# ALGEBRA 2 — GRUPPI

ALESSANDRO D'ANDREA

INDICE

## 1. Prime proprietà dei gruppi

### 1.1. **La nozione di gruppo.** Iniziamo dalla definizione di gruppo:

**Definizione 1.** Un insieme $G$, dotato di un'operazione $\cdot : G \times G \to G$ si dice *gruppo* se

- l'operazione $\cdot$ è associativa;
- esiste in $G$ un elemento $e$, detto "*identità*" , tale che $e \cdot x = x \cdot e = x$ per ogni $x \in G$;
- ogni elemento $g \in G$ ammette un "*inverso*" $g^{-1} \in G$, tale cioè che $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Scriverò spesso $ab$ oppure $a \cdot b$ invece del più pedante $\cdot(a, b)$. Inoltre eviterò quasi sempre di scrivere parentesi per indicare l'ordine nel quale effettuare i prodotti. Questo è in effetti reso superfluo dall'associatività dell'operazione di gruppo. Richiedere che $(ab)c$ sia uguale ad $a(bc)$ basta ad assicurare che ogni possibile moltiplicazione di un numero qualsiasi di elementi dia lo stesso risultato, indipendentemente dall'ordine nel quale viene effettuato, a patto che si rispetti la posizione di ciascun fattore. Ad esempio, per il prodotto di quattro elementi, l'associatività comporta che:

$$a(b(cd)) = a((bc)d) = (a(bc))d = ((ab)c)d) = (ab)(cd),$$

il che mostra che trascurare le parentesi e scrivere $abcd$ non è solo un abuso di notazione, ma la conseguenza di un fenomeno naturale.

Di questo bisognerebbe dare una dimostrazione rigorosa. Farlo è semplice, ma letta la dimostrazione le idee potrebbero essere più confuse di prima.[1] Per avere un'idea di come mostrarlo, date un'occhiata al libro di Artin (la Proposizione 1.4) che vi ho consigliato.

Una notazione compatta per i prodotti $aa, aaa, \dots$ consiste nello scrivere, come già si fa per il prodotto di numeri, $a^2, a^3, \dots$ Con $a^{-n}$ indicherò $(a^{-1})^n$. E' facile convincersi che $a^m a^n = a^{m+n}$ e che $(a^m)^n = a^{mn}$, se si pone $a^0 = e, a^1 = a$.

Abbiamo visto a lezione che l'associatività è una richiesta scontata quando gli elementi del nostro gruppo siano permutazioni su di un insieme, e come la stragrande maggioranza degli esempi di gruppi possano essere interpretati come azioni geometriche su di insiemi particolari, come ad esempio rotazioni in un piano, traslazioni su una retta, ecc...

**Esempi:**

- L'insieme $\mathrm{S}_X$ di tutte le applicazioni invertibili da un insieme $X$ in se stesso, con l'operazione di composizione, è un gruppo, detto il *gruppo delle permutazioni di* $X$. Se $X$ è un insieme finito, allora si sceglie solitamente $X = \{1, 2, ..., n\}$ e si scrive $\mathrm{S}_X = \mathrm{S}_n$. $\mathrm{S}_n$ ha $n!$ elementi.
- L'insieme delle rotazioni nel nel piano centrate nell'origine di angoli multipli di $2\pi/n$ è un gruppo, che si indica con $\mathrm{C}_n$. Abbiamo visto che questo gruppo possiede $n$ elementi, e che è un gruppo *ciclico*. Esso ammette cioè un elemento le cui potenze esauriscano tutti gli elementi del gruppo. Un elemento di tale tipo è detto *generatore* del gruppo ciclico. Ad esempio, la rotazione di $2\pi/n$ genera il gruppo ciclico $\mathrm{C}_n$.
- L'insieme $\mathrm{GL}_n(\mathbf{k})$ delle matrici $n \times n$ **non singolari**, cioè di determinante non nullo, a coefficienti in un campo $\mathbf{k}$ (ad esempio il campo $\mathbf{k} = \mathbb{R}$ dei numeri reali) è un gruppo rispetto al prodotto righe per colonne. Tale prodotto è infatti associativo, ed il prodotto di matrici di determinante non nullo è ancora una matrice di determinante non nullo. Inoltre l'identità ha determinante $1 \neq 0$, ed ogni matrice non singolare ha per inversa una matrice ancora non singolare.
- L'insieme $\mathrm{SL}_n(\mathbf{k})$ delle matrici $n$ per $n$ di determinante $1$ è ancora un gruppo, sempre rispetto al prodotto righe per colonne.
- Gli insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, se considerati con l'operazione $+$ di **somma**, sono gruppi. L'identità è in tutti i casi l'elemento $0$, mentre l'inverso di $\alpha$ è $-\alpha$.

[1] Ogni volta che si cerca di dimostrare un fatto intuitivo ed ovvio, si scopre che la dimostrazione non chiarisce nulla, oppure che il fatto era falso.

La notazione additiva nell'ultimo esempio non deve fuorviare: $+$ è decisamente un'operazione di gruppo. Indicare l'operazione di gruppo con $+$ invece che $\cdot$ è estremamente frequente quando l'operazione è commutativa, cioè quando $ab = ba$ per ogni coppia di elementi $a, b \in G$. Questi gruppi sono detti *abeliani*. Chiaramente, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono abeliani. E' abeliano anche $\mathrm{C}_n$, mentre non lo sono $\mathrm{S}_X$, $\mathrm{GL}_n$ ed $\mathrm{S}_n$.[2] Ora alcuni

**Non-esempi:**

- La famiglia $E_X$ di tutte le applicazioni dall'insieme $X$ in se stesso non è un gruppo.[3] In effetti, la composizione è un'operazione associativa, e l'identità ne è l'elemento neutro. Però un'applicazione ha inversi sinistri se e solo se è iniettiva, ed ha inversi destri se e solo se è suriettiva. Quindi non tutti gli elementi di $E_X$ ammettono inverso.
- L'insieme delle matrici $n \times n$ di determinante nullo non è un gruppo, rispetto al prodotto righe per colonne. Pur essendo tale prodotto associativo, e il prodotto di matrici singolari ancora singolare, non esiste in questo caso un elemento neutro per il prodotto.
- Gli insiemi di matrici $\mathrm{GL}_n(\mathbf{k}), \mathrm{SL}_N(\mathbf{k})$ non sono gruppi rispetto all'operazione di somma tra matrici.
- Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ non sono gruppi se considerati con l'operazione di moltiplicazione. Infatti l'elemento $0$ non ammette un inverso moltiplicativo. $\mathbb{Q} \setminus \{0\}$ e $\mathbb{R} \setminus \{0\}$ sono tuttavia gruppi rispetto alla moltiplicazione.

Nella prima lezione abbiamo dimostrato il semplice

**Teorema 1.1.** *In un gruppo $G$ esiste un'unica identità. Ogni elemento ammette un solo inverso. Inoltre $(g^{-1})^{-1} = g$, e $(gh)^{-1} = h^{-1}g^{-1}$.*

*Dimostrazione.* Siano $e, e'$ elementi neutri per l'operazione di gruppo. Questo vuol dire che

$$ex = xe = e, \qquad e'x = xe' = x$$

per ogni scelta di $x \in G$. In particolare $e = ee' = e'$, e quindi vi è un solo elemento neutro.

Si procede in maniera analoga per mostrare l'unicità dell'inverso: se $x$ e $y$ sono entrambi inversi di $g$, allora $gx = xg = e$, $gy = yg = e$. Ne segue che $x = xe = xgy = ey = y$, e quindi vi è un solo inverso di $g$. Le altre due proprietà seguono subito osservando che $gg^{-1} = g^{-1}g = e$, $ghh^{-1}g^{-1} = geg^{-1} = e$. □

Si vede che per invertire il prodotto $gh$ bisogna moltiplicare gli inversi degli elementi $g$ e $h$, **ma nell'ordine inverso**. Questo dipende dalla (possibile) non commutatività del prodotto. In un gruppo abeliano si avrebbe chiaramente $(ab)^{-1} = a^{-1}b^{-1}$. La stessa avvertenza è da fare con le potenze di un prodotto: infatti $(ab)^3$ non è l'elemento $a^3b^3$, bensì $ababab$!!!

**Definizione 2.** Sia $G$ un gruppo. Si dice che $g \in G$ ha *ordine infinito* se nessuna potenza di $g$ di esponente positivo è uguale all'identità. Altrimenti, l'*ordine* di $g$ è il minimo intero positivo $n$ tale che $g^n = e$.

Ad esempio, l'identità ha sempre ordine $1$, mentre ogni elemento non nullo di $(\mathbb{Z}, +)$ ha ordine infinito. L'ordine di $g$ si indica con $o(g)$.

**Teorema 1.2.** *Ogni elemento di un gruppo finito ha ordine finito.*

*Dimostrazione.* Le potenze di $g$ — e cioè $g, g^2, g^3, g^4, \ldots$ — non possono essere tutte distinte, dal momento che il gruppo al quale appartengono ha un numero finito di elementi. Vi è quindi almeno una ripetizione, cioè possiamo trovare interi $m > n$ tali che $g^m = g^n$. Ma allora, moltiplicando per l'inverso di $g^n$, otteniamo $g^{m-n} = e$, e quindi $g$ ha ordine finito. □

[2] A dire il vero, $\mathrm{S}_X$ è abeliano se $X$ contiene meno di tre elementi, mentre $\mathrm{GL}_n$ ed $\mathrm{SL}_n$ sono abeliani se $n \leq 1$.

[3] ...a meno che $X$ abbia meno di due elementi.

1.2. **Sottogruppi.**

**Definizione 3.** Sia $G$ un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice *sottogruppo*, se $H$ ammette una struttura di gruppo **rispetto alla stesso prodotto** di $G$.

Per indicare che $H$ è un sottogruppo di $G$, si usa la notazione $H < G$. Si vede facilmente che, se $H < G$, allora le identità di $H$ e di $G$ coincidono, e l'inverso di un elemento in $H$ è lo stesso che in $G$. Dal momento che l'operazione di gruppo di $G$ ristretta ad $H$ è automaticamente associativa, abbiamo

**Proposizione 1.3.** *Affinché un sottoinsieme non vuoto $H$ sia un sottogruppo di $G$ è sufficiente*[4] *che:*

- *se $a, b \in H$ allora anche $ab \in H$;*
- *se $a \in H$ allora anche $a^{-1} \in H$.*

*Dimostrazione.* L'identità $e$ appartiene automaticamente ad $H$. □

**Corollario 1.4.** *Affinché un sottoinsieme non vuoto* **e finito** *$H$ sia sottogruppo di $G$ è sufficiente che se $a, b \in H$ allora anche $ab \in H$.*

*Dimostrazione.* Ogni $a \in H$ ha necessariamente ordine finito. Di conseguenza, l'inverso $a^{-1} = a^{o(a)-1}$ può esprimersi come potenza di $a$ di esponente positivo, e quindi giace automaticamente in $H$, una volta che abbiamo controllato che $H$ sia chiuso rispetto al prodotto. □

**Esempi:**

- I sottoinsiemi $\{e\}$ e $G$ sono sempre sottogruppi di $G$: sono detti *sottogruppi banali*.
- Comunque sia scelto $m \in \mathbb{Z}$, l'insieme di tutti i multipli di $m$ è un sottogruppo di $\mathbb{Z}$.
- $\mathrm{SL}_n$ è un sottogruppo di $\mathrm{GL}_n$.
- Sia $g \in G$. L'insieme di tutte le potenze positive e negative $\langle g \rangle = \{g^i | i \in \mathbb{Z}\}$ è un sottogruppo di $G$. Il sottogruppo $\langle g \rangle$ è sempre abeliano.

1.3. **Congruenze modulo un sottogruppo e classi laterali.** Il concetto di congruenza modulo un sottogruppo generalizza quello di congruenza modulo $n$ nel gruppo $\mathbb{Z}$ degli interi, e permette di mostrare il fondamentale teorema di Lagrange, che è punto di partenza per lo studio dei gruppi finiti. Siano $G$ un gruppo, e $H$ un suo sottogruppo.

**Definizione 4.** Se $a, b \in G$, si dice che $a$ è *congruo* a $b$ modulo $H$, e si scrive

$$a \equiv b \mod H$$

se $a^{-1}b \in H$.

**Teorema 1.5.** *La congruenza modulo $H$ è una relazione di equivalenza.*

La dimostrazione è immediata. Qui è sufficiente ricordare che una relazione $\sim$ su di un insieme $X$ si dice *relazione di equivalenza* se valgono:

- $a \sim a$ (proprietà riflessiva)
- Se $a \sim b$ allora anche $b \sim a$ (proprietà simmetrica)
- Se $a \sim b$ e $b \sim c$ allora anche $a \sim c$ (proprietà transitiva)

per ogni scelta di $a, b, c \in X$.

Una classe di equivalenza è un sottoinsieme di elementi tutti equivalenti tra loro. Le relazioni di equivalenza servono a ripartire un insieme in unione disgiunta di classi di equivalenza. Questo dipende dal fatto che, a causa della proprietà transitiva, classi di equivalenza che hanno intersezione non vuota sono uguali: hanno cioé esattamente gli stessi elementi. Due classi di equivalenza sono disgiunte, oppure coincidono!

Nel caso della relazione di congruenza modulo un sottogruppo $H$, le classi di equivalenza sono facili da determinare. Abbiamo infatti mostrato a lezione che gli elementi

[4] Nonché ovviamente necessario...

congrui ad $a \in G$ modulo $H$ sono tutti e soli quegli elementi di $G$ che si scrivono come $ha$ per qualche elemento $h \in H$.

**Proposizione 1.6.** *La classe di congruenza modulo $H$ dell'elemento $a \in G$ coincide con il sottoinsieme $aH = \{ah \,|\, h \in H\}$.*

*Dimostrazione.* $a \equiv b \mod H$ se e solo se $a^{-1}b \in H$. Ad ogni modo, $a^{-1}b = h \in H$ è equivalente a $b = ah \in aH$. In altre parole, gli elementi in relazione con $a$ sono tutti e soli quelli che giacciono in $aH$. □

I sottoinsiemi del tipo $aH$ si dicono *classi laterali sinistre*, o semplicemente *laterali sinistri*, di $H$ in $G$. Avremmo potuto definire la relazione di congruenza modulo $H$ anche tramite la condizione $ab^{-1} \in H$. Questa nuova condizione non è equivalente all'altra che abbiamo dato, e fornisce una relazione differente. Le sue classi di equivalenza sono date dai laterali destri $Ha$ invece che da quelli sinistri. I sottogruppi per i quali i laterali sinistri coincidono con quelli destri, e quindi le due relazioni coincidono, si chiamano *sottogruppi normali*, e rivestono un ruolo rilevante nella teoria dei gruppi.

L'insieme dei laterali sinistri di $H$ in $G$, cioè l'insieme quoziente per la relazione di congruenza sopra introdotta, si indica con $G/H$, mentre quello dei laterali destri possiede la strana notazione $H\backslash G$.

**Proposizione 1.7.** *Gli insiemi $G/H$ e $H\backslash G$ hanno la stessa cardinalità.*

*Dimostrazione.* Le applicazioni $xH \mapsto Hx^{-1}$ e $Hy \mapsto y^{-1}H$ sono ben definite, e si invertono l'una l'altra. □

Come conseguenza, anche nel caso di gruppi infiniti, l'indice di un sottogruppo è un concetto ben definito, ed indipendente dalla decisione di considerare laterali destri o sinistri.

1.4. **Il Teorema di Lagrange e le sue conseguenze.** La proprietà rilevante dei laterali sinistri di un sottogruppo $H < G$ è che hanno tutti la stessa cardinalità.

**Proposizione 1.8.** *L'applicazione $H \ni h \mapsto ah \in aH$ è una corrispondenza biunivoca.*

*Dimostrazione.* La suriettività segue dalla stessa definizione di $aH$. L'iniettività è facile: se $ah_1 = ah_2$, allora moltiplicando a sinistra per $a^{-1}$ si ottiene $h_1 = h_2$. □

**Definizione 5.** L'ordine di un gruppo $G$ è il numero dei suoi elementi, e si indica con $|G|$.

**Definizione 6.** L'indice di un sottogruppo $H$, nel gruppo $G$ che lo contiene, è il numero dei laterali sinistri di $H$ in $G$ (ovvero la cardinalità dell'insieme quoziente $G/H$), e si indica con $[G : H]$.

La conclusione è immediata. $G$ è un insieme che viene ripartito in laterali sinistri $aH$ che hanno tutti la stessa cardinalità di $H$. Se il numero di laterali destri è $[G : H]$ allora si ha:

**Teorema 1.9.** *Se $H < G$ sono gruppi finiti, allora $|G| = [G : H]|H|$*

La notazione utilizzata per l'indice di $H$ in $G$ è suggestiva, infatti $[G : H] = |G|/|H|$. Il "diviso" non è solo un segno di interpunzione: è davvero, in qualche senso, un'operazione di divisione!

*Osservazione* 1.10. L'identità $|G| = [G : H]|H|$ è effettivamente un'uguaglianza tra cardinalità. In effetti, una volta scelto[5] un elemento $x_\alpha$ per ogni laterale sinistro di $H$ in $G$, l'applicazione

$$G/H \times H \ni (x_\alpha H, h) \mapsto x_\alpha h \in G$$

fornisce una corrispondenza biunivoca.

**Teorema 1.11** (Lagrange)**.** *Se $H$ è un sottogruppo del gruppo finito $G$, allora l'ordine di $H$ divide quello di $G$.*

[5] Questo richiede tuttavia l'utilizzo dell'assioma della scelta.

**Corollario 1.12.** *Se $g$ è un elemento del gruppo finito $G$, allora l'ordine di $g$ divide quello di $G$. In particolare $g^{|G|} = e$.*

*Dimostrazione.* L'ordine dell'elemento $g$ è pari a quello del sottogruppo

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$$

generato da $g$. Inoltre, $|G| = o(g) \cdot [G : (g)]$, quindi

$$g^{|G|} = g^{o(g)\cdot[G:(g)]} = (g^{o(g)})^{[G:(g)]} = e^{[G:(g)]} = e.$$

□

**Corollario 1.13.** *Un gruppo di ordine primo è ciclico, e i suoi unici sottogruppi sono quelli banali.*

*Dimostrazione.* Sia $|G| = p$, con $p$ primo. L'ordine degli elementi di $G$ divide $p$, e può quindi essere uguale solo ad $1$ oppure a $p$. L'identità è l'unico elemento che ha ordine $1$, e tutti gli altri devono avere ordine $p$. Questo vuol dire che per ogni scelta di $e \neq g \in G$, il sottogruppo $\langle g \rangle$ possiede $p$ elementi, e coincide quindi con $H$. In conclusione, $G$ è ciclico.

I sottogruppi sono necessariamente banali per lo stesso motivo: l'ordine di un sottogruppo è $1$ oppure $p$, e pertanto ogni dato sottogruppo contiene solo l'identità, oppure tutti gli elementi del gruppo $G$. □

1.5. **Intersezione e prodotto di sottogruppi.** Studiando l'algebra lineare, abbiamo già visto che l'intersezione di sottospazi vettoriali è un sottospazio vettoriale. Per ottenere il sottospazio generato da due sottospazi vettoriali non era invece sufficiente prendere l'unione dei due sottospazi, ma piuttosto la *somma* dei due, ovvero l'insieme di tutte le somme di un elemento del primo sottospazio con un elemento del secondo.

La situazione, nel caso dei gruppi abeliani, è praticamente la stessa. Per quanto riguarda quelli non abeliani bisogna prestare, invece, qualche attenzione.

**Proposizione 1.14.** *L'intersezione $H \cap K$ di due sottogruppi $H, K < G$ è un sottogruppo di $G$.*

*Dimostrazione.* $H \cap K$ è non vuoto, dal momento che l'identità $e$ vi appartiene sicuramente. Per mostrare che se $a, b \in H \cap K$ allora $ab \in H \cap K$ basta notare che $a$ e $b$ appartengono entrambi sia ad $H$ che a $K$. Essendo questi insiemi sottogruppi, sono chiusi rispetto al prodotto, perciò $ab$ giace sia in $H$ che in $K$, quindi nella loro intersezione. Per quanto riguarda l'inverso, il ragionamento è del tutto analogo. □

La dimostrazione data in classe delle seguenti due proposizioni è più o meno la stessa di quella che trovate sull'Herstein.

**Proposizione 1.15.** *Il prodotto $HK = \{hk | h \in H, k \in K\}$ di sottogruppi di $G$ è un sottogruppo se e solo se $HK = KH$.*

**Proposizione 1.16.** *Il sottoinsieme $HK$ ha esattamente $|H||K|/|H \cap K|$ elementi.*

**Corollario 1.17.** *Se $G$ è abeliano, e $H, K < G$, allora $HK$ è sempre un sottogruppo.*

Nel caso si stia utilizzando la notazione additiva all'interno di un gruppo, si scriverà ovviamente $H + K$ invece di $HK$.

**Esempio:** Sia $\mathbb{F}_p = \mathbb{Z}/(p)$ il campo delle classi di resto modulo $p$, dove $p$ è un numero primo. Uno spazio vettoriale $U$ di dimensione $n$ sul campo $\mathbb{F}_p$ è isomorfo a $\mathbb{F}_p^n$ e contiene pertanto $p^n$ elementi. Ogni sottospazio vettoriale di $U$ è in particolare un sottogruppo del gruppo additivo $(U, +)$. Se $V, W \subset U$ sono sottospazi vettoriali, e quindi sottogruppi additivi, si ottiene $|V + W| = |V||W|/|V \cap W|$, da cui

$$p^{\dim(V+W)} = p^{\dim V} p^{\dim W} / p^{\dim(V \cap W)},$$

e quindi $p^{\dim(V+W)+\dim(V\cap W)} = p^{\dim V + \dim W}$. Si nota immediatamente l'analogia con la formula di Grassmann $\dim(V+W)+\dim(V\cap W) = \dim V + \dim W$ che vale per sottospazi

vettoriali (di dimensioni finita) di uno spazio vettoriale qualsiasi.

Vediamo ora una generalizzazione del sottogruppo $\langle g \rangle$ generato da un elemento.

**Definizione 7.** Sia $G$ un gruppo, e $X \subset G$ un suo sottoinsieme. Il *sottogruppo di $G$ generato da $X$* è l'intersezione

$$\langle X \rangle = \bigcap_{H<G, X \subset H} H$$

dei sottogruppi di $G$ che contengono $X$.

