I^n$$

Pertanto abbiamo l'isomorfismo

$$A/I \cong I^{n-1}/I^n$$

da cui, come sopra,

$$\left|A/I\right| = \frac{\left|A/I^n\right|}{\left|A/I^{n-1}\right|} = \frac{\left|A/I^n\right|}{\left|A/I\right|^{n-1}}$$

Da cui la tesi. $\square$

Consideriamo adesso il quoziente di $\mathbb{Z}[i]$ per un generico ideale $I = (z)$, fattorizziamo z in primi di $\mathbb{Z}[i]$:

$$z = u(1+i)^e \prod_{j=1}^{r} (a_j + b_j i)^{e_j} \prod_{h=1}^{s} p_h^{l_h} \qquad u \in \mathbb{Z}[i]^*$$

Gli ideali $(1+i)^e, (a_j + b_j i)^{e_j}, (p^{e_h})$ sono generati da elementi a due a due coprimi, quindi per il Teorema Cinese del Resto

$$\mathbb{Z}[i]/I \cong \frac{\mathbb{Z}[i]}{(1+i)^e} \times \prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j + b_j i)^{e_j}} \times \prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)^{l_h}}$$

La cardinalità di questo quoziente è $N(z)$, infatti applicando il Lemma 2.21 abbiamo

$$\begin{aligned}
\left|{}^{\mathbb{Z}[i]}\!\big/_{I}\right| &= \left|\frac{\mathbb{Z}[i]}{(1+i)^e}\right| \cdot \left|\prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j+b_ji)^{e_j}}\right| \cdot \left|\prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)^{e_h}}\right| = \\
&= \left|\frac{\mathbb{Z}[i]}{(1+i)}\right|^e \cdot \left|\prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j+b_ji)}\right|^{e_j} \cdot \left|\prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)}\right|^{e_h} = \\
&= N(1+i)^e \prod_{j=1}^{r} N(a_j+b_ji)^{e_j} \prod_{h=1}^{s} N(p_h)^{e_h} = \\
&= N\left(u(1+i)^e \prod_{j=1}^{r} (a_j+b_ji)^{e_j} \prod_{h=1}^{s} p_h^{e_h}\right) = N(z)
\end{aligned}$$

§2.7 Un esempio di dominio non euclideo: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

Consideriamo l'elemento $\alpha = \frac{1+\sqrt{-19}}{2} \in \mathbb{C}$. Dimostreremo in questa sezione che $\mathbb{Z}[\alpha]$ non è un dominio euclideo[27], ovverosia che non esiste alcuna norma rispetto cui esiste una divisione euclidea per $\mathbb{Z}[\alpha]$.

Benché il valore α sembri del tutto casuale, vi sono due principali ragioni per cui è stato scelto:

1. Come mostreremo a breve, il polinomio minimo di α su $\mathbb{Q}$ è a coefficienti in $\mathbb{Z}$ ed è primitivo; pertanto si possono descrivere in modo semplici gli elementi di $\mathbb{Z}[\alpha]$ attraverso l'usuale omomorfismo di valutazioni;

2. Esiste una "seminorma" N per $\mathbb{Z}[\alpha]$, indotta dall'usuale norma complessa, e grazie a N possiamo classificare agevolmente gli invertibili di $\mathbb{Z}[\alpha]$.

Combinando questi due risultati dimostreremo poi che $\mathbb{Z}[\alpha]$ non è euclideo.

Osservazione 2.28 (Polinomio minimo di α su $\mathbb{Q}$) — Si ponga $x = \alpha = \frac{1+\sqrt{-19}}{2}$. Allora vale che:

$$2x - 1 = \sqrt{-19} \implies 4x^2 + 1 - 4x = -19 \implies x^2 - x + 5 = 0$$

Poiché α non è reale, allora $x^2 - x + 5$ è necessariamente irriducibile ed è dunque il polinomio minimo[a] di α su $\mathbb{Q}$, che denoteremo come $\mu(x)$.

[a]Utilizzando la teoria di Galois si deduce immediatamente che il polinomio minimo di α è $(x-\alpha)(x-\overline{\alpha}) = x^2 - x + 5$, dal momento che $\mathbb{Q}(\alpha) = \mathbb{Q}(i)$, la cui unica $\mathbb{Q}$-immersione è il coniugio complesso.

Come osservato precedentemente, $\mu(x)$ è a coefficienti interi ed è anche primitivo. A partire da questo risultato si dimostra il:

Lemma 2.29

$$\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$$

Dimostrazione. Si consideri l'omomorfismo di valutazione ϕ di $\mathbb{Q}[x]$ rispetto ad α. Poiché $\mu(x)$ è il polinomio minimo di α su $\mathbb{Q}$, allora $\ker\phi = \mu(x)\mathbb{Q}[x]$.

Si consideri la restrizione ψ di ϕ su $\mathbb{Z}[x]$. Chiaramente $\operatorname{im}\psi$ coincide con $\mathbb{Z}[\alpha]$. Inoltre, $\mu(x)\mathbb{Z}[x] \subseteq \ker\psi$. Se $p(x) \in \ker\psi$, allora $p(x)$ appartiene in particolare a $\ker\phi = \mu(x)\mathbb{Q}[x]$, ed è dunque multiplo di $\mu(x)$ in $\mathbb{Q}[x]$. Allora, per il Lemma di Gauss, $p(x)$ è multiplo di $\mu(x)$ anche in $\mathbb{Z}[x]$, e dunque $p(x) \in \mu(x)\mathbb{Z}[x]$. Pertanto $\ker\psi = \mu(x)\mathbb{Z}[x]$.

Si conclude dunque per il Primo Teorema di Omomorfismo che:

$$\frac{\mathbb{Z}[x]}{\mu(x)\mathbb{Z}[x]} \cong \mathbb{Z}[\alpha]$$

[27]Questo esempio è notevole: $\mathbb{Z}[\alpha]$ è infatti un PID che non è un dominio euclideo.

e dunque che 1 e $\frac{1+\sqrt{-19}}{2}$ formano dunque un insieme di generatori[28] per $\mathbb{Z}[\alpha]$, dal momento che 1 e x lo sono per $\frac{\mathbb{Z}[x]}{\mu(x)\mathbb{Z}[x]}$. $\square$

Osservazione 2.30 — Il risultato appena visto non vale se si sostituisce ad α un generico elemento che in $\mathbb{Q}$ ha come polinomio minimo un polinomio non a coefficienti interi. Se consideriamo per esempio $\beta = \frac{1+\sqrt{3}}{2}$, il suo polinomio minimo su $\mathbb{Q}$ è $x^2 - x - \frac{1}{2}$, che genera lo stesso nucleo di $2x^2 - 2x - 1$. In tal caso il nucleo della valutazione su $\mathbb{Z}[x]$ rispetto ad α è ancora $(2x^2 - 2x - 1)\mathbb{Z}[x]$, ma $\mathbb{Z}[x]/(2x^2 - 2x - 1)\mathbb{Z}[x]$ non è finitamente generato, dacché $2x^2 - 2x - 1$ non ha un coefficiente di testa invertibile.

Lemma 2.31

Gli unici invertibili di $\mathbb{Z}[\alpha]$ sono 1 e -1.

Dimostrazione. Consideriamo la mappa $N : \mathbb{Z}[\alpha] \to \mathbb{N}$ tale per cui $N(a + b\alpha) = |a + b\alpha|^2 = a^2 + 5b^2 + ab$, ossia l'usuale norma quadrata complessa[29]. Si osserva immediatamente che N è moltiplicativa, infatti vale che:

$$N((a + b\alpha)(c + d\alpha)) = |(a + b\alpha)(c + d\alpha)|^2 = |a + b\alpha|^2 \, |c + d\alpha|^2 = N(a + b\alpha)N(c + d\alpha)$$

Pertanto, se u è invertibile in A^*, e dunque esiste $v \in A$ tale per cui $uv = 1$, vale che:

$$N(u)N(v) = N(uv) = N(1) = 1$$

e dunque $N(u)$ è necessariamente 1. D'altronde vale che:

$$N(a + b\alpha) = 1 \iff \left(a + \frac{b}{2}\right)^2 + \left(\frac{19}{2}b\right)^2 = a^2 + 5b^2 + ab = 1$$

e dunque $a + b\alpha$ può essere invertibile solo se $a = \pm 1$ e $b = 0$, le uniche soluzioni dell'equazione appena descritta. Chiaramente sia 1 che -1 sono invertibili, e sono dunque tutti e soli gli invertibili di $\mathbb{Z}[\alpha]$. $\square$

Proposizione 2.32

$\mathbb{Z}[\alpha]$ non è un dominio euclideo.

Dimostrazione. Supponiamo per assurdo che $\mathbb{Z}[\alpha]$ sia un dominio euclideo, e sia $d : \mathbb{Z}[\alpha] \to \mathbb{N}$ la sua norma. Si consideri allora l'insieme:

$$X = \{d(x) \mid x \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}[\alpha]^*\}$$

Dal momento che $X \subseteq \mathbb{N}$, per il Principio del Minimo X ammette un minimo, e dunque un $t \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}[\alpha]^*$ tale per cui $d(t)$ è minimo.

[28] Si ricorda che $\mathbb{Z}[x]/\mu(x)\mathbb{Z}[x]$ non è uno spazio vettoriale. Ciononostante il concetto di generatori è ancora ben definito (e in realtà ben approfondito, dal momento che si stanno studiando dei cosiddetti $\mathbb{Z}$-moduli).

[29] La ben definitezza della mappa proviene dal fatto che ogni elemento di $\mathbb{Z}[\alpha]$, per il Lemma 2.29, si scrive proprio come $a + b\alpha$ per $a, b \in \mathbb{Z}$.

Dal momento che si è supposto che $\mathbb{Z}[\alpha]$ è euclideo, per ogni $a \in \mathbb{Z}[\alpha]$ esistono p, $q \in \mathbb{Z}[\alpha]$ tali per cui $a = pt + q$ con $q = 0$ o $d(q) < d(t)$, se $q \neq 0$. Se $q \neq 0$, allora $d(q)$ è strettamente minore di $d(t)$ e dunque, per ipotesi di minimalità, q deve appartenere a $\mathbb{Z}[\alpha]^*$, che è uguale a $\{\pm 1\}$ per il Lemma 2.31. Pertanto $q \in \{-1, 0, 1\}$.

