Complementi di Algebra 1

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

LEONARDO MIGLIORINI
l.migliorini@studenti.unipi.it

Anno Accademico 2022-23

Indice

Ringraziamenti

Diego Monaco, Niccolò Nannicini, Pietro Crovetto, Leonardo Alfani, Daniele Lapadula, Francesco Sorce, Alessandro Moretti.

§1 Gruppi

§1.1 Insiemi di generatori

Definizione 1.1. Dati un gruppo G e $x_1, \dots, x_n$ elementi di G, chiamiamo **sottogruppo generato** da $x_1, \dots, x_n$ il più piccolo sottogruppo $\langle x_1, \dots x_n \rangle$ di G contenente $x_1, \dots, x_n$, cioè

$$\langle x_1, \dots, x_n \rangle = \bigcap_{\substack{H \leqslant G \\ \{x_1, \dots, x_n\} \subseteq H}} H$$

Osservazione 1.2 — La definizione è ben posta, infatti l'intersezione avviene su una famiglia non vuota di insiemi dal momento che G è un sottogruppo di se stesso contenente $x_1, \dots, x_n$. Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi $x_1, \dots, x_n$.

La definizione data non dà informazioni su come sono fatti gli elementi di $\langle x_1, \dots, x_n \rangle$, cerchiamo quindi di caratterizzare in modo diverso tale sottogruppo. Poiché chiuso per l'operazione indotta da G, $\langle x_1, \dots, x_n \rangle$ deve contenere tutti i prodotti finiti, in qualsiasi ordine, delle potenze di $x_1, \dots, x_n$, cioè deve contenere l'insieme

$$\{g_1^{\pm 1} \dots g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \dots, x_n\} \ \forall i \in \{1, \dots, r\}\}$$

Proposizione 1.3

Dati un gruppo G e $x_1, \dots, x_n$ elementi di G, allora

$$\langle x_1 \dots x_n \rangle = \{g_1^{\pm 1} \dots g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \dots, x_n\} \ \forall i \in \{1, \dots, r\}\}$$

Dimostrazione. Poniamo $S = \{g_1^{\pm 1} \dots g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \dots, x_n\} \ \forall i \in \{1, \dots, r\}\}$, mostriamo che S è un sottogruppo di G. Effettivamente $e \in S$ in quanto è prodotto di nessuna potenza di $x_1, \dots, x_n$, il prodotto di due elementi di S è ancora un elemento di S in quanto prodotto finito di potenze di $x_1, \dots, x_n$ e l'inverso di un elemento $g_1^{\pm 1} \dots g_r^{\pm 1} \in S$ è $(g_1^{\pm 1} \dots g_r^{\pm 1})^{-1} = g_r^{\mp 1} \dots g_1^{\mp 1}$, che è un elemento di S. Abbiamo quindi che S è un sottogruppo di G contenente $x_1, \dots, x_n$, pertanto $\langle x_1, \dots, x_n \rangle \subseteq S$ per minimalità di $\langle x_1, \dots, x_n \rangle$. D'altra parte, per quanto osservato sopra abbiamo che tutti gli elementi della forma $g_1^{\pm 1} \dots g_r^{\pm 1}$ con $r \in \mathbb{N}$, $g_i \in \{x_1, \dots, x_n\}$ per ogni $i \in \{1, \dots, r\}$ devono essere contenuti in $\langle x_1, \dots, x_n \rangle$, pertanto i due sottogruppi coincidono. $\square$

Osservazione 1.4 — Se G è un gruppo ciclico abbiamo che esiste $x \in G$ tale che $\langle x \rangle = G$, cioè tutti gli elementi di G sono potenze di x.

Diciamo che $x_1, \dots, x_n \in G$ sono **generatori** per G, o che l'insieme $\{x_1, \dots, x_n\}$ **genera** G se $\langle x_1, \dots, x_n \rangle = G$.

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

Dato p un primo, vogliamo determinare quanti sono gli automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$, per fare ciò è conveniente definire una struttura di spazio vettoriale, quindi un prodotto per scalari

$$\cdot : \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n : (\overline{\lambda}, v) \longmapsto \overline{\lambda}v$$

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, infatti se $\lambda, \lambda' \in \mathbb{Z}$ sono tali che $\overline{\lambda} = \overline{\lambda'}$, cioè esiste $k \in \mathbb{Z}$ tale che $\lambda = \lambda' + kp$, allora

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

in quanto $\underbrace{v + \ldots + v}_{kp\text{ volte}} = 0$. Si verifica che $((\mathbb{Z}/p\mathbb{Z})^n, +, \cdot)$ è effettivamente uno spazio vettoriale sul campo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (dove $\cdot$ è il prodotto per scalari appena definito). Per come abbiamo definito il prodotto per scalari, abbiamo che per ogni $\varphi \in \operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ vale $\varphi(\lambda v) = \lambda\varphi(v)$ per ogni $\lambda \in \mathbb{F}_p$, pertanto

$$\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = GL((\mathbb{F}_p)^n) = \{\varphi : (\mathbb{F}_p)^n \longrightarrow (\mathbb{F}_p)^n \mid \varphi \text{ isomorfismo di spazi vettoriali}\}$$

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

Proposizione 1.5
Dato p un primo, allora

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

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 dermina univocamente in questo modo. Sia $\{v_1, \ldots, v_n\}$ una base di $(\mathbb{Z}/p\mathbb{Z})^n$ e $\varphi \in \operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$, consideriamo $\varphi(v_1)$: $\varphi(v_1)$ può assumere qualsiasi valore non nullo, pertanto abbiamo $(p^n - 1)$ possibilità per l'immagine del primo vettore. Per quanto riguarda v_2, $\varphi(v_2)$ può assumere qualsiasi valore non nullo che non sia multiplo di $\varphi(v_1)$, che sono $p^n - p$, analogamente $\varphi(v_3)$ può assumere qualsiasi valore non nullo che non sia combinazione lineare di v_1 e v_2, che sono $p^n - p^2$, e così via. Reiteriamo questo ragionamento fino a $\varphi(v_n)$, che può essere scelto in $p^n - p^{n-1}$ modi, da cui

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

□

§1.3 Gruppo diedrale

§1.3.1 Elementi del gruppo

Definizione 1.6. Dato $n \geqslant 2$ un numero naturale consideriamo un poligono regolare di n vertici centrato nell'origine del piano $\mathbb{R}^2$, chiamiamo **gruppo diedrale** su n vertici l'insieme D_n delle isometrie di $\mathbb{R}^2$ che fissano il poligono, cioè che mandano i vertici in se stessi (per $n = 2$ consideriamo le isometrie che mandano un segmento in se stesso).

Osservazione 1.7 — 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, che è anch'essa un'isometria.

Osservazione 1.8 — Una rotazione di angolo $\dfrac{2\pi}{n}$ è un elemento di D_n, così come una simmetria rispetto a un asse.

Proseguendo con questa intuizione geometrica, indicheremo con r una rotazione di angolo $\dfrac{2\pi}{n}$ e con s una simmetria rispetto a un qualsiasi asse. Notiamo che $\operatorname{ord}(r) = n$ e $\operatorname{ord}(s) = 2$ (per convenzione, indichiamo con un angolo positivo una rotazione in senso antiorario e con un angolo negativo una rotazione in senso orario).

Definizione 1.9. Data $r \in D_n$ una rotazione di ordine n, indichiamo con $\mathcal{R}$ il **sottogruppo delle rotazioni** $\langle r \rangle$.

Osservazione 1.10 — Il sottogruppo $\mathcal{R}$ contiene tutte le rotazioni di D_n, infatti se r' è una rotazione di angolo $\dfrac{2k\pi}{n}$, $k \in \mathbb{Z}$, allora $r^k = r'$ in quanto anche r^k è una rotazione di angolo $\dfrac{2k\pi}{n}$.

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.

Osservazione 1.11 — Gli elementi della forma r^k e sr^h sono distinti per ogni $h, k \in \mathbb{Z}$. Infatti sappiamo dall'algebra lineare che il determinante di una simmetria è -1 e che il determinante di una rotazione è 1, per la moltiplicatività del determinante quindi $\det(r^k) = (\det r)^k = 1$ e $\det(sr^h) = (\det s)(\det r)^h = -1$, da cui $r^k \neq sr^h$.

Lemma 1.12

Per ogni rotazione $r \in D_n$ e per ogni simmetria $s \in D_n$ vale

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

Dimostrazione. Senza perdita di generalità possiamo supporre che r sia la rotazione di angolo $\dfrac{2\pi}{n}$ 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

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

svolgendo esplicitamente il prodotto quindi

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

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

Proposizione 1.13
Se $n \geqslant 3$ allora $|D_n| = 2n$.

Dimostrazione. Indicando con $1, \dots, n$ gli n vertici di un poligono regolare di n lati, notiamo che un elemento $g \in D_n$ è univocamente determinato da $g(1), \dots, g(n)$. In particolare, fissato $g(1)$, per il quale abbiamo n possibili scelte, abbiamo al massimo due valori per $g(2)$, cioè $g(2) \in \{g(1)+1, g(1)-1\}$ (a meno di sommare n se uno dei due elementi è negativo). Poiché $g(1)$ e $g(2)$ individuano due vettori nel piano non allineati, cioè linearmente indipendenti, ne costituiscono una base: fissati i valori di $g(1)$ e $g(2)$ abbiamo quindi determinato ogni elemento di D_n in modo unico e, poiché possiamo farlo in al più $2n$ modi, $|D_n| \leq 2n$. Ricordiamo adesso che D_n contiene gli elementi della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$, mostriamo che questi sono infatti $2n$. Gli elementi r^k appartengono al gruppo ciclico $\mathcal{R}$ di ordine n, pertanto sono n elementi distinti, inoltre

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

pertanto anche questi sono n elementi distinti. Poiché gli insiemi $\mathcal{R}$ e $\{sr^h \mid h \in \mathbb{Z}\}$ sono disgiunti (Osservazione 1.11) abbiamo $|D_n| = 2n$. □

Osservazione 1.14 — Abbiamo mostrato che effettivamente $D_n = \langle r, s \rangle$, quindi i suoi elementi sono tutti della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$.

Osservazione 1.15 — Il risultato è valido anche per D_2, ma con motivazioni diverse. Se consideriamo un segmento nel piano $\mathbb{R}^2$ giacente sulla retta $y = 0$, le isometrie che possiamo applicare sono l'identità, la rotazione di angolo π, la simmetria lungo la retta $y = 0$ e la simmetria lungo l'asse passante per il suo punto medio. D_2 contiene quindi quattro elementi, l'identità e tre elementi di ordine 2, pertanto è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

§1.3.2 Sottogruppi

Consideriamo un sottogruppo $H \leqslant D_n$, distinguiamo due possibilità: $H \subseteq \mathcal{R}$ oppure $H \nsubseteq \mathcal{R}$. Nel primo caso abbiamo che $|H| \mid n$, ed è l'unico sottogruppo di $\mathcal{R}$ con questa proprietà in quanto $\mathcal{R}$ è ciclico, in particolare H è ciclico della forma $\langle r^{\frac{n}{d}} \rangle$, con $\mathcal{R} = \langle r \rangle$ e $d \mid n$.
Studiamo quindi il caso $H \nsubseteq \mathcal{R}$: notiamo che $\mathcal{R} \trianglelefteq D_n$ in quanto $[D_n : \mathcal{R}] = 2$, pertanto $D_n/\mathcal{R}$ è un gruppo con l'operazione indotta da D_n e risulta essere isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Consideriamo la proiezione al quoziente

$$\pi_{\mathcal{R}} : D_n \longrightarrow D_n/\mathcal{R} : g \mapsto g\mathcal{R}$$

poiché $H \nsubseteq \mathcal{R}$ abbiamo che esiste $h \in H$ tale che $h \notin \mathcal{R}$, pertanto $\pi_{\mathcal{R}}(h) \neq \mathcal{R}$ e in particolare $\pi_{\mathcal{R}}(H) \nsubseteq \{\mathcal{R}\}$. Dato che i sottogruppi di $D_n/\mathcal{R}$ sono solo $\{\mathcal{R}\}$ e $D_n/\mathcal{R}$ abbiamo $\pi_{\mathcal{R}}(H) = D_n/\mathcal{R}$. Osserviamo inoltre che $\ker \pi_{\mathcal{R}|H} = \ker \pi_{\mathcal{R}} \cap H = \mathcal{R} \cap H$, per il Primo Teorema di Omomorfismo allora $\dfrac{H}{H \cap \mathcal{R}} \cong \mathbb{Z}/2\mathbb{Z}$, quindi $|H \cap \mathcal{R}| = \dfrac{1}{2}|H|$. Dato che $\mathcal{R} \cap H \subseteq \mathcal{R}$, esiste $k \in \mathbb{Z}$ tale che $H \cap \mathcal{R} = \langle r^k \rangle$ in particolare $\langle r^k \rangle$ e $\langle sr^h \rangle$, $h \in \mathbb{Z}$, sono contenuti in H.

Proposizione 1.16

Dati $H \leqslant D_n$ un sottogruppo tale che $H \nsubseteq \mathcal{R}$, se r è un generatore di $\mathcal{R}$ tale che $H \cap \mathcal{R} = \langle r^k \rangle$ e s è una simmetria allora

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

Dimostrazione. Per quanto visto sopra vale $|\langle r^k \rangle| = \dfrac{1}{2}|H|$, inoltre $\operatorname{ord}(sr^h) = 2$:

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

pertanto $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Da questo ricaviamo $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$, infatti per ogni $m \in \mathbb{Z}$

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

cioè $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$ e quindi $\langle r^k \rangle \cdot \langle sr^h \rangle$ è un sottogruppo di D_n[1]. Poiché $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono contenuti in H abbiamo che $\langle r^k \rangle \cdot \langle sr^h \rangle \subseteq H$, inoltre

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

in quanto $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$[2], pertanto i due sottogruppi coincidono. □

Osservazione 1.17 — 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 $H_{h,k}$ contiene tutti i prodotti finiti delle potenze di r^k e sr^h, in particolare gli elementi di H.

[1] Dati K, N sottogruppi di un gruppo G, se vale almeno una delle inclusioni $K \subseteq N_G(N)$, $N \subseteq N_G(K)$ allora $HK = KH$, quindi HK è un sottogruppo di G.

[2] Se H, K sono sottogruppi finiti di un gruppo G e $HK \leqslant G$ allora vale $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Osservazione 1.18 — Per $k \mid n$ e $0 \le h < k$, $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$. 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, simmetricamente $\langle r^k, sr^{h+k} \rangle \subseteq \langle r^k, sr^h \rangle$ in quanto $sr^{h+k} = (sr^h)r^k$ è un elemento del primo gruppo.

Teorema 1.19 (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 $k \mid n$, $0 \le h < k$,

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

Dimostrazione. Abbiamo già visto che i sottogruppi di D_n sono di questo tipo, mostriamo quindi che sono tutti distinti. A meno di cambiare k, possiamo supporre $\mathcal{R} = \langle r \rangle$, cioè $\operatorname{ord}(r) = n$. Consideriamo $H, K \leqslant D_n$ due sottogruppi, abbiamo tre casi:

- se $H = \langle r^k \rangle$ e $K = \langle r^m \rangle$, $m \in \mathbb{Z}$, allora $H = K \iff k = m$ in quanto entrambi sottogruppi di $\mathcal{R}$, pertanto esiste un unico sottogruppo della forma $\langle r^k \rangle$ per $k \mid n$;
- se $H = \langle r^k \rangle$ e $K = \langle r^m, sr^h \rangle$, $m \mid n$, allora $H \neq K$ in quanto H è ciclico e K no;
- se $H = \langle r^k, sr^h \rangle$ e $K = \langle r^m, sr^l \rangle$, con $m \mid n$ e $0 \le l < m$, considerando le intersezioni $H \cap \mathcal{R} = \langle r^k \rangle$ e $K \cap \mathcal{R} = \langle r^m \rangle$ abbiamo

  $$H \cap \mathcal{R} = K \cap \mathcal{R} \iff \langle r^k \rangle = \langle r^m \rangle \iff k = m$$

  Inoltre, se $sr^h \in \langle r^m, sr^l \rangle = \langle r^m \rangle \cdot \langle sr^l \rangle$, allora esiste $t \in \mathbb{Z}$ tale che

  $$sr^h = (r^m)^t sr^l \iff sr^h = s^2 r^{mt} sr^l \iff r^h = r^{-mt+l} \iff h \equiv l - mt \pmod{n}$$

  da cui ricaviamo $h \equiv l \pmod{m}$ in quanto $m \mid n$. Ma allora $h = l$ dato che $0 \le h < k$ e $0 \le l < m$.

□

Lemma 1.20
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 $\varphi_{g|B} \in \operatorname{Aut}(B)$[3]. Dal momento che A è un sottogruppo caratteristico di B abbiamo che $\varphi_{g|B}(A) = \varphi_g(A) = A$, pertanto $A \trianglelefteq G$. □

[3] Notiamo che $\varphi_{g|B}$ in generale non è un coniugio di B, poiché g non appartiene necessariamente a B.