L'intersezione di una collezione di sottogruppi di $G$ è ancora un sottogruppo — la dimostrazione data precedentemente nel caso di due soli sottogruppi si generalizza facilmente — e quindi $\langle X \rangle$ è sicuramente un sottogruppo di $G$, e contiene chiaramente $X$. Per come è stato definito, è il *più piccolo sottogruppo di $G$ che contenga $X$*, il che giustifica il nome di sottogruppo generato da $X$.

Se $H, K < G$, si preferisce indicare $\langle H \cup K \rangle$ con $\langle H, K \rangle$; in modo analogo, si indica $\langle \{g_1, \dots, g_r\} \rangle$ semplicemente con $\langle g_1, \dots, g_r \rangle$. E' evidente che $\langle H, K \rangle$ contiene sia $H$ che $K$, e quindi anche i prodotti $HK$, $KH$. Questo mostra che se $HK$ è un sottogruppo di $G$, allora $\langle H, K \rangle = HK$, a causa della minimalità del sottogruppo generato.

## 2. Esempi

2.1. **Il gruppo $\mathbb{Z}$.** L'insieme $\mathbb{Z}$, con l'operazione $+$ di somma, costituisce un gruppo abeliano. Infatti, $+$ è un'operazione commutativa ed associativa, della quale $0$ è l'elemento neutro. Inoltre, $-n$ è un inverso (additivo) dell'elemento $n$, e pertanto ogni elemento ammette inverso. $\mathbb{Z}$ è un gruppo ciclico; i suoi due generatori ciclici sono $1$ e $-1$. Nel caso del gruppo $\mathbb{Z}$, è tradizione indicare il sottogruppo generato da un sottoinsieme $X$ con $(X)$ invece che con $\langle X \rangle$. Il sottoinsieme $(n) \subset \mathbb{Z}$, composto dai multipli di un intero $n$ fissato, è un sottogruppo (ancora ciclico) di $\mathbb{Z}$.

**Teorema 2.1.** *I sottogruppi di $\mathbb{Z}$ sono tutti della forma $(n)$, per qualche $n \in \mathbb{N}$.*

*Dimostrazione.* Sia $H$ un sottogruppo di $\mathbb{Z}$. Se contiene solo lo $0$, allora $H = (0)$ ed abbiamo concluso. Se invece $H$ non contiene solo lo $(0)$, contiene allora certamente elementi positivi. Sia $n$ il minimo elemento positivo di $H$.

Allora $H = (n)$. Infatti, $H$ contiene certamente tutti i multipli di $n$. Inoltre, $H$ non può contenere un elemento $a$ non multiplo di $n$. Dovrebbe infatti contenere anche il resto della divisione di $a$ per $n$: in effetti, se $a = qn + r$, allora il resto $r = a + (-q) \cdot n$ appartiene ad $H$ poiché sia $a$ che $(-q)n$ appartengono ad $H$. Se il resto $r$ è diverso da $0$, è allora un elemento positivo di $H$ minore di $n$, da cui un assurdo. □

La relazione di congruenza modulo il sottogruppo $(n)$ è la normale congruenza modulo $n$ tra gli interi.

**Proposizione 2.2.** *Siano $c$ e $d$ il minimo comune multiplo ed il massimo comun divisore degli interi $a$ ed $b$. Allora $(a) \cap (b) = (c), (a) + (b) = (d)$.*

*Dimostrazione.* $(a) \cap (b)$ è sicuramente un sottogruppo, i cui elementi sono multipli sia di $a$ che di $b$. Il suo minimo elemento positivo è pertanto $c$, da cui $(a) \cap (b) = (c)$. Anche $(a) + (b)$ è un sottogruppo, pertanto della forma $(d)$. Gli interi $a$ e $b$ appartengono a $(d)$, pertanto $d$ è un divisore comune di $a$ e $b$.

Per mostrare che $d$ è il massimo tra i divisori comuni di $a$ e $b$, notiamo dapprima che $d \in (a) + (b)$, e che quindi si può scrivere come somma di un multiplo di $a$ e di uno di $b$. In altre parole esistono interi $m, n$ tali che $d = ma + nb$. Se $d'$ è un divisore comune di $a$ e $b$, allora deve dividere anche $d = ma + nb$, e pertanto $d' \leq d$. In altre parole, $d$ è il più grande tra i divisori comuni di $a$ e $b$. □

2.2. **Gruppi ciclici e diedrali.** Le isometrie del piano formano gruppo rispetto all'operazione di composizione. Infatti, la composizione di isometrie è chiaramente un'isometria; inoltre, l'identità è isometrica, e l'inverso di ogni isometria è ovviamente ancora una isometria.

Vi sono due tipi di isometrie: quelle che conservano l'orientazione e quelle che la invertono. Un semplice teorema di algebra lineare ci informa che le isometrie del piano che conservano l'orientazione sono traslazioni e rotazioni, mentre quelle che la invertono sono delle simmetrie rispetto ad una retta.

Fissiamo un $n$-agono regolare nel piano, e chiamiamo $\mathrm{D}_n$ (rispettivamente $\mathrm{C}_n$) l'insieme delle isometrie (risp. isometrie che conservano l'orientazione) che lo conservano, cioè che lo sovrappongono esattamente a se stesso. $\mathrm{D}_n$ e $\mathrm{C}_n$ contengono l'identità, e sono quindi insiemi non vuoti. Il gruppo $\mathrm{C}_n$ è generato dalla rotazione di $2\pi/n$ attorno al centro dell'$n$-agono, ed è quindi ciclico di ordine $n$. Il gruppo $\mathrm{D}_n$ si chiama *gruppo diedrale*, e contiene strettamente $\mathrm{C}_n$ come sottogruppo.

**Proposizione 2.3.** $|\,\mathrm{D}_n\,| = 2n$.

*Dimostrazione.* Ogni elemento di $\mathrm{D}_n$ è univocamente determinato dalla scelta delle immagini di due suoi vertici consecutivi. Le possibili immagini sono le coppie ordinate di vertici consecutivi dell'$n$-agono, che sono appunto $2n$. Questo mostra, in particolare, che $\mathrm{D}_n$ contiene $n$ rotazioni ed $n$ simmetrie. □

Sia ora $\rho$ la rotazione in senso antiorario di $2\pi/n$, e scegliamo una simmetria $s \in \mathrm{D}_n$. I due sottogruppi $H = \mathrm{C}_n = \langle\rho\rangle$ e $K = \langle s\rangle$ si intersecano nella sola identità: infatti l'altro elemento $s$ di $K$ non è una rotazione. Per questo motivo il sottoinsieme $HK$ contiene $|H||K|/|H \cap K| = 2n$ elementi, e coincide pertanto con l'intero gruppo $\mathrm{D}_n$. Abbiamo così dimostrato la

**Proposizione 2.4.** *Gli elementi $\rho^i, \rho^i s$, dove $i = 0, 1, \ldots, n-1$, formano una lista completa degli elementi di $\mathrm{D}_n$.*

In particolare tutti gli elementi $\rho^i s$ sono simmetrie, dal momento che gli elementi $\rho^i$ esauriscono tutte le rotazioni di $\mathrm{D}_n$. L'operazione di gruppo in $\mathrm{D}_n$ si descrive in modo semplice.

**Lemma 2.5.** $s\rho^i = \rho^{-i}s$ *per ogni* $i \in \mathbb{N}$.

*Dimostrazione.* L'elemento $\rho^i s$ è una simmetria, ed ha perciò ordine $2$. Questo mostra che $\rho^i s \rho^i s = e$, da cui si ottiene l'enunciato moltiplicando per $\rho^{-i}$ a sinistra, e per $s$ a destra. □

Si ottiene immediatamente:

**Proposizione 2.6.** *La composizione in $\mathrm{D}_n$ è tale che*

$$\begin{aligned} \rho^i \cdot \rho^j &= \rho^{i+j}, & \rho^i \cdot \rho^j s &= \rho^{i+j}s, \\ \rho^i s \cdot \rho^j &= \rho^{i-j}s, & \rho^i s \cdot \rho^j s &= \rho^{i-j}. \end{aligned}$$

Abbiamo già osservato che $\rho^n = e$, e di conseguenza, $\rho^{kn} = e$ per ogni $k \in \mathbb{Z}$. Questo mostra che per calcolare $\rho^i$ è importante conoscere soltanto la classe di resto di $i$ modulo $n$. Nella Proposizione precedente, le somme e le differenze tra esponenti vanno pertanto calcolate modulo $n$. E' facile, ora, determinare tutti i sottogruppi di $\mathrm{C}_n$ e $\mathrm{D}_n$.

**Proposizione 2.7.** *I sottogruppi di $\mathrm{C}_n$ sono tutti ciclici, e precisamente della forma $\mathrm{C}_m = \langle\rho^d\rangle$, dove $d$ ed $m$ sono divisori di $n$, tali che $n = md$.*

*Dimostrazione.* Sia $H$ un sottogruppo di $\mathrm{C}_n = \langle\rho\rangle$. Definiamo $E = \{i \in \mathbb{Z} \,|\, \rho^i \in H\}$. Chiaramente, $n \in E$. Inoltre $E$ è un sottogruppo di $\mathbb{Z}$, quindi è del tipo $(d)$, per qualche $d \in \mathbb{N}$. Dal momento che $n \in E = (d)$, allora $d$ divide $n$, ed $H = \langle\rho^d\rangle$. Se $n = dm$, $H$ è un gruppo ciclico di ordine $m$. □

Vale la pena di notare che, in $\mathrm{D}_n$, $\langle\rho^n\rangle$ è semplicemente $\langle e\rangle$.

**Proposizione 2.8.** *I sottogruppi di $\mathrm{D}_n$ sono ciclici della forma $\langle \rho^d \rangle$, oppure diedrali della forma $\langle \rho^d, \rho^i s \rangle$, dove $d$ è un divisore di $n$ e $0 \leq i < d$.*

*Dimostrazione.* Sia $H$ un sottogruppo di $\mathrm{D}_n$. Vi sono due possibilità: $H$ è completamente contenuto in $\mathrm{C}_n < \mathrm{D}_n$, oppure vi è qualche elemento di $H$ che inverte l'orientazione del piano. Nel primo caso, $H$ è un sottogruppo di $\mathrm{C}_n$, ed è quindi della forma $\mathrm{C}_m = \langle \rho^d \rangle$ per la Proposizione 2.7.

Nel secondo caso, $H$ contiene il sottogruppo $K = H \cap \mathrm{C}_n$, che è della forma $\langle \rho^d \rangle$ per un divisore opportuno $d$ di $n$. La relazione di congruenza modulo $K$ nel sottogruppo $H$ possiede soltanto due classi di equivalenza: quella delle rotazioni e quella delle simmetrie. Infatti, se $a, b \in H$ conservano entrambe, o invertono entrambe, l'orientazione, allora $a^{-1}b \in H$ conserva l'orientazione, ed è perciò una rotazione contenuta in $K$. Se invece una sola tra $a$ e $b$ è una rotazione, allora $ab^{-1}$ è una simmetria, e pertanto non contenuta in $K$.

Questo mostra che $K$ ha indice $2$ in $H$, e quindi $H$ contiene $2|K| = 2n/d$ elementi. Di conseguenza $H$ è generato da $\rho^d$ insieme ad una qualsiasi simmetria $\rho^i s \in H$; è possibile infine fare in modo che $0 \leq i < d$ moltiplicando per un'opportuna potenza di $\rho^d$. □

2.3. **Gruppi di ordine piccolo.** Darò ora la classificazione di tutti i gruppi di ordine minore di $8$. In realtà descriverò, più che i gruppi stessi, le classi di isomorfismo; il problema è che non sappiamo ancora che cosa sia un isomorfismo tra gruppi. Ci accontenteremo di una definizione intuitiva di questo concetto: per il momento, due gruppi *sono lo stesso gruppo* se le uniche differenze tra i due gruppi sono i nomi degli elementi. Ad esempio, il gruppo ciclico $\mathrm{C}_n$ ed il gruppo delle classi di resto modulo $n$ sono chiaramente "lo stesso gruppo".

Andiamo "per ordine". Se $|G| = 1$, allora $G = \langle e \rangle$ e non c'è altro da dire. Se l'ordine $p$ di $G$ è un numero primo, abbiamo già visto come $G$ sia necessariamente ciclico, e quindi $G = \mathrm{C}_p$. Questo risolve i casi $|G| = 2, 3, 5, 7$. Gli unici casi interessanti da trattare sono quindi $|G| = 4$ oppure $6$. Prima di procedere, è utile fare un'osservazione preliminare.

**Lemma 2.9.** *Se, nel gruppo $G$, ogni elemento $g \neq e$ ha ordine $2$, allora $G$ è abeliano.*

*Dimostrazione.* Ogni elemento $g \in G$ soddisfa $g^2 = e$, e quindi $g^{-1} = g$. Comunque siano scelti $a, b \in G$, allora, avremo $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. □

2.3.1. *Gruppi di ordine $4$.* Il teorema di Lagrange, che è per il momento lo strumento più sofisticato che abbiamo, ci dice che l'ordine degli elementi di un gruppo divide l'ordine del gruppo stesso. Se $|G| = 4$, allora, l'ordine degli elementi deve essere $1, 2$ oppure $4$. Se $G$ contiene un elemento di ordine $4$, allora è ciclico, ed è $\mathrm{C}_4$. Se $G$ non contiene elementi di ordine $4$, allora tutti gli elementi oltre l'identità devono avere ordine $2$, e quindi $G$ è abeliano per il Lemma 2.9.

Facciamo un elenco degli elementi. Oltre all'identità avremo tre elementi $a, b, c$. Ognuno di questi elementi ha ordine $2$, e pertanto è uguale al suo inverso. Che elemento otteniamo moltiplicando $a$ e $b$? Il risultato non può essere $a$, perché $ab = a$ implica $b = e$. Per lo stesso motivo non può essere $b$. $ab$ non può neanche essere l'identità, dal momento che $ab = e$ avrebbe come conseguenza $b = a^{-1} = a$. L'unica possibilità è che sia $ab = c$. Questo ragionamento si applica ogni volta che moltiplichiamo due elementi distinti scelti tra $a, b$ e $c$; avremo quindi $ab = ba = c$, $ac = ca = b$, $bc = cb = a$, oltre a $ge = eg = g$ per ogni $g \in G$: si verifica facilmente che questa operazione definisce una struttura di gruppo su $G$.

Questo è l'unico altro gruppo di ordine $4$ oltre a $\mathrm{C}_4$. E' abeliano, e talvolta è chiamato $V_4$, o gruppo di Klein. Vedremo più in là una ricetta per dare un nome ad ogni gruppo abeliano. Il nome che questo gruppo avrà, per il momento misterioso, è $\mathrm{C}_2 \times \mathrm{C}_2$.

2.3.2. *Gruppi di ordine* $6$. Usiamo sempre il teorema di Lagrange: i nostri elementi possono avere ordine $1, 2, 3$ oppure $6$. Se $G$ contiene un elemento di ordine $6$ allora è il gruppo ciclico $\mathrm{C}_6$. Se non contiene elementi di ordine $6$, allora oltre all'identità ci sono solo elementi di ordine $2$ o $3$. Abbiamo tre casi:

(1) **Gli elementi diversi dall'identità hanno tutti ordine** $2$**.** Per il Lemma 2.9, il gruppo è abeliano. Se $a \neq b$ sono elementi diversi da $e$, e poniamo $H = \langle a \rangle, K = \langle b \rangle$, $H$ e $K$ sono sottogruppi di ordine $2$, e $HK = KH$ a causa dell'abelianità del gruppo. Dal momento che $H \cap K = \langle e \rangle$, il sottoinsieme $HK = \{e, a, b, ab\}$ è un sottogruppo di ordine $4$. Ma $4$ non divide $6$, e il Teorema di Lagrange ci fornisce allora una contraddizione. Non esistono quindi gruppi di ordine $6$ di questo tipo.

(2) **Gli elementi diversi dall'identità hanno tutti ordine** $3$**.** Gli elementi di ordine $3$ si raggruppano tutti a coppie di elementi inversi tra loro: $a, a^{-1} = a^2 \neq a$. In $G$ abbiamo pertanto l'identità, e poi coppie di elementi di ordine $3$: in totale un numero dispari di elementi. Ma l'ordine di $G$ è $6$, che non è dispari. Anche questo caso non è quindi possibile.

(3) **Ci sono sia elementi di ordine** $2$ **che di ordine** $3$**.** Sia $a$ un elemento di ordine $3$, e $b$ uno di ordine $2$. Se $H = \langle a \rangle$ e $K = \langle b \rangle$, allora $H \cap K = \langle e \rangle$, e quindi $HK$ ha $6$ elementi, così come $KH$. Questo mostra che $HK = KH = G$. Se

$$H = \{e, a, a^2\}, \qquad K = \{e, b\},$$

allora

$$HK = \{e, a, a^2, b, ab, a^2b\}, \qquad KH = \{e, a, a^2, b, ba, ba^2\}.$$

Questi due elenchi di elementi coincidono per quanto riguarda $e, a, a^2$ e $b$. Gli altri due elementi sono $ab, a^2b$ in un caso e $ba, ba^2$ nell'altro. Pertanto, o $ab = ba$, oppure $ab = ba^2 = ba^{-1}$. Il secondo caso ci dà il gruppo diedrale, ovvero $\mathrm{S}_3$, mentre il primo caso non è possibile! Infatti, qual è l'ordine di $ab$? Poiché $ab = ba$, $G$ è un gruppo abeliano. Allora $(ab)^2 = a^2b^2 = a^2, (ab)^3 = a^3b^3 = b$. Questo vuol dire che $ab$ non ha ordine né $2$ né $3$. Per il Teorema di Lagrange, deve allora avere ordine $6$, un assurdo col fatto di aver supposto che $G$ non contenesse elementi di tale ordine.

Ricapitolando:

- $|G| = 1 \Rightarrow G = \langle e \rangle$
- $|G| = 2 \Rightarrow G = \mathrm{C}_2$
- $|G| = 3 \Rightarrow G = \mathrm{C}_3$
- $|G| = 4 \Rightarrow G = \mathrm{C}_4$ opp. $V_4$
- $|G| = 5 \Rightarrow G = \mathrm{C}_5$
- $|G| = 6 \Rightarrow G = \mathrm{C}_6$ opp. $\mathrm{S}_3 = \mathrm{D}_3$
- $|G| = 7 \Rightarrow G = \mathrm{C}_7$

è la lista dei gruppi di ordine $< 8$. Di questi solo $\mathrm{S}_3$ è non abeliano.

**Esercizio**[6]**:** Trovate tutti i gruppi **non abeliani** di ordine $8$.

Prima di passare ad altro, un'osservazione. Nella classificazione dei gruppi di ordine $6$ abbiamo usato, senza evidenziarlo adeguatamente, il seguente risultato.

**Teorema 2.10.** *Se $|G|$ è pari, allora $G$ contiene un elemento di ordine $2$.*

*Dimostrazione.* Raccogliamo ogni elemento $g$ assieme al proprio inverso $g^{-1}$. Gli unici elementi che stiano da soli sono gli elementi uguali al proprio inverso, ovvero l'identità e gli elementi di ordine $2$.

Se $G$ non contiene elementi di ordine $2$, l'unico elemento a presentarsi singolarmente è l'identità, mentre gli altri vengono a coppie. In altre parole, $G$ conterrebbe un numero dispari di elementi. Dal momento che $|G|$ è pari, vi sono necessariamente elementi di ordine $2$ — ed in totale sono in numero dispari! □

[6]Non facile, con i pochi strumenti che abbiamo finora a disposizione.

Vedremo fra non molto un teorema di Cauchy che generalizza questo risultato:

**Teorema 2.11** (Cauchy)**.** *Se un numero primo $p$ divide $|G|$, allora $G$ contiene almeno un elemento di ordine $p$.*

2.4. **Gruppi simmetrici.** Una permutazione di un insieme $X$ è una applicazione $\sigma : X \to X$ iniettiva e suriettiva, cioè invertibile. L'insieme $\mathrm{S}_X$ delle permutazioni di $X$ è un gruppo rispetto all'operazione di composizione, che indichiamo con $\circ$, o semplicemente sopprimendo il simbolo dell'operazione, e scrivendo $\sigma\tau = \sigma \circ \tau$. L'elemento neutro è l'identità $e = \mathrm{id}_X$.

Per individuare una permutazione bisogna descriverla in qualche maniera. La maggior parte delle volte, $X$ sarà un insieme finito: una situazione notazionalmente comoda si ha quando $X = \{1, \dots, n\}$. $\mathrm{S}_X$ si indica in questo caso con $\mathrm{S}_n$. Quando siamo in questa situazione, una permutazione è individuata fornendo l'immagine di ciascun elemento $1, \dots, n$. Ad esempio

$$\sigma : \begin{cases} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{cases}$$

indica la permutazione tale che $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$.

Esiste una notazione più compatta, e spesso più comoda, che utilizza la *decomposizione di una permutazione in prodotto di permutazioni cicliche disgiunte*.

**Definizione 8.** La $n$-upla ordinata $(x_1, \dots, x_n)$ di elementi di $X$ è *permutata ciclicamente* dalla permutazione $\sigma \in \mathrm{S}_X$ se $\sigma(x_i) = x_{i+1}$ quando $i = 1, \dots, n-1$ e $\sigma(x_n) = x_1$; in tal caso, diremo che $\sigma$ permuta ciclicamente il sottoinsieme $\{x_1, \dots, x_n\}$. Una permutazione $\sigma \in \mathrm{S}_X$ è una *permutazione ciclica*, o più precisamente un $n$-ciclo, se permuta ciclicamente $n > 1$ elementi di $X$, mentre gli altri elementi di $X$ vengono mandati in se stessi. Un $2$-ciclo è una *trasposizione*.

Due permutazioni cicliche si dicono *disgiunte* se gli insiemi che permutano ciclicamente hanno intersezione vuota.

Chiaramente, permutazioni cicliche disgiunte commutano tra loro. Ogni permutazione ciclica è individuata dalla $n$-upla ordinata di elementi che permuta ciclicamente. Ad esempio il $4$-ciclo

$$\tau : \begin{cases} 1 \to 5 \\ 2 \to 3 \\ 3 \to 1 \\ 4 \to 4 \\ 5 \to 2 \end{cases}$$

può essere più semplicemente indicato con $(1523)$, che illustra come $\tau(1) = 5, \tau(5) = 2, \tau(2) = 3, \tau(3) = 1$. Questa notazione non è unica: $(5231), (2315), (3152)$ descrivono la stessa permutazione. Diventa però univocamente determinata se decidiamo di scrivere il ciclo a partire dal suo elemento minimo.