Anche se 1 e -1 fosse equivalenti modulo t, $\mathbb{Z}[\alpha]/(t)$ avrebbe comunque al più 3 rappresentanti, e quindi sarebbe isomorfo come anello a $\mathbb{Z}/2\mathbb{Z}$ o a $\mathbb{Z}/3\mathbb{Z}$. Dal momento che $\mu(x) = x^2 - x + 5$ ha α e $\overline{\alpha}$ come soluzioni in $\mathbb{Z}[\alpha]$, allora $\mu(x)$ è riducibile in almeno uno tra $\mathbb{Z}_2[x]$ e $\mathbb{Z}_3[x]$. Tuttavia questo è assurdo, dal momento che $x^2 - x + 5$ è irriducibile sia in $\mathbb{Z}_2[x]$ che in $\mathbb{Z}_3[x]$, e dunque $\mathbb{Z}[\alpha]$ non è un dominio euclideo. □

§3 Campi

§3.1 Estensioni normali

Ricordiamo che un'estensione di campi algebrica ${}^{L}\!/_{K}$ si dice **normale** se per ogni immersione $\varphi : L \hookrightarrow \overline{K}$ tale che $\varphi_{|K} = id_K$ vale $\varphi(L) = L$. Diciamo che l'estensione è **separabile** se il polinomio minimo su K di ogni elemento di K ha radici distinte nel suo campo di spezzamento. Diciamo anche che un polinomio è separabile su K se le sue radici in $\overline{K}$ sono tutte distinte. Chiamiamo **estensione di Galois finita** un'estensione di campi finita che sia normale e separabile. I campi che considereremo saranno sempre **campi perfetti**, cioè tutte le estensioni saranno separabili.

Esempio 3.1

${}^{\mathbb{Q}(\sqrt[3]{2})}\!/_{\mathbb{Q}}$ non è un'estensione normale di $\mathbb{Q}$. Infatti, poiché il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $\mu(x) = x^3 - 2$, esistono 3 immersioni $\varphi_i : \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \overline{\mathbb{Q}}$ tali che $\varphi_{i|K} = id_K$, $i \in \{0, 1, 2\}$. Poiché il campo $\mathbb{Q}$ è fissato da φ_i, è sufficiente studiare l'immagine delle radici di $\mu(x)$ tramite le immersioni: le possibili immagini di $\sqrt[3]{2}$ sono $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$. Poiché i tre campi $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\zeta_3), \mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$ sono diversi, l'estensione non è normale.

Esempio 3.2

${}^{\mathbb{Q}(\sqrt{2})}\!/_{\mathbb{Q}}$ è un'estensione normale di $\mathbb{Q}$. Infatti, poiché il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è $x^2 - 2$, abbiamo due immersioni $\varphi_1, \varphi_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ che fissano $\mathbb{Q}$ tali che $\varphi_1(\sqrt{2}) = \sqrt{2}$, $\varphi_2(\sqrt{2}) = -\sqrt{2}$. Pertanto le immagini di $\mathbb{Q}(\sqrt{2})$ tramite le immersioni sono

$$\varphi_1(\mathbb{Q}(\sqrt{2})) = \{\varphi_1(a + b\sqrt{2}) \mid a, b \in \mathbb{Q}\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
$$\varphi_2(\mathbb{Q}(\sqrt{2})) = \{\varphi_2(a + b\sqrt{2}) \mid a, b \in \mathbb{Q}\} = \{a - b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

che sono uguali, quindi l'estensione è normale.

Se un'estensione ${}^{L}\!/_{K}$ è normale possiamo definire il **Gruppo di Galois** di ${}^{L}\!/_{K}$ come il gruppo delle immersioni $\varphi : L \hookrightarrow \overline{K}$ che fissano K. Questo coincide con il gruppo degli automorfismi di L che fissano K, e il suo ordine è pari al grado dell'estensione.

Osservazione 3.3 — Un'estensione quadratica è sempre un'estensione normale. Infatti se K è un campo (perfetto) e $\alpha \in \overline{K}$ è tale che $\sqrt{\alpha} \notin K$, allora $K(\alpha)$ è il campo di spezzamento del polinomio $x^2 - \alpha$. Quindi ${}^{K(\alpha)}\!/_{K}$ è normale e $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}/2\mathbb{Z}$.

Diamo qualche esempio di calcolo del gruppo di Galois di un'estensione.

Esempio 3.4

Sia $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ verifichiamo che ${}^{L}\!/_{\mathbb{Q}}$ è un'estensione normale e calcoliamo $\mathrm{Gal}(L/\mathbb{Q})$. ${}^{L}\!/_{\mathbb{Q}}$ è un'estensione normale in quanto L è il campo di spezzamento del polinomio $(x^2-2)(x^2-3)$ su $\mathbb{Q}$, pertanto è ben definito il gruppo di Galois dell'estensione, che ha ordine 4 in quanto $[L : \mathbb{Q}] = 4$. Siano $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ una $\mathbb{Q}$-base di L come spazio vettoriale e $\varphi \in \mathrm{Gal}(L/\mathbb{Q})$, poiché φ è in particolare un'applicazione lineare è sufficiente determinare la sua immagine sulla base. Abbiamo quindi

$$\varphi(\sqrt{2}) = \pm\sqrt{2}$$
$$\varphi(\sqrt{3}) = \pm\sqrt{3}$$
$$\varphi(\sqrt{6}) = \varphi(\sqrt{2})\varphi(\sqrt{3})$$

in particolare abbiamo al più 4 omomorfismi. D'altra parte $\mathrm{Gal}(L/\mathbb{Q})$ contiene esattamente 4 elementi, quindi questi sono tutti e soli gli automorfismi del campo L che fissano $\mathbb{Q}$. Si verifica che questi omomorfismi, ad eccezione dell'identità, hanno ordine 2, pertanto $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Esempio 3.5

Sia $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ il campo di spezzamento del polinomio $x^3 - 2$ su $\mathbb{Q}$, ${}^{L}\!/_{\mathbb{Q}}$ è un'estensione normale di $\mathbb{Q}$ e $[L : \mathbb{Q}] = 6$. Esplicitando le radici del polinomio x^3-2, abbiamo $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2)$. Sappiamo dalla teoria che $\mathrm{Gal}(L/\mathbb{Q})$ si immerge in $\mathcal{S}_3$, poiché sono entrambi gruppi finiti della stessa cardinalità si ha quindi $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathcal{S}_3$.

Definizione 3.6. Dato p un numero primo, l'applicazione

$$\Phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n} : x \longmapsto x^p$$

si dice **automorfismo di Frobenius**

L'automorfismo di Frobenius è effettivamente un automorfismo, poiché $\mathbb{F}_{p^n}$ è un campo finito è sufficiente mostrare che è un omomorfismo iniettivo:

- per ogni $x, y \in \mathbb{F}_{p^n}$
$$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$$
$$\Phi(x+y) = (x+y)^p \overset{[30]}{=} x^p + y^p = \Phi(x) + \Phi(y)$$
pertanto Φ è un omomorfismo:
- sia $x \in \ker \Phi$, allora
$$\Phi(x) = x^p = 0 \iff x = 0$$
in quanto il polinomio t^p ha 0 come unica radice in $\mathbb{F}_{p^n}$, pertanto Φ è iniettivo.

Teorema 3.7

Per ogni primo p, l'estensione ${}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p}$ è normale e $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

[30] Per il Lemma del Binomio Ingenuo.

Dimostrazione. L'estensione ${}^{\mathbb{F}_{p^n}}\!/\!{}_{\mathbb{F}_p}$ è normale in quanto $\mathbb{F}_{p^n}$ è, per costruzione, il campo di spezzamento del polinomio $t^{p^n} - t$ su $\mathbb{F}_p$, e il grado di tale estensione è n. Osserviamo che l'automorfismo di Frobenius Φ è un elemento di $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, infatti per ogni $x \in \mathbb{F}_p$ vale $\Phi(x) = x^p = x$ per il Piccolo Teorema di Fermat. L'ordine di Φ è n, infatti

$$\Phi^k = id_{\mathbb{F}_{p^n}} \iff x^{p^k} = x \ \forall x \in \mathbb{F}_{p^n}$$

e l'equazione è verificata se e solo se il polinomio $t^{p^k} - t$ ha almeno p^n radici, cioè se $k \geq n$. D'altra parte l'ordine di Φ deve dividere n, pertanto $\operatorname{ord}\Phi = n$. Quindi Φ è un generatore di $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, che è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. □

§3.2 Estensioni ciclotomiche

Lemma 3.8

Dato K un campo, il polinomio $x^n - 1$ è separabile su K se e solo se $\operatorname{char} K \nmid n$.

Dimostrazione. Per il Criterio della Derivata il polinomio $x^n - 1$ ha radici multiple in $\overline{K}$ se e solo se $(x^n - 1, nx^{n-1}) \neq 1$. Se $\operatorname{char} K = 0$ allora $\mathbb{Q} \subseteq K$ e le radici di $x^n - 1$ sono le n radici complesse dell'unità, che sono tutte distinte. Se $\operatorname{char} K = p$, p primo, allora $(x^n - 1, nx^{n-1}) \neq 1$ se e solo se $p \mid n$, in quanto in quel caso si ha $nx^{n-1} = 0$. □

Teorema 3.9

Sia $\zeta_n \in \mathbb{C}$ una radice primitiva n-esima dell'unità, allora l'estensione ${}^{\mathbb{Q}(\zeta_n)}\!/\!{}_{\mathbb{Q}}$ è normale e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$.