Corollario 1.21
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 del sottogruppo e $\langle r^k\rangle$ è l'unico sottogruppo di $\mathcal{R}$ di tale ordine ($\mathcal{R}$ 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 1.20 abbiamo $\langle r^k\rangle \trianglelefteqslant D_n$. $\square$

Osservazione 1.22 — $\mathcal{R} = \langle r\rangle$ è caratteristico in D_n per $n \geqslant 3$. Infatti per ogni $\varphi \in \mathrm{Aut}(D_n)$ allora $\mathrm{ord}(r) = \mathrm{ord}(\varphi(r))$, da cui $|\langle\varphi(r)\rangle| = n$. Se fosse $\varphi(r) \notin \mathcal{R}$ avremmo $\mathrm{ord}(\varphi(r)) = 2$, quindi $|\langle\varphi(r)\rangle| = n = 2$, che è assurdo in quanto $|D_n| \geqslant 6$. Questo non è vero per D_2, che contiene una rotazione e due simmetrie: poiché $\mathrm{Aut}(D_2) \cong S_3$ esiste un $\psi \in \mathrm{Aut}(D_2)$ che manda la rotazione in una riflessione.

Corollario 1.23
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 $r, s \in N_{D_n}(H_{k,h})$.

Dimostrazione.

- Se $H_{k,h} \trianglelefteqslant D_n$ allora $N_{D_n}(H_{k,h}) = D_n$, in particolare $r, s \in N_{D_n}(H_{k,h})$;
- se $r, s \in N_{D_n}(H_{k,h})$, poiché il normalizzatore è un sottogruppo di D_n abbiamo che $D_n = \langle r, s\rangle \subseteq N_{D_n}(H_{k,h})$, pertanto $H_{k,h} \trianglelefteqslant D_n$.

$\square$

Vediamo quali sono i sottogruppi normali della forma $\langle r^k, sr^h\rangle$, consideriamo i coniugi

$$\varphi_s : D_n \longrightarrow D_n : x \longmapsto sxs^{-1} \qquad \varphi_r : D_n \longrightarrow D_n : x \longmapsto rxr^{-1}$$

e sia $x_1^{\pm 1} \dots x_m^{\pm 1} \in H_{k,h} = \langle r^k, sr^h\rangle$, allora

$$\varphi_s(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_s(x_1)^{\pm 1} \dots \varphi_s(x_m)^{\pm 1} \in \langle srs, r^h s^{-1}\rangle = \langle sr^k s, r^h s^{-1}\rangle = \langle r^k, sr^{-h}\rangle$$

$$\varphi_r(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_r(x_1)^{\pm 1} \dots \varphi_r(x_m)^{\pm 1} \in \langle r^k, rsr^{h-1}\rangle = \langle r^k, sr^{h-2}\rangle$$

Pertanto $H_{k,h} \trianglelefteqslant D_n$ se e solo se $\langle r^k, sr^{h-2}\rangle = \langle r^k, sr^{-h}\rangle = \langle r^k, sr^h\rangle$, se e solo se $h \equiv h-2 \pmod k$, cioè $k \in \{1, 2\}$.

- Se $k = 1$ allora $H_{k,h} = \langle r, s\rangle = D_n$;
- se $k = 2$ (e n pari) allora $H_{k,h} = \langle r^2, sr\rangle$ oppure $H_{k,h} = \langle r^2, s\rangle$.

Osservazione 1.24 — Il secondo caso si presenta solo se n è pari, questo corrisponde 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. In un poligono con un numero dispari di lati gli assi di simmetria sono tutti passanti per i lati.

§1.3.3 Classi di coniugio

Abbiamo visto che possiamo scrivere ogni elemento di D_n nella forma $s^h r^k$, dove s è una simmetria e r è una rotazione che genera $\mathcal{R}$, con $h \in \{0,1\}$ e $k \in \{0,\dots,n-1\}$ in quanto $\operatorname{ord}(s) = 2$ e $\operatorname{ord}(r) = n$. Inoltre tutti gli elementi della forma sr^k hanno ordine 2.

Consideriamo la classe di coniugio di r, $\mathcal{C}\ell(r) = \{grg^{-1} \mid g \in D_n\}$, fissato $g \in D_n$ abbiamo due possibili valori per grg^{-1}:

- se $g \in \mathcal{R}$ allora g è una potenza di r, pertanto i due elementi commutano e si ha $grg^{-1} = r$;
- se $g \notin \mathcal{R}$ allora $g = sr^h$ con $h \in \mathbb{Z}$, quindi

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

cioè $\mathcal{C}\ell(r) = \{r, r^{-1}\}$. In modo analogo si mostra che $\mathcal{C}\ell(r^k) = \{r^k, r^{-k}\}$ per ogni $k \in \mathbb{Z}$.

Osservazione 1.25 — Se n è pari, scriviamo $n = 2m$ e consideriamo la classe di coniugio di r^m. Poiché $r^m \neq e$ e $r^{2m} = (r^m)^2 = e$ abbiamo che $\operatorname{ord}(r^m) = 2$, cioè $(r^m)^{-1} = r^m$. Allora $\mathcal{C}\ell(r^m) = \{r^m\}$, pertanto abbiamo trovato un elemento del centro di D_n (infatti se G è un gruppo e $x \in G$, allora $x \in Z(G)$ se e solo se $\mathcal{C}\ell(x) = \{x\}$).

Consideriamo adesso la classe di coniugio di sr^h, $\mathcal{C}\ell(sr^h) = \{g(sr^h)g^{-1} \mid g \in D_n\}$, fissato $g \in D_n$ abbiamo due possibili valori per $g(sr^h)g^{-1}$:

- se $g \in \mathcal{R}$ allora $g = r^k$ con $k \in \mathbb{Z}$, pertanto

$$r^k(sr^h)r^{-k} = sr^{-k}r^h r^{-k} = sr^{h-2k}$$

- se $g \notin \mathcal{R}$ allora $g = sr^k$ con $k \in \mathbb{Z}$, pertanto

$$(sr^k)(sr^h)(sr^k)^{-1} = (sr^k)(sr^h)(sr^k) = sr^{2k-h}$$

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

Osservazione 1.26 — La classe di coniugio di sr^h contiene tutte le simmetrie in cui l'esponente di r ha la stessa parità di h. Se n è dispari tutte le simmetrie appartengono alla stessa classe, mentre se n è pari abbiamo due classi distinte: quella delle simmetrie rispetto agli assi passanti per i vertici opposti e quella delle simmetrie rispetto agli assi passanti per i lati.

§1.3.4 Legge di gruppo e omomorfismi

Se g è un elemento di D_n possiamo scrivere g in modo unico come $s^a r^b$ con $a \in \{0,1\}$ e $b \in \{0,\dots,n-1\}$, utilizziamo questa proprietà per esplicitare la legge di gruppo di D_n. Fissati $g_1, g_2 \in D_n$, scriviamo $g_1 = s^{a_1}r^{b_1}$ e $g_2 = s^{a_2}r^{b_2}$ con $a_1, a_2 \in \{0,1\}$ e $b \in \{0,\dots,n-1\}$,

$$g_1 g_2 = (s^{a_1}r^{b_1})(s^{a_2}r^{b_2}) = s^{a_1}s^{a_2}(s^{a_2}r^{b_1}s^{-a_2})r^{b_2} = s^{a_1}s^{a_2}\varphi_{s^{a_2}}(r^{b_1})r^{b_2}$$

dove $\varphi_{s^{a_2}}$ è l'automorfismo di coniugio per s^{a_2} (ricordiamo che $s^{a_2} = s^{-a_2}$). Poiché $\varphi_{s^{a_2}}$ è un omomorfismo e $\varphi_x \circ \varphi_y = \varphi_{xy}$ per ogni $x, y \in G$, abbiamo $(\varphi_{s^{a_2}}(r^{b_1})) = (\varphi_s^{a_2}(r))^{b_1}$, quindi

$$g_1 g_2 = s^{a_1} s^{a_2} (\varphi_s^{a_2}(r))^{b_1} r^{b_2} = s^{a_1+a_2} r^{(-1)^{a_2} b_1 + b_2}$$

Per l'unicità della scrittura che stiamo usando (scegliendo $a \in \{0, 1\}$ e $b \in \{0, \dots, n-1\}$)[4] possiamo identificare ogni elemento $g = s^a r^b \in D_n$ con la coppia (a, b), la legge di gruppo è quindi tale che

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

Usiamo il risultato appena ottenuto per descrivere gli omomorfismi da D_n in un qualsiasi gruppo G. Poiché ogni elemento $g \in D_n$ si scrive come $s^a r^b$, con $a, b \in \mathbb{Z}$, un omomorfismo $\varphi \in \mathrm{Hom}(D_n, G)$ è univocamente determinato da $\varphi(r)$ e $\varphi(s)$: infatti

$$\varphi(g) = \varphi(s^a r^b) = \varphi(s)^a \varphi(r)^b$$

Poniamo $x = \varphi(s)$, $y = \varphi(r)$, necessariamente $\mathrm{ord}(x) \mid 2$ e $\mathrm{ord}(y) \mid n$, cioè $x^2 = e_G$ e $y^n = e_G$, inoltre

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

Mostriamo che effettivamente queste condizioni sono anche sufficienti:

Proposizione 1.27
Dati un gruppo G e un'applicazione

$$\varphi : D_n \longrightarrow G : s^a r^b \longmapsto x^a y^b$$

dove $x = \varphi(s)$ e $y = \varphi(r)$, 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 $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ abbiamo

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

dove φ_g è l'automorfismo di coniugio per $g \in G$. Allora abbiamo che φ è un omomorfismo, infatti per ogni $h_1, h_2, k_1, k_2 \in \mathbb{Z}$

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

□

[4]Ricordiamo che $\varphi_s^m = \underbrace{\varphi_s \circ \dots \circ \varphi_s}_{m \text{ volte}}$ in quanto l'operazione del gruppo degli automorfismi è la composizione di funzioni.

Osservazione 1.28 — Abbiamo visto che le condizioni $D_n = \langle r, s\rangle$ con $\mathrm{ord}(r) = n$, $\mathrm{ord}(s) = 2$ e $srs^{-1} = r^{-1}$ determinano in modo univoco la struttura astratta di D_n, racchiudiamo queste proprietà fondamentali nella scrittura

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

Tale scrittura si chiama **presentazione di un gruppo** e ne determina in modo univoco la classe di isomorfismo. Senza scendere troppo nei dettagli, nella presentazione indichiamo un insieme di generatori minimale e il minor numero di proprietà che i generatori devono rispettare affinché il gruppo abbia la struttura desiderata. Altri esempi di presentazioni sono

$$\langle x \mid x^n = e\rangle$$

$$\langle x\rangle$$

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

rispettivamente dei gruppi $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (notiamo che $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e D_2 hanno la stessa presentazione, e questo ha senso in quanto i due gruppi sono isomorfi).

§1.3.5 Automorfismi

Studiamo separatamente gli automorfismi di D_n per $n \geqslant 3$ e di D_2.
Per $n \geqslant 3$ consideriamo $\varphi \in \mathrm{Aut}(D_n)$, poiché $D_n = \langle r, s\rangle$ è sufficiente studiare le immagini di r, s per determinare φ. Osserviamo che necessariamente $\varphi(r) = r^k$ con $(n, k) = 1$, infatti φ deve preservare l'ordine di r e la sua immagine deve essere un generatore di $\mathcal{R}$, in quanto $\mathcal{R}$ è caratteristico in D_n e isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Per quanto riguarda $\varphi(s)$, se n è dispari allora le simmetrie sono gli unici elementi di ordine 2, pertanto $\varphi(s) = sr^h$ con $0 \leq h < n$. Se n è pari abbiamo apparentemente due possibilità:

(1) $\varphi(s) = sr^h$, con $0 \leq h < n$;

(2) $\varphi(s) = r^{\frac{n}{2}}$, se n è pari.

D'altra parte, se fosse $\varphi(s) = r^{\frac{n}{2}}$ allora φ non sarebbe né iniettiva né surgettiva, pertanto $\varphi(s) = sr^h$ con $0 \leq h \leq n$. Verifichiamo che φ è un omomorfismo, per la caratterizzazione che abbiamo dato sopra 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 $r^k, sr^h \in \mathrm{Im}\varphi$, cioè

$$\langle r^k, sr^h\rangle = \langle r, sr^h\rangle = \langle s, r\rangle = D_n \subseteq \mathrm{Im}\varphi$$

da cui $\mathrm{Im}\varphi = D_n$. Poiché D_n è finito abbiamo che φ è un automorfismo. Gli automorfismi di $D_n = \langle r, s\rangle$ quindi sono tutti e soli gli omomorfismi da D_n in D_n che mandano r in un generatore di $\mathcal{R}$, che sono $\phi(n)$, e s in un'altra simmetria, che sono n, pertanto $|\mathrm{Aut}(D_n)| = n\phi(n)$.

Per $n = 2$, sappiamo che $D_2 \cong (\mathbb{Z}/2\mathbb{Z})^2$, pertanto

$$\mathrm{Aut}(D_2) \cong \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong S_3$$

Alternativamente possiamo considerare $(\mathbb{Z}/2\mathbb{Z})^2$ come spazio vettoriale su $\mathbb{F}_2$, pertanto abbiamo

$$\text{Aut}(D_2) \cong GL_2(\mathbb{F}_2)$$

Per quanto visto nella sezione (1.2), $GL_2(\mathbb{F}_2)$ contiene $(4-1)(4-2) = 6$ elementi, inoltre GL_2 non è un gruppo commutativo (con l'operazione di prodotto tra matrici), pertanto $GL_2(\mathbb{F}_2) \cong S_3$. In particolare, gli elementi di $GL_2(\mathbb{F}_2)$ sono:

- $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, che è l'identità del gruppo;
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, che sono gli elementi di ordine 2 corrispondenti alle trasposizioni;
- $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ che sono gli elementi di ordine 3 corrispondenti ai 3-cicli.

§1.4 Automorfismi di un prodotto diretto

Consideriamo due gruppi finiti H, K, studiamo il gruppo degli automorfismi di $H \times K$. Chiaramente esiste un'inclusione di $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ data dall'omomorfismo

$$\iota : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \hookrightarrow \mathrm{Aut}(H \times K) : (\varphi_1, \varphi_2) \longmapsto \varphi_1 \times \varphi_2$$

con

$$\varphi_1 \times \varphi_2 : H \times K \longrightarrow H \times K : (g_1, g_2) \longmapsto (\varphi_1(g_1), \varphi_2(g_2))$$

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

- per ogni $(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(g_1, g_2), (h_1, h_2) \in H \times K$ abbiamo

$$\begin{aligned}(\varphi_1 \times \varphi_2)((g_1, g_2)(h_1, h_2)) &= (\varphi_1(g_1h_1), \varphi_2(g_2h_2)) = (\varphi_1(g_1)\varphi_1(h_1), \varphi_2(g_2)\varphi_2(h_2)) = \\ &= (\varphi_1(g_1), \varphi_2(g_2))(\varphi_1(h_1), \varphi_2(h_2)) = ((\varphi_1 \times \varphi_2)(g_1, g_2))((\varphi_1 \times \varphi_2)(h_1, h_2))\end{aligned}$$

  cioè $\varphi_1 \times \varphi_2$ è un omomorfismo. Inoltre

$$\ker(\varphi_1 \times \varphi_2) = \{(g_1, g_2) \in H \times K \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K)\} = \{(e_H, e_K)\}$$

  quindi $\varphi_1 \times \varphi_2 \in \mathrm{Aut}(H \times K)$ in quanto $H \times K$ è finito, pertanto ι è ben definita;

- per ogni $(\varphi_1, \varphi_2), (\psi_1, \psi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(g_1, g_2) \in H \times K$ abbiamo

$$\begin{aligned}\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2))(g_1, g_2) &= \iota(\varphi_1\psi_1, \varphi_2\psi_2)(g_1, g_2) = (\varphi_1\psi_1 \times \varphi_2\psi_2)(g_1, g_2) = \\ &= (\varphi_1(\psi_1(g_1)), \varphi_2(\psi_2(g_2))) = (\varphi_1 \times \varphi_2)(\psi_1(g_1), \psi_2(g_2)) = \\ &= ((\varphi_1 \times \varphi_2)(\psi_1 \times \psi_2))(g_1, g_2) = (\iota(\varphi_1, \varphi_2)\iota(\psi_1, \psi_2))(g_1, g_2)\end{aligned}$$

  cioè $\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2)) = \iota(\varphi_1, \varphi_2)\iota(\psi_1, \psi_2)$, quindi ι è un omomorfismo;

- ι è iniettiva, infatti

$$\begin{aligned}\ker \iota &= \{(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid \iota(\varphi_1, \varphi_2) = id_{\mathrm{Aut}(H \times K)}\} = \\ &= \{(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid (\varphi_1(g_1), \varphi_2(g_2)) = (g_1, g_2)\ \forall (g_1, g_2) \in H \times K\} = \\ &= \{(id_{\mathrm{Aut}(H)}, id_{\mathrm{Aut}(K)})\} = \{id_{\mathrm{Aut}(H) \times \mathrm{Aut}(K)}\}\end{aligned}$$