**Proposizione 2.12.** *Sia $X$ un insieme finito. Ogni permutazione $\sigma \in \mathrm{S}_X$ decompone $X$ in unione disgiunta di sottoinsiemi permutati ciclicamente da $\sigma$.*

*Dimostrazione.* La relazione su $X$ definita imponendo che $x \sim y$ se e solo se esiste $n \in \mathbb{Z}$ tale che $y = \sigma^n(x)$ è chiaramente di equivalenza, e quindi decompone $X$ in unione disgiunta di classi di equivalenza. Comunque scegliamo $u \in X$, la sua classe di equivalenza contiene tutti e soli gli elementi della forma $\sigma^k(u), k \in \mathbb{Z}$. Ad ogni modo gli elementi $\sigma^k(u), k \in \mathbb{N}$ non possono essere tutti distinti, e quindi $\sigma^i(u) = \sigma^j(u)$ per qualche valore di $i \neq j$. Scegliendo $0 \leq i < j$ in modo che $i + j$ sia minimo, e applicando $\sigma^{-i}$ a entrambi i membri, si ottiene $\sigma^0(u) = \sigma^{j-i}(u)$, con $0 + (j - i) \leq i + j$. La minimalità di $i + j$ mostra allora che $i = 0$. In conclusione, $u, \sigma(u), \dots, \sigma^{j-1}(u)$ sono distinti, e $\sigma^j(u) = u$. In altre parole, $\sigma$ permuta $U = \{u, \sigma(u), \dots, \sigma^{j-1}(u)\}$ ciclicamente, e quindi $U$ coincide con la classe di equivalenza di $u$. □

**Corollario 2.13.** *Se $X$ è un insieme finito, ogni permutazione $\mathrm{id} \neq \sigma \in \mathrm{S}_X$ si esprime come composizione di permutazioni cicliche disgiunte.*

*Dimostrazione.* La permutazione $\sigma$ decompone $X$ in unione disgiunta di sottoinsiemi che permuta ciclicamente. Allora $\sigma$ è prodotto delle permutazioni cicliche relative ai sottoinsiemi di cardinalità maggiore di $1$. □

La notazione compatta per indicare una permutazione qualsiasi consiste nello scrivere esplicitamente tutti i suoi cicli, trascurando gli elementi che vengono invece mandati in se stessi. Ad esempio le due permutazioni di $\mathrm{S}_7$:

$$\phi : \begin{cases} 1 \to 2 \\ 2 \to 5 \\ 3 \to 7 \\ 4 \to 1 \\ 5 \to 4 \\ 6 \to 3 \\ 7 \to 6 \end{cases} \qquad \psi : \begin{cases} 1 \to 6 \\ 2 \to 4 \\ 3 \to 2 \\ 4 \to 5 \\ 5 \to 1 \\ 6 \to 7 \\ 7 \to 3 \end{cases}$$

si scriveranno $\phi = (1254)(376)$ e $\psi = (1673245)$, mentre $\phi\psi = (1352)$ e $\psi\phi = (1462)$. Dal momento che permutazioni cicliche disgiunte commutano tra loro, le permutazioni $(1254)(376)$ e $(376)(1254)$ coincidono. Il lemma che segue è di dimostrazione immediata.

**Lemma 2.14.** *L'ordine di un $n$-ciclo è $n$. L'ordine di un prodotto di cicli disgiunti è uguale al minimo comune multiplo delle lunghezze dei suoi cicli.*

Sappiamo già che il gruppo $\mathrm{S}_n$ possiede $n!$ elementi. Utilizzando la notazione appena introdotta, i $6$ elementi di $\mathrm{S}_3$ sono: $e, (12), (13), (23), (123), (132)$.

Le permutazioni si distinguono in *pari* e *dispari*. Dato un elemento $\sigma \in \mathrm{S}_n$ ed un polinomio $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$, possiamo definire $f^\sigma(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. E' facile vedere che i polinomi $f^{\sigma\tau}$ e $(f^\sigma)^\tau$ coincidono, e che $(fg)^\sigma = f^\sigma g^\sigma$. Consideriamo ora il polinomio

$$\Delta(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Si vede subito che i fattori presenti nel prodotto

$$\Delta^\sigma(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

sono gli stessi che sono presenti in quello che definisce $\Delta$, a meno eventualmente di un segno.

**Definizione 9.** Il *segno* della permutazione $\sigma \in \mathrm{S}_n$ è il rapporto

$$\mathrm{sgn}(\sigma) = \Delta^\sigma(x_1, \ldots, x_n)/\Delta(x_1, \ldots, x_n) \in \{\pm 1\}.$$

**Proposizione 2.15.** *L'applicazione $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ soddisfa $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ per ogni $\sigma, \tau \in \mathrm{S}_n$; inoltre $\mathrm{sgn}(\tau) = -1$ per ogni trasposizione $\tau$.*

*Dimostrazione.* La proprietà di omomorfismo segue da

$$\mathrm{sgn}(\sigma\tau) = \frac{\Delta^{\sigma\tau}}{\Delta} = \frac{\Delta^\sigma}{\Delta} \cdot \frac{\Delta^{\sigma\tau}}{\Delta^\sigma} = \frac{\Delta^\sigma}{\Delta} \cdot \frac{(\Delta^\sigma)^\tau}{\Delta^\sigma} = \mathrm{sgn}(\sigma) \cdot \frac{(\mathrm{sgn}(\sigma)\Delta)^\tau}{\mathrm{sgn}(\sigma)\Delta} = \mathrm{sgn}(\sigma) \cdot \frac{\Delta^\tau}{\Delta} = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau).$$

Per quanto riguarda la seconda affermazione, quando $\tau = (12)$, $\tau(i) < \tau(j)$ ogni volta che $i < j$, tranne che per $i = 1, j = 2$. Questo mostra che $\Delta^\tau = -\Delta$, e quindi che $\mathrm{sgn}(\tau) = -1$. Ma allora $\mathrm{sgn}((1j)) = \mathrm{sgn}((2j)(12)(2j)) = \mathrm{sgn}((2j))^2\,\mathrm{sgn}(12) = -1$, e $\mathrm{sgn}((ij)) = \mathrm{sgn}((1i)(1j)(1i)) = \mathrm{sgn}((1i))^2\,\mathrm{sgn}(1j) = -1$. □

*Osservazione* 2.16.
- Alla luce della proposizione appena dimostrata, per calcolare il segno di una permutazione è sufficiente esprimerla come prodotto di trasposizioni. Se sono necessarie $n$ trasposizioni, il segno è allora uguale a $(-1)^n$.

- A causa della moltiplicatività di $\mathrm{sgn}$, il sottoinsieme $\{\sigma \in \mathrm{S}_n \mid \mathrm{sgn}(\sigma) = 1\}$ è un sottogruppo di $\mathrm{S}_n$.

**Definizione 10.** Una permutazione $\sigma \in \mathrm{S}_n$ è *pari* se $\mathrm{sgn}(\sigma) = 1$ e *dispari* altrimenti. Il sottogruppo di tutte le permutazioni pari di $\mathrm{S}_n$ è detto *sottogruppo alterno*, e si indica con $\mathrm{A}_n$.

Ad esempio, in $\mathrm{S}_3$, le permutazioni $(12), (13), (23)$ sono dispari, mentre $e, (123), (132)$ sono pari. Questo si vede utilizzando la definizione di $\mathrm{sgn}$, oppure utilizzando l'Osservazione 2.16 insieme al fatto che $(123) = (13)(12), (132) = (12)(13)$.

**Proposizione 2.17.** *$\mathrm{A}_n$ ha indice $2$ in $\mathrm{S}_n$. Se $H$ è un sottogruppo di $\mathrm{S}_n$ non interamente contenuto in $\mathrm{A}_n$, allora $H \cap \mathrm{A}_n$ ha indice $2$ in $H$.*

*Dimostrazione.* Due permutazioni $\sigma$ e $\tau$ sono congrue modulo $\mathrm{A}_n$ quando $\sigma^{-1}\tau$ è pari, cioè quando hanno la stessa parità. Vi sono quindi solo due classi laterali destre di $\mathrm{A}_n$, che ha pertanto indice $2$ e ordine $n!/2$. Lo stesso discorso vale per un sottogruppo $H$ di $\mathrm{S}_n$ non contenuto in $\mathrm{A}_n$. □

2.5. **Sottogruppi di $\mathrm{A}_4$.** Come esercizio, elenchiamo tutti i sottogruppi di $\mathrm{S}_4$. L'ordine dei sottogruppi di $\mathrm{S}_4$ divide $4! = 24$. I divisori di $24$ sono $1, 2, 3, 4, 6, 8, 12$ e $24$. Sia $H < \mathrm{S}_4$: se $|H| = 1$ o $24$ allora $H$ è un sottogruppo banale. I sottogruppi ciclici sono facili da determinare: sono generati da singoli elementi di $\mathrm{S}_4$. Le trasposizioni e i prodotti di due trasposizioni disgiunte generano sottogruppi ciclici di ordine $2$, i $3$-cicli ne generano di ordine $3$, e i $4$-cicli di ordine $4$. D'altronde, i sottogruppi di ordine $2$ e $3$ devono essere necessariamente ciclici, pertanto se $H$ non è ciclico, possiamo limitarci a studiare i casi $|H| = 4, 6, 8, 12$. Prima di procedere, alcune osservazioni utili:

**Lemma 2.18.** *Il sottogruppo alterno $\mathrm{A}_4$ contiene l'identità, i tre prodotti di due trasposizioni disgiunte, e gli otto $3$-cicli.*

**Lemma 2.19.** *Il sottoinsieme $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ è un sottogruppo di $\mathrm{A}_4$.*

**Lemma 2.20.** *$\mathrm{A}_4$ non ha sottogruppi di ordine $6$.*

*Dimostrazione.* Non vi sono elementi di ordine $6$, quindi $\mathrm{A}_4$ non ha sottogruppi ciclici di ordine $6$. Abbiamo visto nel paragrafo 2.3.2 che un gruppo non ciclico di ordine $6$ possiede due elementi di ordine $3$ e tre di ordine $2$. In particolare, contiene i tre prodotti di due trasposizioni disgiunte, e quindi contiene il sottogruppo $V_4$, il che è un assurdo, dal momento che $4$ non divide $6$. □

In ciò che segue, $H$ è un sottogruppo non ciclico di $\mathrm{S}_4$.

2.5.1. $|H| = 4$. Se $H$ è interamente contenuto in $\mathrm{A}_4$, allora $H$ può contenere solo gli elementi $e$, $(12)(34)$, $(13)(24)$ e $(14)(23)$, che sono gli unici ad avere ordine che divide $4$, e quindi $H = V_4$.

Se invece $H$ non è contenuto in $\mathrm{A}_4$, allora $H \cap \mathrm{A}_4$ possiede due elementi, e quindi contiene solo un prodotto di due trasposizioni disgiunte. Gli altri elementi di $H$ devono essere permutazioni dispari, che hanno ordine $2$ essendo $H$ non ciclico. Facciamo un esempio pratico: se $H \cap \mathrm{A}_4 = \{e, (12)(34)\}$, $H$ può contenere solo $(12)$ e $(34)$ perché il prodotto di $(12)(34)$ con le altre permutazioni fornisce come risultato $4$-cicli. Ricapitolando, i quattro sottogruppi non ciclici di ordine $4$ sono quindi

$$\{e, (12)(34), (13)(24), (14)(23)\}, \qquad \{e, (12), (34), (12)(34)\},$$
$$\{e, (13), (24), (13)(24)\}, \qquad \{e, (14), (23), (14)(23)\}.$$

2.5.2. $|H| = 6$. $H$ non è ciclico ed ha quindi tre elementi di ordine $2$ e due di ordine $3$. Questi ultimi sono $3$-cicli, e sono elementi pari. Abbiamo visto che $H$ non è contenuto in $\mathrm{A}_4$, e quindi gli elementi di ordine due devono essere dispari, e perciò trasposizioni. Queste non possono fissare l'elemento fissato dai $3$-cicli, perché altrimenti potremmo ottenere un $4$-ciclo come prodotto di tale trasposizione per il $3$-ciclo — ad esempio:

$(123)(34) = (1243)$ — e $4$ non divide $|H|$. Perciò le trasposizioni muovono gli elementi che sono permutati dai $3$-cicli. Questo ci fornisce $4$ sottogruppi:

$$\{e, (12), (13), (23), (123), (132)\}, \qquad \{e, (12), (14), (24), (124), (142)\},$$
$$\{e, (13), (14), (34), (134), (143)\}, \qquad \{e, (23), (24), (34), (234), (243)\}.$$

2.5.3. $|H| = 8$. $H$ non è contenuto in $\mathrm{A}_4$, poiché $8$ non divide $12$, quindi il sottogruppo degli elementi pari di $H$ è $\{e, (12)(34), (13)(24), (14)(23)\}$. Gli elementi dispari che $H$ può contenere sono trasposizioni o $4$-cicli. In ogni caso, moltiplicando una trasposizione per uno dei tre prodotti di due trasposizioni si ottiene un $4$-ciclo, e quindi $H$ contiene necessariamente un $4$-ciclo. Alla stessa maniera se $H$ contiene un $4$-ciclo, contiene anche una trasposizione — basta moltiplicare il $4$-ciclo per uno, tra gli elementi $(12)(34), (13)(24), (14)(23)$ che non sia il suo quadrato. I possibili sottogruppi di otto elementi sono quindi determinati:

$$\{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\},$$
$$\{e, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\},$$
$$\{e, (14), (23), (12)(34), (13)(24), (14)(23), (1243), (1342)\}.$$

2.5.4. $|H| = 12$. Se $H$ è contenuto in $\mathrm{A}_4$, coincide con esso. Se $H$ non è contenuto in $\mathrm{A}_4$, allora $H \cap \mathrm{A}_4$ ha ordine $6$. Ma abbiamo già visto che $\mathrm{A}_4$ non ha sottogruppi di ordine $6$.

2.6. **Il gruppo delle unità modulo $n$.** Se $A$ è un anello con unità, l'insieme $A^\times$ dei suoi elementi invertibili è un gruppo rispetto alla moltiplicazione. Ci proponiamo di studiare il gruppo moltiplicativo formato dagli invertibili dell'anello $\mathbb{Z}/(n)$ delle classi di resto modulo $n$. Il nostro primo obiettivo è quello di individuare quali e quanti siano i suoi elementi.

Indichiamo con $(a, b)$ il massimo comun divisore di due interi $a$ e $b$. Se $d = (a, b)$ allora, come abbiamo visto prima, $(d) = (a) + (b)$. e quindi esistono interi $h$ e $k$ tali che $d = ha + kb$.

**Definizione 11.** Due interi $a$ e $b$ sono *primi tra loro* quando $(a, b) = 1$.

Alla luce del teorema di fattorizzazione unica in $\mathbb{Z}$, le fattorizzazioni in primi di numeri primi tra loro non hanno fattori primi in comune.

**Lemma 2.21.** *Se $a$ e $b$ sono primi con $n$, allora anche il prodotto $ab$ è primo con $n$.*

*Dimostrazione.* I primi che dividono $n$ non dividono $a$ né $b$, e quindi non dividono neanche $ab$. Perciò, $ab$ e $n$ sono primi tra loro. □

**Lemma 2.22.** *Siano $a$ e $b$ tali che $a \equiv b \mod n$. Allora $a$ è primo con $n$ se e solo se lo è anche $b$. In altre parole il fatto di essere primo con $n$ dipende solo dalla classe di resto modulo $n$.*

*Dimostrazione.* Basta mostrare che $(a, n) = (a + kn, n)$ per ogni $k \in \mathbb{Z}$. Questo è immediato. Se $d$ divide sia $a$ che $n$, allora divide anche $a + kn$. Allo stesso modo, se $d$ divide sia $a + kn$ che $n$, allora divide anche $a = (a + kn) - kn$. Quindi i divisori comuni di $a$ e $n$ coincidono con i divisori comuni di $a + kn$ ed $n$, e $(a, n) = (a + kn, n)$. □

**Lemma 2.23.** *Se $a$ è primo con $n$, allora esiste $b$, primo con $n$, tale che $ab \equiv 1 \mod n$.*

*Dimostrazione.* Poiché $(a, n) = 1$, allora possiamo trovare interi $b, k$ tali che $ab + kn = 1$. Questo mostra che $ab \equiv 1 \mod n$, ed inoltre che $(b, n) = 1$. □

**Definizione 12.** Una classe di resto modulo $n$ si dice una *unità* se è prima con $n$. L'insieme delle unità modulo $n$ si indica con $\mathbb{Z}/(n)^\times$.

*Osservazione* 2.24. E' evidente che se $a$ ammette un inverso modulo $n$, allora deve essere primo con $n$. In effetti, poiché $ab \equiv 1 \mod n$, $ab$ è primo con $n$, e quindi la sua fattorizzazione non ha primi in comuni con quella di $n$. Lo stesso è allora vero per $a$.

**Proposizione 2.25.** *$\mathbb{Z}/(n)^\times$ è un gruppo rispetto alla moltiplicazione.*

*Dimostrazione.* Per il Lemma 2.21, il prodotto di unità modulo $n$ è ancora un'unità. Tale prodotto è associativo, essendo la restrizione del prodotto associativo sugli interi modulo $n$. La classe di resto di $1$ appartiene ad $\mathbb{Z}/(n)^\times$, e ne è l'elemento neutro. Dal Lemma 2.23 segue che ogni elemento di $\mathbb{Z}/(n)^\times$ ha un inverso in $\mathbb{Z}/(n)^\times$. □

**Esempi:** $\mathbb{Z}/(p)^\times = \{1, 2, ..., p-1\}$ se $p$ è primo.
$\mathbb{Z}/(8)^\times = \{1, 3, 5, 7\}$. $\mathbb{Z}/(10)^\times = \{1, 3, 7, 9\}$. $\mathbb{Z}/(15)^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Il numero di elementi di $\mathbb{Z}/(n)^\times$ si indica con $\phi(n)$. Ad esempio $\phi(p) = p-1$ se $p$ è primo, mentre $\phi(8) = 4, \phi(10) = 4, \phi(15) = 8$. Il valore di $\phi(n)$ si calcola facilmente una volta nota la fattorizzazione di $n$. Si ha infatti:

$$\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Alternativamente, si può utilizzare il fatto che se $m$ ed $n$ sono primi tra loro, allora

$$\phi(mn) = \phi(m)\phi(n), \tag{2.1}$$

e che se $p$ è primo, $n > 0$, si ha:

$$\phi(p^n) = (p-1)p^{n-1}.$$

Per compatibilità con (2.1), si pone in genere $\phi(1) = 1$.

**Teorema 2.26** (Eulero)**.** *Se $a$ è primo con $n$, allora $a^{\phi(n)} \equiv 1 \mod n$.*

*Dimostrazione.* Il gruppo $\mathbb{Z}/(n)^\times$ ha ordine $\phi(n)$. Sia $a$ primo con $n$, ed indichiamo con $\overline{a}$ la sua classe di resto modulo $n$. Allora, per il Corollario 1.12, $\overline{a}^{\phi(n)} = \overline{1}$, e quindi $a^{\phi(n)} \equiv 1 \mod n$. □

Questo teorema ha come conseguenza il cosiddetto piccolo Teorema di Fermat.

**Teorema 2.27** (Fermat)**.** *Se $p$ è primo, allora $a^p \equiv a \mod p$.*

*Dimostrazione.* Sappiamo che $\phi(p) = p-1$. Se $a$ è primo con $p$, allora $a^{p-1} \equiv 1 \mod p$. Moltiplicando per $a$ si ottiene $a^p \equiv a \mod p$. Se invece $a$ è divisibile per $p$, allora sia $a^p$ che $a$ sono congrui a $0$ modulo $p$. □

**Esercizi:**

*(a)* Sia $G$ un gruppo **abeliano**, ed $a, b$ elementi di $G$ di ordine $m$ ed $n$ rispettivamente. Che si può dire dell'ordine di $ab$?

*(b)* Dare esempi di gruppi in cui il prodotto di elementi di ordine $2$ abbia ordine $1, 2, 3$.

*(c)* Sull'insieme $\mathbb{Z}$ definiamo il prodotto

$$a \circ b = \begin{cases} a + b \text{ se } a \text{ è pari} \\ a - b \text{ se } a \text{ è dispari} \end{cases}$$

Fate vedere che $\mathbb{Z}$ è un gruppo rispetto all'operazione $\circ$, e che contiene elementi di ordine $2$ il cui prodotto ha ordine infinito. Mostrate inoltre che $(\mathbb{Z}, \circ)$ ammette un sottogruppo infinito di indice $2$.