Dimostrazione. Poiché ζ_n è una radice primitiva dell'unità, l'insieme delle sue potenze coincide con l'insieme delle radici del polinomio $x^n - 1$[31], pertanto ${}^{\mathbb{Q}(\zeta_n)}\!/\!{}_{\mathbb{Q}}$ è normale in quanto $\mathbb{Q}(\zeta_n)$ è il campo di spezzamento di $x^n - 1$ su $\mathbb{Q}$. Per comodità suddividiamo la dimostrazione in passi:

- mostriamo che $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$. Un'immersione $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ è univocamente determinata dall'immagine di ζ_n, inoltre $\psi(\zeta_n)$ è un elemento dell'insieme $\{\zeta_n^k \mid k = 0, \ldots, n-1\}$ in quanto è radice di $x^n - 1$. Supponiamo per assurdo che $\psi(\zeta_n) = \zeta_n^k$ con $d = (k, n) \neq 1$, allora

$$\psi(\zeta_n^{\frac{n}{d}}) = \psi(\zeta_n)^{\frac{n}{d}} = \zeta^{k\frac{n}{d}} = \zeta^{\frac{k}{d}n} = 1$$

  da cui $\zeta_n^{\frac{n}{d}} = 1$ in quanto ψ è iniettiva, quindi ha nucleo banale. Questo è assurdo dato che $\operatorname{ord}\zeta_n = n$. Pertanto $\psi(\zeta_n) \in \{\zeta_n^k \mid k < n, \ (n,k) = 1\}$, quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$;

- siano p un primo che non divide n, $f(x)$ e $g(x)$ i polinomi minimi su $\mathbb{Q}$ rispettivamente di ζ_n e ζ_n^p, osserviamo che $f(x) \mid g(x^p)$ in quanto $g(\zeta_n^p) = 0$;

[31] Ricordiamo che l'insieme delle radici complesse di $x^n - 1$ è un gruppo isomorfo a $\mathbb{Z}/n\mathbb{Z}$, i cui generatori sono le radici primitive.

- supponiamo per assurdo $f(x) \neq g(x)$, allora $f(x)$ e $g(x)$ sono coprimi in $\mathbb{Q}[x]$ ed entrambi dividono $x^n - 1$, pertanto $f(x)g(x) \mid x^n - 1$. Per il Lemma di Gauss esistono $q(x), r(x) \in \mathbb{Z}[x]$ tali che

  $$f(x)g(x)q(x) = x^n - 1 \qquad f(x)r(x) = g(x^p)$$

  Riducendo modulo p abbiamo

  $$g(x)^p = g(x^p) = f(x)r(x)$$

  in $\mathbb{F}_p[x]$. Pertanto se $\alpha \in \overline{\mathbb{F}_p}$ è una radice di $f(x)$ allora è anche una radice di $g(x)$. Pertanto α è una radice almeno doppia di $x^n - 1 \in \mathbb{F}_p[x]$, che è assurdo in quanto $x^n - 1$ è separabile su $\mathbb{F}_p$ per il Lemma 3.8. Pertanto $f(x) = g(x)$;

- abbiamo quindi che ζ_n e ζ_n^p hanno lo stesso polinomio minimo su $\mathbb{Q}$. Ripetendo lo stesso ragionamento con qualsiasi altro primo q che non divide n otteniamo che ζ_n e ζ_n^q hanno lo stesso polinomio minimo su $\mathbb{Q}$, quindi questo è valido in generale per ζ_n e ζ_n^k con $(n, k) = 1$. In particolare ζ_n^k è radice di $f(x)$ per ogni $k < n$ con $(n, k) = 1$, pertanto $\deg f \geq \phi(n)$;

- poiché $\deg f = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$ abbiamo che effettivamente $\deg f = \phi(n)$, quindi $\# \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n)$. Gli elementi di $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sono tutti e soli della forma

  $$\psi_k : \mathbb{Q}(\zeta_n) \longrightarrow \overline{\mathbb{Q}} : \zeta_n \longmapsto \zeta_n^k$$

  con $k < n$ e $(n, k) = 1$, inoltre $\psi_k \circ \psi_h = \psi_{kh} = \psi_{hk}$ in quanto

  $$\psi_k(\psi_h(\zeta_n)) = \psi_k(\zeta_n^h) = \psi_k(\zeta_n)^h = \zeta_n^{hk} = \zeta_n^{kh} = \psi_h(\zeta_n^k) = \psi_h(\psi_k(\zeta_n))$$

  abbiamo quindi un isomorfismo

  $$\Psi : \mathbb{Z}/n\mathbb{Z}^* \longmapsto \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : k \longmapsto \psi_k$$

$\square$

Definizione 3.10 (Polinomio ciclotomico)**.** Data $\zeta_n \in \mathbb{C}$ una radice primitiva n-esima dell'unità, chiamiamo ***n*-esimo polinomio ciclotomico** il polinomio minimo $\Phi_n(x)$ di ζ_n su $\mathbb{Q}$.

Osservazione 3.11 — Poiché gli elementi di $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sono

$$\psi_k : \mathbb{Q}(\zeta_n) \longrightarrow \overline{\mathbb{Q}} : \zeta_n \longmapsto \zeta_n^k$$

per $0 \leq k \leq n$, $(k, n) = 1$, possiamo scrivere $\Phi_n(x)$ come

$$\Phi_n(x) = \prod_{\substack{0 \leq k \leq n \\ (k,n)=1}} (x - \zeta_n^k)$$

Notiamo che le radici di $\Phi_n(x)$ sono tutte e sole le radici primitive n-esime dell'unità e che $\deg \Phi_n = \phi(n)$.

Proposizione 3.12

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Dimostrazione. Sia $f(x) = \prod_{d|n} \Phi_d(x)$, notiamo che:

- sia α una radice di $x^n - 1$, allora esiste un intero d che divide n tale che $\alpha^d = 1$, pertanto α è una radice primitiva d-esima. In particolare ogni radice di $x^n - 1$ è una radice di $f(x)$, cioè $x^n - 1 \mid f(x)$;
- sia α una radice di $f(x)$, allora α è una radice primitiva d-esima dell'unità con $d \mid n$, in particolare$\alpha^d = 1$ e quinci $\alpha^n = 1$. Allora α è una radice n-esima dell'unità, cioè $f(x) \mid x^n - 1$;
- dai due punti precedenti si deduce che esiste $\lambda \in \mathbb{Q}^*$ tale che $x^n - 1 = \lambda f(x)$, d'altra parte entrambi i polinomi sono monici, quindi $x^n - 1 = f(x)$.

□

§3.3 Gruppi di Galois in uno stesso diagramma a confronto

In questa sezione si mettono in correlazione i gruppi di Galois del traslato e del composto di un diagramma di campi.

Proposizione 3.13
Siano K/F un'estensione di Galois finita e L/F un'estensione finita. Allora vale che:

(1) KL/L è un'estensione di Galois finita,

(2) $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$.

Dimostrazione. Consideriamo il seguente diagramma di campi:

$$\begin{tikzcd}
 & KL \arrow[dl, no head] \arrow[dr, no head] \arrow[dd, no head] & \\
K \arrow[dr, no head] \arrow[ddr, no head] & & L \arrow[dl, no head] \arrow[ddl, no head] \\
 & K \cap L \arrow[d, no head] & \\
 & F &
\end{tikzcd}$$

Dal momento che K/F è un'estensione finita, anche KL/L lo è. Inoltre, poiché sia K/F che L/F sono normali, allora anche KL/L lo è, e dunque è di Galois.

Consideriamo la seguente mappa di restrizione:

$$\Phi : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/K \cap L), \; \varphi \mapsto \varphi\big|_K$$

Tale mappa è ben definita, dal momento che $\varphi\big|_K$ è una mappa che fissa L e dunque anche $K \cap L$. Inoltre Φ è chiaramente un omomorfismo di gruppi.

Mostriamo che Φ è iniettiva. Sia $\varphi \in \ker \Phi$, allora $\varphi\big|_K = \mathrm{id}_K$. Poiché allora φ fissa anche L per ipotesi, $\varphi = \mathrm{id}_{KL}$, e dunque il nucleo di Φ è banale. Pertanto Φ è iniettiva.

Consideriamo adesso $H = \operatorname{im} \Phi$. Il sottocampo di K fissato da H è K^H, ovverosia:

$$K^H = \{x \in K \mid \psi(x) = x \; \forall \, \psi \in H\}$$

Dal momento che H è formato da tutte le restrizioni a K degli elementi di $\mathrm{Gal}(KL/L)$, ciò è equivalente ad esprimere K^H come:

$$K^H = \{x \in K \mid \varphi(x) = x \; \forall \varphi \in \mathrm{Gal}(KL/L)\} = K \cap (KL)^{\mathrm{Gal}(KL/L)} = K \cap L$$

Pertanto, per il Teorema di Corrispondenza di Galois, vale che $H = \mathrm{Gal}(K/K^H) = \mathrm{Gal}(K/K \cap L)$, e dunque Φ è surgettiva. Si conclude che Φ è un isomorfismo, da cui la tesi. $\square$

Corollario 3.14
Siano K/F un'estensione di Galois finita e L/F un'estensione finita. Se $K \cap L = F$, allora $[KL : F] = [K : F][L : F]$.

Dimostrazione. Per la Proposizione 3.13 vale che $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L) = \mathrm{Gal}(K/F)$, e dunque che $[KL : L] = [K : F]$. Pertanto, per il Teorema delle Torri algebriche vale che:

$$[KL : F] = [KL : L][L : F] = [K : F][L : F]$$

da cui la tesi. □

Proposizione 3.15

Siano K_1/F, K_2/F due estensioni di Galois finite. Allora vale che:

(1) K_1K_2/F è un'estensione di Galois,

(2) esiste un'immersione $\Phi : \mathrm{Gal}(K_1K_2/F) \hookrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$,

(3) $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ se e solo se $K_1 \cap K_2 = F$.

Dimostrazione. Si dimostrano i tre risultati separatamente.

(1) Dal momento che K_1/F è un'estensione finita, anche K_1K_2/K_2 lo è. Poiché allora sia K_1K_2/K_2 che K_2/F sono estensioni finite, per il Teorema delle Torri algebriche, K_1K_2/F è un'estensione finita. Dacché sia K_1/F che K_2/F sono normali, anche K_1K_2/F lo è, ed è dunque di Galois.

(2) Consideriamo la mappa:

$$\Phi : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F),\ \varphi \mapsto \left(\varphi|_{K_1}, \varphi|_{K_2}\right)$$

Chiaramente Φ è un omomorfismo di gruppi ed è ben definito dal momento che φ fissa F.

Sia $\varphi \in \ker \Phi$. Allora φ agisce come identità sia su K_1 che su K_2. Pertanto φ agisce come identità anche su $K_1K_2 = K_1(K_2)$, e dunque $\varphi = \mathrm{id}_{K_1K_2}$. Si conclude dunque che φ è iniettiva e che dunque è un'immersione.