Proposizione 1.29

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 ι è surgettiva allora ogni elemento di $\mathrm{Aut}(H \times K)$ può essere scritto come $\varphi_1 \times \varphi_2$ con $\varphi_1 \in \mathrm{Aut}(H)$ e $\varphi_2 \in \mathrm{Aut}(K)$. Allora abbiamo

$$(\varphi_1 \times \varphi_2)(H \times \{e_K\}) = (\varphi_1(H), \varphi_2(\{e_K\})) = H \times \{e_K\}$$

$$(\varphi_1 \times \varphi_2)(\{e_H\} \times K) = (\varphi_1(\{e_H\}), \varphi_2(K)) = \{e_H\} \times K$$

cioè $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$. Viceversa, se i due sottogruppi sono caratteristici, dato $\varphi \in \mathrm{Aut}(H \times K)$ poniamo $\varphi_1 \in \mathrm{Aut}(H)$ tale che $\varphi(g_1, e_K) = (\varphi_1(g_1), e_K)$ e $\varphi_2 \in \mathrm{Aut}(K)$ tale che $\varphi(e_H, g_2) = (e_H, \varphi_2(g_2))$ per ogni $g_1 \in H$, per ogni

$g_2 \in K$ (questo possiamo farlo in quanto $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici). Allora abbiamo

$$\begin{aligned}\varphi(g_1, g_2) = \varphi((g_1, e_K)(e_H, g_2)) = \varphi(g_1, e_K)\varphi(e_H, g_2) = \\ = (\varphi_1(g_1), e_K)(e_H, \varphi_2(g_2)) = (\varphi_1(g_1), \varphi_2(g_2)) = (\varphi_1 \times \varphi_2)(g_1, g_2)\end{aligned}$$

cioè ι è surgettiva e quindi un isomorfismo tra $\operatorname{Aut}(H) \times \operatorname{Aut}(K)$ e $\operatorname{Aut}(H \times K)$. □

Esempio 1.30

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, quindi l'immagine di un generatore è un altro generatore del sottogruppo. Poiché gli elementi di G di ordine finito sono tutti della forma $(0, d)$ abbiamo che $\varphi(\{0\} \times \mathbb{Z}/n\mathbb{Z}) = \{0\} \times \mathbb{Z}/n\mathbb{Z}$. Viceversa, l'immagine di φ su un generatore di $\mathbb{Z} \times \{0\}$, ad esempio $\varphi(1, 0)$, è della forma (a, b), e questo implica che $\mathbb{Z} \times \{0\}$ non è caratteristico. Se φ è surgettivo, necessariamente esiste $(x, y) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tale che $\varphi(x, y) = (\pm 1, 0)$, da cui, posti $\varphi(1, 0) = (a, b)$ e $\varphi(0, 1) = (0, d)$ con n e d coprimi, abbiamo

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

Viceversa, se $a = \pm 1$ allora 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 $y \equiv d^{-1}(y_0 - x_0 ab) \pmod{n}$ abbiamo

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

e questo ci permette di concludere che $\mathbb{Z} \times \{0\}$ non è un sottogruppo caratteristico. In questo caso abbiamo solo un'immersione del gruppo $\operatorname{Aut}(\mathbb{Z}) \times \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ dentro a $\operatorname{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$, in quanto gli automorfismi che mandano $(\pm 1, 0)$ in (a, b) con $a = \pm 1$ e $b \neq 0$ non possono essere ristretti ad automorfismi di $\mathbb{Z} \times \{0\}$.

È utile riuscire a determinare se i sottogruppi $H \times \{e_K\}$, $\{e_H\} \times K$ sono caratteristici in $H \times K$, da cui il seguente risultato:

Proposizione 1.31

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

$$S = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^n = (e_H, e_K)\}$$

Osserviamo che $H \times \{e_K\} = S$, infatti $H \times \{e_K\} \subseteq S$ in quanto tutti gli elementi di $H \times \{e_K\}$ hanno ordine che divide n. D'altra parte dato $(g_1, g_2) \in S$, se $\operatorname{ord}(g_1, g_2) \mid n$ allora $\operatorname{ord}(g_1) \mid n$ e $\operatorname{ord}(g_2) \mid n$, ma $\operatorname{ord}(g_2) \mid m$ per il Teorema di Lagrange, quindi $\operatorname{ord}(g_2) = 1$ e $S \subseteq H \times \{e_K\}$, da cui l'uguaglianza. Con un ragionamento analogo possiamo caratterizzare $\{e_H\} \times K$ come

$$\{e_H\} \times K = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^m = (e_H, e_K)\}$$

Poiché un automorfismo di $H \times K$ deve preservare gli ordini degli elementi, per la caratterizzazione data abbiamo che i due sottogruppi sono caratteristici. $\square$

Corollario 1.32

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

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

§1.5 Gruppo derivato

Definizione 1.33. Dati un gruppo G e x, y elementi di G, chiamiamo **commutatore** di x e y l'elemento $[x, y] = xyx^{-1}y^{-1}$. Chiamiamo **sottogruppo derivato** di G, oppure **sottogruppo dei commutatori** di G il sottogruppo

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

Osservazione 1.34 — $[x, y] = e$ se e solo se x e y commutano.

Proposizione 1.35
Dato un gruppo G, valgono i seguenti fatti:

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

(2) ${}^{G}\!/_{G'}$ è un gruppo abeliano;

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

Dimostrazione. Mostriamo le affermazioni singolarmente:

(1) consideriamo $\varphi \in \text{Aut}(G)$, poiché φ preserva la struttura di gruppo è sufficiente descrivere come φ agisce sui generatori di G' per determinare $\varphi(G')$. Fissati $x, y \in G$ abbiamo

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

pertanto $\varphi(G') \subseteq G'$, da cui l'uguaglianza in quanto φ è bigettiva;

(2) dati $x, y \in G$, $xG' \cdot yG' = yG' \cdot xG'$ se e solo se $xyG' = yxG'$, che è equivalente a richiedere $xyx^{-1}y^{-1} \in G'$. Dato che effettivamente $xyx^{-1}y^{-1} = [x, y]$ è un elemento di G' abbiamo che ${}^{G}\!/_{G'}$ è abeliano;

(3) dati $x, y \in G$, abbiamo

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

e questo coincide con l'identità di A in quanto A è abeliano. Poiché l'immagine di φ è un sottogruppo di A allora $G' \subseteq \ker \varphi$, in quanto il commutatore di ogni coppia di elementi di G è contenuto in $\ker \varphi$.

□

Osservazione 1.36 — Come conseguenza del Primo Teorema di Omomorfismo abbiamo che ${}^{G}\!/_{G'}$ è il "più grande" quoziente abeliano di G, o analogamente che G' è il "più piccolo" sottogruppo di G che produce un quoziente abeliano. In questo senso, G' misura quanto è abeliano il gruppo G.

Osservazione 1.37 — Dato A un gruppo abeliano, il Primo Teorema di Omomorfismo produce una bigezione naturale tra $\mathrm{Hom}(G, A)$ e $\mathrm{Hom}\left({}^{G}\!/\!_{G'}, A\right)$. Consideriamo infatti $\varphi \in \mathrm{Hom}(G, A)$, $\pi_{G'} : G \longrightarrow {}^{G}\!/\!_{G'}$ la proiezione al quoziente e $\overline{\varphi} : {}^{G}\!/\!_{G'} \longrightarrow A$, il Teorema fornisce un'unico omomorfismo $\overline{\varphi} : {}^{G}\!/\!_{G'} \longrightarrow A$ che rende commutativo il diagramma

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

Viceversa, dato un omomorfismo $\overline{\varphi} : {}^{G}\!/\!_{G'} \longrightarrow A$ otteniamo un'unico omomorfismo $\varphi : G \longrightarrow A$ con la composizione $\overline{\varphi} \circ \pi_{G'}$.

Esempio 1.38

Consideriamo il gruppo S_3, chiaramente $(S_3)' \neq \{id\}$ in quanto ${}^{S_3}\!/\!_{\langle id \rangle} \cong S_3$ che non è abeliano, pertanto abbiamo due possibilità: $(S_3)' = S_3$ oppure $(S_3)' = \langle (1\ 2\ 3) \rangle$[a]. D'altra parte ${}^{S_3}\!/\!_{\langle (1\ 2\ 3) \rangle}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, che è abeliano, pertanto $(S_3)'$ è contenuto in $\langle (1\ 2\ 3) \rangle$, da cui necessariamente $(S_3)' = \langle (1\ 2\ 3) \rangle$. Più in generale vedremo che $(S_n)' = \mathcal{A}_n$, dove $\mathcal{A}_n$ è il sottogruppo di S_n delle permutazioni pari (sappiamo già che $(S_n)' \subseteq \mathcal{A}_n$ in quanto ${}^{S_n}\!/\!_{\mathcal{A}_n} \cong \mathbb{Z}/2\mathbb{Z}$).

[a] Gli unici sottogruppi normali di S_3 sono $\{id\}$, $\langle (1\ 2\ 3) \rangle$, S_3.

§1.6 Azioni di gruppo

§1.6.1 Azioni transitive

Definizione 1.39. Siano G un gruppo e X un insieme, un'azione

$$\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g$$

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

Lemma 1.40

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

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

Dimostrazione. Poniamo $K = \bigcup_{g \in G} gHg^{-1}$, osserviamo che gli elementi della forma xHx^{-1} con $x \in N_G(H)$ contribuiscono una sola volta all'unione, in quanto $xHx^{-1} = H$, pertanto K è unione di $[G : N_G(H)] = \dfrac{|G|}{|N_G(H)|}$ elementi distinti[5]. Poiché $H \subseteq N_G(H)$ e $|gHg^{-1}| = |H|$ per ogni $g \in G$, possiamo stimare la cardinalità di K nel seguente modo

$$|K| \leq \frac{|G|}{|N_G(H)|}|H| \leq \frac{|G|}{|H|}|H| = |G|.$$

D'altra parte, per il Principio di Inclusione-Esclusione abbiamo che $|K|$ è somma delle cardinalità dei singoli termini dell'unione se e solo se l'unione è disgiunta, ma questo è falso in quanto ogni classe di coniugio di H contiene l'identità del gruppo, quindi $|K| < |G|$, cioè $G \neq K$. □

Proposizione 1.41

Dati un gruppo G e un insieme X, se

$$\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g$$

è un'azione transitiva valgono i seguenti fatti:

(1) per ogni $x, y \in X$ esiste $g \in G$ tale che $g\,\mathrm{St}(x)g^{-1} = \mathrm{St}(y)$;

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

Dimostrazione. Mostriamo i due fatti singolarmente:

[5] Infatti, se $X = \{N \mid N \leqslant G\}$ e φ è l'azione di coniugio su X, per ogni $N \in X$ abbiamo $\mathrm{St}(N) = N_G(N)$ e $\mathrm{Orb}(N) = \mathcal{C}\ell(N) = \{gNg^{-1} \mid g \in G\}$. Vale quindi la relazione $|G| = |\mathcal{C}\ell(N)| \cdot |N_G(N)|$.

(1) sia $g \in G$ tale che $\varphi_g(x) = y$, dato $h \in g\,\mathrm{St}(x)g^{-1}$ esiste $w \in \mathrm{St}(x)$ tale che $h = gwg^{-1}$. Allora

$$\varphi_h(y) = \varphi_{gwg^{-1}}(y) = \varphi_g(\varphi_w(\varphi_g^{-1}(y))) = \varphi_g(\varphi_w(x)) = \varphi_g(x) = y$$

pertanto $g\,\mathrm{St}(x)g^{-1} \subseteq \mathrm{St}(y)$. Osservando che $\varphi_{g^{-1}}(y) = x$ e ragionando in modo simmetrico otteniamo l'inclusione $g^{-1}\,\mathrm{St}(y)g \subseteq \mathrm{St}(x)$, da cui $g\,\mathrm{St}(x)g^{-1} = \mathrm{St}(y)$;

(2) un elemento $g \in G$ con tali proprietà non può essere contenuto nello stabilizzatore di nessun elemento di X, cioè cerchiamo $g \in G$ tale che

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

che è equivalente a

$$g \notin \bigcup_{x \in X} \mathrm{St}(x) = \bigcup_{h \in G} h\,\mathrm{St}(x_0)h^{-1}$$

per il fatto precedente, fissato $x_0 \in G$. Osserviamo che $\mathrm{St}(x_0) \neq G$, infatti se fosse $\mathrm{St}(x_0) = G$ avremmo

$$|\operatorname{Orb}(x_0)| = \frac{|G|}{|\operatorname{St}(x_0)|} = 1$$

ma questo è assurdo in quanto $\operatorname{Orb}(x_0) = X$ per la transitività di φ e $|X| \geqslant 2$. Allora per il Lemma 1.40 abbiamo

$$G \neq \bigcup_{h \in G} h\,\mathrm{St}(x_0)h^{-1}$$

pertanto esiste almeno un elemento $g \in G$ con la proprietà voluta.

□

Osservazione 1.42 — Se φ è l'azione di un gruppo G su un insieme X, restringendo φ all'orbita di un elemento $x \in X$ otteniamo per definizione un'azione transitiva su $\operatorname{Orb}(x)$. Pertanto gli stabilizzatori degli elementi di $\operatorname{Orb}(x)$ sono tra loro coniugati.

Proposizione 1.43

Dato G un gruppo finito e $H \lneq G$ un sottogruppo proprio, se $[G : H] = p$ con p 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

$$\psi : G \longrightarrow S\left(G/H\right) : g \longmapsto \psi_g$$

con

$$\psi_g : G/H \longrightarrow G/H : g'H \longmapsto gg'H$$

Poiché l'immagine di ψ è un sottogruppo di $S\left(G/H\right)$, che è isomorfo a S_p, abbiamo che $|\mathrm{Im}\psi| \mid p!$, inoltre $|\mathrm{Im}\psi| = \dfrac{|G|}{|\ker\psi|}$ come conseguenza del Primo Teorema di Omomorfismo. Pertanto $|\mathrm{Im}\psi| \mid (p!, |G|) = p$, in quanto p è il più piccolo primo che divide

$|G|$, quindi $|\mathrm{Im}\psi| \in \{1, p\}$. D'altra parte osserviamo che ψ è un'azione transitiva, infatti per ogni $g_1, g_2 \in G$ abbiamo $\psi_{g_2 g_1^{-1}}(g_1 H) = g_2 g_1^{-1} g_1 H = g_2 H$, pertanto non è possibile $\mathrm{Im}\psi = \{id\}$, da cui $|\mathrm{Im}\psi| = p$ e $[G : \ker \psi] = p$. Consideriamo il nucleo di ψ

$$\ker \psi = \{g \in G \mid gg'H = g'H \ \forall g' \in G\}$$

nel caso particolare $g' = e$ otteniamo l'inclusione

$$\ker \psi \subseteq \{g \in G \mid gH = H\} = H$$

in quanto stiamo indebolendo la condizione di appartenenza all'insieme. Poiché $[G : \ker \psi] = [G : H] = p$ e G è un gruppo finito abbiamo che effettivamente $\ker \psi = H$, cioè H è normale in G. $\square$

§1.6.2 Teorema di Cauchy e Piccolo Teorema di Fermat

Vediamo una dimostrazione alternativa del Teorema di Cauchy e del Piccolo Teorema di Fermat, di cui ricordiamo gli enunciati, che fa uso del concetto di azione.

Teorema 1.44 (Teorema di Cauchy)
Dato un gruppo G e un numero primo p, se $p \mid |G|$ allora esiste $g \in G$ tale che $\mathrm{ord}(g) = p$.

Teorema 1.45 (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 unicità dell'inverso). Definiamo un'azione di $\mathbb{Z}/p\mathbb{Z}$ su X nel seguente modo:

$$\psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow S(X) : a \longmapsto \psi_a$$

con

$$\psi_a : X \longrightarrow X : (g_1, \ldots, g_p) \longmapsto (g_{1+a}, \ldots, g_p, g_1, \ldots, g_a)$$

Fissato $x \in X$, poiché la cardinalità di $\mathrm{Orb}(x)$ divide l'ordine di $\mathbb{Z}/p\mathbb{Z}$ abbiamo che $|\mathrm{Orb}(x)| \in \{1, p\}$, in particolare le orbite di cardinalità 1 sono date dalle p-uple della forma $(g, \ldots, g)$ con $g^p = e$. Poniamo $S = \{g \in G \mid \mathrm{ord}(g) = p\}$ e $\mathcal{R}$ un insieme di rappresentanti per la relazione di equivalenza indotta da ψ, poiché le orbite degli elementi di X formano una partizione dell'insieme abbiamo

$$|G|^{p-1} = |X| = \sum_{x \in \mathcal{R}} |\mathrm{Orb}(x)| = 1 + |S| + \sum_{x \in \mathcal{R} \setminus S} |\mathrm{Orb}(x)|$$

dove l'ultimo termine della somma è divisibile per p. Distinguiamo quindi due casi:

- se $p \mid |G|$, riducendo modulo p la formula sopra otteniamo $|S| \equiv -1 \pmod p$, in particolare 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 riducendo modulo p la formula sopra otteniamo $n^{p-1} \equiv 1 \pmod p$ (Piccolo Teorema di Fermat).