## 3. Omomorfismi di gruppi e sottogruppi normali

### 3.1. Sottogruppi normali e gruppi quoziente.

**Definizione 13.** Un sottogruppo $N < G$ si dice *normale* se $gNg^{-1} \subset N$ per ogni $g \in G$.

Abbiamo visto a lezione la rilevanza dei sottogruppi normali: sono quelli per i quali l'operazione di gruppo in $G$ definisce una buona operazione di composizione sull'insieme $G/N$ delle classi laterali. Il teorema dimostrato a lezione era:

**Teorema 3.1.** *Sia $N$ un sottogruppo di un gruppo $G$. Sono proprietà equivalenti di $N$:*

(1) *$gNg^{-1} \subset N$ per ogni $g \in G$.*

(2) $gNg^{-1} = N$ *per ogni* $g \in G$.
(3) $Ng = gN$ *per ogni* $g \in G$.
(4) *La moltiplicazione* $(Na) \cdot (Nb) = Nab$ *è ben definita.*

*Dimostrazione.* (1) $\Rightarrow$ (2): Sappiamo già che $gNg^{-1} \subset N$; basta quindi mostrare che $N \subset gNg^{-1}$. Ma si può ottenere $n$ come $g(g^{-1}ng)g^{-1}$. La normalità di $N$ mostra che $n' = g^{-1}ng \in g^{-1}N(g^{-1})^{-1}$ è un elemento di $N$, ed abbiamo quindi scritto $n = g^{-1}n'g$ per un'opportuna scelta di $n' \in N$.
(2) $\Rightarrow$ (3): Se $gng^{-1} \in N$ ogni volta che $n \in N$, allora $gn \in Ng$ per ogni $g \in G, n \in N$. Questo mostra che $gN \subset Ng$. Inoltre $ng = g(g^{-1}ng)$ e quindi $Ng \subset gN$. Pertanto $Ng = gN$.
(3) $\Rightarrow$ (4): Se $X, Y$ sono sottoinsiemi di $G$, indichiamo con $XY$ l'insieme dei prodotti $xy, x \in X, y \in Y$. Allora possiamo scrivere

$$(Na)(Nb) = (aN)(Nb) = aNNb = aNb = (aN)b = (Na)b = Nab.$$

Questo mostra che scegliendo un elemento da $Na$ e moltiplicandolo per un elemento di $Nb$, si ottiene un risultato che appartiene sempre ad $Nab$. In altre parole, la classe di congruenza modulo $N$ di $ab$ dipende solo dalle classi di congruenza di $a$ e $b$. Pertanto il prodotto è ben definito.
(4) $\Rightarrow$ (1): Se la moltiplicazione è ben definita, allora $(na)(n'b) \in Nab$. Questo vuol dire che $nan'b \in Nab$ per ogni $a, b \in G, n, n' \in N$, e quindi $nan'a^{-1} \in N$. Allora anche $an'a^{-1} \in N$. Perciò $aNa^{-1} \subset N$ per ogni $a \in G$. □

**Corollario 3.2.** *Un sottogruppo di indice* $2$ *è normale.*

*Dimostrazione.* Un sottogruppo $H < G$ di indice $2$ ha solo due laterali destri. Uno di questi è $H$ stesso, e l'altro non può che essere il suo complementare. Lo stesso ragionamento vale per i laterali sinistri. Perciò ogni laterale sinistro è anche destro, e $H \lhd G$. □

**Esempi:**

- Ogni sottogruppo di un gruppo abeliano è normale.
- $\mathrm{A}_n$ è un sottogruppo normale di $\mathrm{S}_n$. Infatti, ha indice $2$.
- Se $\sigma = (12), H = (\sigma)$ allora $H$ non è normale in $\mathrm{S}_3$. Infatti $(13)(12)(13)^{-1} = (23) \notin H$.
- Sia $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Allora $H \lhd \mathrm{A}_4$. Vedremo in seguito che per $n \geq 5$ $\mathrm{A}_n$ non ha sottogruppi normali non banali.
- Non è vero che se i sottogruppi di un gruppo sono tutti normali, il gruppo deve essere necessariamente abeliano. Sia infatti $\mathrm{Q}_4$ il gruppo delle unità dei quaternioni. I suoi sottogruppi di ordine $4$ hanno indice $2$, e sono normali. Vi è un solo sottogruppo di ordine $2$, e precisamente $\{\pm 1\}$, che giace nel centro di $\mathrm{Q}_4$ ed è quindi normale. Gli altri sottogruppi sono quelli banali, che sono automaticamente normali. Quindi ogni sottogruppo di $\mathrm{Q}_4$ è normale.

Quando $N$ è un sottogruppo normale di $G$, i due insiemi quoziente $G/N$ e $G\backslash N$ coincidono, e li indicheremo entrambi con $G/N$. Abbiamo visto come il prodotto in $G$ induca un'operazione sul quoziente $G/N$ se $N \lhd G$.

**Teorema 3.3.** *L'operazione indotta da* $G$ *su* $G/N$ *definisce una struttura di gruppo.*

*Dimostrazione.* La dimostrazione è ovvia: $Ne$ è l'identità, $Ng^{-1}$ è l'inverso di $Ng$. Inoltre il prodotto è associativo poiché $(NaNb)Nc = NabNc = N(ab)c = Na(bc) = Na(Nbc) = Na(NbNc)$. □

Si noti che se definiamo $\pi_N : G \to G/N$ come $\pi_N(g) = Ng = gN$, allora $\pi_N(ab) = \pi_N(a)\pi_N(b)$. Su questa proprietà è basato il concetto di omomorfismo.

**Esercizi:**
*(a)* Il centro $Z$ di un gruppo $G$ è un sottogruppo normale di $G$.
*(b)* Sia $H < G$. Il sottoinsieme $\{g \in G | g^{-1}Hg = H\}$ è detto *normalizzatore* di $H$ in $G$, e si indica con $N(H)$. Mostrate che $H \lhd N(H)$.

*(c)* Sia $H < G$. Mostrate che il sottoinsieme $\{g \in G | gHg^{-1} \subseteq H\}$ è un sottogruppo di $G$ *se $G$ è un gruppo finito*, ed in tal caso coincide con il normalizzatore di $H$ in $G$.
*(d)* Sia $G$ il sottoinsieme di $\mathrm{GL}_2(\mathbb{Q})$ costituito da tutte le matrici della forma

$$\begin{pmatrix} 2^k & q \\ 0 & 2^{-k} \end{pmatrix},$$

dove $k \in \mathbb{Z}, q \in \mathbb{Q}$, e sia

$$H = \left\{ \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}, q \in \mathbb{Z} \right\} \subset G.$$

Mostrate che $H \lhd G$, e che il sottoinsieme $\{g \in G | gHg^{-1} \subseteq H\}$ **non** è un sottogruppo di $G$.
*(e)* Sia $H < G$. Il centralizzatore di $H$ in $G$ è il sottoinsieme $C(H) = \{g \in G | gh = hg$ per ogni $h \in H\}$. Mostrate che $C(H)$ è un sottogruppo di $G$ e che $C(H) \lhd G$ se $H \lhd G$.

3.2. **Omomorfismi di gruppi.** Siano $G, \overline{G}$ due gruppi

**Definizione 14.** $\phi : G \to \overline{G}$ è un *omomorfismo di gruppi*, o più semplicemente un *omomorfismo*, se

$$\phi(ab) = \phi(a)\phi(b)$$

per ogni scelta di $a, b \in G$. Un omomorfismo invertibile si dice *isomorfismo*, mentre un isomorfismo di un gruppo su se stesso si dice *automorfismo*.

**Proposizione 3.4.** *Se $\phi : G \to \overline{G}$ è un omomorfismo di gruppi, allora $\phi(e) = \bar{e}$ e $\phi(g^{-1}) = \phi(g)^{-1}$ per ogni $g \in G$.*

*Dimostrazione.* Poiché $e \cdot e = e$ in $G$, si ha $\phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$. Moltiplicando a sinistra per l'inverso di $\phi(e)$ in $\overline{G}$ si ottiene $\phi(e) = \bar{e}$. Allo stesso modo, da $g \cdot g^{-1} = e$ segue $\bar{e} = \phi(e) = \phi(g \cdot g^{-1}) = \phi(g)\phi(g^{-1})$. Di conseguenza, $\phi(g^{-1})$ è l'inverso di $\phi(g)$.
□

**Esempi:**

- L'applicazione che manda ogni elemento del gruppo $G$ nell'identità di un altro gruppo è un omomorfismo.
- L'applicazione identità da un gruppo in sé è un omomorfismo. E' l'automorfismo identico del gruppo
- L'applicazione $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ è un omomorfismo. Infatti $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ per ogni $\sigma, \tau \in \mathrm{S}_n$.
- L'applicazione $\det : \mathrm{GL}_n(\mathbf{k}) \to \mathbf{k}^*$ che manda ogni matrice $M$ nel suo determinante $\det M \in \mathbf{k}^* = \mathbf{k} \setminus \{0\}$ è un omomorfismo. Infatti $\det(AB) = \det(A)\det(B)$.
- L'applicazione $\exp : \mathbb{R} \to \mathbb{R}^*$ definita come $\exp(x) = e^x$ è un omomorfismo di gruppi. Infatti l'operazione di gruppo di $\mathbb{R}$ è la somma, e si ha $\exp(x + y) = \exp(x)\exp(y)$.
- Se $g$ è un elemento del gruppo $G$, $n \mapsto g^n$ definisce un omomorfimo $\mathbb{Z} \to G$. Infatti $g^m g^n = g^{m+n}$.
- Ogni spazio vettoriale può essere visto come gruppo abeliano rispetto alla sola operazione di somma tra vettori. Allora una applicazione lineare tra spazi vettoriali è sempre un omomorfismo di gruppi.

Sia $\phi : G \to \overline{G}$ un omomorfismo.

**Definizione 15.** Il *nucleo* di $\phi$ è l'insieme degli elementi $g$ di $G$ tali che $\phi(g) = \bar{e}$. L'*immagine* di $\phi$ è l'insieme degli elementi $\bar{g}$ di $\overline{G}$ per i quali esiste $g \in G$ tale che $\phi(g) = \bar{g}$.

Indicheremo il nucleo e l'immagine di un omomorfismo $\phi$ con $\ker\phi$, $\mathrm{Im}\phi$ rispettivamente. Una semplice verifica mostra che $\mathrm{Im}\phi$ è sempre un sottogruppo di $\overline{G}$, mentre $\ker\phi$ è un sottogruppo normale di $G$. Questi fatti ammettono un'immediata generalizzazione.

**Proposizione 3.5.** *Sia $\rho : G \to \overline{G}$ un omomorfismo di gruppi.*

- *Se $H < G$, allora $\rho(H) < \overline{G}$. Inoltre, se $H \lhd G$, allora $\rho(H) \lhd \rho(H)$.*
- *Se $\overline{H} < \overline{G}$, allora $\rho^{-1}(\overline{H}) < G$. Inoltre, se $\overline{H} \lhd \overline{G}$, allora $\rho^{-1} \lhd G$.*

*Dimostrazione.* Per quanto riguarda il primo enunciato, $x \in \rho(H)$ se e solo se esiste $h \in H$ tale che $x = \rho(h)$. Dal momento che $\rho$ è un omomorfismo di gruppi, sappiamo che $\rho(h_1)\rho(h_2) = \rho(h_1 h_2)$ e che $\rho(h)^{-1} = \rho(h^{-1})$. Questo mostra che $\rho(H) < \overline{G}$. Per mostrare che $\rho(H) \lhd \overline{G}$ se $H$ è normale in $G$, basta invece osservare che $\rho(g)\rho(h)\rho(g)^{-1} = \rho(ghg^{-1}) \in \rho(H)$ per ogni $h \in H, g \in G$.

La dimostrazione del secondo enunciato si fa in maniera simile, osservando che $x \in \rho^{-1}(\overline{H})$ se e solo se $\rho(x) \in \overline{H}$. Allora da $x, y \in \rho^{-1}(\overline{H})$ segue $\rho(x), \rho(y) \in \overline{H}$, e quindi $\rho(xy) = \rho(x)\rho(y) \in \overline{H}$ da cui $xy \in \rho^{-1}(\overline{H})$. Allo stesso modo:

$$x \in \rho^{-1}(\overline{H}) \Rightarrow \rho(x) \in \overline{H} \Rightarrow \rho(x^{-1}) = \rho(x)^{-1} \in \overline{H} \Rightarrow x^{-1} \in \rho^{-1}(\overline{H}).$$

Per mostrare che se $\overline{H} \lhd \overline{G}$ allora $\rho^{-1}(\overline{H}) \lhd G$, basta osservare che la composizione $\pi \circ \rho$, dove $\pi : \overline{G} \to \overline{G}/\overline{H}$ è la proiezione al quoziente, è ancora un omomorfismo, ed il suo nucleo è precisamente $\rho^{-1}(\overline{H})$. (perché?) □

**Esempi:**

- L'applicazione identità da un gruppo in sé è un omomorfismo iniettivo; infatti solo l'identità giace nel suo nucleo. L'immagine coincide con l'intero gruppo.
- Il nucleo di $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ è il sottogruppo $\mathrm{A}_n$ delle permutazioni pari.
- Il nucleo di $\det : \mathrm{GL}_n(\mathbf{k}) \to \mathbf{k}^*$ è dato dal sottogruppo $\mathrm{SL}_n(\mathbf{k})$ delle matrici di determinante $1$. L'immagine è tutto $\mathbf{k}^*$.
- L'omomorfismo $\exp : \mathbb{R} \to \mathbb{R}^*$ non è un isomorfismo. E' infatti iniettivo, poiché $e^x = 1 \Rightarrow x = 0$, ma non è suriettivo, poiché la sua immagine è il sottogruppo dei numeri reali positivi in $\mathbb{R}^*$.
- L'omomorfismo $\mathbb{Z} \ni n \mapsto g^n \in G$ ha per immagine il sottogruppo di $G$ generato da $g$, e per nucleo il sottogruppo di $\mathbb{Z}$ generato da $o(g)$ se l'ordine di $g$ è finito, e $(0)$ se è infinito.
- La proiezione $\pi_N : G \to G/N$ è suriettiva, ed ha $N$ come nucleo.

L'ultimo esempio in particolare ci dice che un sottogruppo è normale se e solo se è il nucleo di qualche omomorfismo. Applicando la Proposizione 3.5 alla proiezione al quoziente $\pi : G \to G/N$, dove $N \lhd G$, si vede subito che $\pi(H) < G/N$ quando $H < G$, e che $\pi^{-1}(\overline{H})$ è un sottogruppo di $G$ che contiene $N$, se $\overline{H} < G/N$.

### 3.3. **La proiezione al quoziente.**

**Lemma 3.6.** *Se $\pi : G \to G/N$ è la proiezione al quoziente per il sottogruppo normale $N$, allora $\pi(H) = \pi(HN)$.*

*Dimostrazione.* L'inclusione $\pi(H) \subset \pi(HN)$ è ovvia. Per mostra che $\pi(HN) \subset \pi(H)$ basta osservare che $[hn] = [h][n] = [h][e] = [h]$ per ogni $h \in H, n \in N$. □

*Osservazione* 3.7. Quando $H$ contiene $N$, è naturale indicare con $H/N$ la proiezione $\pi(H)$. Il lemma appena dimostrato ci dice che quando $N \not\subset H$, allora $\pi(H) = \pi(HN) = HN/N$.

**Proposizione 3.8.** *Sia $N \lhd G$, e $\pi : G \to G/N$ la proiezione al quoziente.*

- *Se $H < G$, allora $\pi^{-1}(\pi(H)) = HN$. In particolare, se $N \subset H$, allora $\pi^{-1}(\pi(H)) = H$.*
- *Se $\overline{H} < G/N$, allora $\pi(\pi^{-1}(\overline{H})) = \overline{H}$.*

*Dimostrazione.* Da $\pi(H) = \pi(HN)$ segue che $HN \subset \pi^{-1}(\pi(H))$. Per mostrare che $\pi^{-1}(\pi(H)) \subset HN$, basta osservare che $x \in \pi^{-1}(\pi(H))$ se e solo se $\pi(x) \in \pi(H)$, cioè se esiste $h \in H$ tale che $\pi(x) = \pi(h)$. Ma allora $h^{-1}x \in \ker \pi = N$, e quindi $x \in hN \subset HN$.

Per quanto riguarda la seconda affermazione, $\pi(\pi^{-1}(\overline{H})) = \overline{H} \cap \pi(G)$ che coincide con $\overline{H}$ per la suriettività di $\pi$. □

**Teorema 3.9.** *Sia $N \lhd G$, e $\pi : G \to G/N$ la proiezione al quoziente. Allora $H \mapsto \pi(H)$ costituisce una corrispondenza biunivoca tra i sottogruppi di $G$ che contengono $N$ e i sottogruppi di $G/N$. In tale corrispondenza, a sottogruppi normali di $G$ corrispondono sottogruppi normali di $G/N$ e viceversa.*

*Dimostrazione.* La Proposizione 3.8 mostra che $\overline{H} \mapsto \pi^{-1}(\overline{H})$ è un'inversa sia destra che sinistra di $H \mapsto \pi(H)$. L'affermazione sulla normalità segue dalla Proposizione 3.5. □

## 3.4. **Teoremi di omomorfismo e isomorfismo.**

3.4.1. *Il teorema di omomorfismo.* Il teorema che segue è l'analogo gruppale di un enuncato riguardante le relazioni di equivalenza su insieme dimostrato all'inizio del corso.

**Teorema 3.10.** *Sia $N$ un sottogruppo normale di un gruppo $G$, ed $f : G \to H$ un omomorfismo di gruppi tale che $N \subset \ker f$. Allora esiste un unico omomorfismo di gruppi $F : G/N \to H$ tale che, indicata con $\pi : G \to G/N$ la proiezione al quoziente, si abbia $f = F \circ \pi$. L'immagine di $F$ coincide con quella di $f$, ed $F$ è iniettiva se e solo se $N = \ker f$.*

*Dimostrazione.* Mostriamo innanzitutto l'unicità di $F$. Dal momento che $\pi(g) = [g] = gN$, se $F$ soddisfa l'enunciato del teorema, deve valere $F([g]) = f(g)$ per ogni $g \in G$. Rimane da controllare che tale applicazione $F$ sia ben definita, e che sia effettivamente un omomorfismo.

Per controllare la buona definizione di $F$, è sufficiente verificare che se $[g_1] = [g_2]$, allora $f(g_1) = f(g_2)$. Sappiamo che $[g_1] = [g_2]$ se e solo se $g_1 \equiv g_2 \mod N$, cioè esattamente quando $g_1^{-1}g_2 \in N$. Ma allora $f(g_2) = f(g_1 g_1^{-1} g_2) = f(g_1)f(g_1^{-1}g_2) = f(g_1) \cdot \bar{e} = f(g_1)$, poiché $N \subset \ker f$. Se è ben definita, $F$ è chiaramente un omomorfismo. In effetti

$$F([a][b]) = F([ab]) = f(ab) = f(a)f(b) = F([a])F([b]),$$

per ogni $a, b \in G$.

L'affermazione $\mathrm{Im}F = \mathrm{Im}f$ segue da $f = F \circ \pi$ e dalla suriettività della proiezione $\pi : G \to G/N$. Per quanto invece concerne l'iniettività di $F$, si vede facilmente che $\ker F = \{[a] \in G/N | f(a) = e\} = \pi(\ker f)$. Poiché $N \subset \ker f$, si ha $\pi(kerf) = \{[e]\}$ se e solo se $\ker f = N$. □

*Osservazione* 3.11. Il teorema appena dimostrato richiede qualche spiegazione sulle sue possibili applicazioni. E' intanto ovvio che se conosciamo un omomorfismo di gruppi $F : G/N \to H$, possiamo costruire la composizione $f = F \circ \pi$, e questa è nuovamente un omomorfismo $f : G \to H$, che per costruzione contiene $N$ nel suo nucleo.

Il teorema ci spiega che questa costruzione può essere invertita: ogni omomorfismo $f : G \to H$ che contenga $N$ nel suo nucleo si ottiene nel modo appena descritto, ed inoltre si ottiene in tal modo per *precisamente una scelta* di $F : G/N \to H$. In altre parole, esiste una corrispondenza biunivoca tra gli omomorfismi da $G$ in $H$ che contengono $N$ nel loro nucleo, e gli omomorfismi da $G/N$ in $H$. Che cosa vuol dire esattamente quest'affermazione?

Evidentemente, se abbiamo bisogno di costruire un omomorfismo $G/N \to H$ e questo è difficile da fare direttamente, possiamo limitarci a costruire un omomorfismo $G \to H$ — la qual cosa potrebbe rivelarsi più semplice — e poi semplicemente verificare che $N$ è contenuto nel suo nucleo.

**Esempio.** Costruiamo tutti gli omomorfismi dal gruppo $(\mathbb{Z}/(15), +)$ al gruppo $(\mathbb{Z}/(10), +)$. Il gruppo $\mathbb{Z}/(15)$ è quoziente di $\mathbb{Z}$ per il sottogruppo normale generato da $15$ — può valere la pena di ricordare che ogni sottogruppo di $\mathbb{Z}$ è normale, dal momento che $\mathbb{Z}$ è un gruppo abeliano. Per il Teorema 3.10, alla luce dell'Osservazione 3.11, è sufficiente costruire tutti gli omomorfismi $f : \mathbb{Z} \to \mathbb{Z}/(10)$ che contengano il sottogruppo $(15)$ nel loro nucleo.

Tutti gli omomorfismi da $\mathbb{Z}$ in un gruppo $G$ si costruiscono scegliendo un elemento $g \in G$ e ponendolo come immagine di $1 \in \mathbb{Z}$: sono in altre parole della forma $\phi(n) = g^n$ per ogni $n \in \mathbb{Z}$. Un elenco completo di omomorfismi $f : \mathbb{Z} \to \mathbb{Z}/(10)$ è quindi dato da $f(n) = [an]$, con $[a] \in \mathbb{Z}/(10)$. Ora dobbiamo comprendere quali di tali omomorfismi (uno per ogni $[a]$) *scendano al quoziente*, cioè fattorizzino attraverso la proiezione al quoziente. Conosciamo già la condizione da verificare, e cioè che $(15)$ sia contenuto nel nucleo di $f$. Dal momento che $(15)$ è generato da $15$, è sufficiente controllare quando $15$ appartenga al nucleo, cioè quando $f(15) = [0]$.

Ma questo accade esattamente quando $15a \equiv 0 \mod 10$, cioè quando $3a \equiv 0 \mod 2$ cioè quando $a \equiv 0 \mod 2$. Vanno scelte quindi le classi $[a] \in \mathbb{Z}/(10)$ con $a$ pari, il che fornisce gli omomorfismi:

- $f(n) = [0]$,
- $f(n) = [2n]$,
- $f(n) = [4n]$,
- $f(n) = [6n]$,
- $f(n) = [8n]$.

3.4.2. *I teoremi di isomorfismo.*

**Teorema 3.12** (Primo teorema di isomorfismo)**.** *Se $f : G \to H$ è un omomorfismo di gruppi, allora la sua immagine $f(G)$ è isomorfa al quoziente $G/\ker f$.*

*Dimostrazione.* A meno di sostituire $H$ con $f(G)$, possiamo supporre che $f$ sia suriettiva. Applicando il Teorema 3.10 ad $N = \ker f$ si ottiene una $F : G/N \to f(G)$ che è sia iniettiva che suriettiva, cioè un isomorfismo. □

**Teorema 3.13** (Secondo teorema di isomorfismo)**.** *Se $H, N \lhd G$, con $N \subset H$, allora $H/N \lhd G/N$ ed i quozienti $G/H$ e $(G/N)/(H/N)$ sono isomorfi.*

*Dimostrazione.* Applichiamo il Teorema 3.10 all'omomorfismo $f = \pi_H : G \to G/H$ di proiezione al quoziente, e al sottogruppo $N \subset \ker f = H$. Risulta individuato un unico omomorfismo $F : G/N \to G/H$ tale che[7] $F(gN) = gH$ per ogni $g \in G$, che è suriettivo per la suriettività di $f$.

Il nucleo di $F$ è $\ker F = \{gN \in G/N | gH = H\} = \{gN \in G/N | g \in H\} = H/N$. Questo mostra che $H/N$ è un sottogruppo normale di $G/N$ (come seguiva anche dalla Proposizione 3.5) in quanto nucleo di un omomorfismo, e per il Teorema 3.12 si ha: $G/H = \mathrm{Im}F \simeq (G/N)/\ker F = (G/N)/(H/N)$. □

**Teorema 3.14** (Terzo teorema di isomorfismo)**.** *Se $H, N$ sono sottogruppi di $G$, con $N \lhd G$, allora vi è un isomorfismo tra $HN/N$ e $H/H \cap N$*

*Dimostrazione.* Sia $\pi : G \to G/N$ l'omomorfismo di proiezione al quoziente. La restrizione — chiamiamola $f$ — di $\pi$ ad $H$ è ancora un omomorfismo $f : H \to G/N$ la cui immagine coincide, grazie all'Osservazione 3.7, con $HN/N$.