(3) Dal momento che tutti i gruppi in questione sono finiti e che per il punto (2) esiste un'immersione di uno nel prodotto degli altri, l'isomorfismo sussiste se e solo se questi due gruppi hanno la stessa cardinalità, ossia se e solo se:

$$[K_1K_2 : F] = [K_1 : F][K_2 : F]$$

Per il Proposizione 3.13, $[K_1K_2 : F] = [K_1K_2 : K_2][K_2 : F] = [K_1 : K_1 \cap K_2][K_2 : F]$. Pertanto l'isomorfismo sussiste se e solo se:

$$[K_1 : K_1 \cap K_2] = [K_1 : F]$$

Dal momento che $F \subseteq K_1 \cap K_2$, ciò accade se e solo se $K_1 \cap K_2 = F$, da cui la tesi.

□

§3.4 Gruppo di Galois di un polinomio di grado 3

Consideriamo un polinomio $f(x)$ di grado 3 che non sia completamente fattorizzabile in $\mathbb{Q}[x]$, cioè che ha campo di spezzamento K su $\mathbb{Q}$ diverso da $\mathbb{Q}$. Dalla teoria sappiamo che 3 divide l'ordine di $\mathrm{Gal}(K/\mathbb{Q})$ e che questo è isomorfo a un sottogruppo di $\mathcal{S}_3$, pertanto $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_3$ oppure $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Vediamo che entrambi i casi sono possibili con due esempi.
Consideriamo il polinomio $f(x) = x^3 - 2$, le sue radici in $\overline{\mathbb{Q}}$ sono $\alpha_0 = \sqrt[3]{2}$, $\alpha_1 = \sqrt[3]{2}\zeta_3$, $\alpha_2 = \sqrt[3]{2}\zeta_3^2$, dove ζ_3 è una radice primitiva terza di 1. In particolare, il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Infatti $\sqrt[3]{2} = \alpha_0$ e $\zeta_3 = \frac{\alpha_1}{\alpha_0}$, quindi $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \subseteq \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$, d'altra parte $\alpha_i = \sqrt[3]{(2)}\zeta_3^i$ per $i = 0, 1, 2$, pertanto si ha anche l'altra inclusione, da cui l'uguaglianza. Consideriamo il diagramma di campi

$$
\begin{tikzcd}
 & K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[dl, no head] \arrow[dd, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, no head] & & \mathbb{Q}(\zeta_3) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

l'estensione ${}^{\mathbb{Q}(\sqrt[3]{2})}\!\big/_{\mathbb{Q}}$ ha grado 3 in quanto il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$, mentre l'estensione ${}^{\mathbb{Q}(\zeta_3)}\!\big/_{\mathbb{Q}}$ ha grado 2 in quanto il polinomio minimo di ζ_3 su $\mathbb{Q}$ è $x^2 + x + 1$. Dato che i gradi sono coprimi, l'estensione ${}^{K}\!\big/_{\mathbb{Q}}$ ha grado 6, di conseguenza $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_3$.

Adesso vogliamo determinare un polinomio il cui gruppo di Galois sia isomorfo a $\mathbb{Z}3$. Consideriamo l'estensione ${}^{\mathbb{Q}(\zeta_7)}\!\big/_{\mathbb{Q}}$, dove ζ_7 è una radice primitiva settima di 1, per il Teorema 3.9 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z}^* \cong \mathbb{Z}/6\mathbb{Z}$. Vale il seguente risultato.

Proposizione 3.16
Sia $\zeta_n \in \overline{\mathbb{Q}}$ una radice primitiva n-esima di 1 per $n \geq 3$, allora $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2$.

Dimostrazione. Sia $\alpha = \zeta_n + \zeta_n^{-1}$, poiché $\overline{\zeta_n} = \zeta_n^{-1}$ si ha $\overline{\alpha} = \overline{\zeta_n + \zeta_n^{-1}} = \zeta_n + \zeta_n^{-1} = \alpha$, cioè $\alpha \in \mathbb{R}$ e quindi $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Il polinomio $x^2 - \alpha x + 1$ è a coefficienti reali e si annulla in ζ_n, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] \leq 2$. D'altra parte $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\zeta_n) \cap \mathbb{R}$, quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2$. $\square$

Osservazione 3.17 — In realtà vale che $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Infatti il polinomio $x^2 - \alpha x + 1$, con le notazioni di sopra, è un polinomio a coefficienti in $\mathbb{Q}(\alpha)$ che si annulla in ζ_n, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] \leq 2$. D'altra parte $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\alpha)$, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$ e quindi $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$.

Abbiamo quindi che la sottoestensione $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ ha grado 3 su $\mathbb{Q}$, mostriamo quindi che è una sua estensione normale. Posto $\alpha = \zeta_7 + \zeta_7^{-1}$, le immersioni di $\mathbb{Q}(\alpha) \longhookrightarrow \overline{\mathbb{Q}}$ sono le restrizioni a $\mathbb{Q}(\alpha)$ degli elementi di $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, pertanto sono univocamente determinate dalle assegnazioni

$$\zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7 + \zeta_7^{-1} \qquad \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^2 + \zeta_7^{-2} \qquad \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^3 + \zeta_7^{-3}$$

Il polinomio minimo di α su $\mathbb{Q}$ è quindi

$$\mu_\alpha(x) = (x - (\zeta_7 + \zeta_7^{-1}))(x - (\zeta_7^2 + \zeta_7^{-2}))(x - (\zeta_7^3 + \zeta_7^{-3})) = x^3 + x^2 - 2x - 1$$

Notiamo che $\zeta_7^2 + \zeta_7^{-2}$ e $\zeta_7^3 + \zeta_7^{-3}$ sono elementi di $\mathbb{Q}(\alpha)$, in quanto

$$\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 2$$

$$\zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 + \zeta_7^{-1})$$

pertanto $\mathbb{Q}(\alpha)/\mathbb{Q}$ è un'estensione normale di grado 3 in quanto campo di spezzamento di $\mu_\alpha(x)$ su $\mathbb{Q}$, quindi il suo gruppo di Galois è isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

§3.5 Realizzabilità dei gruppi come gruppi di Galois

In questa sezione studiamo quali gruppi finiti possono realizzarsi come gruppi di Galois di un'estensione di campi qualsiasi. Il seguente lemma risulterà fondamentale in questo intento.

Lemma 3.18

Se p è un numero primo, allora $\mathcal{S}_p$ è generato da un p-ciclo e da una trasposizione.

Dimostrazione. Consideriamo $S(p)$ come il gruppo delle permutazioni di $\mathbb{Z}/p\mathbb{Z}$. Si osserva preliminarmente che $\mathcal{S}_p$ è isomorfo a $S(p)$. In particolare, un p-ciclo di $\mathcal{S}_p$ può essere fatto corrisposto al p-ciclo $\sigma = (0\ 1\ \cdots\ p-1)$ di $S(p)$. A partire da questa corrispondenza, ad una trasposizione di $\mathcal{S}_p$ corrisponderà una trasposizione $\tau = (a\ b)$ di $S(p)$, con $a \neq b$. Si pone $H = \langle \sigma, \tau \rangle$.

Si osserva che $\sigma^k \tau \sigma^{-k}$ è $(a+k\ b+k)$. Pertanto, in H vi appartiene in particolare $\rho = (0\ \alpha)$, dove si è posto $\alpha = b - a$ e $k = -a$. Analogamente si osserva che $\tau_j = \sigma^j \rho \sigma^{-j} = (j\ \alpha + j) \in H$. In particolare $\tau_{i\alpha} = (i\alpha\ (i+1)\alpha) \in H$.

A partire da queste trasposizioni si possono costruire iterativamente tutte le trasposizioni delle forma $(0\ n\alpha)$:

$$(0\ \alpha)(\alpha\ 2\alpha)(0\ \alpha) = \tau \tau_1 \tau^{-1} = (0\ 2\alpha)$$

$$(0\ 2\alpha)(2\alpha\ 3\alpha)(0\ 2\alpha) = (0\ 3\alpha)$$

$$(0\ 3\alpha)(3\alpha\ 4\alpha)(0\ 3\alpha) = (0\ 4\alpha)$$

$$\cdots$$

Poiché $a \neq b$, $\alpha = b - a$ è diverso da zero, e dunque è invertibile in $\mathbb{Z}/p\mathbb{Z}$. Se allora n è un inverso moltiplicativo di α, $(0\ 1) = (0\ n\alpha)$ è un elemento di H. Quindi H contiene sia σ che $(0\ 1)$, che generano $S(p)$. Pertanto $H = S(p)$, e così anche $\mathcal{S}_p$ è generato dal p-ciclo e dalla trasposizione corrispondente dall'inizio. $\square$

Osservazione 3.19 — In generale, se n non è necessariamente primo, è ancora sufficiente che alla trasposizione corrisponda in $S(n)$ un elemento $(a\ b)$ con $b - a$ invertibile modulo n, ossia con $(b-a, n) = 1$.

Lemma 3.20

Sia p un primo e sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p. Se $f(x)$ ha esattamente $p-2$ radici reali e 2 radici non reali e K è il suo campo di spezzamento su $\mathbb{Q}$, allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_p$.

Dimostrazione. Ricordiamo che $\mathrm{Gal}(K/\mathbb{Q})$ agisce in modo naturale e fedele sulle radici di $f(x)$, e quindi $\mathrm{Gal}(K/\mathbb{Q})$ si immerge naturalmente in un sottogruppo H di $\mathcal{S}_p$. Dal momento che p divide $|\mathrm{Gal}(K/\mathbb{Q})|$ il sottogruppo H contiene un p-ciclo. Inoltre, il coniugio complesso ristretto a K è un elemento di $\mathrm{Gal}(K/\mathbb{Q})$ che corrisponde a scambiare le uniche due radici non reali di $f(x)$, e dunque a una trasposizione in H. Poiché H contiene una trasposizione e un p-ciclo, H è esattamente $\mathcal{S}_p$ per il Lemma 3.18, da cui la tesi. $\square$

Lemma 3.21 (Lemma di Artin)

[a] Dato K un campo e G un sottogruppo finito di $\mathrm{Aut}(K)$, allora ${}^{K}\!/_{K^G}$ è un'estensione di Galois finita e $\mathrm{Gal}(K/K^G) = G$.

[a] La dimostrazione è da revisionare nella parte della dimostrazione della finitezza dell'estensione.

Dimostrazione. Consideriamo un'immersione $\varphi : K \longrightarrow \overline{K}$ tale che $\varphi_{|K^G} = id_{K^G}$, per definizione di K^G si ha che $\varphi \in G$. In particolare G è l'insieme delle immersioni di K in $\overline{K}$ che fissano K^G, pertanto $[K : K^G] = |G|$, cioè ${}^{K}\!/_{K^G}$ è un'estensione finita.