Esercizio 1.46. Mostrare che i gruppi di ordine 15 sono ciclici.

Soluzione. Sia G un gruppo di ordine 15, poiché 5 è un primo che divide $|G|$ esiste $h \in G$ tale che $\operatorname{ord}(h) = 5$ per il Teorema di Cauchy. Inoltre, posto $H = \langle h \rangle$, abbiamo che $[G : H] = 3$ e quindi, dato che 3 è il più piccolo primo che divide $|G|$, H è un sottogruppo normale di G. Mostriamo che $H \subseteq Z(G)$, questo è equivalente a richiedere che l'omomorfismo

$$\varphi : G \longrightarrow \operatorname{Aut}(H) : g \longmapsto \varphi_{g|H}$$

dove φ_g è il coniugio per g, abbia come unico elemento dell'immagine l'applicazione

$$id_H : H \longrightarrow H : h \longmapsto h$$

Poiché $H \cong \mathbb{Z}/5\mathbb{Z}$, abbiamo $\operatorname{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$, d'altra parte $|\operatorname{Im}\varphi_{|H}|$ divide $(|G|, |\operatorname{Aut}(H)|) = 1$, pertanto $|\operatorname{Im}\varphi| = 1$ e l'omomorfismo è banale, cioè $H \subseteq Z(G)$. Diamo adesso due modi per concludere l'esercizio:

(1) osserviamo che se G è un gruppo abeliano, cioè se $Z(G) = G$, allora abbiamo che G è ciclico. Infatti posto $k \in G$ un elemento di ordine 3 (che esiste in virtù del Teorema di Cauchy), abbiamo che $\operatorname{ord}(hk) = \operatorname{ord}(h)\operatorname{ord}(k) = 15$ in quanto i due elementi hanno ordine coprimo. D'altra parte, se G non fosse abeliano allora avremmo necessariamente $Z(G) = H$, quindi ${}^{G}/_{Z(G)}$ sarebbe ciclico in quanto di ordine 3, pertanto G sarebbe un gruppo abeliano, da cui la tesi per quanto appena detto;

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

$$Z_G(k) = \{x \in G \mid xk = kx\}$$

Osserviamo che $k \in Z_G(k)$ e $Z(G) \subseteq Z_G(k)$, pertanto h è un elemento di $Z_G(k)$. Abbiamo quindi che $\operatorname{ord}(h) \mid |Z_G(k)|$ e $\operatorname{ord}(k) \mid |Z_G(k)|$, da cui $|Z_G(k)| = 15$. Abbiamo che tutti gli elementi di ordine 3 sono contenuti nel centro di G, che quindi coincide con G. Allora G è ciclico in quanto abeliano e contenente un elemento di ordine 3 e uno di ordine 5, quindi uno di ordine 15.

□

Osservazione 1.47 — In generale dati $x, y \in G$, se x e y commutano allora $\operatorname{ord}(xy) = [\operatorname{ord}(x), \operatorname{ord}(y)]$ anche se G non è un gruppo abeliano.

Esercizio 1.48. Dato d un numero dispari, mostrare che ogni gruppo di ordine $2d$ ammette un sottogruppo normale di indice 2.

Soluzione. Consideriamo la rappresentazione regolare a sinistra di G

$$\lambda : G \longrightarrow S(G) : g \longmapsto \lambda_g$$

con

$$\lambda_g : G \longrightarrow G : x \longmapsto gx$$

Fissato un isomorfismo $\psi : S(G) \longrightarrow S_{2d}$ poniamo $\varphi = \psi \circ \lambda : G \longrightarrow S_{2d}$, φ è un omomorfismo iniettivo (infatti nella dimostrazione del Teorema di Cayley abbiamo visto che λ è un omomorfismo iniettivo). Consideriamo il sottogruppo $\varphi^{-1}(\mathcal{A}_{2d})$, mostriamo che il suo indice in G è al più 2: posta $\pi_{\mathcal{A}_{2d}}$ la proiezione al quoziente

$$\pi_{\mathcal{A}_{2d}} : G \longrightarrow {S_{2d}}/{\mathcal{A}_{2d}} \cong \mathbb{Z}/2\mathbb{Z}$$

possiamo caratterizzare $\varphi^{-1}(\mathcal{A}_{2d})$ come

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

pertanto $\varphi^{-1}(\mathcal{A}_{2d}) \trianglelefteq G$. Per il Primo Teorema di Omomorfismo abbiamo che esiste un omomorfismo iniettivo da ${G}/{\ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)}$ in $\mathbb{Z}/2\mathbb{Z}$, da cui $[G : \ker(\pi_{\mathcal{A}_{2d}})] \leq 2$. Tale sottogruppo ha indice 1 se e solo se $G = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$, cioè $\varphi(G) \subseteq \mathcal{A}_{2d}$, mostriamo che in effetti esiste un elemento di G la cui immagine tramite φ è una permutazione dispari. Consideriamo $g \in G$ un elemento di ordine 2, poiché φ è un omomorfismo iniettivo abbiamo che $\operatorname{ord}(\varphi(g)) = \operatorname{ord}(g) = 2$, pertanto la permutazione $\varphi(g)$ ha una decomposizione in d 2-cicli, cioè è dispari. Pertanto $G \neq \varphi^{-1}(\mathcal{A}_{2d})$, da cui $[G : \varphi^{-1}(\mathcal{A}_{2d})] = 2$, □

Possiamo generalizzare il ragionamento appena usato nel seguente risultato

Proposizione 1.49

Dato un gruppo G e $H \lneq G$ un sottogruppo tale che $[G : H] = 2$, se K è un sottogruppo di G allora $H \cap K$ ha indice 1 o 2 in K, cioè $[K : H \cap K] \in \{1, 2\}$.

Dimostrazione. Distinguiamo due casi:

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

$$\pi_H : G \longrightarrow {G}/{H} : g \longmapsto gH$$

  Poiché ${G}/{H} \cong \mathbb{Z}/2\mathbb{Z}$ abbiamo che gli unici sottogruppi del quoziente sono $\{H\}$ e ${G}/{H}$, pertanto $\pi_H(K) = {G}/{H}$. Osserviamo che $\ker \pi_{H|K} = \ker \pi_H \cap K$, per il Primo Teorema di Omomorfismo allora ${K}/{H \cap K} \cong \mathbb{Z}/2\mathbb{Z}$, cioè $[K : H \cap K] = 2$.

□

§1.6.3 Teorema di Poincaré

Vediamo un risultato che sarà utile nel futuro, che permette di esibire, se esistono, sottogruppi normali non banali di un gruppo finito.

Teorema 1.50 (Teorema di Poincaré)

Dato un gruppo G finito e $H \leqslant G$ un suo sottogruppo, se $[G : H] = n$ allora esiste un sottogruppo normale $N \triangleleft G$ tale che:

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

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

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

$$\psi : G \longrightarrow S\left({}^{G}\!/\!{}_{H}\right) : g \longmapsto \psi_g$$

con

$$\psi_g : {}^{G}\!/\!{}_{H} \longrightarrow {}^{G}\!/\!{}_{H} : g'H \longmapsto gg'H$$

(1) Consideriamo il nucleo di ψ

$$\ker\psi = \{g \in G \mid gg'H = g'H \ \forall g' \in G\}$$

nel caso particolare $g' = e$ otteniamo l'inclusione

$$\ker\psi \subseteq \{g \in G \mid gH = H\} = H$$

in quanto stiamo indebolendo la condizione di appartenenza all'insieme, pertanto $\ker\psi \leqslant H$;

(2) poiché $\ker\psi \leqslant H$ abbiamo $[G : H] \mid [G : \ker\psi]$, cioè $n \mid [G : \ker\psi]$. Dal Primo Teorema di Omomorfismo abbiamo che ${}^{G}\!/\!{}_{\ker\psi} \cong \mathrm{Im}\psi$, che è un sottogruppo di $S\left({}^{G}\!/\!{}_{H}\right) \cong S_n$, pertanto $[G : \ker\psi] \mid n!$.

Poiché $\ker\psi$ è normale in G abbiamo che $N = \ker\psi$ è un sottogruppo con le proprietà cercate. $\square$

Osservazione 1.51 — In particolare, se G ha un sottogruppo di indice n e $n! < |G|$ allora G ammette sottogruppi normali non banali.

§1.7 Gruppo simmetrico

§1.7.1 Generatori di S_n

Esibiamo alcuni insiemi di generatori per S_n:

- $\{(i\ j) \mid i, j \in \{1, \dots, n\}, i < j\}$, abbiamo visto che ogni permutazione può essere scritta come prodotto di trasposizioni;
- $\{(1\ j) \mid j \in \{2, \dots, n\}\}$, infatti per ogni $i < j$ abbiamo
$$(i\ j) = (1\ i)(1\ j)(1\ i)$$
- $\{(i\ i+1) \mid i \in \{1, \dots, n-1\}\}$, infatti per ogni j abbiamo
$$(1\ j) = (j-1\ j)(1\ j-1)(j-1\ j)$$
- $\{(1\ 2), (1\ 2\ \dots\ n)\}$, infatti per ogni i abbiamo
$$(i\ i+1) = (1\ \dots\ n)^{i-1}(1\ 2)(1\ \dots\ n)^{1-i}$$

Osservazione 1.52 — Non è vero in generale che una trasposizione e un n-ciclo generano S_n, consideriamo ad esempio $\langle \sigma, \rho \rangle \leqslant S_4$ con $\sigma = (1\ 2\ 3\ 4)$, $\rho = (2\ 4)$. Abbiamo $\sigma^4 = \rho^2 = 1$ e $\rho\sigma\rho^{-1} = (1\ 4\ 3\ 2) = \sigma^{-1}$, pertanto $\langle \sigma, \rho \rangle$ è isomorfo a un quoziente di D_4. D'altra parte $\langle \sigma \rangle \cap \langle \rho \rangle = \{id\}$ e $\rho \in N_{S_4}(\sigma)$, pertanto $\langle \sigma, \rho \rangle = \langle \sigma \rangle \langle \rho \rangle$ e $|\langle \sigma, \rho \rangle| = 8$, pertanto è isomorfo a D_4.

§1.7.2 Sottogruppi abeliani massimali di S_n

Vogliamo studiare i sottogruppi abeliani di S_n, caratterizzando in particolare i suoi sottogruppi abeliani massimali.

Definizione 1.53. Un sottogruppo $G \leqslant S_n$ si dice **transitivo** se l'azione
$$\varphi : G \longrightarrow S_n : \sigma \longmapsto \sigma$$
indotta da G su $\{1, \dots, n\}$ è transitiva, cioè se per ogni $i, j \in \{1, \dots, n\}$ esiste $\sigma \in G$ tale che $\sigma(i) = j$.

Lemma 1.54
Dato G un sottogruppo abeliano di S_n, se G è transitivo allora $|G| = n$.

Dimostrazione. Consideriamo l'azione di G su $\{1, \dots, n\}$
$$\psi : G \longrightarrow S_n : \sigma \longmapsto \sigma$$
poiché G è transitivo, per la Proposizione 1.41 gli stabilizzatori degli elementi di $\{1, \dots, n\}$ sono tra loro coniugati. D'altra parte, poiché lo stabilizzatore è un sottogruppo di G, che è un gruppo abeliano, la restrizione del coniugio agli stabilizzatori coincide con l'applicazione identità, da cui $\mathrm{St}(i) = \mathrm{St}(j)$ per ogni $i, j \in \{1, \dots, n\}$. Osserviamo infine che
$$\bigcap_{i=1}^{n} \mathrm{St}(i) = \{id_{S_n}\}$$

in quanto id_{S_n} è l'unica permutazione che fissa tutti gli elementi di $\{1,\dots,n\}$, pertanto $\mathrm{St}(i) = \{id_{S_n}\}$ per ogni $i \in \{1,\dots,n\}$. Fissato $i \in \{1,\dots,n\}$, abbiamo

$$|G| = |\operatorname{Orb}(i)| \cdot |\operatorname{St}(i)| = |\operatorname{Orb}(i)| = n$$

in quanto G è transitivo. $\square$

Lemma 1.55

Se $a_1,\dots,a_k$ 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 $i \in \{1,\dots,k\}$.

Dimostrazione. Senza perdita di generalità, a meno di aumentare k possiamo supporre $a_i \in \{1,2,3\}$ per ogni $i \in \{1,\dots,k\}$, 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 $i \in \{1,\dots,n\}$, 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 $i \in \{1,\dots,k\}$ in quanto possiamo supporre $a_i \in \{1,2,3\}$ senza perdita di generalità. $\square$

Lemma 1.56

Dati $\sigma,\tau \in S_n$, se $\sigma = (x_1\ \dots\ x_k)$ è un k-ciclo allora

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

Dimostrazione.

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

per ogni $i \in \{1,\dots,k\}$, pertanto

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

$\square$

Esercizio 1.57. Posto $n = 3m$, mostrare che la massima cardinalità di un sottogruppo abeliano di S_n è 3^m e caratterizzare la sua classe di isomorfismo.

Soluzione. Per prima cosa, osserviamo che 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 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 S_n di ordine massimo, data

$$\psi : G \longrightarrow S_n : \sigma \longmapsto \sigma$$

l'azione naturale di G su $\{1, \ldots, n\}$ chiamiamo $\Omega_1, \ldots, \Omega_k$ le orbite. Consideriamo le mappe $\varphi_i : G \longrightarrow S(\Omega_i)$ 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 $G_i = \mathrm{Im}\varphi_i = \mathrm{Im}\psi \cap S(\Omega_i)$. 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

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

per ogni $i \in \{1, \ldots, k\}$, che è equivalente a $\sigma = id_{S_n}$ dato che le orbite ricoprono $\{1, \ldots, n\}$, da cui $\ker \varphi = \{id_{S_n}\}$. 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 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 1.58 — 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 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 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 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 1.59 — I sottogruppi di 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 S_n di ordine massimo (per semplicità supponiamo $n = 3m$, gli altri due casi si studiano in modo analogo) consideriamo $\sigma \in S_n$ 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.

§1.7.3 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 $\mathcal{C}\ell_{S_n}(\sigma)$. Poiché valgono $|\mathcal{A}_n| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| \cdot |Z_{\mathcal{A}_n}(\sigma)|$ e $Z_{\mathcal{A}_n}(\sigma) = Z_{S_n}(\sigma) \cap \mathcal{A}_n$, abbiamo

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{|\mathcal{A}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2}\frac{|S_n|}{|Z_{S_n}(\sigma) \cap \mathcal{A}_n|}$$

Dato che $[S_n : \mathcal{A}_n] = 2$, per la Proposizione 1.49 abbiamo $[Z_{S_n}(\sigma) : Z_{S_n}(\sigma) \cap \mathcal{A}_n] \in \{1, 2\}$, distinguiamo quindi due casi:

- $|Z_{S_n}(\sigma) \cap \mathcal{A}_n| = \frac{1}{2}|Z_{S_n}(\sigma)|$;
- $|Z_{S_n}(\sigma) \cap \mathcal{A}_n| = |Z_{S_n}(\sigma)|$.

Nel primo caso otteniamo

$$|\mathcal{C}\ell_{\mathcal{A}_n}| = \frac{1}{2}\frac{|S_n|}{|Z_{S_n}(\sigma) \cap \mathcal{A}_n|} = \frac{|S_n|}{|Z_{S_n}(\sigma)|} = |\mathcal{C}\ell_{S_n}(\sigma)|$$

poiché $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \subseteq \mathcal{C}\ell_{S_n}(\sigma)$ abbiamo che le due classi coincidono. In particolare questo succede se $Z_{S_n}(\sigma) \nsubseteq \mathcal{A}_n$.

Nel secondo caso invece, che si verifica se $Z_{S_n}(\sigma) \subseteq \mathcal{A}_n$,

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{1}{2}\frac{|S_n|}{|Z_{S_n}(\sigma) \cap \mathcal{A}_n|} = \frac{1}{2}\frac{|S_n|}{|Z_{S_n}(\sigma)|} = \frac{1}{2}|\mathcal{C}\ell_{S_n}(\sigma)|$$

Più precisamente, abbiamo $\mathcal{C}\ell_{S_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$ per ogni τ permutazione dispari. Infatti $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1}) \subseteq \mathcal{C}\ell_{S_n}(\sigma)$ (i coniugati di $\tau\sigma\tau^{-1}$ sono anche coniugati di σ), d'altra parte per ogni $\rho \in S_n$ abbiamo $\rho\sigma\rho^{-1} \in \mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$ 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, da cui l'uguaglianza. Abbiamo altri due casi:

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

Tuttavia se fosse $|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1})|$ avremmo $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$, che è assurdo in quanto $\tau\sigma\tau^{-1} \notin \mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$, pertanto

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

Poiché $|\mathcal{C}\ell_{S_n}(\sigma)| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| + |\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})|$, per il Principio di Inclusione-Esclusione abbiamo che l'unione è disgiunta, cioè

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

§1.7.4 Studio di S_5

Consideriamo gli elementi di S_5 $\sigma = (1\ 2\ 3\ 4\ 5), \tau = (2\ 5)(3\ 4)$, studiamo il sottogruppo $H = \langle \sigma, \tau \rangle$, in particolare siamo interessati a determinare una regola di commutazione per σ e τ. Osserviamo che

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

e che questo coincide con σ^{-1}. Abbiamo quindi che H è generato da un elemento τ di ordine 2 e da un elemento σ di ordine 5 che soddisfano la relazione $\tau\sigma\tau^{-1} = \sigma^{-1}$, pertanto H è isomorfo a un sottogruppo del gruppo diedrale D_5. D'altra parte, da questa relazione ricaviamo che $\langle \tau \rangle \subseteq N_{S_5}(\langle \sigma \rangle)$, pertanto possiamo scrivere $H = \langle \sigma \rangle \cdot \langle \tau \rangle$ in quanto $\langle \sigma \rangle \cdot \langle \tau \rangle$ è un sottogruppo di H che ha la sua stessa cardinalità. In particolare otteniamo che $|H| = 10 = |D_5|$, quindi $H \cong D_5$.