E' facile calcolare il nucleo di $f$; infatti $\ker f = \{h \in H | [h] = [e]\} = H \cap N$, il che mostra che $H \cap N$ è normale in $H$. Per il Teorema 3.12 si ha allora che $HN/N = \mathrm{Im}f \simeq H/\ker f = H/H \cap N$. □

I tre teoremi appena illustrati sono solitamente detti primo, secondo e terzo teorema di omomorfismo per i gruppi. Vediamone due facili applicazioni.

**Proposizione 3.15.** *L'ordine di $[a]$ nel gruppo (additivo) $\mathbb{Z}/(n)$ è uguale a $n/(a, n)$.*

*Dimostrazione.* Un'osservazione preliminare: dal momento che l'operazione di gruppo in $\mathbb{Z}$ è indicata additivamente, il prodotto di sottogruppi sarà indicato con $H + K$ e non con $HK$.

Indichiamo con $\pi : \mathbb{Z} \to \mathbb{Z}/(n)$ la proiezione al quoziente. Se $K = (a)$ e $N = (n)$, allora $\pi(K) = \pi(K + N) = (K + N)/N$; d'altronde il sottogruppo generato in $\mathbb{Z}/(n)$ da $[a]$ è esattamente $\pi(K)$. Sappiamo già che $K + N$ è il sottogruppo generato dal massimo comun divisore $(a, n)$ — che per comodità di notazione, e per evitare troppe parentesi, indichiamo comunque con $(a, n)$.

Ricapitolando, se $G = \mathbb{Z}$, $H = K + N = (a, n)$, $N = (n)$, allora $G/N = \mathbb{Z}/(n)$ e $H/N = ([a])$. Dal secondo teorema di omomorfismo si ottiene $G/H \simeq (G/N)/(H/N)$, cioè $\mathbb{Z}/(a, n) \simeq (\mathbb{Z}/(n))/([a])$. Ora, il gruppo $\mathbb{Z}/(a, n)$ possiede $(a, n)$ elementi, mentre il gruppo $\mathbb{Z}/(n)$ ne possiede $n$. Per il teorema di Lagrange, il sottogruppo $([a])$ deve contenere allora $n/(a, n)$ elementi, e quindi l'ordine di $[a]$ in $\mathbb{Z}/(n)$ è $n/(a, n)$. □

[7] Sono purtroppo costretto ad indicare $[g]$ con $gN$ oppure $gH$, per evitare ambiguità di notazione.

**Proposizione 3.16.** *Siano $a, b \in \mathbb{Z}$ elementi non nulli. Allora il minimo comune multiplo di $a$ e $b$ è dato da $ab/(a, b)$.*

*Dimostrazione.* Siano $H = (a), N = (b)$ sottogruppi di $\mathbb{Z}$. Se $d$ è il loro massimo comun divisore, ed $m$ è il loro minimo comune multiplo, allora sappiamo già che $H + N = (d), H \cap N = (m)$.

Per il terzo teorema di omomorfismo, abbiamo allora $H + N/N \simeq H/H \cap N$, cioè $(d)/(b) = (a)/(m)$. Confrontando le cardinalità dei due quozienti[8] si ottiene $m = ab/d$. □

3.5. **Gruppo moltiplicativo di un campo.** Avendo calcolato l'ordine degli elementi del gruppo additivo $\mathbb{Z}/(n)$, è ora facile dimostrare un sorprendente fatto algebrico. Iniziamo con alcuni fatti ormai ben chiari.

**Lemma 3.17.** *Ogni sottogruppo di un gruppo ciclico è ciclico.*

*Dimostrazione.* Un gruppo ciclico è isomorfo al gruppo additivo $\mathbb{Z}$, o a uno dei suoi quozienti $\mathbb{Z}/(n)$. E' sufficiente mostrare che ogni sottogruppo di tali gruppi possiede un generatore ciclico.

Per quanto riguarda $\mathbb{Z}$, abbiamo mostrato che i suoi sottogruppi sono tutti della forma $(d), d \in \mathbb{Z}$, e quindi possiedono il generatore ciclico $d$. Per i quozienti $\mathbb{Z}/(n)$ possiamo invece utilizzare la corrispondenza delineata nel Teorema 3.9. □

**Lemma 3.18.** *Se $d|n$, il gruppo ciclico $\mathrm{C}_n$ contiene esattamente un sottogruppo di ordine $d$.*

*Dimostrazione.* Per il Teorema 3.9, i sottogruppi di ordine $d$, e quindi indice $n/d$ in $\mathrm{C}_n \simeq \mathbb{Z}/(n)$ sono in corrispondenza biunivoca con i sottogruppi di $\mathbb{Z}$ (che contengono $n$) di indice $n/d$. Vi è un solo tale sottogruppo in $\mathbb{Z}$, generato da $n/d$. Pertanto l'unico sottogruppo di $\mathbb{Z}/(n)$ di ordine $d$ è quello generato da $[n/d]$. □

**Lemma 3.19.** *Se $d|n$, il gruppo $\mathrm{C}_n$ contiene esattamente $\phi(d)$ elementi di ordine $d$.*

*Dimostrazione.* Se $d = n$, l'affermazione segue dalla Proposizione 3.15. In generale, gli elementi di ordine $d$ sono tutti contenuti nell'unico sottogruppo di $\mathrm{C}_n$ di ordine $d$, che è ciclico, e quindi isomorfo a $\mathrm{C}_d$. Il loro numero è pertanto $\phi(d)$. □

**Corollario 3.20.** *Vale l'uguaglianza*

$$n = \sum_{d|n} \phi(d).$$

*Dimostrazione.* $\mathrm{C}_n$ contiene $n$ elementi, che possono essere contati raggruppandoli per ordine. □

Sia ora $G$ un gruppo finito nel quale $x^d = 1$ ha al più $d$ soluzioni per ogni $d \in \mathbb{N}$.

**Lemma 3.21.** *Se $G$ contiene qualche elemento di ordine $d$, allora $\{x \in G \,|\, x^d = 1\}$ è un sottogruppo ciclico di ordine $d$. In particolare, $G$ contiene $\phi(d)$ elementi di ordine $d$.*

*Dimostrazione.* Se $g$ ha ordine $d$, ogni elemento del sottogruppo $(g)$ soddisfa $x^d = e$. Poiché $(g)$ contiene $d$ elementi, e $x^d = 1$ ha al più $d$ soluzioni, concludiamo che le soluzioni di $x^d = e$ sono tutti e soli gli elementi di $(g)$. □

**Corollario 3.22.** *$G$ possiede elementi di ordine $|G|$. In particolare, $G$ è ciclico.*

*Dimostrazione.* Supponiamo che $G$ abbia ordine $n$. Se $d$ è l'ordine di qualche elemento in $G$, allora $d|n$ e il numero di elementi di ordine $d$ è $\phi(d)$. Allora abbiamo

$$n = \sum_{d=o(g), g \in G} \phi(d),$$

dove sommiamo sui $d$ che sono ordine di qualche elemento di $G$, quindi su alcuni dei divisori di $n$. Alla luce del Corollario 3.20, poiché tutti gli addendi sono positivi, questo è possibile solo se sono tutti presenti. In particolare, l'addendo $\phi(n)$ è presente nella somma, e quindi $G$ possiede elementi di ordine $n$. □

[8] Attenzione: la cardinalità di $(d)/(b)$ è $b/d$ e quella di $(a)/(m)$ è $m/a$!!!

**Teorema 3.23.** *Sia* $\mathrm{k}$ *un campo,* $\Gamma \subset \mathrm{k}^\times$ *un sottogruppo finito del suo gruppo moltiplicativo. Allora* $\Gamma$ *è ciclico.*

*Dimostrazione.* Un'equazione algebrica in un'indeterminata, a coefficienti in un campo $\mathrm{k}$, ha un numero di soluzioni in $\mathrm{k}$ limitato dal suo grado.
$\Gamma$ deve allora soddisfare le ipotesi del Corollario 3.22, ed è quindi ciclico. □

**Corollario 3.24.** *Se* $\mathrm{k}$ *è un campo finito, allora* $\mathrm{k}^\times$ *è un gruppo ciclico. In particolare,* $\mathbb{Z}/(p)^\times$ *è ciclico per ogni numero primo* $p$*.*

3.6. **Automorfismi di gruppi.** Sia $g \in G$. L'applicazione $I_g$ che manda $x \mapsto gxg^{-1}$ è un omomorfismo. Infatti $I_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = I_g(x)I_g(y)$. Inoltre $I_g$ è un isomorfismo. L'iniettività segue da $gxg^{-1} = e \Rightarrow x = g^{-1}eg = e$, mentre la suriettività dal fatto che ogni $x \in G$ si può scrivere come $x = g(g^{-1}xg)g^{-1}$.

**Definizione 16.** $I_g$ è l'*automorfismo interno* di $G$ indotto dall'elemento $g$.

L'insieme degli automorfismi interni è un gruppo rispetto alla composizione:

**Lemma 3.25.** *La composizione di automorfismi interni è ancora un automorfismo interno.*

*Dimostrazione.* Si ha $I_g \circ I_h = I_{gh}$. Infatti $I_g(I_h(x)) = I_g(hxh^{-1}) = g(hxh^{-1})g^{-1}$. Mentre $I_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1}$. □

**Teorema 3.26.** *Gli automorfismi interni di un gruppo* $G$ *formano un gruppo rispetto alla composizione, che si indica con* $\operatorname{Int} G$*.*

*Dimostrazione.* Per esercizio. □

**Esercizi:**
*(a)* Dimostrare che $\operatorname{Int}(G)$ è isomorfo a $G/Z$ dove $Z$ è il centro di $G$.
*(b)* Mostrate che $\operatorname{Int}(G)$ è un sottogruppo normale di $\operatorname{Aut}(G)$.
*(c)* Come è fatto il gruppo degli automorfismi di $\mathrm{S}_3$? E' vero che ogni automorfismo di $\mathrm{S}_3$ è interno?
*(d)* Determinare il gruppo degli automorfismi del gruppo non ciclico di quattro elementi.
*(e)* Mostrare che $\operatorname{Aut}(\mathrm{C}_n)$ è isomorfo al gruppo moltiplicativo $\mathbb{Z}/(n)^\times$.

## 4. Azioni di gruppo e applicazioni

Molte proprietà aritmetiche dei gruppi si dimostrano in maniera combinatoria, attraverso tecniche di conteggio, che dimostrano l'esistenza di elementi o sottogruppo di ordini particolari. Queste dimostrazioni hanno una filosofia comune, che può essere resa esplicita attraverso il concetto di azione di gruppo su un insieme.

4.1. **Azione di un gruppo su un insieme.** Iniziamo subito con la definizione, passando poi a dare numerosi esempi.
***Gli esempi devono diventare paragrafi, e l'immersione di Cayley deve essere fatta in dettaglio***

**Definizione 17.** Un'azione del gruppo $G$ sull'insieme $X$ è un applicazione $G \times X \ni (g, x) \mapsto g.x \in X$ che soddisfa

- $e.x = x$;
- $(gh).x = g.(h.x)$,

per ogni scelta di $g, h \in G$ e di $x \in X$. L'azione di $G$ su $X$ si dice *transitiva* se, per ogni scelta di $x, y \in X$, esiste $g \in G$ tale che $y = g.x$; si dice *semplicemente transitiva* quando tale elemento è unico.

**Esempi:**

- Sia $X$ uno spazio affine, e $G$ il gruppo abeliano delle traslazioni[9] di $X$ rispetto alla composizione. Allora $t.P = t(P)$ definisce un'azione di $G$ su $X$, che è semplicemente transitiva.
- Se $G$ è un gruppo, poniamo $X = G$. Allora, la moltiplicazione sinistra $g.x = gx$ definisce un'azione di $G$ su $X$, che è semplicemente transitiva.
- L'azione *banale* del gruppo $G$ sull'insieme $X$ è data da $g.x = x$ per ogni $g \in G, x \in X$.
- Il gruppo $\mathrm{S}_X$ agisce sull'insieme $X$ tramite $\sigma.x = \sigma(x)$. L'azione di $\mathrm{S}_X$ su $X$ è transitiva, ma non semplicemente transitiva.
- Se $X = G$, l'assegnazione $g.x = xg$ è un'azione di gruppo solo se $G$ è abeliano. In effetti, anche se $e.x = xe = x$, si ha $(gh).x = xgh$ mentre $g.(h.x) = g.(xh) = xhg$, e generalmente $xgh \neq xhg$.
- Se $X = G$, $g.x = xg^{-1}$ definisce un'azione di $G$ su $X$.
- Siano $V, W$ spazi vettoriali, $X = \mathrm{Hom}(V, W)$, $G = \mathrm{GL}(V) \times GL(W)$. Possiamo allora definire un'azione di $G$ su $X$ tramite $(A, B).T = B \circ T \circ A^{-1}$.
- Se $V$ è uno spazio vettoriale, $X = \mathrm{End}(V)$, $G = \mathrm{GL}(V)$, allora $G$ agisce su $X$ tramite $A.T = A \circ T \circ A^{-1}$.
- Sia $G$ un gruppo, $H < G$ un suo sottogruppo, $X = G/H$. Allora $g.aH = (ga)H$ definisce un'azione di $G$ su $X$.

**Definizione 18.** Data un'azione del gruppo $G$ su $X$, l'*orbita* di $x \in X$ sotto l'azione di $G$, o più brevemente $G$-orbita di $x$, è l'insieme $G.x = \{g.x \,|\, g \in G\} \subset X$; lo stabilizzatore di $x$ è il sottoinsieme di $G$ definito da $\mathrm{Stab}(x) = \{g \in G \,|\, g.x = x\}$.

**Proposizione 4.1.** *Se il gruppo $G$ agisce su $X$, lo stabilizzatore di ciascun elemento $x \in X$ è un sottogruppo di $G$.*

*Dimostrazione.* Segue immediatamente dalla definizione. □

**Proposizione 4.2.** *Sia data un'azione del gruppo $G$ sull'insieme $X$. Allora $X$ è unione disgiunta di $G$-orbite.*

*Dimostrazione.* La relazione ottenuta imponendo che $x \sim y$ se e solo se esiste $g \in G$ tale che $g.x = y$ è di equivalenza, come si vede facilmente. La classe di equivalenza di $x$ è data da $\{y \,|\, x \sim y\}$ e coincide quindi con l'orbita $G.x$. L'insieme $X$ è unione disgiunta di classi di equivalenza, e l'affermazione segue osservando che la classe di equivalenza di $x$ è data da $\{y \,|\, x \sim y\}$ e coincide quindi con l'orbita $G.x$. □

Se $A$ è un insieme finito, indichiamo con $|A|$ il numero di elementi di $A$.

**Teorema 4.3.** *Se il gruppo finito $G$ agisce sull'insieme $X$, e $x \in X$, allora l'orbita $G.x$ e lo stabilizzatore $\mathrm{Stab}(x)$ sono entrambi finiti, e si ha $|G| = |G.x||\mathrm{Stab}(x)|$; in particolare, $|G.x|$ divide $|G|$.*

*Dimostrazione.* Lo stabilizzatore $\mathrm{Stab}(x)$ è finito in quanto sottogruppo di un gruppo finito. Inoltre, $g \mapsto g.x$ definisce un'applicazione suriettiva $G \to G.x$, e quindi anche l'orbita di $x$ è finita.

Per quanto riguarda l'ultima affermazione, osserviamo che da $g.x = h.x$ segue

$$x = e.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.(h.x) = (g^{-1}h).x,$$

e quindi $g^{-1}h \in \mathrm{Stab}(x)$. Questo accade se e soltanto se $g$ e $h$ giacciono nello stesso laterale sinistro del sottogruppo $\mathrm{Stab}(x) < G$. In conclusione, esiste una corrispondenza biunivoca tra elementi di $G.x$ e laterali di $\mathrm{Stab}(x)$ in $G$, e quindi $|G.x| = |G/\mathrm{Stab}(x)| = |G|/|\mathrm{Stab}(x)|$. □

[9] Se $X$ è uno spazio affine modellato sullo spazio vettoriale $V$, $G$ non è altro che $V$ visto come gruppo additivo.

4.2. **Il Teorema di Cauchy.** Come prima applicazione del linguaggio delle azioni di gruppo, dimostriamo il Teorema di Cauchy, anche se può essere ottenuto come caso particolare del Teorema di Sylow, che verrà dimostrato più tardi.

**Teorema 4.4** (Cauchy)**.** *Sia $G$ un gruppo finito, e supponiamo che il numero primo $p$ divida $|G|$. Allora $G$ possiede almeno un elemento di ordine $p$.*

*Dimostrazione.* L'insieme $X = \{(g_1, g_2, \dots, g_p) \in G^p \mid g_1 g_2 \dots g_p = e\}$ possiede esattamente $|G|^{p-1}$ elementi. In effetti, comunque siano scelti $g_1, g_2, \dots, g_{p-1} \in G$, la $p$-upla $(g_1, \dots, g_p)$ appartiene a $X$ se e solo se $g_p = (g_1 g_2 \dots g_{p-1})^{-1}$. Dal momento che $p$ divide $|G|$, anche $|X|$ è un multiplo di $p$.

Osserviamo, ora, che se $(g_1, \dots, g_p) \in X$, allora anche la $p$-upla $(g_2, g_3, \dots, g_p, g_1)$, ottenuta ruotando i coefficienti di una posizione verso destra, appartiene ad $X$. In effetti,

$$g_2 g_3 \dots g_p g_1 = (g_1^{-1} g_1) g_2 g_3 \dots g_p g_1 = g_1^{-1}(g_1 g_2 g_3 \dots g_p) g_1 = g_1^{-1} e g_1 = e.$$

Possiamo allora definire un'azione di $G = \mathrm{C}_p = \langle \rho \rangle$ su $X$ imponendo $\rho.(g_1, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1)$, ed estendendo a tutto $G$ per composizione. Allora $X$ è unione di $G$-orbite, ed il numero di elementi di ciascuna orbita è un divisore di $p$, e contiene quindi $p$ elementi, oppure uno solo. Dal momento che $|X|$ è un multiplo di $p$, il numero di orbite che contengono esattamente un elemento è anch'esso multiplo di $p$.

Una $p$-upla $(g_1, \dots, g_p) \in X$ possiede un'orbita composta di un solo elemento se e solo se ha tutti i coefficienti uguali; ad ogni modo $(g, g, \dots, g)$ appartiene ad $X$ esattamente quando $g^p = e$. Il numero di elementi $g \in G$ tali che $g^p = e$ è quindi un multiplo di $p$. L'identità $e$ è uno di tali elementi, e quindi devono esservene almeno altri $p - 1$. □

*Osservazione* 4.5. Il ragionamento appena presentato dimostra, più precisamente, che il numero di elementi di ordine $p$ è $\equiv -1 \mod p$.

4.3. **La relazione di coniugio.**

**Definizione 19.** Due elementi $x$ e $y$ di un gruppo $G$ si dicono coniugati se esiste $g \in G$ tale che $y = g^{-1} x g$.

Abbiamo mostrato a lezione (è semplice e noioso) che la relazione di essere coniugati è una relazione di equivalenza.

**Proposizione 4.6.**
- *Elementi coniugati hanno lo stesso ordine.*
- *$a \in G$ è l'unico coniugato di se stesso se e solo se è centrale in $G$.*
- *Il numero di elementi coniugati ad $a \in G$ è pari a $[G : C(a)]$ dove $C(a)$ è il centralizzatore di $a$.*

*Dimostrazione.* $a$ e $b = g^{-1} a g$ hanno lo stesso ordine. Infatti $a^n = e$ implica $(g^{-1} a g)^n = g^{-1} a^n g = e$. Inoltre, se $b^n = e$ allora $a^n = (g b g^{-1})^n = e$ per lo stesso motivo. Quindi $a^n = e \iff b^n = e$.

La seconda affermazione segue dalla terza, quindi mi limiterò a dimostrare quest'ultima. Affinché $g^{-1} a g = h^{-1} a h$, è necessario che sia $h g^{-1} a g h^{-1} = e$ cioè $(g h^{-1})^{-1} a (g h^{-1}) = a$. Questo vuol dire che $g h^{-1}$ commuta con $a$, cioè che giace nel centralizzatore $C(a)$. Ma allora $g$ e $h$ coniugano $a$ allo stesso elemento se e solo se sono congruenti modulo $C(a)$, cioè se giacciono nello stesso laterale destro di $C(a)$. Vi è pertanto un coniugato di $a$ per ogni laterale di $C(a)$ in $G$, e quindi il numero dei coniugati di $a$ è pari all'indice di $C(a)$ in $G$. □

Possiamo riassumere questa proposizione nella cosiddetta equazione delle classi: gli elementi di $G$ che giacciono nel centro hanno classi coniugate di ordine $1$. L'ordine delle altre classi coniugate può essere calcolato tramite l'indice del centralizzatore di un qualsiasi elemento. Pertanto in un gruppo $G$:

$$|G| = |Z(G)| + \sum_{[a] \not\subset Z(G)} \frac{|G|}{|C(a)|},$$

dove la somma si intende su un rappresentante $a$ per ciascuna classe di coniugio.

**Teorema 4.7.** *Sia $G$ un gruppo il cui ordine sia una potenza di un numero primo $p$: $|G| = p^n$. Allora il centro di $G$ non si limita alla sola identità, e il suo indice in $G$ è diverso da $p$.*

*Dimostrazione.* Applichiamo l'equazione delle classi al gruppo $G$. Ogni addendo della somma è una potenza positiva di $p$, in quanto una classe coniugata possiede un elemento solo se appartiene al centro. Allora la sommatoria fornisce come risultato un multiplo di $p$, come multiplo di $p$ è anche il primo membro. Allora $|Z(G)|$ deve essere anch'esso un multiplo di $p$, e pertanto non può essere uguale ad $1$: vi devono essere elementi nel centro diversi dall'identità.