Per il Teorema dell'Elemento Primitivo esiste $\alpha \in K$ tale che $K = K^G(\alpha)$, posto $\mu(x) \in K^G[x]$ il polinomio minimo di α su K^G sia L il campo di spezzamento di $\mu(x)$ su K^G, vale l'inclusione $K \subseteq L$ in quanto $K = K^G(\alpha)$. Consideriamo il polinomio

$$f(x) = \prod_{g \in G} (x - g(\alpha)) \in K[x]$$

In realtà si ha $f(x) \in K^G[x]$, in quanto per ogni $h \in G$ vale

$$h(f(x)) = \prod_{g \in G} (x - (hg)(\alpha)) = f(x)$$

in quanto la composizione per h induce una bigezione tra gli elementi di G, quindi un riordinamento del prodotto. Poiché $f(\alpha) = 0$ si ha che $\mu(x) \mid f(x)$, pertanto le radici di $\mu(x)$ sono tutte della forma $g(\alpha)$ per opportuni $g \in G$. Allora le radici di $\mu(x)$ sono tutti elementi di K, pertanto $L = K$ e quindi ${}^{K}\!/_{K^G}$ è un'estensione di Galois. Sia $H = \mathrm{Gal}(K/K^G)$, allora

$$K^H = K^{\mathrm{Gal}(K/K^G)} = K^G$$

da cui $H = G$ per il Teorema di Corrispondenza di Galois. □

Proposizione 3.22

Ogni gruppo finito G si realizza come gruppo di Galois di un'estensione di campi.

Dimostrazione. Sia $|G| = n$ e $p \geq n$ un primo, si hanno le immersioni

$$G \hookrightarrow \mathcal{S}_n \hookrightarrow S_p$$

Consideriamo $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p avente esattamente $p - 2$ radici reali e 2 radici non reali e sia K il suo campo di spezzamento su $\mathbb{Q}$. Per il Lemma 3.19 vale $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$, per il Lemma di Artin allora ${}^{K}\!/_{K^G}$ è un'estensione di Galois finita e il suo gruppo di Galois è isomorfo a G. □

§3.6 Estensioni quadratiche di $\mathbb{Q}$

Teorema 3.23

Siano $p_1, \dots, p_n \in \mathbb{Z}$ primi distinti, poniamo $K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. ${}^{K_n}\!/\!_{\mathbb{Q}}$ è un'estensione di Galois e $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$.

Dimostrazione. Mostriamo la tesi per induzione su $n \geq 1$. Per $n = 1$ si ha $K_1 = \mathbb{Q}(\sqrt{p_1})$, che è un'estensione di Galois di $\mathbb{Q}$ in quanto di grado 2, e il suo gruppo di Galois è isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Per $n > 1$, supponiamo che l'estensione ${}^{K_n}\!/\!_{\mathbb{Q}}$ sia di Galois e che $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$, mostriamo la tesi per $n+1$. Consideriamo il seguente diagramma di campi

$$\begin{tikzcd}
 & K_{n+1} \arrow[dl, no head] \arrow[dd, no head] \arrow[dr, no head] & \\
K_n \arrow[dr, no head] & & \mathbb{Q}(\sqrt{p_{n+1}}) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

l'estensione ${}^{K_{n+1}}\!/\!_{\mathbb{Q}}$ è di Galois in quanto composto di due estensioni di Galois su $\mathbb{Q}$. Notiamo che si ha la tesi nel caso in cui $K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$, e che se questo non si verifica allora $\mathbb{Q}(\sqrt{p_{n+1}}) \subseteq K_n$. Per il Teorema di Corrispondenza di Galois le sottoestensioni di K_n di grado due su $\mathbb{Q}$ sono tante quanti i sottogruppi di indice due di $(\mathbb{Z}/2\mathbb{Z})^n$, che a loro volta sono tanti quanti gli iperpiani di $(\mathbb{F}_2)^n$[32], che sono $2^n - 1$. Consideriamo le sottoestensioni quadratiche $\mathbb{Q}(\sqrt{p_1^{\varepsilon_1} \dots p_n^{\varepsilon_n}})$ con $\varepsilon_i \in \{0, 1\}$ non tutti nulli, se queste sono due a due distinte allora sono tutte e sole le sottoestensioni quadratiche di K_n, in quanto sono $2^n - 1$. In effetti, le estensioni $\mathbb{Q}(\sqrt{p_1^{\varepsilon_1} \dots p_n^{\varepsilon_n}})$ e $\mathbb{Q}(\sqrt{p_1^{\delta_1} \dots p_n^{\delta_n}})$, con $\varepsilon_i, \delta_i \in \{0, 1\}$ non tutti nulli, coincidono se e solo se $(p_1^{\varepsilon_1} \dots p_n^{\varepsilon_n})(p_1^{\delta_1} \dots p_n^{\delta_n})$ è un quadrato in $\mathbb{Q}$, quindi in $\mathbb{Z}$. Questo è equivalente a richiedere $\varepsilon_i + \delta_i \equiv 0 \pmod 2$ per ogni i, ovvero $\varepsilon_i = \delta_i$ per ogni i. Abbiamo quindi determinato tutte e sole le sottoestensioni di K_n quadratiche su $\mathbb{Q}$. Notiamo quindi che $\mathbb{Q}(\sqrt{p_{n+1}}) \not\subseteq K_n$ in quanto p_{n+1} non è un quadrato in $\mathbb{Q}$ essendo irriducibile in $\mathbb{Z}$, quindi per la Proposizione 3.15 si ha $\mathrm{Gal}(K_{n+1}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^{n+1}$. □

Osservazione 3.24 — Otteniamo come corollario che $\mathbb{Q}$ ammette infinite estensioni quadratiche.

Osservazione 3.25 — Un elemento primitivo per l'estensione ${}^{K_n}\!/\!_{\mathbb{Q}}$ è dato da $\alpha = \sum_{i=1}^{n} \sqrt{p_i}$. Consideriamo infatti le immersioni $\mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$ che fissano $\mathbb{Q}$, poiché $\mathbb{Q}(\alpha) \subseteq K_n$ queste si estendono a immersioni $K_n \hookrightarrow \overline{\mathbb{Q}}$, che sono gli elementi di $\mathrm{Gal}(K_n/\mathbb{Q})$. In particolare, se $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ si ha $\sigma(\alpha) = \sum_{i=1}^{n} a_i \sqrt{p_i}$, con

[32] Stiamo qua considerando la struttura di spazio vettoriale di $(\mathbb{F}_2)^n$.

$a_i \in \{1, -1\}$. Le immagini di α tramite gli elementi di $\mathrm{Gal}(K_n/\mathbb{Q})$ sono quindi tutte distinte in quanto $\sqrt{p_1}, \ldots, \sqrt{p_n}$ sono elementi di una base di K_n su $\mathbb{Q}$, pertanto la scrittura di $\sigma(\alpha)$ come combinazione lineare di tali elementi è unica al variare di $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$. In particolare α ha 2^n immagini distinte, pertanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ e quindi $\mathbb{Q}(\alpha) = K_n$.

§3.7 Gruppo di Galois di un polinomio biquadratico

Teorema 3.26

Siano $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ un polinomio irriducibile, definiamo $\Delta = a^2 - 4b$. Posto K il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ si ha:

(1) se $\sqrt{b} \notin \mathbb{Q}$ e $\sqrt{b\Delta} \notin \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$;

(2) se $\sqrt{b} \in \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

(3) se $\sqrt{b\Delta} \in \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$;

Dimostrazione. Sostituendo $t = x^2$ e risolvendo l'equazione $t^2 + at + b$ ricaviamo le radici di $f(x)$ in $\overline{\mathbb{Q}}$

$$x_1 = \sqrt{\frac{-a+\sqrt{\Delta}}{2}} \qquad x_2 = -\sqrt{\frac{-a+\sqrt{\Delta}}{2}} \qquad x_3 = \sqrt{\frac{-a-\sqrt{\Delta}}{2}} \qquad x_4 = -\sqrt{\frac{-a-\sqrt{\Delta}}{2}}$$

quindi $K = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_3)$. Per ogni $i \in \{1, 2, 3, 4\}$ osserviamo che $\mathbb{Q}(x_i^2) = \mathbb{Q}(\sqrt{\Delta})$, consideriamo quindi il seguente diagramma di campi

$$\begin{tikzcd}[arrows=dash]
& K \arrow[dl] \arrow[dr] & \\
\mathbb{Q}(x_1) \arrow[dr] & & \mathbb{Q}(x_3) \arrow[dl] \\
& \mathbb{Q}(\sqrt{\Delta}) \arrow[d] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Poiché $f(x)$ è irriducibile su $\mathbb{Q}[x]$ si ha $\sqrt{\Delta} \notin \mathbb{Q}$, pertanto $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$. Per il Teorema delle Torri allora il grado di $\mathbb{Q}(x_1)$ e di $\mathbb{Q}(x_3)$ su $\mathbb{Q}(\sqrt{\Delta})$ è uguale a 2, quindi $[K : \mathbb{Q}] \in 4, 8$. In particolare $[K : \mathbb{Q}] = 4$ se e solo se $\mathbb{Q}(x_1) = \mathbb{Q}(x_3)$, cioè se e solo se $x_1^2 x_3^2$ è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$, cioè $x_1 x_3 \in \mathbb{Q}(\sqrt{\Delta})$.

$$x_1 x_3 = \sqrt{\frac{-a+\sqrt{\Delta}}{2} \cdot \frac{-a-\sqrt{\Delta}}{2}} = \sqrt{\frac{a^2-\Delta}{4}} = \sqrt{b}$$

quindi $\mathbb{Q}(x_1) = \mathbb{Q}(x_3)$ se e solo se $\sqrt{b} \in \mathbb{Q}(\Delta)$, cioè se e solo se $\sqrt{b} \in \mathbb{Q}$ oppure $\sqrt{b\Delta} \in \mathbb{Q}$. Distinguiamo tre casi:

(1) se $\sqrt{b} \notin \mathbb{Q}$ e $\sqrt{b\Delta} \notin \mathbb{Q}$ allora $[K : \mathbb{Q}] = 8$. Allora $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ in quanto $\mathrm{Gal}(K/\mathbb{Q})$ è isomorfo a un sottogruppo di $\mathcal{S}_4$ e i 2-Sylow di $\mathcal{S}_4$ sono isomorfi a D_4;