Abbiamo visto che le classi di coniugio in un gruppo simmetrico su n elementi sono parametrizzate dalle partizioni di n

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

(Nel calcolo della cardinalità della classe associata alla partizione 2 + 2 + 1 dividiamo per 2 in quanto contiamo i cicli a meno dell'ordine, e le coppie di trasposizioni che stiamo considerando commutano). Di queste, le permutazioni che appartengono a $\mathcal{A}_5$ sono quelle la cui classe di coniugio è associata alle partizioni 5, 3 + 1 + 1, 2 + 2 + 1, 1 + 1 + 1 + 1 + 1, cioè le permutazioni σ, τ, ρ aventi una decomposizione in cicli disgiunti della forma

$$\sigma = (a_1\ a_2\ a_3\ a_4\ a_5)$$

$$\tau = (b_1\ b_2\ b_3)$$

$$\rho = (c_1\ c_2)(d_1\ d_2)$$

e l'identità. Vediamo come sono fatte le loro classi di coniugio in $\mathcal{A}_5$. Chiaramente $\mathcal{C}\ell_{\mathcal{A}_n}(id) = \mathcal{C}\ell_{S_n}(id) = \{id\}$, studiamo quindi le classi di σ, τ, ρ fissate come sopra.

- $Z_{S_5}(\sigma) = \langle (a_1\ a_2\ a_3\ a_4\ a_5) \rangle$, infatti

  $$|Z_{S_5}(\sigma)| = \frac{|S_5|}{|\mathcal{C}\ell_{S_5}(\sigma)|} = \frac{5!}{4!} = 5$$

  Allora $Z_{S_5}(\sigma)$ contiene solo permutazioni pari, fissata ψ una permutazione dispari la sua classe di coniugio in S_5 si scrive come

  $$\mathcal{C}\ell_{S_5}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_5}(\sigma) \sqcup \mathcal{C}\ell_{\mathcal{A}_5}(\psi\sigma\psi^{-1})$$

- $Z_{S_5}(\tau)$ non è contenuto in $\mathcal{A}_5$, infatti una trasposizione ψ disgiunta da τ è una permutazione dispari che appartiene al centralizzatore. Pertanto

  $$\mathcal{C}\ell_{S_5}(\tau) = \mathcal{C}\ell_{\mathcal{A}_5}(\tau)$$

- $Z_{S_5}(\rho)$ non è contenuto in $\mathcal{A}_5$, infatti la trasposizione $(c_1\ c_2)$ è una permutazione dispari che commuta con ρ (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

  $$\mathcal{C}\ell_{S_5}(\rho) = \mathcal{C}\ell_{\mathcal{A}_5}(\rho)$$

§1.7.5 Sottogruppi normali di $\mathcal{A}_n$

Esibiamo alcuni insiemi di generatori per $\mathcal{A}_n$:

- $\{(i\ j)(k\ l) \mid i \neq j, k \neq l\}$, infatti ogni elemento di $\mathcal{A}_n$ può essere scritto come prodotto di coppie di trasposizioni in quanto permutazione pari;
- $\{(i\ j\ k) \mid i, j, k \text{ distinti}\}$. Infatti se $\{i, j\} = \{k, l\}$ allora $(i\ j)(k\ l) = id$ è un elemento generato dall'insieme, se invece $|\{i, j\} \cap \{k, l\}| = 1$, ad esempio $j = k$, abbiamo $(i\ j)(k\ l) = (i\ j)(j\ l) = (i\ j\ l)$, che è un elemento generato dall'insieme. Nel caso $\{i, j\} \cap \{k, l\} = \emptyset$ abbiamo $(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ j\ k)(j\ k\ l)$, che è un elemento generato dall'insieme. Possiamo quindi ottenere il precedente insieme di generatori a partire da questo;

Definizione 1.60. Un gruppo non banale G si dice **semplice** se i suoi unici sottogruppi normali sono $\{e\}$ e G.

Proposizione 1.61

$\mathcal{A}_5$ è un gruppo semplice.

Dimostrazione. Ricordiamo le cardinalità delle classi di coniugio in $\mathcal{A}_5$:

Rappresentante della classe	Cardinalità della classe
$(1\ 2\ 3\ 4\ 5)$	12
$(2\ 1\ 3\ 4\ 5)$	12
$(1\ 2)(3\ 4)$	15
$(1\ 2\ 3)$	20
id	1

In generale, un sottogruppo è normale se e solo se è unione disgiunta delle classi di coniugio dei suoi elementi, quindi la cardinalità di $N \trianglelefteq \mathcal{A}_5$ deve essere somma di alcuni termini nella seconda colonna, compreso 1. D'altra parte $|N| \mid |\mathcal{A}_5| = 60$, da cui $|N| = 1$ oppure $|N| = 60$. Pertanto $\mathcal{A}_5$ è semplice. $\square$

Lemma 1.62

Dati un gruppo G e $N \trianglelefteq G$ un sottogruppo normale di indice finito, N contiene ogni elemento di G il cui ordine è coprimo con $[G : N]$.

Dimostrazione. Sia $g \in G$ tale che $(\operatorname{ord}(g), [G : N]) = 1$, consideriamo la proiezione

$$\pi_N : G \longrightarrow {}^{G}\!/_{N} (x \longmapsto xN)$$

Poiché π_N è un omomorfismo abbiamo $\operatorname{ord}(\pi_N(g)) \mid (\operatorname{ord}(g), [G : N]) = 1$, pertanto $\pi_N(g) = N$, cioè $g \in N$. $\square$

Diamo adesso una dimostrazione alternativa della semplicità di $\mathcal{A}_5$.

Dimostrazione. Consideriamo un sottogruppo normale $N \trianglelefteqslant \mathcal{A}_5$. Distinguiamo tre casi:

- se $2 \nmid [\mathcal{A}_5 : N]$, per il Lemma 1.62 N contiene tutti gli elementi di $\mathcal{A}_5$ di ordine 2, cioè le permutazioni della forma $(a\ b)(c\ d)$ con $a \neq b$ e $c \neq d$, da cui $N = \mathcal{A}_5$ in quanto contiene un suo insieme di generatori;
- se $3 \nmid [\mathcal{A}_5 : N]$, per il Lemma 1.62 N contiene tutti gli elementi di $\mathcal{A}_5$ di ordine 3, cioè i 3-cicli, da cui $N = \mathcal{A}_5$ in quanto contiene un suo insieme di generatori;
- se $6 \mid [\mathcal{A}_5 : N]$ allora $|N| \mid 10$, ma l'unica classe di coniugio di $\mathcal{A}_5$ di cardinalità minore di 10 è $\{id\}$, pertanto $N = \{id\}$.

Quindi $\mathcal{A}_5$ è semplice. $\square$

In effetti vale un risultato più generale

Proposizione 1.63

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

Dimostrazione. Procediamo per induzione su n, per $n = 5$ la tesi è garantita dalla Proposizione 1.61, supponiamo quindi che $\mathcal{A}_n$ sia un gruppo semplice e mostriamo che anche $\mathcal{A}_{n+1}$ lo è. Consideriamo un sottogruppo normale $N \trianglelefteqslant \mathcal{A}_{n+1}$ e i sottogruppi

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

questi sono tutti isomorfi a $\mathcal{A}_n$ (infatti gli elementi di H_i sono tutte e sole le permutazioni pari su $n+1$ elementi che fissano l'i-esimo, cioè sono permutazioni pari su n elementi). Notiamo che l'azione naturale di $\mathcal{A}_{n+1}$ su $\{1, \ldots, n+1\}$

$$\psi : \mathcal{A}_{n+1} \longrightarrow S_{n+1} : \sigma \longmapsto \sigma$$

è transitiva, infatti per $i, j \in \{1, \ldots, n+1\}$ distinti la permutazione pari $\rho = (i\ j)(h\ k)$, con $(i\ j)$ disgiunta da $(h\ k)$, è tale che $\rho(i) = j$. Per costruzione vale $\mathrm{St}(i) = H_i$ per ogni $i \in \{1, \ldots, n+1\}$, pertanto per la Proposizione 1.41 abbiamo che gli H_i sono tutti coniugati.
Fissato $i \in \{1, \ldots, n+1\}$, consideriamo $N \cap H_i$: questo è un sottogruppo normale di H_i, infatti per ogni $h \in H_i$ si ha $h(N \cap H_i)h^{-1} = N \cap H_i$ in quanto N è normale in $\mathcal{A}_{n+1}$ e $h \in H_i$, d'altra parte $H_i \cong \mathcal{A}_n$ è un gruppo semplice per ipotesi induttiva, pertanto $N \cap H_i$ coincide con $\{id\}$ oppure con H_i.
Se $N \cap H_i = H_i$ allora $H_i \subseteq N$, pertanto N contiene almeno un 3-ciclo $(i\ j\ k)$ e tutti i suoi coniugati in $\mathcal{A}_{n+1}$. Notiamo che una trasposizione $(a\ b)$ disgiunta da $(i\ j\ k)$ (che esiste in quanto $n \geq 5$) è una permutazione dispari in $Z_{S_{n+1}}((i\ j\ k))$, pertanto $\mathcal{C}\ell_{\mathcal{A}_{n+1}}((i\ j\ k)) = \mathcal{C}\ell_{S_{n+1}}((i\ j\ k))$ e N contiene l'insieme dei 3-cicli di S_{n+1}, quindi $N = \mathcal{A}_{n+1}$ dal momento che contiene un suo insieme di generatori.
Altrimenti $N \cap H_i = \{id\}$ per ogni $i \in \{1, \ldots, n+1\}$, cioè l'unico elemento di N avente almeno un punto fisso è l'identità, vogliamo mostrare che in effetti $N = \{id\}$. Osserviamo che se $\sigma \in N$ ha una decomposizione in cicli disgiunti della forma

$$\sigma = (x_1^{(1)}\ \ldots\ x_{l_1}^{(1)}) \ldots (x_1^{(k)}\ \ldots\ x_{l_k}^{(k)})$$

con $l_1 \leqslant l_2 \leqslant \ldots \leqslant l_k$, allora i suoi cicli hanno tutti la stessa lunghezza, cioè $l_i = l_j$ per ogni $i \neq j$. Infatti, posto $r = \min\{l_i \mid 1 \leqslant i \leqslant k\} = l_1$, abbiamo

$$\sigma^{l_1} = id \cdot (x_1^{(2)}\ \ldots\ x_{l_2}^{(2)})^{l_1} \ldots (x_1^{(k)}\ \ldots\ x_{l_k}^{(k)})^{l_1}$$

da cui $\sigma^{l_1} = id$ in quanto ha almeno un punto fisso e quindi $l_1 = l_2 = \ldots = l_k$. Fissata $\sigma \in N$ possiamo quindi scrivere $\sigma = \sigma_1 \ldots \sigma_k$, dove σ_i sono l-cicli disgiunti con $l = \dfrac{n+1}{k}$. Supponiamo per assurdo $N \cap H_i \neq \{id\}$, distinguiamo tre casi:

- se $k = 1$ abbiamo $l = n + 1$, cioè σ è un $n + 1$-ciclo. Scriviamo $\sigma = (a_1 \ \ldots \ a_l)$ e consideriamo la permutazione pari $\tau = (a_1 \ a_2)(a_3 \ a_4)$, poiché N è normale in $\mathcal{A}_{n+1}$ contiene
$$\tau\sigma\tau^{-1} = (a_2 \ a_1 \ a_4 \ a_3 \ a_5 \ a_6 \ \ldots \ a_l)$$
Consideriamo $\rho = (\tau\sigma\tau^{-1})\sigma \in N$, notiamo che $\rho \neq id$ in quanto
$$\rho(a_4) = (\tau\sigma\tau^{-1})(\sigma(a_4)) = (\tau\sigma\tau^{-1})(a_5) = a_6 \neq a_4$$
d'altra parte a_1 è un punto fisso per ρ, che è assurdo;
- se $k > 1$ e $l > 2$, poiché σ_1^{-1} è un l-ciclo disgiunto da $\sigma_2, \ldots, \sigma_k$ la permutazione $\rho = \sigma_1^{-1}\sigma_2 \ldots \sigma_k$ è un elemento di N. Consideriamo $\alpha = \rho\sigma \in N$, osserviamo che
$$\alpha = \sigma_2^2 \ldots \sigma_k^2 \neq id$$
in quanto $ord(\sigma_i) = l > 2$ per ogni $i \in \{1, \ldots, k\}$, tuttavia a_1 è un punto fisso per α, che è assurdo;
- se $k > 1$ e $l = 2$, scriviamo σ come prodotto di k trasposizioni disgiunte
$$\sigma = (a_1 \ b_1) \ldots (a_k \ b_k)$$
Consideriamo la permutazione pari $\tau = (a_1 \ a_2 \ b_1)$, poiché N è normale in $\mathcal{A}_{n+1}$ contiene
$$\rho = \tau\sigma\tau^{-1} = (a_2 \ a_1)(b_1 \ b_2)(a_3 \ b_3) \ldots (a_k \ b_k)$$
e anche la permutazione
$$\alpha = \rho\sigma = ((a_2 \ a_1)(b_1 \ b_2))((a_1 \ b_1)(a_2 \ b_2)) = (a_1 \ b_2)(a_2 \ b_1) \neq id$$
ma a_3 è un punto fisso per α, che è assurdo.

Pertanto $N \cap H_i = \{id\}$, cioè $\mathcal{A}_{n+1}$ è un gruppo semplice. $\square$

Corollario 1.64
L'insieme $X = \{\sigma \in S_n \mid \sigma \text{ è un 5-ciclo}\}$ genera $\mathcal{A}_n$ per $n \geqslant 5$.

Dimostrazione. Sia $\sigma \in X$ un 5-ciclo, per ogni $\tau \in \mathcal{A}_n$ abbiamo che $\tau\sigma\tau^{-1}$ è ancora un elemento di X, pertanto $\langle X \rangle$ è un sottogruppo normale di $\mathcal{A}_n$, da cui $\langle X \rangle = \mathcal{A}_n$ in quanto diverso da $\{id\}$. $\square$

§1.7.6 Sottogruppi normali di S_n

Lemma 1.65
Per $n \geq 3$ il centro di S_n è banale, cioè $Z(S_n) = \{id\}$.

Dimostrazione. Sia $\sigma \in Z(S_n) \setminus \{id\}$, allora esistono distinti $x, y \in \{1, \dots, n\}$ tali che $\sigma(x) = y$. Fissiamo $z \in \{1, \dots, n\} \setminus \{x, y\}$ e consideriamo la permutazione $\tau = (y\ z)$, abbiamo

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

che è assurdo in quanto $y \neq z$. Pertanto $Z(S_n) = \{id\}$. □

Proposizione 1.66

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

Dimostrazione. Sia N un sottogruppo normale di S_n, consideriamo $K = N \cap \mathcal{A}_n$. K è normale in $\mathcal{A}_n$, pertanto $K = \{id\}$ oppure $K = \mathcal{A}_n$, distinguiamo 2 casi:

- se $K = \mathcal{A}_n$ allora $\mathcal{A}_n \leqslant N$: per il Teorema di Corrispondenza i sottogruppi di S_n contenenti $\mathcal{A}_n$ sono in bigezione con i sottogruppi di ${}^{S_n}\!/_{\mathcal{A}_n} \cong \mathbb{Z}/2\mathbb{Z}$, pertanto $N = \mathcal{A}_n$ oppure $N = S_n$;

- se $K = \{id\}$, poiché $[S_n : \mathcal{A}_n] = 2$ per la Proposizione 1.49 vale $[N : K] \in \{1, 2\}$, da cui $|N| \leq 2$. Se $|N| = 1$ allora $N = \{id\}$, se $|N| = 2$ consideriamo l'azione di coniugio di $S_n = N_{S_n}(N)$ su N

  $$\varphi : N_{S_n}(N) \longrightarrow Aut(N) : g \longmapsto \varphi_g$$

  dove φ_g è la mappa

  $$\varphi_g : N \longrightarrow N : h \longmapsto ghg^{-1}$$

  il nucleo di φ coincide con $Z_{S_n}(N)$. Per il Primo Teorema di Omomorfismo allora abbiamo un omomorfismo iniettivo

  $$\psi : \frac{N_{S_n}(N)}{Z_{S_n}(N)} \hookrightarrow \mathrm{Aut}(N)$$

  Poiché $|N| = 2$ abbiamo $N \cong \mathbb{Z}/2\mathbb{Z}$, pertanto $\mathrm{Aut}(N) = \{id\}$. Dato che $N_{S_n}(N) = S_n$ per la normalità di N questo implica che sia $Z_{S_n}(N) = S_n$, cioè che $N \subseteq Z(S_n)$, ma questo è assurdo in quanto $Z(S_n) = \{id\}$ per il Lemma 1.65.