Supponiamo ora che l'indice di $Z(G)$ in $G$ sia $p$. Allora il suo ordine è $p^{n-1}$. Sia $a \notin Z(G)$. Allora $a$ commuta con se stesso, e commuta anche con tutti gli elementi di $Z(G)$. Quindi $C(a)$ è un sottogruppo che contiene almeno $p^{n-1}+1$ elementi, e cioè i $p^{n-1}$ elementi di $Z(G)$, e l'elemento $a$, che non appartiene a $Z(G)$. Ma $C(a)$ è un sottogruppo, e il suo ordine deve dividere $|G| = p^n$. L'unico divisore di $p^n$ maggiore di $p^{n-1}$ è $p^n$ stesso, e quindi $a$ commuta con tutti gli elementi del gruppo $G$, quindi giace in $Z(G)$, un assurdo. □

**Corollario 4.8.** *Un gruppo di ordine $p^2$ è abeliano.*

*Dimostrazione.* Il suo centro non può avere ordine $1$, e non può avere indice $p$. Perciò deve essere tutto il gruppo. □

Come esempi della relazione di coniugio, abbiamo determinato le classi coniugate nei gruppi abeliani, in quelli simmetrici e in quelli diedrali.

**Proposizione 4.9.** *In un gruppo abeliano ogni classe di coniugio è composta di un solo elemento.*

*Dimostrazione.* Ogni elemento è centrale, e quindi è il proprio unico coniugato. □

**Proposizione 4.10.** *Sia $n$ dispari. Allora le classi di coniugio in $\mathrm{D}_n$ sono:*

- $[e] = \{e\}$
- $[\rho^i] = \{\rho^i, \rho^{-i}\}$, *se* $i \neq 0$
- $[s] = \{\rho^j s, j = 0, 1, \ldots, n-1\}$

*Dimostrazione.* Una rotazione $\rho^i$ commuta con tutte le rotazioni, quindi almeno con la metà degli elementi di $\mathrm{D}_n$. Inoltre $s\rho^i = \rho^{-i}s \neq \rho^i s$ perciò $\rho$ non commuta con tutti gli elementi di $\mathrm{D}_n$. Quindi $C(\rho^i)$ ha esattamente $n$ elementi, e $\rho^i$ ha $2n/n$ coniugati. Poiché $s\rho^i s = \rho^{-i}$, il suo altro coniugato è $\rho^{-i}$.

Abbiamo visto come nessuna rotazione commuti con $s$. Infatti, $s$ commuta solamente con $e$ e con se stesso: se commutasse con un altra simmetria $\rho^i s$ dovrebbe commutare anche col suo prodotto per $s$, cioè con una rotazione. Allora $C(s)$ ha $2$ elementi, e quindi $s$ ha $2n/2 = n$ coniugati. Questi coniugati possono essere soltanto le $n$ simmetrie. □

**Proposizione 4.11.** *Sia $n = 2m$ pari. Allora le classi coniugate in $\mathrm{D}_n$ sono:*

- $[e] = \{e\}$
- $[\rho^m] = \{\rho^m\}$
- $[\rho^i] = \{\rho^i, \rho^{-i}\}$, *se* $i \neq 0, m$
- $[s] = \{\rho^{2j} s, j = 0, \ldots, m-1\}$
- $[\rho s] = \{\rho^{2j+1} s, j = 0, \ldots, m-1\}$

*Dimostrazione.* La dimostrazione è come nel caso dispari, con la differenza che $\rho^m$ è un elemento centrale. Pertanto ogni rotazione commuta con $n$ elementi, tranne $e$ e $\rho^m$ che commutano con tutti i $2n$ elementi. Inoltre ogni simmetria $s$ commuta solamente con $e, s, \rho^m, \rho^m s$, quindi la sua classe di coniugio contiene $2n/4 = m$ elementi. Ci sono quindi due classi di coniugio tra le simmetrie. Corrispondono alle simmetrie il cui asse passa per vertici opposti, e a quelle il cui asse taglia a metà lati opposti. □

**Proposizione 4.12.** *Due permutazioni in $\mathrm{S}_n$ sono coniugate se e solo se hanno la stessa struttura in cicli.*

*Dimostrazione.* Segue dal fatto che $\sigma^{-1}\phi\sigma$ si ottiene dalla rappresentazione in cicli disgiunti di $\phi$ semplicemente sostituendo ad ogni numero la sua immagine tramite $\sigma$. Ha pertanto la sua stessa struttura in cicli (cambiano soltanto gli elementi permutati). □

**Esercizi (svolti):**
*(a)* Calcolare $\sigma^{-1}\phi\sigma$ se $\sigma = (13)(256)$ e $\phi = (123)(4567)$.

Basta sostituire a ciascun numero che compare nell'espressione di $\phi$ il suo corrispondente tramite $\sigma$. Poiché $\sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 4, \sigma(5) = 6, \sigma(6) = 2, \sigma(7) = 7$, si avrà:

$$\sigma^{-1}\phi\sigma = (351)(4627) = (135)(2746).$$

*(b)* Trovare tutti gli elementi di $\mathrm{S}_6$ che commutano con $(12)$.

L'indice del centralizzatore di $(12)$ si può determinare calcolando il numero dei coniugati di $(12)$: tali coniugati sono tutte le trasposizioni di $\mathrm{S}_6$, che sono esattamente $\binom{6}{2} = 15$ elementi. Allora l'ordine del centralizzatore è $|G|/[G : \mathrm{C}(\sigma)] = 6!/15 = 720/15 = 48$. Gli elementi che commutano con $(12)$ sono quindi esattamente $48$. Elencarli tutti è semplice: $(12)$ sposta soltanto $1$ e $2$, e commuta quindi con ogni permutazione che sposti gli altri $4$ elementi. Le permutazioni sugli elementi $3, 4, 5, 6$ sono $4! = 24$. Gli altri $24$ elementi che commutano con $(12)$ si ottengono moltiplicando le permutazioni su $3, 4, 5, 6$ per $(12)$.
*(c)* Determinare tutti i sottogruppi normali di $\mathrm{S}_5$.

Calcoliamo le classi coniugate degli elementi di $\mathrm{S}_5$, assieme al loro ordine:

- $[e]$ possiede $1$ elemento,
- $[(12)]$ possiede $10$ elementi,
- $[(123)]$ possiede $20$ elementi,
- $[(1234)]$ possiede $30$ elementi,
- $[(12345)]$ possiede $24$ elementi,
- $[(12)(34)]$ possiede $15$ elementi,
- $[(123)(45)]$ possiede $20$ elementi.

Un sottogruppo normale è unione di classi coniugate, ed in più il suo ordine divide $|\,\mathrm{S}_5\,| = 120$. Ogni sottogruppo deve inoltre contenere necessariamente l'identità e se contiene le trasposizioni deve essere tutto $\mathrm{S}_5$, perché ogni permutazione si scrive come prodotto di trasposizioni.

Cerchiamo quindi i sottogruppi normali non banali: contengono almeno $16 = 1 + 15$ elementi (la classe di coniugio più piccola dopo quella delle trasposizioni ha $15$ elementi). I divisori di $120$ maggiori o uguali di $16$ sono: $20, 24, 30, 40, 60, 120$. Sono tutti numeri pari, ed essendo le uniche classi laterali di ordine dispari quella dell'identità e quella di ordine $15$, esse devono essere entrambe presenti. Deve comparire perciò qualche altra classe di coniugio (diversa da quella delle trasposizioni). La più piccola ha ordine $20$, pertanto un sottogruppo normale non banale deve contenere almeno $36 = 1 + 15 + 20$ elementi. Gli unici casi che rimangono solo $40$ e $60$, ed effettivamente riusciamo a trovare unioni di classi coniugate che abbiano esattamente questi ordini. Le possibilità sono:

- $[e], [(12)(34)], [(12345)]$ con $40$ elementi,
- $[e], [(12)(34)], [(123)(45)], [(12345)]$ con $60$ elementi,
- $[e], [(12)(34)], [(123)], [(12345)]$ con $60$ elementi.

L'ultimo dei casi è una nostra vecchia conoscenza: è il sottogruppo alterno $\mathrm{A}_5$ di $\mathrm{S}_5$, che contiene tutte e sole le permutazioni pari. Il primo dei tre casi non è invece un sottogruppo di $\mathrm{S}_5$: se lo fosse sarebbe un sottogruppo anche di $\mathrm{A}_5$ — tutti i suoi elementi sono permutazioni pari — mentre $40$ non divide $|\,\mathrm{A}_5\,| = 60$.

Nemmeno il secondo sottoinsieme è un sottogruppo, per un analogo motivo. Se fosse un sottogruppo, la sua intersezione con $\mathrm{A}_5$ sarebbe anch'essa un sottogruppo. Ma l'intersezione è il sottoinsieme del primo caso, che abbiamo già escluso. L'unico sottogruppo normale non banale di $\mathrm{S}_5$ è pertanto $\mathrm{A}_5$.

**Esercizi:**

*(d)* Determinare le classi di coniugio in $\mathrm{A}_5$. Determinare tutti i sottogruppi normali di $\mathrm{A}_5$. *[Attenzione: le classi di coniugio in* $\mathrm{A}_5$ *non sono esattamente le stesse che in* $\mathrm{S}_5$*...]*
*(e)* Determinare le classi di coniugio nel gruppo $\mathrm{Q}_4$ delle unità dei quaternioni.
*(f)* Quante sono le classi di coniugio in $\mathrm{S}_8$?
*(g)* Determinare tutti gli elementi di $\mathrm{S}_6$ che commutano con $(12)(34)(56)$? *[Sugg.: quanti elementi commutano con questa permutazione? A questo punto occorre un po' di fantasia: non dimenticate i* $6$*-cicli!!!]*
*(h)* Dimostrate il Teorema di Cauchy nel caso dei $p$-gruppi: ogni $p$-gruppo contiene almeno un elemento di ordine $p$.
*(i)* Alla luce del Teorema 4.7, mostrate che ogni potenza di $p$ che divide l'ordine di un $p$-gruppo è ordine di qualche sottogruppo. *[Sugg.: Trovate un elemento di ordine* $p$ *nel centro, e quozientate per il sottogruppo che genera. Per induzione, l'enunciato sarà valido per il gruppo quoziente...]*

4.4. **Il Teorema di Sylow.** Il teorema di Lagrange ci informa che l'ordine di un sottogruppo di un gruppo finito $G$ divide l'ordine di $G$. Questo risultato tuttavia non si inverte: se $d$ è un divisore dell'ordine di $G$, non è detto che esista un sottogruppo di $G$ di ordine $d$: abbiamo già visto, nelle scorse note, come $\mathrm{A}_4$, che ha ordine $12$, non abbia sottogruppi di ordine $6$. Il teorema di Sylow ci assicura dell'esistenza di sottogruppi di particolare ordine.

**Teorema 4.13** (Prima parte del Teorema di Sylow)**.** *Sia $G$ un gruppo finito, e $p$ un numero primo. Se $p^n$ è la massima potenza di $p$ che divide $|G|$, allora $G$ ammette un sottogruppo di ordine esattamente $p^n$.*

Un sottogruppo di tale tipo si chiama *$p$-sottogruppo di Sylow* di $G$, o più semplicemente *$p$-Sylow*.
**Esempi:**
(1) Il gruppo simmetrico $\mathrm{S}_3$ ammette sottogruppi di Sylow. Infatti, ha ordine $6$, ed i suoi $2$- e $3$-Sylow sono pertanto i sottogruppi di ordine $2$ e $3$. I suoi $2$-Sylow sono quindi

$$\{e, (12)\}, \qquad \{e, (13)\}, \qquad \{e, (23)\}$$

mentre il suo unico $3$-Sylow è

$$\{e, (123), (132)\}.$$

(2) Nel gruppo ciclico $\mathrm{C}_6 = (\rho)$, l'unico $2$-Sylow è $(\rho^3)$, e l'unico $3$-Sylow è $(\rho^2)$.
(3) Il gruppo alterno $\mathrm{A}_4$ di ordine $12$ possiede un unico $2$-Sylow:

$$\{e, (12)(34), (13)(24), (14)(23)\},$$

e ben quattro $3$-Sylow:

$$\{e, (123), (132)\}, \qquad \{e, (124), (142)\}, \qquad \{e, (134), (143)\}, \qquad \{e, (234), (243)\}.$$

(4) Sia $\mathbb{F}_p$ il campo delle classi di resto modulo $p$, e $G = \mathrm{GL}_n(\mathbb{F}_p)$. Allora il sottogruppo $U$ delle matrici triangolari superiori unipotenti è un $p$-sottogruppo di Sylow di $G$. Infatti, l'ordine di $G$ è $(p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$, mentre l'ordine di $U$ è $p^{n(n-1)/2}$, che è la massima potenza di $p$ che divide $|G|$.

Per la dimostrazione del teorema di Sylow sfrutteremo il concetto di classe laterale doppia.

**Definizione 20.** Siano $H, K$ sottogruppi di $G$. Un laterale doppio di $H$ e $K$ in $G$ è un insieme del tipo

$$HxK = \{hxk | h \in H, k \in K\}.$$

Così come i laterali destri e sinistri erano classi di equivalenza rispetto a particolari relazioni, lo stesso accade per i laterali doppi. La relazione $\approx$ che li induce come classi di equivalenza è quella per la quale $a \approx b$ se esistono $h \in H, k \in K$ tali che $b = hak$.

**Lemma 4.14.** *La relazione $\approx$ è di equivalenza.*

*Dimostrazione.* La relazione $\approx$ gode della proprietà riflessiva: infatti $a \approx a$ dal momento che $a = e \cdot a \cdot e$. La proprietà simmetrica segue da $b = hak \Rightarrow a = h^{-1}bk^{-1}$. Inoltre, se $b = hak$ e $c = h'bk'$, allora $c = h'(hak)k' = (h'h)a(kk')$, quindi $\approx$ è anche transitiva. □

**Corollario 4.15.** *Laterali doppi distinti di $H$ e $K$ in $G$ sono disgiunti.*

Possiamo utilizzare le classi laterali doppie per ripartire un gruppo finito $G$ in sottoinsiemi il cui ordine è facilmente calcolabile.

**Lemma 4.16.** *Il numero di elementi del laterale doppio $HxK$ è $|H||K|/|H \cap xKx^{-1}|$.*

*Dimostrazione.* Sia $x$ un fissato elemento di $G$. La moltiplicazione destra per $x^{-1}$ realizza una bigezione tra gli insiemi $HxK$ e $H\,xKx^{-1}$. E' pertanto sufficiente contare gli elementi di $H(xKx^{-1})$ per contare anche quelli di $HxK$. Ora, $xKx^{-1}$ è un sottogruppo di $G$, e quindi per contare gli elementi di $H(xKx^{-1})$ basta applicare una formula incontrata durante le prime lezioni. Otteniamo

$$|H(xKx^{-1})| = \frac{|H||xKx^{-1}|}{|H \cap xKx^{-1}|}.$$

Ma l'ordine del sottogruppo $xKx^{-1}$ è pari a quello di $K$, e quindi

$$|HxK| = |H(xKx^{-1})| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

□

Lo strumento fondamentale per la dimostrazione delle varie parti del teorema di Sylow è il seguente (lo trovate anche sull'Herstein).

**Proposizione 4.17.** *Sia $G$ un sottogruppo del gruppo $M$, e $Q$ un $p$-Sylow di $M$. Allora è possibile trovare $x \in M$ in modo che $G \cap xQx^{-1}$ sia un $p$-Sylow di $G$.*

*Dimostrazione.* Sia $|M| = p^m a$ con $a$ non divisibile per $p$. Allora $|Q| = p^m$ e $|G| = p^n b$ con $n \leq m$ e $b$ non divisibile per $p$. Scomponiamo il gruppo $M$ in classi laterali doppie rispetto ai sottogruppi $G$ e $Q$. L'ordine della classe laterale $GxQ$ è pari a

$$\frac{|G||Q|}{|G \cap xQx^{-1}|} = \frac{p^{m+n}b}{|G \cap xQx^{-1}|}.$$

L'intersezione $G \cap xQx^{-1}$ è un sottogruppo sia di $G$ che di $xQx^{-1}$. Il suo ordine divide $|xQx^{-1}| = |Q| = p^m$ ed è perciò una potenza di $p$; divide inoltre anche $|G| = p^n b$ ed è quindi una potenza $p^l$ minore o uguale a $p^n$. Perciò $|GxQ| = p^{m+n-l}b$, con $l \leq n$, e $l = n$ soltanto quando il sottogruppo $G \cap xQx^{-1}$ ha ordine esattamente $p^n$.

Supponiamo per assurdo che per nessun valore di $x \in M$ il sottogruppo $G \cap xQx^{-1}$ abbia ordine $p^n$. Allora $p^{m+1}$ divide $|GxQ| = p^{m+(n-l)}b$ per ogni $x \in M$. Ma $M$ è unione disgiunta di laterali doppi, ed il suo ordine è pertanto somma di termini del tipo $|GxQ|$, che sono tutti divisibili per $p^{m+1}$; di conseguenza $p^{m+1}$ divide anche $|M| = p^m a$, una contraddizione. Deve quindi esistere $x \in M$ tale che il sottogruppo $G \cap xQx^{-1}$ abbia ordine esattamente $p^n$. □

**Lemma 4.18.** *Sia $|G| = n$, $p$ primo. Allora $G$* si immerge *in $\mathrm{GL}_n(\mathbb{F}_p)$: esiste cioè un omomorfismo iniettivo $\phi : G \to \mathrm{GL}_n(\mathbb{F}_p)$.*

*Dimostrazione.* Sia $V$ uno spazio vettoriale sul campo $\mathbb{F}_p$ una cui base sia data da elementi $v_g, g \in G$ indicizzati dagli elementi del gruppo $G$: in altre parole ogni elemento di $V$ è una combinazione lineare degli elementi linearmente indipendenti $v_g, g \in G$. Chiaramente, $V$ è uno spazio vettoriale di dimensione $n = |G|$.

Per ogni elemento $x \in G$, sia $T_x : V \to V$ l'unica applicazione lineare tale che $T_x(v_g) = v_{xg}$. Allora $T_x$ è un'applicazione lineare invertibile, in quanto la base $\{v_g\}$ viene semplicemente permutata, e $T_x \circ T_y = T_{xy}$ dal momento che $T_x \circ T_y(v_g) = T_x(T_y(v_g)) = T_x(v_{yg}) = v_{xyg} = T_{xy}(v_g)$. Inoltre $T_x = \mathrm{id}$ soltanto quando $x = e$.

Se $M_x$ è la matrice associata a $T_x$ nella base $\{v_g\}$, l'applicazione $x \mapsto M_x$ definisce allora un omomorfismo di gruppi $\phi : G \to \mathrm{GL}_n(\mathbb{F}_p)$, che è iniettivo, in quanto $M_x = \mathrm{id}$

soltanto quando $x = e$. $\phi$ è allora un omomorfismo iniettivo di $G$ in $\mathrm{GL}_n(\mathbb{F}_p)$, e la sua immagine è un sottogruppo di $\mathrm{GL}_n(\mathbb{F}_p)$ isomorfo a $G$. □

Tutti gli enunciati che seguono sono applicazione diretta della Proposizione 4.17.

*Dimostrazione del Teorema 4.13:* Abbiamo già visto come $\mathrm{GL}_n(\mathbb{F}_p)$ possieda almeno un $p$-Sylow, e cioè il sottogruppo $U$ di tutte le matrici triangolari superiori unipotenti. Sia $M = \mathrm{GL}_n(\mathbb{F}_p), Q = U$. Il gruppo $G$ si immerge in $M$, e quindi esiste un sottogruppo di $M$ isomorfo a $G$, che possiamo identificare con $G$. Allora, per la Proposizione 4.17, $G \cap xMx^{-1}$ è un $p$-Sylow di $G$ per qualche $x \in M$, e quindi $G$ contiene almeno un $p$-sottogruppo di Sylow. □

**Proposizione 4.19** (Seconda parte del Teorema di Sylow)**.** *I $p$-Sylow di un gruppo sono tutti coniugati tra loro.*

*Dimostrazione.* Sia $M$ un gruppo, e $P, Q$ suoi $p$-Sylow. La Proposizione 4.17, applicata al sottogruppo $G = P$ di $M$, mostra che per una opportuna scelta di $x$ in $M$, il sottogruppo $P \cap xQx^{-1}$ è un $p$-Sylow di $P$. Ma l'ordine di $P$ è una potenza di $p$, e pertanto il suo unico $p$-Sylow è $P$ stesso. Allora $P \cap xQx^{-1} = P$, da cui $P = xQx^{-1}$, dal momento che $P$ e $xQx^{-1}$ hanno lo stesso numero di elementi. □

**Corollario 4.20.** *In un gruppo $G$ un $p$-Sylow è normale se e solo se è l'unico $p$-Sylow di $G$.*

**Proposizione 4.21.** *Ogni $p$-sottogruppo di un gruppo finito è contenuto in qualche $p$-Sylow.*

*Dimostrazione.* Sia $M$ il gruppo finito con $p$-Sylow $Q$, e $G$ il suo $p$-sottogruppo. Ancora la Proposizione 4.17 mostra che un coniugato di $Q$ contiene $G$. □

La terza parte del Teorema di Sylow riguarda il numero dei $p$-Sylow contenuti in un gruppo $G$.

**Lemma 4.22.** *Sia $H < G$. Il numero dei coniugati di $H$ in $G$ è pari all'indice $[G : N(H)]$, dove $N(H) = \{g \in G | g^{-1}Hg = H\}$ è il normalizzatore di $H$.*

*Dimostrazione.* $a^{-1}Ha = b^{-1}Hb$ esattamente quando $(ab^{-1})^{-1}H(ab^{-1}) = H$, cioè se $a$ e $b$ giacciono nello stesso laterale (destro) di $N(H)$. Quindi vi sono tanti coniugati di $H$ quanti laterali destri ha $N(H)$ in $G$. □

**Proposizione 4.23** (Terza parte del Teorema di Sylow)**.** *Il numero dei $p$-Sylow di un gruppo finito $G$ è un divisore di $|G|$ congruo a $1$ modulo $p$.*

*Dimostrazione.* Il numero $n$ dei $p$-Sylow è pari a $[G : N(P)]$, ed è perciò un divisore di $|G|$. Per mostrare che $n \equiv 1 \mod p$, decomponiamo $G$ in laterali doppi rispetto alla coppia di sottogruppi $P, P$:

$$G = \bigcup_x PxP.$$

Se $x \in N(P)$, allora $xPx^{-1} = P$, quindi $Px = xP$ e $xP = PxP = Px$. In tal caso $Px \subset N(P)$, perciò un laterale doppio è interamente contenuto in $N(P)$, oppure non lo interseca.