(2) se $\sqrt{b} \in \mathbb{Q}$ (e di conseguenza $\sqrt{b\Delta} \notin \mathbb{Q}$) allora $K = \mathbb{Q}(x_1)$, quindi $[K : \mathbb{Q}] = 4$ e $\mathrm{Gal}(K/\mathbb{Q})$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oppure a $\mathbb{Z}/4\mathbb{Z}$. Siano $\varphi_i \in \mathrm{Gal}(K/\mathbb{Q})$ per $i \in \{1, 2, 3, 4\}$ gli omomorfismi determinati dalle seguenti assegnazioni

$$\varphi_1 : x_1 \longmapsto x_1 \qquad \varphi_2 : x_1 \longmapsto x_2 \qquad \varphi_3 : x_1 \longmapsto x_3 \qquad \varphi_4 : x_1 \longmapsto x_4$$

poiché $x_2 = -x_1$ abbiamo che $\varphi_2^2 = \varphi_1 = id$, cioè φ_2 ha ordine 2. Sfruttando la relazione $x_1 x_3 = \sqrt{b}$ abbiamo

$$\varphi_3^2(x_1) = \varphi_3(x_3) = \varphi_3\left(\frac{\sqrt{b}}{x_1}\right) = \frac{\varphi_3(\sqrt{b})}{\varphi_3(x_1)}^{33} = \frac{\sqrt{b}}{x_3} = x_1$$

pertanto anche φ_3 ha ordine 2. Allora $\mathrm{Gal}(K/\mathbb{Q})$ non è ciclico, quindi è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

(3) se $\sqrt{b\Delta} \in \mathbb{Q}$ (e di conseguenza $\sqrt{b} \notin \mathbb{Q}$) scriviamo $b = \Delta q^2$, con $q \in \mathbb{Q}$. Ragionando allo stesso modo e con le stesse notazioni si ha che φ_2 ha ordine 2 e

$$\varphi_3^2(x_1) = \varphi_3(x_3) = \varphi_3\left(\frac{\sqrt{b}}{x_1}\right) = \frac{\varphi_3(\sqrt{\Delta}q)}{\varphi_3(x_1)} = q\frac{\varphi_3(\sqrt{\Delta})}{x_3}$$

Poiché $\sqrt{\Delta} = 2x_1^2 + a$ si ha $\varphi_3(\sqrt{\Delta}) = 2x_3^2 + a = -\sqrt{\Delta}$, pertanto

$$\varphi_3^2(x_1) = -q\frac{\sqrt{\Delta}}{x_3} = -\frac{\sqrt{b}}{x_3} = -x_1$$

quindi φ_3 ha ordine 4. Allora $\mathrm{Gal}(K/\mathbb{Q})$ è ciclico, in particolare è isomorfo a $\mathbb{Z}/4\mathbb{Z}$.

□

[33] L'uguaglianza è data dal fatto che $\sqrt{b}$ è un elemento di $\mathbb{Q}$, pertanto è fissato da tutti gli elementi di $\mathrm{Gal}(K/\mathbb{Q})$.

§3.8 Contare le sottoestensioni quadratiche di un campo

Consideriamo un'estensione di Galois finita ${}^{F}\!/_{K}$, sia $G = \mathrm{Gal}(F/K)$, le sottoestensioni di F di grado due su K sono in corrispondenza con i sottogruppi di G di indice 2. Osserviamo che un sottogruppo $H \leqslant G$ di indice 2 contiene il sottogruppo

$$\mathscr{G} = \langle g^2 \mid g \in G \rangle$$[34]

Infatti se consideriamo il quoziente ${}^{G}\!/_{H} \cong \mathbb{Z}/2\mathbb{Z}$, per ogni $g \in G$ si ha

$$(gH)^2 = g^2 H = H$$

da cui $g^2 \in H$ e quindi anche $\mathscr{G} \leqslant H$. Per il Teorema di Corrispondenza tra sottogruppi abbiamo una bigezione

$$\{H \leqslant G \mid [G : H] = 2\} \longleftrightarrow \left\{\mathcal{H} \leqslant {}^{G}\!/_{\mathscr{G}} \,\middle|\, \left[{}^{G}\!/_{\mathscr{G}} : \mathcal{H}\right] = 2\right\}$$

Gli elementi di ${}^{G}\!/_{\mathscr{G}}$ hanno ordine al più 2. Questo implica che sia un gruppo abeliano, infatti per ogni $a, b \in {}^{G}\!/_{\mathscr{G}}$ si ha

$$aba^{-1}b^{-1} = abab = (ab)^2 = e$$

pertanto $ab = ba$. Essendo un gruppo finito per il Teorema di Struttura dei Gruppi Abeliani Finiti si ha ${}^{G}\!/_{\mathscr{G}} \cong (\mathbb{Z}/2\mathbb{Z})^k$, dove k è un parametro che dipende da G. Il numero di sottogruppi di indice 2 di $(\mathbb{Z}/2\mathbb{Z})^k$ è uguale al numero di iperpiani dello spazio vettoriale $(\mathbb{F}_2)^k$, quindi $2^k - 1$, e questo è il numero di sottoestensioni di F quadratiche su K.

Esempio 3.27
Sia $F = \mathbb{Q}(i, \zeta_3, \sqrt[3]{3})$, si verifica che il gruppo di Galois dell'estensione ${}^{F}\!/_{\mathbb{Q}}$ è isomorfo a $G = \mathcal{S}_3 \times \mathbb{Z}/2\mathbb{Z}$. Il sottogruppo $\langle g^2 \mid g \in G \rangle$ è isomorfo al sottogruppo $\mathscr{G} = \mathcal{A}_3 \times \{0\}$, pertanto ${}^{G}\!/_{\mathscr{G}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, che contiene tre sottogruppi di indice 2. Quindi F contiene tre sottoestensioni quadratiche su $\mathbb{Q}$, che sono $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$.

Osservazione 3.28 — Possiamo ripetere la costruzione di sopra per cercare i sottogruppi normali di indice k, in quanto questi contengono il sottogruppo $\langle g^k \mid g \in G \rangle$, ma la caratterizzazione del quoziente è più complicata in generale.

[34] Stiamo usando la notazione moltiplicativa. In notazione additiva allora $\mathscr{G} = \langle 2g \mid g \in G \rangle$.

§3.9 Radici dell'unità

Consideriamo un'estensione di Galois finita ${}^{K}\!/_{\mathbb{Q}}$ con gruppo di Galois G, sia ζ_n una radice primitiva n-esima dell'unità, vogliamo capire come determinare se ζ_n è contenuta in F al variare di $n \in \mathbb{N}$.

$$\begin{tikzcd}
K \arrow[dr, dash] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\
& F = K \cap \mathbb{Q}(\zeta_n) \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Il gruppo $\mathrm{Gal}(F/\mathbb{Q})$ è un sottogruppo di $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, che è isomorfo a $\mathbb{Z}/n\mathbb{Z}^*$ per il Teorema 3.9, in particolare $\mathrm{Gal}(F/\mathbb{Q})$ è un gruppo abeliano e ${}^{F}\!/_{\mathbb{Q}}$ è un'estensione normale in quanto tutte le sottoestensioni di $\mathbb{Q}(\zeta_n)$ sono normali. D'altra parte $\mathrm{Gal}(F/\mathbb{Q})$ è isomorfo a un quoziente ${}^{G}\!/_{H}$, con $H \trianglelefteq G$, in particolare H deve contenere il sottogruppo derivato G' in quanto il quoziente è abeliano (Proposizione 1.35).

Esempio 3.29

Per $n \geq 3$, sia $f(x) \in \mathbb{Q}[x]$ che il gruppo di Galois del suo campo di spezzamento K su $\mathbb{Q}$ è isomorfo a $\mathcal{S}_n$, consideriamo i sottogruppi normali H di $\mathcal{S}_n$ che contengono $\mathcal{S}_n'$. Poiché $\mathcal{S}_n' = \mathcal{A}_n$ tali sottogruppi sono solo $\mathcal{A}_n$ e $\mathcal{S}_n$. Se $H = \mathcal{S}_n$ allora $\mathbb{Q}(\zeta_n) \cap K = \mathbb{Q}$ in quanto ${}^{\mathrm{Gal}(K/\mathbb{Q})}\!/_{H}$ è il gruppo banale, quindi le uniche radici dell'unità contenute in K sono 1 e -1 (che sono rispettivamente ζ_1 e ζ_2). Se $H = \mathcal{A}_n$ allora $[\mathbb{Q}(\zeta_n) \cap K : \mathbb{Q}] = 2$. Poiché una sottoestensione di $\mathbb{Q}(\zeta_n)$ è della forma $\mathbb{Q}(\zeta_d)$ con $d \mid n$, abbiamo che $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = 2$. I possibili d sono quindi da determinare tra le soluzioni dell'equazione $\phi(m) = 2$, cioè $d \in 3, 4, 6$. In particolare le uniche radici dell'unità non banali che possono essere contenute in K sono ζ_3, ζ_4 e ζ_6, e quali di queste sono effettivamente elementi del campo dipende dalle radici del polinomio $f(x)$.

Consideriamo adesso le estensioni ciclotomiche $\mathbb{Q}(\zeta_p)$ con p primo, vogliamo determinare quando una sottoestensione quadratica di $\mathbb{Q}(\zeta_p)$ è reale oppure no. Il gruppo di Galois dell'estensione è isomorfo a $\mathbb{Z}/p\mathbb{Z}^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$, che è un gruppo ciclico, quindi $\mathbb{Q}(\zeta_n)$ contiene un'unica sottoestensione quadratica su $\mathbb{Q}$. Osserviamo che l'insieme dei quadrati di $\mathbb{Z}/p\mathbb{Z}^*$ è un sottogruppo di indice 2, in quanto la mappa

$$\varphi : \mathbb{Z}/p\mathbb{Z}^* \longrightarrow \mathbb{Z}/p\mathbb{Z}^* : x \longmapsto x^2$$

è un omomorfismo di gruppi, essendo $\mathbb{Z}/p\mathbb{Z}^*$ abeliano, e il suo nucleo è $\{1, -1\}$, pertanto $|\mathrm{Im}\varphi| = \dfrac{p-1}{2}$. Siano $K = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$, F_2 l'unica sottoestensione quadratica di $\mathbb{Q}(\zeta_p)$, K è il campo fissato dal coniugio complesso, pertanto corrisponde al sottogruppo $\langle -1 \rangle \leqslant \mathbb{Z}/p\mathbb{Z}^*$, mentre F_2 corrisponde al sottogruppo dei quadrati di $\mathbb{Z}/p\mathbb{Z}^*$. Allora $F_2 \subseteq K$ se e solo se -1 è un quadrato in $\mathbb{Z}/p\mathbb{Z}^*$, cioè se e solo se $p \equiv 1 \pmod 4$.