□

Osservazione 1.67 — L'enunciato è vero anche per $n = 3$ con la stessa dimostrazione, infatti $\mathcal{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ è un gruppo semplice, mentre per $n = 4$ è falso. Infatti $\mathcal{A}_4$ non è semplice, e il sottogruppo di Klein

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

è un suo sottogruppo normale non banale. Notiamo che V_4 è normale in S_4 in quanto unione delle classi di coniugio di tutti i suoi elementi.

§1.7.7 Sottogruppi isomorfi a S_{n-1}

[6]

Abbiamo osservato più volte che S_{n-1} si immerge naturalmente in S_n, vediamo adesso un risultato che generalizza questo fatto ad alcuni sottogruppi di S_n.

Proposizione 1.68

Dato un sottogruppo $H \leqslant S_n$ con $n \geq 5$, se $[S_n : H] = n$ allora H è isomorfo a S_{n-1}.

Dimostrazione. Consideriamo l'azione di moltiplicazione a sinistra di S_n sull'insieme quoziente ${}^{S_n}\!/_{H}$:

$$\varphi : S_n \longrightarrow S\left({}^{S_n}\!/_{H}\right) \cong S_n$$

tale azione è transitiva in quanto per ogni $\sigma, \rho \in S_n$ vale

$$\varphi(\sigma\rho^{-1})(\rho H) = \sigma\rho\rho^{-1}H = \sigma H$$

in particolare $\ker\varphi \neq S_n$. Poiché $\ker\varphi \trianglelefteq S_n$ allora il nucleo di φ è banale oppure è $\mathcal{A}_n$. D'altra parte se fosse $\ker\varphi = \mathcal{A}_n$ avremmo $|\mathrm{Im}\varphi| = 2$, pertanto l'orbita di ogni elemento di ${}^{S_n}\!/_{H}$ contiene al più due elementi, ma questo è assurdo in quanto per la transitività di φ si ha $\mathrm{Orb}(\rho H) = {}^{S_n}\!/_{H}$ per ogni $\rho \in S_n$, che contiene almeno 5 elementi. Pertanto $\ker\varphi = \{id\}$, cioè φ è un omomorfismo iniettivo e in particolare un isomorfismo. Notiamo che H è lo stabilizzatore della classe H, infatti

$$\mathrm{St}(H) = \{\sigma \in S_n \mid \sigma H = H\} = \{\sigma \in H\} = H$$

pertanto $\varphi(H)$ è lo stabilizzatore di un elemento di ${}^{S_n}\!/_{H}$ per l'azione naturale di $S\left({}^{S_n}\!/_{H}\right)$ su ${}^{S_n}\!/_{H}$. Tramite la corrispondenza tra ${}^{S_n}\!/_{H}$ e $\{1, \ldots, n\}$ possiamo identificare $\varphi(H)$ con le permutazioni di S_n che fissano un elemento di $\{1, \ldots, n\}$, che a loro volta costituiscono un gruppo isomorfo a S_{n-1}, pertanto $H \cong S_{n-1}$. □

Utilizzando il seguente teorema (di cui non diamo la dimostrazione) possiamo dire qualcosa di più forte nei casi $n \neq 2$ e $n \neq 6$.

Teorema 1.69

Per $n \notin \{2, 6\}$ i gruppi S_n e $\mathrm{Aut}(S_n)$ sono isomorfi, e l'isomorfismo è dato dall'azione di coniugio

$$\varphi : S_n \longrightarrow \mathrm{Aut}(S_n) : \sigma \longmapsto \varphi_\sigma$$

Osservazione 1.70 — In particolare gli automorfismo di S_n sono tutti interni nei casi $n \notin \{2, 6\}$, cioè sono coniugi per elementi di S_n

Con le stesse notazioni di sopra chiamiamo φ' l'isomorfismo tra $S\left({}^{S_n}\!/_{H}\right)$ e S_n, componendo φ' con φ otteniamo un isomorfismo

$$\psi : S_n \longrightarrow S_n$$

[6] Non sono sicuro di essere stato chiarissimo in questa sezione, se ci sono dei passi che ritenete poco comprensibili fatemelo sapere :)

che, per $n \notin \{2,6\}$, è il coniugio per un elemento di S_n. Abbiamo quindi che $\psi(H)$ è lo stabilizzatore di un elemento per l'azione naturale di S_n su $\{1,\dots,n\}$, ma allora anche H è uno stabilizzatore per tale azione in quanto coniugato a $\psi(H)$[7].Pertanto i sottogruppi di S_n isomorfi a S_{n-1} sono tra loro coniugati e ognuno è lo stabilizzatore di un elemento per l'azione naturale di S_n su $\{1,\dots,n\}$.

§1.7.8 Costruzione di un automorfismo esterno di S_6

Abbiamo visto che i casi $n=2$ e $n=6$ sono gli unici per cui non vale che $S_n \cong \mathrm{Aut}(S_n)$. Per $n=2$ il motivo è semplice, infatti essendo S_2 isomorfo a $\mathbb{Z}/2\mathbb{Z}$ il suo gruppo di automorfismi è banale, per $n=6$ invece abbiamo che gli automorfismi di S_6 non sono tutti elementi di $\mathrm{Inn}(S_n)$, vogliamo quindi esibire un automorfismo di S_6 che non sia interno.

Iniziamo osservando che S_5 contiene 6 5-Sylow, infatti tali sottogruppi sono isomorfi a $\mathbb{Z}/5\mathbb{Z}$ e, essendo i 5-cicli gli unici elementi di ordine 5, S_5 ne contiene esattamente

$$\frac{1}{\phi(5)}\binom{5}{4}3! = 6$$

Posto $X=\{P_1,\dots,P_6\}$ l'insieme dei 5-Sylow di S_5, consideriamo l'azione di coniugio di S_5 su X

$$\varphi : S_5 \longrightarrow S(X) \cong S_6$$

dove l'isomorfismo tra $S(X)$ e S_6 è dato dall'associare P_i a i, poniamo Φ la composizione di φ con tale isomorfismo, notiamo che Φ è un'immersione di S_5 in S_6. L'azione φ è transitiva in quanto i 5-Sylow di S_5 sono tutti coniugati, pertanto $\ker\varphi = \{id\}$ oppure $\ker\varphi = \mathcal{A}_5$. D'altra parte se fosse $\ker\varphi = \mathcal{A}_5$ si avrebbe che $|\mathrm{Im}\varphi| = 2$, pertanto l'orbita di ogni elemento ha cardinalità 2, che è assurdo in quanto $\mathrm{Orb}(P_i) = X$ per ogni $P_i \in X$ per transitività di φ, quindi l'azione è inettiva.
La transitività di φ implica che Φ sia un'azione transitiva di S_5 sull'insieme $\{1,\dots,6\}$, notiamo quindi che $\mathrm{Im}\Phi$ non può essere lo stabilizzatore di un elemento di $\{1,\dots,6\}$ per l'azione naturale di S_6 su tale insieme. Infatti se lo fosse esisterebbe $k \in \{1,\dots,n\}$ tale che $\Phi(\sigma)(i) = i$ per ogni $\sigma \in S_5$, ma questo è assurdo in quanto per la Proposizione 1.41 S_5 contiene una permutazione che agisce su $\{1,\dots,6\}$ senza punti fissi.

Abbiamo che $H = \mathrm{Im}\Phi$ è un sottogruppo di S_6 di indice 6 e possiamo considerare l'azione transitiva e iniettiva di moltiplicazione a sinistra di S_6 su ${}^{S_6}\!/_{H}$

$$\alpha : S_6 \longrightarrow S\left({}^{S_6}\!/_{H}\right) \cong S_6$$

chiamiamo $\psi : S_6 \longrightarrow S_6$ l'isomorfismo risultante dalla composizione di α con l'isomorfismo tra $S\left({}^{S_6}\!/_{H}\right)$ e S_6. Sia $i \in \{1,\dots,6\}$ l'elemento associato alla classe H, abbiamo visto nella dimostrazione della Proposizione 1.68 che $\psi(H) = \mathrm{St}(i)$ per l'azione naturale di S_6 sull'insieme $\{1,\dots,6\}$. Concludiamo osservando che se ψ fosse un automorfismo interno di S_6, allora anche ψ^{-1} sarebbe un automorfismo interno, cioè ψ^{-1} sarebbe il coniugio per un qualche $\sigma \in S_6$ fissato, da cui

$$H = \psi^{-1}(\mathrm{St}(i)) = \sigma\,\mathrm{St}(i)\sigma^{-1} = \mathrm{St}(\sigma(i))$$

che è assurdo in quanto H non può essere uno stabilizzatore per tale azione, pertanto $\psi \notin \mathrm{Inn}(S_6)$.

[7] Notiamo che l'azione naturale di S_n su $\{1,\dots,n\}$ è transitiva, pertanto gli stabilizzatori sono tra loro coniugati.

§1.8 Prodotti semidiretti

§1.8.1 Descrizione di S_4 come prodotto semidiretto

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

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

dove $(a\ b)$ è una trasposizione di S_n, vogliamo però dare una decomposizione di 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 $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$ lo stabilizzatore di 4 secondo l'azione naturale di S_4 su $\{1, 2, 3, 4\}$, osserviamo che V_4 è normale in S_4 in quanto unione delle classi di coniugio di ogni suo elemento[8] e che H è isomorfo a 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 $V_4H = S_4$ in quanto i due insiemi hanno la stessa cardinalità. Possiamo quindi scrivere

$$S_4 \cong V_4 \rtimes H \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi S_3$$

con

$$\varphi : S_3 \longrightarrow \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

Specifichiamo come agisce la mappa φ[9]: consideriamo gli isomorfismi

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

$$\beta : H \longrightarrow S_3 : \sigma \longmapsto \sigma_{|\{1,2,3\}}$$

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

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

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

[8] Le classe di coniugio in S_4 di $(1\ 2)(3\ 4)$ è $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

[9] Se descriviamo S_4 come prodotto semidiretto di due sottogruppi questo non è necessario, in quanto tale mappa è sempre il coniugio.

§1.8.2 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 nulla ed è chiuso per composizione). Notiamo che un elemento di G è univocamente determinato dalla coppia $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$[10], pertanto G contiene $n\phi(n)$ elementi. In realtà possiamo essere più precisi:

Proposizione 1.71
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 $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$, 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

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

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

Proposizione 1.72
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. $\square$

§1.8.3 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

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

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 1.73

Dato un gruppo G non abeliano, esiste un omomorfismo

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

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

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

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

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

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 1.74 (Criterio di isomorfismo tra prodotti semidiretti)
Siano H, N due gruppi e $\varphi : H \longrightarrow \mathrm{Aut}(N)$ un omomorfismo. Dato $f \in \mathrm{Aut}(H)$ 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 1.75
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 $\mathrm{ord}(a) = q$ (poiché $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ questo è equivalente a fissare un omomorfismo tra $\mathbb{Z}/q\mathbb{Z}$ e $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$), possiamo scrivere

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

Posto $f_k \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ 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 1.76

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

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

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

§1.9 Classificazione dei gruppi semplici di ordine al più 100

In questa sezione vogliamo determinare quali sono i sottogruppi semplici di ordine minore o uguale a 100. Facciamo prima una serie di osservazioni che ci permetterà di ridurre lo studio a pochi casi interessanti.

- Gli unici gruppi abeliani semplici sono i gruppi $\mathbb{Z}/p\mathbb{Z}$ con p primo, in quanto i loro sottogruppi sono solo quelli banali e tutti i sottogruppi di un gruppo abeliano sono normali;
- i gruppi G di ordine p^k con p primo e $k > 1$ non sono semplici in quanto hanno centro non banale e il centro è un sottogruppo caratteristico, in particolare normale (alternativamente, dal Teorema di Sylow abbiamo che G contiene un sottogruppo proprio di ordine p^{k-1}, che è normale in quanto il suo indice è p, il più piccolo primo che divide $|G|$);
- i gruppi di ordine $2d$ con d dispari non sono semplici in quanto contengono un sottogruppo di indice 2, che è normale e non banale, per l'Esercizio 1.48;
- i gruppi di ordine pq con $q > p$ primi non sono semplici, in quanto possiamo scriverli come prodotto semidiretto dei loro sottogruppi di Sylow, pertanto almeno uno di questi è normale e non banale;
- $\mathcal{A}_5$ è un gruppo semplice di ordine 60.

Ci riduciamo quindi a studiare i gruppi di ordine 56, 60, 72, 80, 96.

$|G| = 56 = 2^3 \cdot 7$: 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.

$|G| = 96 = 2^5 \cdot 3$: sia P_2 un 2-Sylow di G, poiché $[G : P_2] = 3$ per il Teorema 1.50 esiste un sottogruppo $N \triangleleft G$ tale che $N \subseteq P_2$ e $[G : N] \mid 3!$, da cui $N \neq G$ e $N \neq \{e\}$ in quanto $[G : \{e\}] = |G|$. Pertanto G non è semplice.

$|G| = 72 = 2^3 \cdot 3^2$: 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

  $$\varphi : G \longrightarrow S(X) \cong S_4$$

  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 $S(X) \cong S_4$. 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 esserre 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 ${}^{G}\!/_{P_2}$
  $$\varphi : G \longrightarrow S\left({}^{G}\!/_{P_2}\right) \cong S_5$$
  Poiché $|G| \nmid |S_5|$ 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 1.77

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

$$\operatorname{St}(5) = \{\sigma \in \mathcal{A}_5 \mid \sigma(5) = 5\} \cong \mathcal{A}_4 \text{ [11]}$$

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 $n_2 = 5$. □

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

Proposizione 1.78
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

  $$\varphi : G \longrightarrow S(X) \cong S_3$$

  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 $|G| > |S_3|$;

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

  $$\varphi : G \longrightarrow S(X) \cong S_5$$

  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 $H \leqslant S_5$ 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 $\mathcal{A}_5$;

- supponiamo per assurdo $n_2 = 15$, notiamo che due 2-Sylow distinti di G si intersecano banalmente o in un sottogruppo isomorfo a $\mathbb{Z}/2\mathbb{Z}$[12]. 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 S_2 2-Sylow distinti di G tali che $H = S_1 \cap S_2 \cong \mathbb{Z}/2\mathbb{Z}$, consideriamo il normalizzatore $N_G(H)$. Osserviamo che S_1 e 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 proprio di ordine al più 3!, che è assurdo. Abbiamo quindi $|N_G(H)| = 12$, consideriamo l'azione di moltiplicazione a sinistra di G sull'insieme quoziente ${}^{G}\!/_{H}$

  $$\varphi : G \longrightarrow S\left({}^{G}\!/_{H}\right) \cong S_5$$

[12] 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

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 si mostra come sopra che $G \cong \mathcal{A}_5$, ma questo è assurdo in quanto $\mathcal{A}_5$ contiene 5 2-Sylow.

$\square$

§1.10 Studio di $SL_2(\mathbb{F}_3)$

Consideriamo il gruppo $GL_2(\mathbb{F}_3)$, ricordiamo che il determinante è un omomorfismo di gruppi surgettivo

$$\det : GL_2(\mathbb{F}_3) \longrightarrow \mathbb{F}_3^*$$

e che il suo nucleo è il gruppo $SL_2(\mathbb{F}_3) = \{M \in GL_2(\mathbb{F}_3) \mid \det M = 1\}$, che è quindi un sottogruppo normale di $GL_2(\mathbb{F}_3)$. Inoltre, poiché $\mathbb{F}_3^* \cong \mathbb{Z}/2\mathbb{Z}$ abbiamo che $SL_2(\mathbb{F}_3)$ ha indice 2 in $GL_2(\mathbb{F}_3)$, pertanto $|SL_2(\mathbb{F}_3)| = 24$ in quanto $|GL_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 48$.

Consideriamo quindi il gruppo $S = SL_2(\mathbb{F}_3)$, 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 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

$$\Phi : S \longrightarrow S(X) \cong S_4$$

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 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

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ [13]

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 $Z(S) \subseteq S'$[14]. 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 $S' = J$.

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

[14] 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 via TCR

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

Proposizione 2.1

Siano $a_1, \dots, a_n \in \mathbb{Q}$ valori distinti e $b_1, \dots, b_n \in \mathbb{Q}$, 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 $i \in \{1, \dots, n\}$.