Allora possiamo scrivere

$$G = \bigcup_{x \in N(P)} Px \ \cup \bigcup_{x \notin N(P)} PxP,$$

dove stiamo considerando un $x$ per ogni laterale doppio. Il primo termine nel secondo membro è chiaramente uguale a $N(P)$, perciò:

$$|G| = |N(P)| + \sum_{x \notin N(P)} |PxP|.$$

L'ordine di $PxP$ è pari a $|P||P|/|P \cap xPx^{-1}|$, ed il sottogruppo $P \cap xPx^{-1}$ è propriamente contenuto in $P$, dal momento che $x$ non normalizza $P$. Sia $|G| = p^n b, |P| = p^n, |N(P)| =$

$p^n c$; allora se $|P \cap xPx^{-1}| = p^{l_x}, l_x < n$ abbiamo $|PxP| = p^{2n-l_x} = p^{n+(n-l_x)}$, che è divisibile per $p^{n+1}$. Dividendo entrambi i membri dell'ultima equazione per $|N(P)|$ si ottiene

$$[G : N(P)] = 1 + \frac{1}{p^n c} \sum_{x \notin N(P)} p^{2n-l_x},$$

dove il secondo addendo del secondo membro è un intero, perché differenza tra $[G : N(P)]$ e $1$, divisibile per $p$, perché il numeratore è divisibile per $p^{n+1}$ mentre il denominatore solo per $p^n$. Allora $[G : N(P)]$ è la somma di $1$ e di un multiplo di $p$. □

La stessa tecnica dimostrativa permette di ottenere un altro risultato, che sarà rilevante nello studio della costruibilità con riga e compasso.

**Proposizione 4.24.** *Sia $G$ un $p$-gruppo finito, $p$ primo, $H \subset G$ un suo sottogruppo proprio. Allora il normalizzatore $N(H)$ contiene propriamente $H$. In particolare tutti i sottogruppi di $G$ di indice $p$ sono normali.*

*Dimostrazione.* Notiamo innanzitutto che l'intersezione $H \cap xHx^{-1}$ è sempre un sottogruppo di $H$, e coincide con $H$ se e solo se $xHx^{-1} = H$, cioè quando $x \in N(H)$. Decomponiamo $G$ in laterali doppi $HxH$. Se $|G| = p^n, |H| = p^m$, allora $HxH = |H|^2/|H \cap xHx^{-1}| \geq p^m$ e, per quanto detto prima, l'uguaglianza si ha esattamente quando $x \in N(H)$. In ogni altro caso, $|HxH|$ è una potenza di $p$ di esponente maggiore di $m$, e quindi è divisibile per $p^{m+1}$. Poiché $|G| > |H|$, anche $|G|$ è divisibile per $p^{m+1}$.

Se $x \in N(H)$, ricordando che $H \subset N(H)$, e che $N(H)$ è un sottogruppo di $G$, si ottiene $HxH \subset N(H)$. Questo mostra che un laterale doppio che intersechi $N(H)$ è tutto contenuto in $N(H)$ e che tali laterali doppi sono gli unici a possedere $p^m$ elementi.

In conclusione, $G$ si può esprimere come unione disgiunta di $N(H)$ e di laterali doppi $HxH$ non contenuti in $N(H)$. L'ordine $|N(H)|$ è allora differenza di $|G|$ e della somma di termini del tipo $|HxH|, x \notin N(H)$, che sono tutti multipli di $p^{m+1}$. Di conseguenza, anche $|N(H)|$ è multiplo di $p^{m+1}$ e quindi $|N(H)| > |H|$, o in altre parole $N(H)$ contiene propriamente $H$. □

Attraverso il teorema di Sylow, possiamo ora dare una seconda dimostrazione del Teorema di Cauchy.

**Teorema 4.25** (Cauchy)**.** *Siano $G$ un gruppo, $p$ primo tali che $p$ divida $|G|$. Allora $G$ contiene un elemento di ordine $p$.*

*Dimostrazione.* Per il Teorema di Sylow, esiste un sottogruppo di $G$ di ordine $p^n$. Scegliamo un elemento $g \neq e$ di tale sottogruppo. Se $g$ ha ordine $p^k$, allora $g^{p^{k-1}}$ ha ordine $p$. □

**Esercizi:**
*(a)* Se $G$ è un $p$-gruppo finito, e $H < G$ è un suo sottogruppo, mostrate che è possibile trovare una catena di sottogruppi

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_r = G,$$

tali che $[H_{i+1} : H_i] = p$ per ogni $0 \leq i < r$.
*(b)* Mostrate che se $P$ è un $p$-Sylow di $G$, allora $N(N(P)) = N(P)$. *[Sugg.: Il normalizzatore $N(H)$ di un sottogruppo $H$ è il più grande sottogruppo $N$, $H < N < G$ nel quale $H$ sia normale. $P$ è un sottogruppo caratteristico di $N(P)$, cioè è fissato da ogni automorfismo di $N(P)$. Inoltre un sottogruppo caratteristico di un sottogruppo normale è normale...]*
*(c)* Dire quanti e quali siano i $p$-Sylow di $\mathrm{S}_5$.
*(d)* Sia $p^n$ la massima potenza di $p$ che divide $|G|$, e supponiamo che esattamente $p^n$ elementi di $G$ abbiano ordine una potenza di $p$. Allora vi è un unico $p$-Sylow in $G$.
*(e)* Mostrate che se una matrice $M$ in $\mathrm{GL}_n(\mathbb{F}_p)$ è tale che $M^p = \mathrm{id}$, allora esiste un cambiamento di base che la rende triangolare superiore unipotente. *[Provate sia per mezzo dell'algebra lineare, sia attraverso la teoria dei gruppi...]*
*(f)* Sia $G$ un gruppo di ordine $pq, p < q$. Se $p$ non divide $q - 1$ allora il $p$-Sylow di $G$ è normale. *[Sugg.: quanti sono i $p$-Sylow?]*
*(g)* Un gruppo di ordine $15$ è necessariamente ciclico.

*(h)* Esiste un gruppo non ciclico di ordine 21.
*(i)* A lezione l'immersione di un gruppo $G$ in $\mathrm{GL}_n(\mathbb{F}_p)$ era stata data componendo un'immersione di $G$ in $\mathrm{S}_n$ (secondo il Teorema di Cayley) con un'immersione di $\mathrm{S}_n$ in $\mathrm{GL}_n(\mathbf{k})$, che però non ho costruito esplicitamente. Determinate un omomorfismo iniettivo di $\mathrm{S}_n$ in $\mathrm{GL}_n(\mathbf{k})$.
*(j)* Se $p$ è primo, e $p^n$ divide l'ordine di $G$, allora esiste almeno un sottogruppo di $G$ di ordine esattamente $p^n$.

## 5. Prodotti diretti e semidiretti

### 5.1. **Prodotto diretto di gruppi.**

**Definizione 21.** Siano $H$ e $K$ gruppi. Allora il *prodotto diretto* di $H$ e $K$ è l'insieme prodotto cartesiano $G = H \times K$ dotato dell'operazione $(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2)$.

**Proposizione 5.1.** *Il prodotto diretto $H \times K$ è un gruppo.*

*Dimostrazione.* La dimostrazione è del tutto ovvia. Innanzitutto l'associatività del prodotto segue da quella delle operazioni di gruppo in $H$ e $K$, dal momento che l'operazione in $H \times K$ è definita attraverso quelle nei due gruppi fattori.

L'identità in $H \times K$ è l'elemento $(e, e)$, come si verifica calcolando $(h, k)(e, e) = (h, k) = (e, e)(h, k)$. L'inverso di $(h, k)$ è a questo punto chiaramente l'elemento $(h^{-1}, k^{-1})$. □

**Proposizione 5.2.** *Valgono le seguenti proprietà:*

- $|H \times K| = |H||K|$*;*
- $H \times K$ *è abeliano se e solo se* $H$ *e* $K$ *sono abeliani;*
- *Se* $H' < H$*,* $K' < K$ *allora* $H' \times K' = \{(h, k) \in H \times K \,|\, h \in H', k \in K'\}$ *è un sottogruppo di* $H \times K$*. Se* $H' \lhd H, K' \lhd K$ *allora* $H' \times K' \lhd H \times K$*.*
- *Se* $H' \lhd H, K' \lhd K$*, allora* $(H \times K)/(H' \times K') \simeq (H/H') \times (K/K')$*.*
- *Il centro di* $H \times K$ *è* $Z(H) \times Z(K)$*.*
- *I sottogruppi* $\bar{H} = H \times (e)$ *e* $\bar{K} = (e) \times K$ *sono normali in* $H \times K$ *e soddisfano* $\bar{H} \cap \bar{K} = (e)$*,* $\bar{H}\bar{K} = H \times K$*. Inoltre ogni elemento di* $\bar{H}$ *commuta con ogni elemento di* $\bar{K}$*.*

*Dimostrazione.* Gli enunciati sono tutti di immediata dimostrazione, e vengono lasciati per esercizio. Come esempio, diamo tuttavia una dimostrazione del quarto enunciato.

Sia $\phi : H \times K \to (H/H') \times (K/K')$ l'omomorfismo definito come $\phi(h, k) = ([h], [k])$, dove $[h]$ e $[k]$ sono le classi laterali $H'h$ e $K'k$ rispettivamente. Allora $\phi$ è un omomorfismo di gruppi, che è chiaramente suriettivo. Inoltre il nucleo di $\phi$ è costituito dalle coppie $(h, k)$ con la proprietà che $H'h = H', K'k = K'$, cioè tali che $h \in H', k \in K'$. Quindi $\ker \phi = H' \times K'$. Per il teorema di isomorfismo dimostrato qualche tempo fa

$$(H \times K)/(H' \times K') = (H \times K)/\ker \phi \simeq (H/H') \times (K/K').$$

□

L'ultima proprietà enunciata nella Proposizione è per noi sufficientemente importante da separarla in un Lemma a parte.

**Lemma 5.3.** *Se* $H, K \lhd G$ *e* $H \cap K = (e)$*, allora ogni elemento di* $H$ *commuta con ogni elemento di* $K$*.*

*Dimostrazione.* Siano $h \in H, k \in K$. L'elemento $hkh^{-1}k^{-1}$ giace nell'intersezione $H \cap K$. Infatti $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ è prodotto di elementi di $K$. Allo stesso modo $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ è prodotto di elementi di $H$. Ma $H \cap K = (e)$, quindi $hkh^{-1}k^{-1} = e$ da cui $hk = kh$. □

La maniera più semplice di controllare che un gruppo sia isomorfo ad un prodotto diretto di gruppi è quella di esibire dei sottogruppi dei quali sia *prodotto diretto interno*.

**Definizione 22.** Siano $H, K$ sottogruppi di $G$. Allora $G$ è prodotto diretto interno di $H$ e $K$ se

- $H$ e $K$ sono normali in $G$;

- $H \cap K = (e)$;
- $HK = G$.

**Proposizione 5.4.** *Siano $H, K < G$. Allora sono fatti equivalenti:*

- $H \cap K = (e)$, $HK = G$;
- $H \cap K = (e)$, $|H||K| = |G|$;
- *Ogni elemento $g \in G$ si scrive in modo unico come prodotto $g = hk, h \in H, k \in K$;*
- *Se $1 = hk$, con $h \in H, k \in K$, allora $h = k = 1$.*

*Dimostrazione.* Anche queste dimostrazioni sono molto facili. Fatele per esercizio. □

La seguente proposizione mostra che prodotto diretto di gruppi, e decomposizione in prodotto diretto interno di sottogruppi sono in realtà la stessa nozione.

**Proposizione 5.5.** *Se $G$ è prodotto diretto interno dei suoi sottogruppi normali $H$ e $K$, allora $G$ è isomorfo al prodotto diretto $H \times K$. Viceversa, se $G$ è isomorfo al prodotto di gruppi $H \times K$, allora $G$ è prodotto diretto interno di due suoi sottogruppi isomorfi a $H$ e $K$ rispettivamente.*

*Dimostrazione.* Supponiamo che $G$ sia prodotto diretto interno dei sottogruppi normali $H$ e $K$. L'applicazione $\phi : H \times K \to G$ definita come $\phi(h, k) = hk$ è allora un isomorfismo. La suriettività segue da $HK = G$, l'iniettività da $H \cap K = (e)$. $\phi$ è inoltre un omomorfismo poiché

$$\phi(hh', kk') = hh'kk' = hkh'k' = \phi(h, k)\phi(h', k'),$$

dove abbiamo sfruttato in modo essenziale la commutatività degli elementi di $H$ e $K$.

Viceversa, supponiamo che sia dato un isomorfismo $\phi : H \times K \to G$. I sottogruppi $\bar{H} = H \times (e)$ e $\bar{K} = (e) \times K$ hanno la proprietà che $\bar{H} \cap \bar{K} = (e)$, $\bar{H}\bar{K} = H \times K$. Essi sono inoltre normali in $H \times K$, e sono isomorfi ad $H$ e $K$ rispettivamente. Ma allora le loro immagini tramite $\phi$ sono sottogruppi di $G$ con le stesse proprietà. $G$ è quindi prodotto diretto interno di sottogruppi isomorfi ad $H$ e $K$. □

Avremo bisogno della nozione di prodotto diretto di gruppi soprattutto nella classificazione dei gruppi abeliani finiti, ma in quel caso ci servirà anche il prodotto diretto di più di due gruppi.

**Definizione 23.** Il prodotto diretto dei gruppi $G_1, \ldots, G_n$ è il prodotto cartesiano $G_1 \times \ldots \times G_n$ con l'operazione $(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$.

Con questo prodotto $G_1 \times \ldots \times G_n$ diventa un gruppo, per il quale valgono le ovvie generalizzazioni delle proprietà elencate nella Proposizione 5.2. Il concetto di prodotto diretto interno di $n$ sottogruppi è anche analogo:

**Definizione 24.** $G$ si dice prodotto diretto interno dei suoi sottogruppi $H_1, \ldots, H_n$ se

- I sottogruppi $H_1, \ldots, H_n$ sono normali in $G$;
- Esiste un unico modo di esprimere ciascun elemento $g \in G$ come prodotto $g = h_1h_2 \ldots h_n$ con $h_i \in H_i$.

Questa definizione non è simile alla Definizione 22, ma sfrutta una delle proprietà equivalenti elencate nella Proposizione 5.4. Il motivo di questa scelta è chiarito dalla seguente:

**Proposizione 5.6.** *Siano $H_1, \ldots, H_n \lhd G$. Allora sono fatti equivalenti:*

- $(H_1 \ldots H_k) \cap H_{k+1} = (e)$ *per* $k = 1, \ldots, n-1$, $H_1H_2 \ldots H_n = G$;
- $|H_1 \ldots H_k| = |H_1| \ldots |H_k|$ *per* $k = 1, \ldots, n$, $|H_1| \ldots |H_n| = |G|$;
- *Ogni elemento $g \in G$ si scrive in modo unico come prodotto $g = h_1 \ldots h_n$, con $h_i \in H_i$.*
- *Se $1 = h_1 \ldots h_n$, con $h_i \in H_i$, allora $h_1 = \ldots = h_n = 1$.*

**Osservazione:** Controllare invece che $H_i \cap H_j = (e)$, $H_1H_2 \ldots H_n = G$ non è sufficiente a garantire l'unicità della rappresentazione come prodotto. Per convincercene, consideriamo in $G = \mathrm{C}_2 \times \mathrm{C}_2 = \{e, a, b, c = ab\}$ i sottogruppi $A = (a), B = (b), C = (c)$. Allora

l'intersezione di due qualsiasi di questi sottogruppi contiene solo l'identità, e chiaramente $G = ABC$. Ma la decomposizione in prodotto non può essere unica, essendovi in $G$ solo quattro elementi, ed essendo possibili ben otto prodotti in $ABC$.

La proposizione che segue è la traduzione della Proposizione 5.5 al caso di più sottogruppi:

**Proposizione 5.7.** *Se $G$ è prodotto diretto interno dei suoi sottogruppi normali $H_1, \ldots, H_n$, allora $G$ è isomorfo al prodotto diretto $H_1 \times \ldots \times H_n$. Viceversa, se $G$ è isomorfo al prodotto diretto di gruppi $H_1 \times \ldots \times H_n$, allora $G$ è prodotto diretto interno di suoi sottogruppi isomorfi a $H_1, \ldots, H_n$ rispettivamente.*

**Esempi:** (1) Siano $m$ ed $n$ numeri primi tra loro. Allora il gruppo ciclico $\mathrm{C}_{mn}$ è isomorfo al prodotto diretto $\mathrm{C}_m \times \mathrm{C}_n$. Sia infatti $\rho$ il generatore di $\mathrm{C}_{mn}$. Allora $\rho^m$ genera un sottogruppo ciclico di ordine $n$, e $\rho^n$ uno di ordine $m$. L'intersezione di questi due sottogruppi ha per ordine un divisore comune di $m$ ed $n$, e contiene quindi solo l'identità. Inoltre il prodotto dei loro ordini è pari all'ordine del gruppo $\mathrm{C}_{mn}$ che li contiene. Quindi $\mathrm{C}_{mn}$ è prodotto diretto interno di sottogruppi isomorfi a $\mathrm{C}_m$ e $\mathrm{C}_n$ rispettivamente.

L'isomorfismo tra $\mathrm{C}_{mn}$ e $\mathrm{C}_m \times \mathrm{C}_n$ è talvolta chiamato Teorema cinese del resto, ed indica come il resto modulo $mn$ di un numero sia determinato dai suoi resti modulo $m$ ed $n$.

(2) Sia $G$ un gruppo di ordine $pq$, con $p < q$ primi con la proprietà che $p$ non divida $q-1$. Allora il $q$-Sylow è certamente normale, in quanto il numero di $q$-Sylow è un divisore di $p$ congruo ad $1$ modulo $q$. Inoltre anche il $p$-Sylow è normale, in quanto se $p$ non divide $q-1$ allora $q \not\equiv 1$ modulo $p$.

Il $p$-Sylow ed il $q$-Sylow sono sottogruppi normali che si intersecano nell'identità, ed il prodotto dei loro ordini è pari all'ordine di $G$. Allora $G$ è prodotto diretto dei due Sylow. Per il Teorema cinese del resto, è un gruppo ciclico di ordine $pq$.

(3) Sia $G$ un gruppo finito in cui tutti i Sylow sono normali. Allora $G$ è prodotto diretto dei suoi sottogruppi di Sylow. Sia $P_i$ il $p_i$-Sylow di $G$, dove $p_1, \ldots, p_n$ sono i primi che dividono l'ordine di $G$. Devo mostrare che $(P_1 P_2 \ldots P_k) \cap P_{k+1} = (e)$. Ma il sottoinsieme $P_1 P_2 \ldots P_k$ è un sottogruppo di $G$ (mostrare!) e il suo ordine è $|P_1||P_2| \ldots |P_k|$ (mostrare!), che è primo con $|P_{k+1}|$. Quindi l'intersezione può avere solo ordine $1$, e contiene solo l'identità. Che $|P_1||P_2| \ldots |P_n|$ sia pari a $|G|$ è ovvio.

Per la cronaca, i gruppi finiti che hanno tutti i Sylow normali sono detti *nilpotenti*.

Quest'ultima proposizione ci sarà utile al momento di dimostrare il Teorema di classificazione dei gruppi abeliani finiti.

**Proposizione 5.8.** *Sia $G = H_1 \times \ldots \times H_n$. Se gli omomorfismi $\phi_i : H_i \to K$ sono tali che per $i \neq j$, $\phi_i(x)$ commuta con $\phi_j(y)$ per ogni scelta di $x \in H_i, y \in H_j$, allora esiste un unico omomorfismo $\phi : G \to K$ con la proprietà che $\phi(h_1, \ldots, h_n) = \phi_1(h_1) \ldots \phi_n(h_n)$.*

## 5.2. **Prodotto semidiretto di gruppi.**

**Definizione 25.** Siano $N$ e $H$ gruppi, e sia $\phi : H \to \mathrm{Aut}\, N$ un omomorfismo[10]. Allora il *prodotto semidiretto* $N \rtimes_\phi H$ di $N$ e $H$ tramite $\phi$ è l'insieme prodotto cartesiano $G = N \times H$ dotato dell'operazione $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2)$.

**Proposizione 5.9.** *Il prodotto semidiretto $N \rtimes_\phi H$ è un gruppo.*

*Dimostrazione.* Mostriamo innanzitutto che la moltiplicazione è associativa. Abbiamo

$$((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) = (n_1 \phi_{h_1}(n_2), h_1 h_2) \cdot (n_3, h_3) = (n_1 \phi_{h_1}(n_2) \phi_{h_1 h_2}(n_3), h_1 h_2 h_3),$$

mentre

$$(n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)) = (n_1, h_1) \cdot (n_2 \phi_{h_2}(n_3), h_2 h_3) = (n_1 \phi_{h_1}(n_2 \phi_{h_2}(n_3)), h_1 h_2 h_3).$$

Ora, $\phi_{h_1}$ è un omomorfismo, quindi

$$\phi_{h_1}(n_2 \phi_{h_2}(n_3)) = \phi_{h_1}(n_2) \phi_{h_1}(\phi_{h_2}(n_3)),$$

[10] Per motivi di chiarezza tipografica, scrivo $\phi_h$ al posto di $\phi(h)$

ma anche $\phi$ è un omomorfismo, perciò

$$\phi_{h_1}(\phi_{h_2}(n_3)) = (\phi_{h_1} \circ \phi_{h_2})(n_3) = \phi_{h_1 h_2}(n_3),$$

e l'associatività è dimostrata.

Si controlla facilmente che $(e, e)$ è l'elemento neutro di questa moltiplicazione. Lievemente più complesso è controllare che ogni elemento ammetta un inverso. Per farlo, notiamo che un inverso destro di $(n, h)$ deve essere tale che

$$(n, h) \cdot (n', h') = (n\phi_h(n'), hh') = (e, e).$$

Allora da $hh' = e$ si ha $h' = h^{-1}$ e da $n\phi_h(n') = e$ segue $\phi_h(n') = n^{-1} \Rightarrow n' = \phi_{h^{-1}}(n^{-1})$. L'unico inverso destro di $(n, h)$ è perciò

$$(\phi_{h^{-1}}(n^{-1}), h^{-1}).$$

Controlliamo quindi che tale elemento è anche inverso sinistro di $(n, h)$:

$$(\phi_{h^{-1}}(n^{-1}), h^{-1}) \cdot (n, h) = ((\phi_{h^{-1}}(n^{-1})\phi_{h^{-1}}(n), h^{-1}h) = (\phi_{h^{-1}}(n^{-1}n), h^{-1}h) = (e, e).$$

□

**Esempio:** Se $\phi : H \to \operatorname{Aut} N$ è tale che $\phi_h = \mathrm{id}$ per ogni $h \in H$, allora $N \rtimes_\phi H$ è semplicemente il prodotto diretto $N \times H$. In questo caso il prodotto semidiretto si dice *banale*.