Più in generale vale il seguente teorema, di cui non diamo la dimostrazione.

Teorema 3.30

Dato p un primo dispari, l'unica sottoestensione di $\mathbb{Q}(\zeta_p)$ quadratica su $\mathbb{Q}$ è

(1) $\mathbb{Q}(\sqrt{p})$ se $p \equiv 1 \pmod 4$;

(2) $\mathbb{Q}(\sqrt{-p})$ se $p \equiv 3 \pmod 4$.

§3.10 Il discriminante polinomiale

In questa sezione si illustra il *discriminante polinomiale* e le sue principali applicazioni nella teoria di Galois.

Definizione 3.31. Sia $p \in K[x]$. Se $\deg p = n$ e α_1, ..., $\alpha_n \in \overline{K}$ sono le radici di p, si definisce il **discriminante polinomiale** $\operatorname{disc} p$ in modo tale che:

$$\operatorname{disc} p = \operatorname{disc} p(x) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K[\alpha_1, \ldots, \alpha_n]$$

Si verifica facilmente che p ha radici multiple se e solo se $\operatorname{disc} p = 0$. Inoltre, l'annullamento di $\operatorname{disc} p$ è indipendente dal coefficiente di testa a_n del polinomio, dal momento che polinomi associati condividono le stesse radici[35]. Altrettanto semplicemente si verifica che $\operatorname{disc} p$ è un polinomio simmetrico negli α_i, ovverosia una qualsiasi permutazione degli α_i in p restituisce ancora p.

Si osserva facilmente che $\operatorname{disc} p$ è invariante per traslazioni. Infatti, se si considera $p(x+a)$ con $a \in K$, le radici di $p(x+a)$ sono $\alpha_1 - a$, ..., $\alpha_n - a$. Pertanto vale che:

$$\operatorname{disc} p(x+a) = \prod_{i<j} (\alpha_i - a - \alpha_j + a)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \operatorname{disc} p(x)$$

Esempio 3.32 (disc p per polinomi di grado 2)

Sia $p(x) = ax^2 + bx + c$ con $a \neq 0$. Se α_1 e α_2 sono le radici di p in $\overline{K}$, allora vale che:

$$\operatorname{disc} p(x) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = \frac{b^2}{a^2} - 4\frac{c}{a} = \frac{\Delta}{a^2}$$

dove si è utilizzato il fatto per cui $\alpha_1 + \alpha_2 = -\frac{b}{a}$, $\alpha_1\alpha_2 = \frac{c}{a}$ e dove Δ indica l'usuale delta delle equazioni di secondo grado.

Osservazione 3.33 (Utilizzo della matrice di Vandermonde) — Un'espressione di $\operatorname{disc} p$ può anche essere calcolata attraverso le matrici di Vandermonde. Infatti, se M è la matrice di Vandermonde di α_1, ..., α_n radici di p, vale che:

$$M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

e quindi:

$$\det(M) = \prod_{i<j} (\alpha_i - \alpha_j)$$

[35] In generale, compare sempre un termine a_n^{2n-2} al denominatore di $\operatorname{disc} p(x)$. Pertanto, in letteratura si definisce $\operatorname{disc} p(x)$ anche come il prodotto tra a_n^{2n-2} e il discriminante qui definito. In tal caso, il discriminante di un polinomio di secondo grado è esattamente Δ.

Pertanto vale che:

$$\det(M^2) = \det(MM^T) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \operatorname{disc} p(x)$$

Osservazione 3.34 — Sia $p \in K[x]$ di grado n e siano $\alpha_1, \ldots, \alpha_n$ le sue radici. Se allora $\sigma \in S(\{\alpha_1, \ldots, \alpha_n\})$, vale che:

$$\prod_{i<j} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{i<j} \frac{\sigma(\alpha_i) - \sigma(\alpha_j)}{\alpha_i - \alpha_j} \prod_{i<j} (\alpha_i - \alpha_j) = \operatorname{sgn}(\sigma) \prod_{i<j} (\alpha_i - \alpha_j)$$

Pertanto, se $L = K(\alpha_1, \ldots, \alpha_n)$ è un campo di spezzamento di p su K e ogni fattore irriducibile di p è separabile, elevando al quadrato, vale che:

$$\sigma(\operatorname{disc} p) = \operatorname{disc} p \qquad \forall \sigma \in \operatorname{Gal}\left({}^{L}\!/_{K}\right)$$

e quindi[a] $\operatorname{disc} p \in L^G = K$.

[a] In generale, $\operatorname{disc} p$ appartiene sempre a K. Infatti $\operatorname{disc} p$ è un polinomio simmetrico negli α_i, e in quanto tale, per il Teorema fondamentale dei polinomi simmetrici, può scriversi come elemento di $K[e_1, \ldots, e_n]$, dove:

$$e_0 = 1, \qquad e_i = \sum_{1 \leq j_1 \leq \cdots \leq j_i \leq n} \alpha_{j_1} \cdots \alpha_{j_i} \quad \forall\, 1 \leq i \leq n$$

Pertanto, poiché per le formule di Viète vale che $a_i = (-1)^{n-i} a_n e_{n-i} \in K$, e dunque $e_i \in K$, $\operatorname{disc} p$, essendo combinazione dei vari e_i, è sempre un elemento di K.

L'utilità del discriminante polinomiale per la teoria di Galois è sancita dalla seguente proposizione:

Proposizione 3.35

Sia p un polinomio irriducibile e separabile di grado n. Allora, se L è il suo campo di spezzamento su K, $\operatorname{Gal}\left({}^{L}\!/_{K}\right) \hookrightarrow \mathcal{A}_n$ se e solo se $\operatorname{disc} p$ è un quadrato[a] in K.

[a] Questa proposizione è ancora vera utilizzando il discriminante moltiplicato per a^{2n-2}, e quindi vale ancora per la definizione alternativa di discriminante.

Dimostrazione. Sia $G := \operatorname{Gal}\left({}^{L}\!/_{K}\right)$. Allora $G \hookrightarrow \mathcal{A}_n$ se e solo se $\operatorname{sgn}(\sigma) = 1$ $\forall \sigma \in G$. Siano $\alpha_1, \ldots, \alpha_n$ le radici di p in $\overline{K}$. Allora vale la seguente identità:

$$\sigma\left(\prod_{i<j} (\alpha_i - \alpha_j)\right) = \prod_{i<j} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \operatorname{sgn}(\sigma) \prod_{i<j} (\alpha_i - \alpha_j)$$

dove si è utilizzata la precedente osservazione. Poiché gli elementi fissati da tutte le $\sigma \in G$ sono esattamente gli elementi di K, se $G \hookrightarrow \mathcal{A}_n$, $\operatorname{sgn}(\sigma)$ è sempre uguale ad 1, e quindi $\left(\prod_{i<j} (a_i - a_j)\right) \in K$. In tal caso $\operatorname{disc} p$ è un quadrato in K, essendo $\left(\prod_{i<j} (a_i - a_j)\right)$ una sua radice quadrata. Analogamente, se $\operatorname{disc} p$ è un quadrato in K, $x^2 - \operatorname{disc} p$ ammette una soluzione in K, e quindi deve scomporsi linearmente. Pertanto anche $\left(\prod_{i<j} (a_i - a_j)\right)$ deve appartenere a K, e quindi σ deve fissarlo. Affinché σ lo fissi deve dunque valere $\operatorname{sgn}(\sigma) = 1$, da cui la tesi. $\square$

Osservazione 3.36 ($\operatorname{disc} p$ per polinomi *depressi* di grado 3) — Sia $p(x) = x^3 + px + q$. Si calcola il suo discriminante polinomiale in termini di p e q. Siano α_1, α_2 e α_3 le radici di $p(x)$. Allora per le osservazioni precedenti vale che:

$$\operatorname{disc} p(x) = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix} = \det \begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}$$

dove[a] $s_p := \alpha_1^p + \alpha_2^p + \alpha_3^p$.

Chiaramente $s_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0$, dal momento che il coefficiente[b] di x^2 è nullo. Si calcola ora s_2:

$$s_2 = s_1^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) = s_1^2 - 2p = -2p$$

dove $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = e_2(\alpha_1, \alpha_2, \alpha_3) = p$ per le formule di Viète. Si calcola s_3:

$$s_3 = s_1^3 - 3\alpha_1^2(\alpha_2 + \alpha_3) - 3\alpha_2^2(\alpha_1 + \alpha_3) - 3\alpha_3^2(\alpha_1 + \alpha_2) - 6\alpha_1\alpha_2\alpha_3$$

Sempre per le formule di Viète, vale che $\alpha_1\alpha_2\alpha_3 = -q$, e quindi:

$$s_3 = s_1^3 - 3\alpha_1^2(s_1 - \alpha_1) - 3\alpha_2^2(s_1 - \alpha_2) - 3\alpha_3^2(s_1 - \alpha_3) + 6q$$

da cui, ricordando che $s_1 = 0$, si ricava che:

$$s_3 = 3s_3 + 6q \implies s_3 = -3q$$

Si calcola infine s_4:

$$s_4 = s_1^4 - 4(\alpha_1^3(s_1 - \alpha_1) + \alpha_2^3(s_1 - \alpha_2) + \alpha_3^3(s_1 - \alpha_3)) - 12\alpha_1\alpha_2\alpha_3 s_1 - 6(\alpha_1^2\alpha_2^2 + \alpha_2^2\alpha_3^2 + \alpha_3^2\alpha_1^2)$$

Ricordando che $s_1 = 0$, vale allora che:

$$s_4 = 4s_4 - 3(\alpha_1^2(s_2 - \alpha_1^2) + \alpha_2^2(s_2 - \alpha_2^2) + \alpha_3^2(s_2 - \alpha_3^2))$$

da cui:

$$-3s_4 = -3(s_2^2 - s_4) \implies s_4 = \frac{s_2^2}{2} = 2p^2$$

Pertanto si può ora concludere che:

$$\operatorname{disc} p(x) = \det \begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} = 3 \begin{vmatrix} -2p & -3q \\ -3q & 2p^2 \end{vmatrix} - 2p \begin{vmatrix} 0 & -2p \\ -2p & -3q \end{vmatrix}$$

e quindi che:

$$\operatorname{disc} p(x) = 3(-4p^3 - 9q^2) - 2p(-4p^2) = -12p^3 - 27q^2 + 8p^3 = \boxed{-4p^3 - 27q^2}$$

[a] In realtà esistono delle relazioni esplicite per il termine s_p, dette formule di Newton-Girard, che dunque permettono di estendere i calcoli a gradi più alti con più efficienza.