Dimostrazione. Posto $I_i = (x - a_i)$ per $i \in \{1, \dots, n\}$, 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

$$\frac{\mathbb{Q}[x]}{I_1 \dots I_n} \cong \mathbb{Q}[x]/_{I_1} \times \dots \times \mathbb{Q}[x]/_{I_n}$$

tramite l'isomorfismo

$$\Phi : \frac{\mathbb{Q}[x]}{I_1 \dots I_n} \longrightarrow \mathbb{Q}[x]/_{I_1} \times \dots \times \mathbb{Q}[x]/_{I_n} : \overline{p(x)} \longmapsto (p(x) + I_1, \dots, p(x) + I_n)$$

abbiamo inoltre che $\mathbb{Q}[x]/_{I_i} \cong \mathbb{Q}$ per ogni $i \in \{1, \dots, n\}$ 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

$$\Psi \circ \Phi : \frac{\mathbb{Q}[x]}{I_1 \dots I_n} \longrightarrow \mathbb{Q}^n : \overline{p(x)} \longmapsto (p(a_1), \dots, p(a_n))$$

in particolare per ogni n-upla di razionali $(b_1, \dots, b_n)$ esiste un unico[15] polinomio $p \in \mathbb{Q}[x]$ con $\deg p \leq n-1$ tale che $p(a_i) = b_i$ per ogni $i \in \{1, \dots, n\}$. $\square$

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 $a_1, \dots, a_n$ tali che $a_i - a_j$ sia invertibile per ogni $i \neq j$.

[15] L'unicità deriva dal fatto che gli elementi di $\frac{\mathbb{Q}[x]}{I_1 \dots I_n}$ 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

Sia $P = (p)$ un ideale primo non nullo di $\mathbb{Z}$, consideriamo $S = \mathbb{Z} \setminus P$. S è una parte moltiplicativa di $\mathbb{Z}$, infatti

- $0 \notin S$ in quanto $0 \in P$;
- $1 \in S$ in quanto $0 \notin P$;
- per ogni $x, y \in S$ vale $xy \in S$, infatti se $x, y \notin P$ allora $xy \notin P$ poiché P è un ideale primo.

Per quanto già visto, sappiamo che $S^{-1}\mathbb{Z}$ è un anello contenente un unico ideale massimale, detto anche **anello locale**. Più precisamente, tale ideale è $S^{-1}\mathbb{Z} \setminus (S^{-1}\mathbb{Z})^*$ e il gruppo degli elementi invertibili è

$$(S^{-1}\mathbb{Z})^* = \left\{ \frac{a}{s} \;\middle|\; a, s \in S \right\}$$

Inoltre, gli ideali di $S^{-1}\mathbb{Z}$ sono tutti della forma $S^{-1}(m)$ con $(m) \subseteq \mathbb{Z}$ un ideale, e vale

$$S^{-1}(m) = \left\{ \frac{mk}{s} \;\middle|\; k \in \mathbb{Z}, s \in S \right\} = \left\{ m\frac{k}{s} \;\middle|\; \frac{k}{s} \in S^{-1}\mathbb{Z} \right\} = (m)S^{-1}\mathbb{Z}$$

Vediamo un esempio esplicito per $P = (2)$, descrivendo esplicitamente gli ideali di $S^{-1}\mathbb{Z}$.

$$S^{-1}\mathbb{Z} = \left\{ \frac{m}{s} \;\middle|\; s \text{ dispari} \right\}$$

Per prima cosa osserviamo che la corrispondenza tra gli ideali di $\mathbb{Z}$ e quelli di $S^{-1}\mathbb{Z}$ non è biunivoca, ma solo surgettiva. Infatti alcuni ideali di $\mathbb{Z}$ diventano uguali quando localizziamo l'anello rispetto a S, in particolare

$$S^{-1}(m) = S^{-1}(n) \iff \exists u \in (S^{-1}\mathbb{Z})^* \text{ tale che } m = un \iff u = \frac{m}{n} \in (S^{-1}\mathbb{Z})^*$$

dove l'ultima uguaglianza è giustificata dal fatto che $S^{-1}\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$, pertanto esiste $\dfrac{m}{n}$ come numero razionale ed è l'unico valore per cui l'equazione è verificata. D'altra parte abbiamo

$$(S^{-1}\mathbb{Z})^* = \left\{ \frac{m}{s} \;\middle|\; m, s \in S \right\} = \left\{ \frac{m}{n} \;\middle|\; m, n \text{ entrambi dispari} \right\}$$

pertanto $S^{-1}(m) = S^{-1}(n)$ se e solo se la massima potenza di due che divide m e n è la stessa[16]. Gli ideali di $S^{-1}\mathbb{Z}$ sono quindi tutti e soli quelli della forma $S^{-1}(2^k)$. Consideriamo la bigezione

$$\{\text{Ideali primi di } S^{-1}\mathbb{Z}\} \longleftrightarrow \{\text{Ideali primi } P \subseteq \mathbb{Z} \mid P \cap S = \emptyset\}$$

poiché gli unici ideali primi di $\mathbb{Z}$ che non intersecano $S = \mathbb{Z} \setminus (2)$ sono (0) e (2), abbiamo che gli unici ideali primi di $S^{-1}\mathbb{Z}$ sono (0) e $S^{-1}(2)$.

[16] In tal caso infatti il razionale $\frac{m}{n}$, se ridotto ai minimi termini, ha numeratore e denominatore entrambi dispari, quindi è un'unità dell'anello.

§2.3 Ideali massimali e primi di $\mathbb{Z}[x]$

Lemma 2.3
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. $P \cap A$ è un ideale di A in quanto controimmagine di P tramite l'omomorfismo di anelli

$$\varphi : A \hookrightarrow R : a \longmapsto a$$

Poiché P è un ideale primo di R, per ogni $a, b \in A$ tali che $ab \in P \cap A$ si ha $a \in P$ oppure $b \in P$, cioè $a \in P \cap A$ oppure $b \in P \cap A$, quindi $P \cap A$ è un ideale primo di A. $\square$

Consideriamo $P \subseteq \mathbb{Z}[x]$ un ideale primo, studiamo l'intersezione $P \cap \mathbb{Z}$. Questo è un ideale primo di $\mathbb{Z}$ per il Lemma 2.3, pertanto $P \cap \mathbb{Z} = (0)$ oppure esiste un primo $p \in \mathbb{Z}$ tale che $P \cap \mathbb{Z} = (p)$. Se non è l'ideale nullo allora $(p)\mathbb{Z}[x]$ è un ideale contenuto in P, per il Teorema di Corrispondenza gli ideali primi di $\mathbb{Z}[x]$ contenenti $(p)\mathbb{Z}[x]$ sono in bigezione con gli ideali primi del quoziente $\mathbb{Z}[x] / (p)\mathbb{Z}[x] \cong \mathbb{F}_p[x]$ e vale la stessa cosa per gli ideali massimali. Poiché $\mathbb{F}_p[x]$ è un dominio a ideali principali, i suoi ideali primi sono $(\overline{0})$ e quelli generati da un polinomio irriducibile, in particolare tutti i suoi ideali primi non nulli sono anche massimali. Pertanto se $\overline{f(x)} \in \mathbb{F}_p[x]$ è un polinomio irriducibile allora $(\overline{f(x)})$ è un ideale primo di $\mathbb{F}_p[x]$ e quindi $(p, f(x))$ è un ideale primo e massimale di $\mathbb{Z}[x]$. Abbiamo quindi che l'insieme degli ideali massimali di $\mathbb{Z}[x]$ contenenti p è

$$\mathcal{M}_p = \{(p, f(x)) \mid \overline{f(x)} \text{ è irriducibile in } \mathbb{F}_p[x]\}$$

mentre l'insieme degli ideali primi di $\mathbb{Z}[x]$ contenenti p è

$$\mathcal{P}_p = \mathcal{M}_p \cup (p)\mathbb{Z}[x]$$

Supponiamo adesso che P sia un ideale primo di $\mathbb{Z}[x]$ tale che $P \cap \mathbb{Z} = 0$. $S = \mathbb{Z} \setminus \{0\}$ è una parte moltiplicativa di $\mathbb{Z}$ e l'ipotesi appena data su P può essere espressa come $P \cap S = \emptyset$. Consideriamo la bigezione

$$\{\text{Ideali primi di } S^{-1}\mathbb{Z}[x]\} \longleftrightarrow \{\text{Ideali primi } P \subseteq \mathbb{Z}[x] \mid P \cap S = \emptyset\} : \mathfrak{P} \longmapsto \mathfrak{P} \cap \mathbb{Z}[x]$$

poiché $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$ abbiamo che P corrisponde a un unico ideale primo di $\mathbb{Q}[x]$. Essendo $\mathbb{Q}[x]$ un dominio a ideali principali, questi sono l'ideale nullo e gli ideali generati da polinomi irriducibili. Se $f(x) \in \mathbb{Q}[x]$ è un polinomio irriducibile il cui ideale corrisponde a P allora, posto m il minimo comune denominatore dei suoi coefficienti, abbiamo che $P = (f(x))\mathbb{Q}[x] \cap \mathbb{Z}[x] = (mf(x))\mathbb{Q}[x] \cap \mathbb{Z}[x] = (mf(x))\mathbb{Z}[x]$. In particolare P è generato da un polinomio primitivo irriducibile. Gli ideali primi di $\mathbb{Z}[x]$ possono quindi avere la seguente forma:

- (0);
- $(p)\mathbb{Z}[x]$ con $p \in \mathbb{Z}$ primo;
- $(p, f(x))$ con $p \in \mathbb{Z}$ primo e $\overline{f(x)}$ irriducibile in $\mathbb{F}_p[x]$;
- $(f(x))$ con $f(x)$ primitivo e irriducibile in $\mathbb{Z}[x]$.

Mostriamo che gli ideali primi di quest'ultimo tipo non sono massimali.
Siano $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo, irriducibile, non costante, $a \in \mathbb{Z}$ tale che $f(a) \notin \{-1, 0, 1\}$, $p \in \mathbb{Z}$ un primo che divide $f(a)$ e consideriamo le applicazioni

$$\varphi : \mathbb{Z}[x] \longrightarrow {}^{\mathbb{Z}[x]}\!\big/_{(p)\mathbb{Z}[x]} : g(x) \longmapsto \overline{g(x)}$$

$$\psi : {}^{\mathbb{Z}[x]}\!\big/_{(p)\mathbb{Z}[x]} \longrightarrow \mathbb{F}_p : \overline{g(x)} \longmapsto g(a)$$

Osserviamo che $(\psi \circ \varphi)(f(x)) = a \equiv 0 \pmod p$ e che $(\psi \circ \varphi)(p) = p \equiv 0 \pmod p$, pertanto $p, f(x) \in \ker \psi \circ \varphi$ e quindi $(p, f(x)) \subseteq \ker(\psi \circ \varphi) \neq \mathbb{Z}[x]$. Abbiamo quindi $(f(x)) \subseteq (p, f(x))$, se $(f(x))$ fosse massimale allora conterrebbe p, che è assurdo in quanto $\deg f \geq 1$.

Poiché gli ideali di questo tipo non sono massimali, gli ideali massimali di $\mathbb{Z}[x]$ sono tutti e soli quelli della forma

$$(p, f(x)) \text{ con } \overline{f(x)} \text{ irriducibile in } \mathbb{F}_p[x]$$

§2.4 Criterio di Eisenstein

Conosciamo il Criterio di Eisenstein per verificare che un polinomio a coefficienti interi è irriducibile in $\mathbb{Z}[x]$. Lo stesso risultato vale in generale in ogni anello UFD con praticamente la stessa dimostrazione, che ricordiamo.

Proposizione 2.4 (Criterio di Eisenstein)

Siano A un UFD, $p \in A$ un elemento primo e $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio a coefficienti in A se sono verificate le ipotesi

- $p \nmid a_n$;
- $p \mid a_i$ per $i \in \{0, \dots, n-1\}$;
- $p^2 \nmid a_0$;

allora $f(x)$ è irriducibile in $A[x]$.

Dimostrazione. Supponiamo per assurdo che $f(x)$ sia riducibile, allora possiamo scrivere $f(x) = g(x)h(x)$ con $g(x), h(x) \in A[x]$, $\deg g = m \geq 1$, $\deg h = n-m \geq 1$. Consideriamo l'omomorfismo di proiezione

$$\pi : A[x] \longrightarrow {}^{A}\!/_{(p)}[x] : \sum_{j=0}^{k} \alpha_i x^i \longmapsto \sum_{j=0}^{k} \overline{\alpha_i} x^i$$

abbiamo che

$$\pi(f(x)) = \overline{a_n} x^n \neq \overline{0} \qquad \pi(f(x)) = \pi(g(x))\pi(h(x))$$

Scriviamo

$$g(x) = \sum_{i=0}^{m} b_i x^i \qquad h(x) = \sum_{i=0}^{n-m} c_i x^i$$

poiché A è UFD lo è anche $A[x]$, pertanto le proiezioni di $g(x)$ e di $h(x)$ sono necessariamente della forma

$$\pi(g(x)) = \overline{b_m} x^m \qquad \pi(h(x)) = \overline{c_{n-m}} x^{n-m}$$

da cui $\overline{b_0} = \overline{c_0} = \overline{0}$, cioè $p \mid b_0$ e $p \mid c_0$. D'altra parte $a_0 = b_0 c_0$ e quindi $p^2 \mid a_0$, che è assurdo. □

§2.5 Domini a ideali principali

Proposizione 2.5

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, supponiamo per assurdo che esista un ideale M tale che

$$P \subsetneq M \subsetneq A$$

Poiché A è un dominio a ideali principali, esiste $x \in A$ tale che $M = (x)$, quindi $x \mid p$ dato che $P \subsetneq M$. Poiché P è un ideale primo si ha che $p \in A$ è un elemento primo, quindi irriducibile[17]. Sia $q \in A$ tale che $p = xq$, dato che $x \notin A^*$ abbiamo che $q \in A^*$, cioè $(x) = (p)$, che è assurdo. $\square$

Corollario 2.6

Siano A un PID e B un dominio di integrità e $\varphi : A \longrightarrow B$ un omomorfismo di anelli surgettivo, allora φ è un isomorfismo oppure B è un campo.

Dimostrazione. Notiamo che $\ker \varphi$ è un ideale primo di A in quanto $A/\ker \varphi \cong B$ è un dominion di integrità. Se $\ker \varphi = (0)$, allora φ è un isomorfismo di anelli. Altrimenti $\ker \varphi$ è un ideale massimale, pertanto $A/\ker \varphi \cong B$ è un campo. $\square$

Corollario 2.7

Se C è un anello tale che $C[x]$ è un PID, allora C è un campo.

Dimostrazione. Dall'inclusione $C \subseteq C[x]$ abbiamo che C è un dominio di integrità. L'ideale (x) è quindi primo in $C[x]$ in quanto $C[x]/(x) \cong X$ è un dominio, quindi è massimale dato che $C[x]$ è un PID. Pertanto C è un campo. $\square$

[17] Questo perché PID $\Longrightarrow$ UFD.

§2.6 Operazioni tra ideali

Ricordiamo che in un anello commutativo con identità A, sono ben definite le seguenti operazioni su due ideali I, J e danno luogo a un terzo ideale (possibilmente uguale a uno dei due):

- $I \cap J = \{k \in A \mid k \in I, k \in J\}$;
- $I + J = (I, J) = \{i + j \mid i \in I, j \in J\}$;
- $IJ = (\{ij \mid i \in I, j \in J\})$;
- $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} \text{ per cui } x^n \in I\}$;
- $(I : J) = \{x \in A \mid xJ \subseteq I\}$.

Proposizione 2.8

Dati A un anello commutativo con identità, $I, J \subseteq A$ due ideali, allora

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

Dimostrazione. Poiché vale l'inclusione $IJ \subseteq I \cap J$ abbiamo che $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. Viceversa, se $a \in \sqrt{I \cap J}$ allora esiste $n \in \mathbb{N}$ tale che $a^n \in I \cap J$, allora abbiamo

$$a^{2n} = \underbrace{a^n}_{\in I} \cdot \underbrace{a^n}_{\in J} \in IJ$$

da cui $\sqrt{I \cap J} \subseteq \sqrt{IJ}$ e quindi l'uguaglianza.
Consideriamo adesso $b \in \sqrt{I} \cap \sqrt{J}$, allora esistono $m, n \in \mathbb{N}$ tali che $b^m \in I$ e $b^n \in J$, da cui

$$b^{m+n} = \underbrace{b^m}_{\in I} \cdot \underbrace{b^n}_{\in J} \in I \cap J$$

Pertanto $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$. Viceversa, Se $c \in \sqrt{I \cap J}$ allora esiste $n \in \mathbb{N}$ tale che $c^n \in I \cap J$, in particolare $c^n \in I$ e $c^n \in J$, quindi $c \in \sqrt{I} \cap \sqrt{J}$, da cui l'uguaglianza. □

Proposizione 2.9

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

$$x^{h+k} \in (M, a)(M, b) \subseteq (M, a) \cap (M, b) \subseteq M$$

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 2.10

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 2.11

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 $n \in \mathbb{N}$ tale che $t^n = 0$, dalla fattorizzazione

$$1 - t^n = (1 - t) \left(\sum_{i=0}^{n-1} t^i \right)$$

otteniamo

$$1 = a_0^{-1} p(x) \left(\sum_{i=0}^{n-1} t^i \right)$$

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 $P \subseteq A$ 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 2.12

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

$$(i + j + k)^N = \sum_{x+y+z=N} \binom{N}{x, y, z} i^x j^y k^z \text{[18]}$$

[18]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 $(x+y+z)^N = 1$ 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

$$1 = (i_1 + j_1)(j_2 + k_1)(i_2 + k_2) \in IJ + JK + IK$$

$\square$

§2.7 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.

§2.7.1 Elementi primi

Lemma 2.13

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 2.14

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 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 2.15

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 2.16

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

$$\frac{\mathbb{Z}[i]}{(i+1)} \cong \frac{\mathbb{Z}[x]}{(2, 1+x)} \cong \frac{\mathbb{Z}[x]\big/(2)}{(2, 1+x)\big/(2)} \cong \frac{\mathbb{F}_2[x]}{(1+x)} \cong \mathbb{F}_2$$

□

Lemma 2.17

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 2.18

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 $1 + i$.

□

§2.7.2 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 2.19

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. 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 2.20 — 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 2.21 — 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 2.22

Siano A un PID e $I \subseteq A$ un ideale. Se il quoziente ${}^{A}\!/\!_{I}$ è finito allora vale

$$\left| {}^{A}\!/\!_{I^n} \right| = \left| {}^{A}\!/\!_{I} \right|^n$$ [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 $\mathbb{Z}[i]$:

$$z = u(1+i)^e \prod_{j=1}^{r} (a_j + b_j i)^{e_j} \prod_{h=1}^{s} p_h^{e_h} \qquad u \in \mathbb{Z}[i]^*$$

Gli ideali $(1+i)^e, (a_j + b_j)^{e_j}, (p^{e_h})$ sono a due a due coprimi, in quanto massimali, quindi per il Teorema Cinese del Resto

$$\mathbb{Z}[i]/I \cong \frac{\mathbb{Z}[i]}{(1+i)^e} \times \prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j + b_j i)^{e_j}} \times \prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)^{e_h}}$$

La cardinalità di questo quoziente è $N(z)$, infatti applicando il Lemma 2.21 abbiamo

$$\begin{aligned}
\left|{}^{\mathbb{Z}[i]}\!\big/_{I}\right| &= \left|\frac{\mathbb{Z}[i]}{(1+i)^e}\right| \cdot \left|\prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j+b_ji)^{e_j}}\right| \cdot \left|\prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)^{e_h}}\right| = \\
&= \left|\frac{\mathbb{Z}[i]}{(1+i)}\right|^e \cdot \left|\prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j+b_ji)}\right|^{e_j} \cdot \left|\prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)}\right|^{e_h} = \\
&= N(1+i)^e \prod_{j=1}^{r} N(a_j+b_ji)^{e_j} \prod_{h=1}^{s} N(p_h)^{e_h} = \\
&= N\left(u(1+i)^e \prod_{j=1}^{r} (a_j+b_ji)^{e_j} \prod_{h=1}^{s} p_h^{e_h}\right) = N(z)
\end{aligned}$$

§2.8 Esempio di dominio non euclideo

Consideriamo l'anello $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, vogliamo mostrare che non è un dominio euclideo.

Proposizione 2.23

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\frac{1+\sqrt{-19}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

Dimostrazione. Sia $\alpha = \frac{1+\sqrt{-19}}{2}$, il polinomio minimo di α su $\mathbb{Q}$ è $\mu(x) = x^2 - x + 5$. Consideriamo l'omomorfismo di valutazione

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C} : p(x) \longmapsto p(\alpha) \qquad \mathrm{Im}\varphi = \mathbb{Z}[\alpha]$$

poiché φ è la restrizione dell'usuale omomorfismo di valutazione su $\mathbb{Q}[x]$, che è un PID, abbiamo

$$\ker\varphi = \mathbb{Z}[x] \cap \{f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0\} = \mathbb{Z}[x] \cap (x^2 - x + 5)\mathbb{Q}[x] = (x^2 - x + 5)\mathbb{Z}[x]$$

dove l'ultima uguaglianza è giustificata dal fatto che $\mu(x)$ è un polinomio a coefficienti interi primitivo e per il Lemma di Gauss. Pertanto per il Primo Teorema di Omomorfismo abbiamo

$$\frac{\mathbb{Z}[x]}{(x^2 - x + 5)} \cong \mathrm{Im}\varphi = \{a + b\alpha \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\alpha]$$

□

Osservazione 2.24 — Il risultato appena visto non è un fatto ovvio. Consideriamo $\beta = 1 + \frac{\sqrt{3}}{2}$, il suo polinomio minimo su $\mathbb{Q}$ è $\mu(x) = x^2 - x - \frac{1}{2}$. Ragionando in modo analogo a quanto fatto sopra, il nucleo della valutazione in β è

$$\mathbb{Z}[x] \cap \left(x^2 - x - \frac{1}{2}\right)\mathbb{Q}[x] = (2x^2 - 2x - 1)\mathbb{Z}[x]$$

E $\frac{\mathbb{Z}[x]}{(2x^2 - x - 1)} \cong \mathbb{Z}[\beta]$. D'altra parte

$$\mathbb{Z}[\beta] \neq \{a + b\beta \mid a, b \in \mathbb{Z}\}$$

in quanto il quoziente $\frac{\mathbb{Z}[x]}{(2x^2 - x - 1)}$ contiene delle classi di resto della forma $\overline{x^k}$ per ogni $k \in \mathbb{N}$, in quanto x^k e $x^2 - x - 1$ sono coprimi in $\mathbb{Z}[x]$. Notiamo che il risultato di sopra non è valido in questo caso in quanto il polinomio minimo di β non ha coefficienti interi.

Mostriamo che A non è un domino euclideo. Sia $\omega = \frac{1+\sqrt{-19}}{2}$, consideriamo l'applicazione

$$N : A \longrightarrow \mathbb{N} : a + b\omega \longmapsto (a + b\omega)(a + b\overline{\omega}) = a^2 + 5b^2 + ab$$

N è la restrizione all'anello A dell'usuale norma su $\mathbb{C}$, pertanto è moltiplicativa. Osserviamo inoltre che se $u \in A^*$ si ha $N(u) = 1$, infatti se $v \in A$ è tale che $uv = 1$ allora $N(uv) = N(u)N(v) = 1$ da cui $N(u) = N(v) = 1$ necessariamente. D'altra parte l'equazione

$$a^2 + ab + 5b^2 = \left(a + \frac{1}{2}b\right)^2 + \frac{19}{4}b^2 = 1$$

ha soluzione se e solo se $a = \pm 1$ e $b = 0$, pertanto $A^* = \{-1, 1\}$.

Supponiamo per assurdo che A sia un dominio euclideo, cioè che esista un'applicazione

$$\mathcal{N} : A \setminus \{0\} \longrightarrow \mathbb{N}$$

che rispetta gli assiomi di norma euclidea, ricordiamo che gli elementi invertibili di A^* sono gli elementi di norma $\mathcal{N}$ minima. Consideriamo l'insieme $X = \{\mathcal{N}(x) \mid x \in A \setminus A^*\}$, poiché X è un sottoinsieme non vuoto di $\mathbb{N}$ esiste un elemento minimo $m \in X$, sia $x \in A \setminus A^*$ tale che $\mathcal{N}(x) = m$. Per definizione di dominio euclideo, per ogni $a \in A$ esistono $q, r \in A$ tali che $a = qx + r$, con $r = 0$ oppure $\mathcal{N}(r) < \mathcal{N}(x)$. Se $r \neq 0$ allora $r \in A^*$ per minimalità di $\mathcal{N}(x)$, pertanto l'insieme dei possibili resti della divisione per x è $\{0, 1, -1\}$. Abbiamo quindi che l'insieme $\{0, 1, -1\}$ è un insieme di rappresentanti, possibilmente con ripetizioni, per gli elementi del quoziente ${}^{A}\!/_{(x)}$, che è quindi isomorfo a $\mathbb{F}_2$ oppure $\mathbb{F}_3$.
Il polinomio $\mu(x) = x^2 - x + 5$ ha come soluzioni in A ω e $\overline{\omega}$, pertanto è riducibile in $A[x]$. Da questo si ricava che le classi di ω e $\overline{\omega}$ nel quoziente ${}^{A}\!/_{(x)}$ sono le radici della classe del polinomio $\mu(x)$, che è assurdo in quanto $\mu(x)$ è irriducibile in $\mathbb{F}_2[x]$ e in $\mathbb{F}_3[x]$. Pertanto A 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 S_3, poiché sono entrambi gruppi finiti della stessa cardinalità si ha quindi $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

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 $x, y \in \mathbb{F}_{p^n}$
$$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$$
$$\Phi(x + y) = (x + y)^p \overset{[19]}{=} x^p + y^p = \Phi(x) + \Phi(y)$$
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 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

[19] 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 $x^n - 1$[20], 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 $\zeta_n^{\frac{n}{d}} = 1$, che è assurdo in quanto $\operatorname{ord} \zeta_n = n$. 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 $g(\zeta_n^p) = 0$;

- 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

$$f(x)g(x)q(x) = x^n - 1 \qquad f(x)r(x) = g(x^p)$$

[20] 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.

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
$$\Psi : \mathbb{Z}/n\mathbb{Z}^* \longmapsto \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : k \longmapsto \psi_k$$

□

§3.3 Gruppo di Galois del traslato e del composto

Proposizione 3.10
Siano K/F un'estensione di Galois finita e L/F un'estensione finita, allora

(1) KL/L è un'estensione di Galois;

(2) $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$.

Dimostrazione. Consideriamo il seguente diagramma di campi, mostriamo i due enunciati separatamente

$$\begin{tikzcd}[arrows=dash]
& KL \arrow[dl] \arrow[d] \arrow[dr] & \\
K \arrow[r] \arrow[dr] & K \cap L \arrow[d] & L \arrow[l] \arrow[dl] \\
& F &
\end{tikzcd}$$

(1) poiché K/F è un'estensione di Galois finita possiamo scrivere K come $F(\alpha_1, \dots, \alpha_n)$, dove $\alpha_1, \dots, \alpha_n \in \overline{K}$ sono le radici di un certo polinomio $p(x) \in F[x]$. Allora abbiamo che $KL = L(\alpha_1, \dots, \alpha_n)$ è il campo di spezzamento di $p(x)$ su L, pertanto KL/L è un'estensione di Galois;

(2) l'estensione $K/K \cap L$ è di Galois, in quanto lo è K/F. Consideriamo la mappa di restrizione
$$\Phi : \mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/K \cap L) : \varphi \longmapsto \varphi_{|K}$$
questa è ben definita in quanto ogni immersione $KL \hookrightarrow \overline{F}$ che fissa L fissa anche $K \cap L$. Chiaramente Φ è un omomorfismo di gruppi, mostriamo che in realtà è un isomorfismo. $\Phi(\varphi) = id$ se e solo se $\varphi_{|K} = id$, ma questo è possibile se e solo se $\varphi = id$ in quanto se φ è la mappa identità su K e su L allora lo è anche sul composto KL, pertanto Φ è iniettivo. Mostriamo adesso che è anche surgettivo. Sia $H = \mathrm{Im}\Phi$, il sottocampo di K fissato da H è
$$K^H = \{x \in K \mid \psi(x) = x \ \forall \psi \in H\}$$
Poiché H contiene le restrizioni a K degli elementi di $\mathrm{Gal}(KL/L)$, si ha
$$\begin{aligned} K^H &= \{x \in K \mid \psi(x) = x \ \forall \psi \in \mathrm{Gal}(KL/L)\} = \\ &= K \cap \{x \in KL \mid \psi(x) = x \ \forall \psi \in \mathrm{Gal}(KL/L)\} = \\ &= K \cap (KL)^{\mathrm{Gal}(KL/L)} = K \cap L \end{aligned}$$
pertanto $H = \mathrm{Gal}(K/K \cap L)$ per il Teorema di Corrispondenza di Galois. Quindi Φ è surgettivo, di conseguenza è un isomorfismo tra $\mathrm{Gal}(KL/L)$ e $\mathrm{Gal}(K/K \cap L)$.

□

Leonardo Migliorini
l.migliorini@studenti.unipi.it (Anno Accademico 2022-23)

Corollario 3.11

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. Consideriamo il seguente diagramma di campi

$$\begin{tikzcd}
 & KL \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

per il Teorema delle Torri abbiamo $[KL : F] = [KL : L][L : F]$. Poiché $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L) = \mathrm{Gal}(K/F)$ per la Proposizione 3.10, in particolare $[KL : L] = [K : F]$, quindi $[KL : F] = [K : F][L : F]$. $\square$

Proposizione 3.12

Siano ${}^{K_1}\!/_{F}$, ${}^{K_2}\!/_{F}$ estensioni di Galois finite, allora ${}^{K_1K_2}\!/_{F}$ è un'estensione di Galois. Inoltre:

(1) esiste un'immersione $\Phi : \mathrm{Gal}(K_1K_2/F) \hookrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$;

(2) $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ se e solo se $K_1 \cap K_2 = F$.

Dimostrazione. Poiché ${}^{K_1}\!/_{F}$ e ${}^{K_2}\!/_{F}$ sono estensioni normali, esistono $p_1(x), p_2(x) \in F[x]$ tali che K_1 e K_2 sono rispettivamente i campi di spezzamento di $p_1(x)$ e $p_2(x)$ su F. Allora il composto K_1K_2 è il campo di spezzamento del polinomio $p_1(x)p_2(x)$ su F, quindi ${}^{K_1K_2}\!/_{F}$ è un'estensione di Galois.

(1) Consideriamo la mappa

$$\Phi : \mathrm{Gal}(K_1K_2/F) \longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) : \varphi \longmapsto (\varphi_{|K_1}, \varphi_{|K_2})$$

chiaramente Φ è un omomorfismo di gruppi, mostriamo quindi che il suo nucleo è banale. $\Phi(\varphi) = (id_{K_1}, id_{K_2})$ se e solo se $\varphi_{|K_1} = id_{K_1}$ e $\varphi_{|K_2} = id_{K_2}$, ma allora φ è l'identità anche sul composto K_1K_2, pertanto Φ è iniettivo;

(2) poiché i gruppi in questione sono finiti, è sufficiente mostrare che hanno la stessa cardinalità per concludere che sono isomorfi. Per il Teorema delle Torri abbiamo $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$, d'altra parte $[K_1K_2 : K_1] = [K_2 : K_1 \cap K_2]$ per la Proposizione 3.10. Pertanto $|\,\mathrm{Gal}(K_1K_2/F)| = |\,\mathrm{Gal}(K_1/F)| \cdot |\,\mathrm{Gal}(K_2/F)|$ se e solo se $[K_2 : K_1 \cap K_2][K_1 : F] = [K_1 : F][K_2 : F]$, cioè se e solo se $[K_2 : K_1 \cap K_2] = [K_2 : F]$, ovvero $K_1 \cap K_2 = F$.

$\square$

§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 S_3, pertanto $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ oppure $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}3$. 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

$$\begin{tikzcd}[column sep=small]
 & K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

l'estensione ${}^{\mathbb{Q}(\sqrt[3]{2})}\!/_{\mathbb{Q}}$ ha grado 3 in quanto il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$, mentre l'estensione ${}^{\mathbb{Q}(\zeta_3)}\!/_{\mathbb{Q}}$ 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 ${}^{K}\!/_{\mathbb{Q}}$ ha grado 6, di conseguenza $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

Adesso vogliamo determinare un polinomio il cui gruppo di Galois sia isomorfo a $\mathbb{Z}3$. Consideriamo l'estensione ${}^{\mathbb{Q}(\zeta_7)}\!/_{\mathbb{Q}}$, 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 3.13
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 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2$. □

Osservazione 3.14 — 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 $\mathbb{Q}(\alpha) \hookrightarrow \overline{(QQ)}$ 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

$$\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 1$$

$$\zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 - \zeta_7^{-1})$$

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 Possibili gruppi di Galois

Vogliamo vedere quali gruppi finiti si possono realizzare come gruppi di Galois di un'estensione di campi.

Lemma 3.15

Dati p un primo e $f(x) \in \mathbb{Q}[x]$ 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 $\mathrm{Gal}(K/\mathbb{Q})S_p$.

Dimostrazione. Poiché $\deg f = p$ esiste un omomorfismo iniettivo

$$\Phi : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_p$$

inoltre $p \mid [K : \mathbb{Q}]$ in quanto $f(x)$ è irriducibile su $\mathbb{Q}$, pertanto $\Phi(\mathrm{Gal}(K/\mathbb{Q}))$ contiene un p-ciclo. Notiamo che contiene anche una trasposizione, che corrisponde alla restrizione del coniugio complesso in $\mathrm{Gal}(K/\mathbb{Q})$. □

Lemma 3.16 (Lemma di Artin)

Dato K un campo e G un sottogruppo finito di $\mathrm{Aut}(K)$, allora ${}^{K}\!/\!{}_{K^G}$ è un'estensione di Galois finita e $\mathrm{Gal}(K/K^G) = G$.

Dimostrazione. (In seguito scriverò la dimostrazione) □