[b] Se si sta considerando un polinomio non depresso, ossia per il quale tale coefficiente è non nullo, si può applicare la trasformazione di Tschirnhaus, ossia si può considerare $p\left(x - \frac{a_{n-1}}{n\, a_n}\right)$. Infatti, come visto prima, il discriminante è invariante per traslazione.

Esempio 3.37 (Gruppo di Galois di un polinomio cubico, irriducibile e separabile)
Sia $p(x) = x^3 + px + q \in K[x]$ irriducibile e separabile. Sia L un campo di spezzamento di p su K. Dalla teoria di Galois sappiamo che $3 \mid [L : K] \mid 3! = 6$. Poiché $G = \operatorname{Gal}\left({}^{L}\!/_{K}\right)$ si immerge in $\mathcal{S}_3$ agendo sulle radici di $p(x)$, G è isomorfo a $\mathcal{A}_3$ o a $\mathcal{S}_3$.

Per la proposizione precedente, G è isomorfo a $\mathcal{A}_3$ se e solo se $\operatorname{disc} p(x) = -4p^3 - 27q^2$ è un quadrato in K, e quindi:

$$G \cong \begin{cases} \mathcal{A}_3 & \text{se } -4p^3 - 27q^2 \text{ è quadrato in } K \\ \mathcal{S}_3 & \text{altrimenti} \end{cases}$$

§3.11 Risoluzione delle equazioni di terzo grado ⋆

Si illustra adesso il metodo risolutivo delle equazioni di terzo grado, tramite la cosiddetta **formula di Cardano-Tartaglia-Del Ferro**.

Innanzitutto, si assume che $\varphi(x)$ sia un polinomio *depresso* di terzo grado della forma $x^3 + px + q$. Se invece tale polinomio non è depresso (ossia se il coefficiente di x^2 non è nullo) ed è della forma $ax^3 + bx^2 + cx + d$ con $b \neq 0$, è sufficiente sostituire $x = y - \frac{b}{3a}$ per ottenere un polinomio di tale tipo[36].

Sia $x = u + v$. Allora $\varphi(u + v) = u^3 + v^3 + 3u^2v + 3uv^2 + p(u + v) + q = (u^3 + v^3 + q) + (3uv + p)(u + v)$. Si impone allora il seguente sistema di equazioni:

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \implies u^3v^3 = -\frac{p^3}{27} \end{cases}$$

Infatti, se il precedente sistema ammette soluzione, $\varphi(x) = \varphi(u + v)$ si annulla e $u + v$ è soluzione.

Dal momento che abbiamo sia la somma che il prodotto di u^3 e v^3, è possibile ricavare queste due quantità risolvendo l'equazione di secondo grado associata:

$$0 = y^2 - (u^3 + v^3)y + u^3v^3 = y^2 + qy - \frac{p^3}{27}$$

Una volta ottenuti sia u^3 che v^3, prendendone la radice cubica, si otterrà dunque una radice di $\varphi(x)$. In particolare varrà che:

$$y_{1,2} = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

e quindi:

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Le altre due soluzioni di $\varphi(x)$ si possono poi computare facilmente riducendosi a considerare il polinomio di secondo grado $\varphi(x)/(x - \alpha)$, dove α è la soluzione ottenuta.

[36] Questa è ancora la cosiddetta trasformazione di Tschirnhaus.

Gabriel Antonio Videtta (g.videtta1@studenti.unipi.it)
Leonardo Migliorini (l.migliorini@studenti.unipi.it)
Università di Pisa (Anno Accademico 2022-23)

§3.12 Teorema fondamentale dell'algebra

Teorema 3.38 (Teorema fondamentale dell'algebra)
$\mathbb{C}$ è algebricamente chiuso, ovvero ogni polinomio non costante in $\mathbb{C}[x]$ ammette almeno una radice in $\mathbb{C}$.

Dimostrazione. Dato $p(x) \in \mathbb{C}[x]$, non costante, vogliamo dimostrare che $\exists \alpha \in \mathbb{C}$ tale che $p(\alpha) = 0$; detto:

$$q(x) := p(x) \cdot \overline{p(x)} \in \mathbb{R}[x]$$

dove $\overline{p(x)}$ è il polinomio coniugato di $p(x)$[37] e $q(x) \in \mathbb{R}[x]$ in quanto ad esempio:

$$\overline{q(x)} = \overline{p(x)} \cdot \overline{\overline{p(x)}} = \overline{p(x)} \cdot p(x)$$

quindi coincide con il suo coniugato e dunque sta in $\mathbb{R}[x]$[38]. A questo punto è sufficiente far vedere che $q(x)$ ha una radice complessa, in quanto, se $q(\alpha) = 0$, o $p(\alpha) = 0$ e quindi abbiamo la tesi, oppure $\overline{p(\alpha)} = 0 \iff \overline{\overline{p(\alpha)}} = 0$ che è equivalente al dire che $\exists \overline{\alpha} \in \mathbb{C}$ tale che $p(\overline{\alpha}) = 0$ e quindi di nuovo la tesi (sostanzialmente se il coniugato si annulla, allora anche il polinomio iniziale deve annullarsi). Possiamo quindi considerare $q(x) \in \mathbb{R}[x]$ e chiamare K il campo di spezzamento di $q(x)$ su $\mathbb{R}$, sia $G = \mathrm{Gal}\left({}^{K}\!/_{\mathbb{R}}\right)$ e $P_2 < G$ un 2-Sylow di G, abbiamo il diagramma:

$$\begin{tikzcd} K \arrow[dd, dash] \arrow[dr, dash, "|P_2|"] & \\ & K^{P_2} = \mathbb{R}(\beta) \arrow[dl, dash, "d"] \\ \mathbb{R} & \end{tikzcd}$$

con $d = [K^{P_2} : \mathbb{R}]$ dispari in quanto $d = \dfrac{|G|}{|P_2|}$ e per definizione $|P_2|$ è la massima potenza di 2 che divide $|G|$[39], inoltre per il Teorema dell'elemento primitivo, essendo ${}^{K^{P_2}}\!/_{\mathbb{R}}$ un'estensione finita è generata da un singolo elemento $\beta \in K$, possiamo quindi concludere che il polinomio minimo di β su K, $\mu_\beta(x)$ ha grado dispari. Poiché $\mu_\beta(x) \in \mathbb{R}[x]$ e $\mu_\beta(x)$ è un polinomio di grado dispari, vale il Teorema di esistenza degli zeri, dunque $\mu_\beta(x)$ ha almeno una radice in $\mathbb{R}$, ma per definizione di polinomio minimo $\mu_\beta(x)$ è irriducibile su $\mathbb{R}$, dunque l'unica possibilità è che $d = \deg \mu_\beta(x) = 1$[40], pertanto il gruppo di Galois dell'estensione ${}^{K}\!/_{\mathbb{R}}$ non può contenere sottoestensioni di grado dispari, quindi $[K : \mathbb{R}] = 2^n$, $n \in \mathbb{N}$. Essendo G un p-gruppo, sappiamo dalla teoria che esiste una catena del tipo:

$$\{e\} = G_n \trianglelefteq \ldots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$$

in cui l'indice di ogni sottogruppo normale nel successivo è esattamente p (quindi 2 in questo caso), ciò si riflette per Corrispondenza di Galois in una catena di sottoestensioni

[37] Il polinomio che si ottiene da $p(x)$ scambiando i suoi coefficienti con i loro complessi coniugati.
[38] La stessa cosa si poteva giustificare anche dai coefficienti.
[39] Nel caso in cui il 2-Sylow fosse banale avremmo che $K = \mathbb{R}$ e quindi non stiamo veramente estendendo il campo.
[40] Il fatto che gli unici polinomi irriducibili in $\mathbb{R}[x]$ siano di grado 1 o 2 è una conseguenza del Teorema fondamentale dell'algebra, quindi in questo caso non stiamo usando quel risultato.

di $K/\mathbb{R}$ del tipo:

$$\begin{tikzcd}
K = K^{G_n} \arrow[d, dash, "2"'] \\
K^{G_{n-1}} \arrow[d, dash, "2"'] \\
\vdots \arrow[d, dash, "2"'] \\
K^{G_2} = \mathbb{C}(\sqrt{\gamma_2}) \arrow[d, dash, "2"'] \\
K^{G_1} = \mathbb{R}(\sqrt{\gamma_1}) \arrow[d, dash, "2"'] \\
\mathbb{R}
\end{tikzcd}$$

dove $K^{G_1} = \mathbb{R}(\sqrt{\gamma_1})$ in quanto ogni estensione di grado 2 (in caratteristica diversa da 2) si ottiene estraendo una radice quadrata, inoltre se $\gamma_1 > 0$, allora $K^{G_1} = \mathbb{R}$, ma questo non è possibile perché di grado 2, quindi $\gamma_1 < 0$, ed in questo caso $K^{G_1} = \mathbb{C}$ poiché $\mathbb{R}(\sqrt{\gamma_1}) = \mathbb{R}(\sqrt{-1}) \iff (-1) \cdot \gamma_1 > 0$ è un quadrato in $\mathbb{R}$, ed essendo il prodotto positivo è sempre vero, dunque $K^{G_1} = \mathbb{C}$. Infine, si osserva che ancora una volta K^{G_2}, avendo grado 2, si ottiene estraendo una radice quadrata da $K^{G_1} = \mathbb{C}$, ma in $\mathbb{C}$ ogni elemento è un quadrato, quindi $\mathbb{C}$ non si può estendere ulteriormente, dunque $K = \mathbb{C}$, pertanto i polinomi a coefficienti reali hanno tutte le loro radici in $\mathbb{C}$ e per quanto detto all'inizio ciò significa che tutti i polinomi in $\mathbb{C}[x]$ hanno tutte le loro radici in $\mathbb{C}$, che quindi è algebricamente chiuso. $\square$