**Proposizione 5.10.** *Valgono le seguenti proprietà:*

- $|N \rtimes_\phi H| = |N||H|$;
- $N \rtimes_\phi H$ *è abeliano se e solo se* $N$ *e* $H$ *sono abeliani e* $\phi_h = \mathrm{id}$ *per ogni* $h \in H$;
- *Se* $H' < H$ *e* $N'$ *è un sottogruppo caratteristico di* $N$ *allora* $N' \rtimes H' = \{(n, h) \in N \rtimes_\phi H | n \in N', h \in H'\}$ *è un sottogruppo di* $N \rtimes_\phi H$.
- *I sottoinsiemi* $\bar{N} = N \rtimes (e)$ *e* $\bar{H} = (e) \rtimes H$ *sono sottogruppi di* $N \rtimes_\phi K$ *ed* $\bar{N}$ *è normale. Essi soddisfano inoltre* $\bar{N} \cap \bar{H} = (e)$, $\bar{N}\bar{H} = N \rtimes_\phi H$.

Come nel caso dei prodotti diretti, il modo più semplice di controllare che un gruppo sia isomorfo ad un prodotto semidiretto di gruppi è quella di esibire dei sottogruppi dei quali sia *prodotto semidiretto interno*.

**Definizione 26.** Siano $N, H$ sottogruppi di $G$. Allora $G$ è prodotto semidiretto interno di $N$ e $H$ se

- $N$ è normale in $G$;
- $H \cap K = (e)$;
- $HK = G$.

**Proposizione 5.11.** *Se* $G$ *è prodotto semidiretto interno dei suoi sottogruppi* $N$ *e* $H$, *allora esiste* $\phi : H \to \operatorname{Aut} N$ *per il quale* $G$ *sia isomorfo al prodotto diretto* $N \rtimes_\phi H$. *Viceversa, se* $G$ *è isomorfo al prodotto di gruppi* $N \rtimes_\phi K$, *allora* $G$ *è prodotto diretto interno di due suoi sottogruppi isomorfi a* $N$ *e* $H$ *rispettivamente.*

*Dimostrazione.* Supponiamo che $G$ sia prodotto semidiretto interno dei sottogruppi $N$ e $H$. Poiché $N$ è normale in $G$, la coniugazione per $h \in H$ induce un automorfismo di $N$. Sia $\phi_h(n) = hnh^{-1}, n \in N$. Allora $\phi : H \to \operatorname{Aut} N$ è un omomorfismo di gruppi.

L'applicazione $\psi : N \rtimes_\phi H \to G$ definita come $\psi(n, h) = nh$ è allora un isomorfismo. La suriettività segue da $NH = G$, l'iniettività da $N \cap H = (e)$. $\psi$ è inoltre un omomorfismo poiché

$$\psi(n\phi_h(n'), hh') = n\phi_h(n')hh' = nhn'h^{-1}hh' = nhn'h' = \psi(n, h)\psi(n', h').$$

Viceversa, supponiamo che sia dato un isomorfismo $\psi : N \rtimes_\phi H \to G$. I sottogruppi $\bar{N} = N \rtimes (e)$ e $\bar{H} = (e) \rtimes H$ hanno la proprietà che $\bar{N} \cap \bar{H} = (e)$, $\bar{N}\bar{H} = N \rtimes_\phi H$. Inoltre sono isomorfi ad $N$ e $H$ rispettivamente, e $\bar{N}$ è normale. Ma allora le loro immagini tramite $\psi$ sono sottogruppi di $G$ con le stesse proprietà. $G$ è quindi prodotto semidiretto interno di sottogruppi isomorfi ad $N$ e $H$. □

**Esempi:** (1) Il gruppo diedrale $\mathrm{D}_n$ è prodotto semidiretto interno del suo sottogruppo normale $\mathrm{C}_n$ e di un qualsiasi sottogruppo $S = \{e, s\}$ di ordine 2. Infatti $S \cap \mathrm{C}_n = (e)$, e $|S||\,\mathrm{C}_n\,| = 2n = |\,\mathrm{D}_n\,|$. L'omomorfismo $\phi : S \to \operatorname{Aut}\mathrm{C}_n$ è tale che $\phi_s(x) = x^{-1}$ per ogni $x \in \mathrm{C}_n$, mentre chiaramente $\phi_e = \mathrm{id}$.

(2) Sia $G$ un gruppo con 21 elementi. Allora il 7-Sylow è normale, mentre per il Teorema di Sylow, il numero dei 3-Sylow può essere 1 o 7. Se anche il 3-Sylow è unico, allora è anch'esso normale. $G$ è quindi prodotto diretto del 3- e del 7-Sylow, ed è pertanto ciclico di ordine 21.

Se invece il 3-Sylow non è normale, $G$ è soltanto prodotto semidiretto del 7-Sylow con il 3-Sylow, e quindi $G \simeq \mathrm{C}_7 \rtimes_\phi \mathrm{C}_3$ per qualche $\phi : \mathrm{C}_3 \to \operatorname{Aut}\mathrm{C}_7$. Per costruire l'omomorfismo $\phi$, analizziamo il gruppo $\operatorname{Aut}\mathrm{C}_7$: un automorfismo di $\mathrm{C}_7$ è determinato dall'immagine del generatore $\rho$, che sarà un altro generatore di $\mathrm{C}_7$, cioè uno degli elementi $\rho^i, i = 1, ..., 6$. Facendo un po' di conti si vede che $\rho \mapsto \rho^2$ e $\rho \mapsto \rho^4$ sono gli unici due automorfismi di ordine 3 in $\operatorname{Aut}\mathrm{C}_7$. Un omomorfismo $\phi : \mathrm{C}_3 \to \operatorname{Aut}\mathrm{C}_7$ deve mandare il generatore di $\mathrm{C}_3$ in un automorfismo di ordine 3 oppure nell'identità.

Abbiamo già visto che se $\phi(h) = \mathrm{id}$ per ogni $h \in H$, il prodotto semidiretto si riduce a quello diretto, pertanto non siamo interessati a questo caso, che abbiamo già compreso abbondantemente. Se $\phi \not\equiv \mathrm{id}$ allora un generatore di $\mathrm{C}_3$ viene mandato in $\rho \mapsto \rho^2$ mentre l'altro viene mandato in $\rho \mapsto \rho^4$.

Ricapitoliamo: se $G$ ha 21 elementi e non è ciclico, allora in ogni suo 3-Sylow posso trovare un elemento $x$ la coniugazione per il quale induce sul sottogruppo normale $\mathrm{C}_n$ l'automorfismo $T$ che manda ogni elemento nel suo quadrato. Allora $G \simeq \mathrm{C}_3 \rtimes_\phi \mathrm{C}_7$ con $\phi(x) = T$, dove $x$ è un generatore di $\mathrm{C}_3$. In altre parole, ogni gruppo non ciclico di ordine 21 è isomorfo a questo particolare prodotto semidiretto. Vi è quindi un solo gruppo non ciclico di ordine 21, a meno di isomorfismi.

(3) Siano $p, q$ primi, e supponiamo che inoltre $p$ divida $q - 1$. Il gruppo $\operatorname{Aut}\mathrm{C}_q$ ha $q - 1$ elementi (un automorfismo è determinato dall'immagine di un generatore, ed abbiamo $q - 1$ scelte possibili), e quindi $p$ divide l'ordine di $\operatorname{Aut}\mathrm{C}_q$. Per il Teorema di Cauchy, vi sono automorfismi di $\mathrm{C}_q$ di ordine $p$, ed è perciò possibile costruire un omomorfismo non banale $\phi : \mathrm{C}_p \to \operatorname{Aut}\mathrm{C}_q$.

Questo mostra l'esistenza di un prodotto semidiretto non banale di $\mathrm{C}_q$ con $\mathrm{C}_p$. E' un gruppo non ciclico (e non abeliano!) di ordine $pq$. Quando avremo imparato un minimo di teoria dei campi, vedremo che $\operatorname{Aut}\mathrm{C}_q$ è sempre un gruppo ciclico, e da questo mostreremo che vi può essere un solo gruppo non abeliano di ordine $pq$, a meno di isomorfismi.

5.3. **Il teorema di classificazione dei gruppi abeliani finiti.** Il teorema di struttura dei gruppi abeliani finiti *"classifica"* tali gruppi. In altre parole fornisce una lista di gruppi abeliani finiti che possiede due proprietà essenziali: ogni gruppo abeliano finito è isomorfo ad un gruppo della lista, e i gruppi della lista sono tra loro non isomorfi. In altre parole, ogni gruppo abeliano finito è isomorfo ad uno e solo uno dei gruppi elencati dal teorema.

L'enunciato del teorema è il seguente:

**Teorema 5.12.** *Sia $G$ un gruppo abeliano finito. Allora risultano univocamente determinati dei numeri naturali $n_1 \geq n_2 \geq \ldots \geq n_k > 1$, con la proprietà che $n_i$ divide $n_j$ se $i > j$, tali che $G$ sia isomorfo al prodotto diretto di gruppi ciclici $\mathrm{C}_{n_1} \times \mathrm{C}_{n_2} \times \ldots \times \mathrm{C}_{n_k}$.*

La dimostrazione è lunga ma non particolarmente sofisticata. Richiamo qui all'inizio tutti i fatti elementari che utilizzerò nella dimostrazione, e che dovreste già conoscere bene se avete provato a fare gli esercizi dell'Herstein.

**Lemma 5.13.** *Sia $\mathrm{C}_n = (\rho)$ un gruppo ciclico con $n$ elementi. Allora $\rho^m$ ha ordine $n/(m, n)$.*

*Dimostrazione.* L'ordine di $\rho^m$ è al più $n/(m, n)$. Infatti $(\rho^m)^{n/(m,n)} = \rho^{mn/(m,n)}$. Ma $mn/(m, n)$ è il minimo comune multiplo di $m$ ed $n$. Perciò è un multiplo di $n$, e quindi $\rho^{mn/(m,n)} = \rho^{kn} = e$.

Sia $i$ l'ordine di $\rho^m$. Allora $(\rho^m)^i = \rho^{mi} = e$. Ma questo può accadere soltanto quando $mi$ è un multiplo di $n$. Ma allora $mi$ è un multiplo comune di $m$ ed $n$, perciò $mi \geq mn/(m,n)$. Allora $i \geq n/(m,n)$. L'ordine di $\rho^m$ è quindi almeno $n/(m,n)$. Avevamo già visto che doveva essere al più $n/(m,n)$. Ne concludiamo che è esattamente $n/(m,n)$. □

**Lemma 5.14.** *I sottogruppi non banali di $\mathrm{C}_n = (\rho)$ sono ciclici, generati da $\rho^d$ con $d$ un divisore (non banale) di $n$. Se $n = dh$, allora $(\rho^d) \simeq \mathrm{C}_h$. Il quoziente $\mathrm{C}_n / \mathrm{C}_h$ è isomorfo a $\mathrm{C}_d$.*

*Dimostrazione.* Sia $H$ un sottogruppo di $\mathrm{C}_n$. Poniamo $\Gamma = \{m \in \mathbb{Z} | \rho^m \in H\}$. Allora $\Gamma$ è chiaramente un sottogruppo di $\mathbb{Z}$, che contiene $(n)$. Quindi $\Gamma = (d)$, dove $d$ è un divisore di $n$. Se $d = n$ otteniamo il sottogruppo $(e)$. Negli altri casi, $H = (\rho^d)$.

Ogni quoziente $\mathrm{C}_n$ è ancora ciclico, perché generato dalla classe laterale cui $\rho$ appartiene. Il quoziente $\mathrm{C}_n / \mathrm{C}_h$ è quindi un gruppo ciclico che possiede $n/h = d$ elementi: deve essere isomorfo a $\mathrm{C}_d$. □

**Lemma 5.15.** *L'equazione $x^m = e$ ha esattamente $(m,n)$ soluzioni in $\mathrm{C}_n$. Le soluzioni sono tutte e sole le potenze di $\rho^{n/(m,n)}$, dove $\rho$ è un generatore di $\mathrm{C}_n$.*

*Dimostrazione.* L'insieme $\{x \in \mathrm{C}_n | x^m = e\}$ è un sottogruppo (mostrare!), ed è quindi generato da $\rho^d$, con $d$ un divisore di $n$. $d$ è il minimo naturale per il quale $\rho^{dm} = e$, cioè per cui $dm$ sia un multiplo di $n$. Ma allora $dm$ è il minimo comune multiplo $mn/(m,n)$ di $m$ ed $n$, e quindi $d = n/(m,n)$. □

**Lemma 5.16.** *Se un gruppo abeliano $G$ contiene un elemento di ordine $m$ ed uno di ordine $n$, allora contiene anche un elemento di ordine il minimo comune multiplo tra $m$ ed $n$.*

*Dimostrazione.* Sia $a$ l'elemento di ordine $m$, e $b$ l'elemento di ordine $n$. Se $(m,n) = 1$ allora $(a) \cap (b) = (e)$, poiché $1$ è l'unico divisore comune di $m$ ed $n$. Questo vuol dire che l'unica potenza di $a$ che sia anche una potenza di $b$ è l'identità.

Affinché $(ab)^i = a^i b^i$ sia l'identità, è necessario che $a^i = b^{-i}$, quindi che $a^i = b^i = e$. Allora $i$ è un multiplo sia di $m$ che di $n$, quindi di $mn$. Ma $(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n (b^n)^m = e$, quindi l'ordine di $ab$ è esattamente $mn$.

Se invece $(m,n) \neq 1$, notiamo che il minimo comune multiplo tra $m$ ed $n$ si può sempre scrivere come $hk$ dove $h$ è un divisore di $m$, $k$ è un divisore di $N$, e $(h,k) = 1$. Ma allora un'opportuna potenza di $a$ avrà ordine $h$, un'opportuna potenza di $b$ avrà ordine $k$, ed il loro prodotto avrà ordine $hk = mn/(m,n)$. □

**Lemma 5.17.** *Sia $g$ un elemento di ordine massimo nel gruppo abeliano finito $G$. Allora $o(h)$ divide $o(g)$ per ogni $h \in G$.*

*Dimostrazione.* Se $o(h)$ non dividesse $o(g)$, ci sarebbe per il Lemma precedente un elemento di ordine il minimo comune multiplo tra $o(h)$ e $o(g)$, che è maggiore di $o(g)$. □

**Proposizione 5.18.** *Sia $G$ un gruppo abeliano finito. Allora $G$ possiede sottogruppi ciclici $H_1, \ldots, H_k$ tali che:*

- *$G$ è prodotto diretto dei sottogruppi $H_1, \ldots, H_k$;*
- *$|H_i|$ divide $|H_j|$ quando $i > j$, e $|H_k| > 1$.*

*Dimostrazione.* Per induzione su $|G|$, la base dell'induzione $|G| = 1$ essendo banale, dal momento che il gruppo con un elemento è prodotto diretto vuoto.

Sia $x$ un elemento di ordine massimo in $G$, e sia $N = (x)$, il sottogruppo che genera. $G$ è abeliano, quindi $N$ è normale. Il quoziente $G/N$ ha ordine minore di $G$, ed è quindi prodotto di gruppi ciclici per ipotesi induttiva. Abbiamo:

$$\overline{G} = G/N \simeq \overline{H}_1 \times \ldots \times \overline{H}_k,$$

con $|\overline{H}_k| > 1$ e tali che $|\overline{H}_i|$ divide $|\overline{H}_j|$ se $i > j$.

Sia $\overline{y}_i$ un generatore ciclico di $\overline{H}_i$ in $G/N$. Voglio mostrare che esiste un elemento $x_i \in G$ con la proprietà che $\overline{y}_i = [x_i] \in G/N$ e l'ordine di $x_i$ coincide con l'ordine di $\overline{y}_i$.

Scegliamo $y_i \in G$ tale che $[y_i] := y_i N = \overline{y}_i$. Allora $y_i^{n_i}$ giace in $N$, dal momento che $\overline{y}_i^{n_i} = [e]$ in $G/N$. Poiché $N$ è generato ciclicamente da $x$, questo significa che $y_i^{n_i} = x^{m_i}$ per qualche $m_i$. L'ordine di $y_i$ è allora pari al prodotto di $n_i$ per l'ordine di $x^{m_i}$ in $N$, che abbiamo visto essere $n/(m_i, n)$. In conclusione, l'ordine di $y_i$ è quindi $nn_i/(m_i, n)$.

Ora, l'ordine di ciascun elemento di $G$ divide l'ordine di $x$, cioè $n$, quindi $nn_i/(m_i, n)$ si scrive come $n/d_i$, con $d_i$ intero. Da questo segue che $(m_i, n) = d_i n_i$. Ma $m_i = (m_i, n)h_i$ per qualche intero $h_i$, quindi $m_i = d_i h_i n_i$. Ricapitolando, $y_i^{n_i} = x^{d_i h_i n_i}$, cioè $(y_i x^{-d_i h_i})^{n_i} = e$, e l'ordine di $x_i := y_i x^{-d_i h_i}$ divide $n_i$. Ad ogni modo, $[x_i] = [y_i][x]^{-d_i h_i} = [y_i] = \overline{y}_i$, e quindi l'ordine di $x_i$ è anche multiplo di $n_i$. In conclusione, $\overline{y}_i = [x_i]$ e l'ordine di $x_i$ coincide con l'ordine di $\overline{y}_i$, come desiderato.

Il nostro obiettivo è adesso quello di mostrare che $G$ è prodotto diretto dei sottogruppi $N, H_1, \ldots, H_k$, dove $H_i = (x_i)$, e che tali sottogruppi soddisfano le condizioni dell'enunciato. In effetti, $G/N$ è prodotto diretto dei sottogruppi $\overline{H}_i = (\overline{x}_i)$ e quindi ogni suo elemento si scrive nella forma $[x_1]^{a_1} \ldots [x_k]^{a_k}$; questo vuol dire che ogni $g \in G$ coincide con qualche $x_1^{a_1} \ldots x_k^{a_k}$ modulo $N$, e quindi $g = x^a x_1^{a_1} \ldots x_k^{a_k}$ per una scelta opportuna di $a, a_1, \ldots, a_k \in \mathbb{Z}$. Pertanto $G = NH_1 \ldots H_k$.

Per mostrare che il prodotto è diretto, dobbiamo far vedere che se $x^a x_1^{a_1} \ldots x_k^{a_k} = e$, allora $x^a = x_1^{a_1} = \cdots = x_k^{a_k} = e$. Tuttavia, se $x^a x_1^{a_1} \ldots x_k^{a_k} = e$, allora $[x_1]^{a_1} \ldots [x_k]^{a_k} = [e]$, e dal momento che $G/N$ è prodotto diretto di $\overline{H}_1, \ldots, \overline{H}_k$, si ha $[x_1]^{a_1} = \ldots = [x_k]^{a_k} = [e]$. Poiché l'ordine di $x_i$ coincide con l'ordine di $[x_i]$, si ha $x_1^{a_1} = \ldots = x_k^{a_k} = e$, e di conseguenza anche $x^a = e$.

L'ultimo dettaglio da osservare è che ogni $n_i$ deve dividere $n$, in quanto $n$ è il massimo ordine di un elemento in $G$. □

**Corollario 5.19.** *Sia $G$ un gruppo abeliano finito. Allora esistono numeri naturali $n_1 \geq n_2 \geq \ldots \geq n_k > 1$, con la proprietà che $n_i$ divide $n_j$ se $i > j$, tali che $G$ sia isomorfo al prodotto diretto di gruppi ciclici $\mathrm{C}_{n_1} \times \mathrm{C}_{n_2} \times \ldots \times \mathrm{C}_{n_k}$.*

*Dimostrazione.* L'enunciato segue immediatamente dalle Proposizioni 5.7 e 5.18. □

Per dimostrare il Teorema 5.12, rimane da far vedere che $G$ individua univocamente gli ordini $n_1, \ldots, n_k$. Lo facciamo in una serie di passi.

**Lemma 5.20.** *Il numero di soluzioni nel gruppo $\mathrm{C}_{n_1} \times \mathrm{C}_{n_2} \times \ldots \times \mathrm{C}_{n_h}$ dell'equazione $x^d = e$ è pari a $(n_1, d)(n_2, d) \ldots (n_h, d)$.*

*Dimostrazione.* L'elemento $(a_1, \ldots, a_h)$ è soluzione di $x^d = e$ se e solo se $a_i^d = e$ per ogni $i = 1, \ldots, h$. E' sufficiente quindi calcolare le soluzioni di $x^d = e$ in $\mathrm{C}_{n_i}$, che sono esattamente $(n_i, d)$. □

**Proposizione 5.21.** *Siano $\{n_i\}_{i=1,\ldots,h}$ e $\{m_j\}_{j=1,\ldots,k}$, $n_h > 1, m_k > 1$, numeri naturali con la proprietà che se $i > j$, $n_i$ divide $n_j$ e $m_i$ divide $m_j$.*

*Se i gruppi*

$$\mathrm{C}_{n_1} \times \ldots \times \mathrm{C}_{n_h} \qquad \text{e} \qquad \mathrm{C}_{m_1} \times \ldots \times \mathrm{C}_{m_k}$$

*sono isomorfi, allora $h = k$ e $n_i = m_i$ per ogni $i = 1, \ldots, h$.*

*Dimostrazione.* Per induzione sull'ordine dei gruppi. Supponiamo che $h > k$. Se $d = n_h$, il numero delle soluzioni di $x^d = e$ nel primo gruppo è $d^h$, mentre nel secondo è $(m_1, d)(m_2, d) \ldots (m_k, d) \leq d^k < d^h$, il che è un assurdo, perché in gruppi isomorfi devo avere lo stesso numero di soluzioni. Se $h < k$ posso ripetere il ragionamento a ruoli scambiati, pertanto l'unica possibilità è che sia $h = k$. Inoltre $n_h$ è il massimo naturale $d$ per cui il numero delle soluzioni sia esattamente $d^h$. Anche questo numero dipende solo dalla classe di isomorfismo del gruppo, quindi $n_h = m_h$.

Il sottogruppo delle soluzioni dell'equazione $x^{n_h} = e$ è isomorfo a $\mathrm{C}_{n_h} \times \mathrm{C}_{n_h} \times \ldots \times \mathrm{C}_{n_h}$ in entrambi i casi. Se $\mathrm{C}_{n_h}$ compare $r$ volte nella prima fattorizzazione $\mathrm{C}_{n_1} \times \ldots \times \mathrm{C}_{n_h}$, ed $s$ volte nella seconda $\mathrm{C}_{m_1} \times \ldots \times \mathrm{C}_{m_k}$, quozientando i due gruppi per tale sottogruppo si ottiene rispettivamente:

$$\mathrm{C}_{n_1/n_h} \times \ldots \times \mathrm{C}_{n_{h-r-1}/n_h} \qquad \mathrm{C}_{m_1/n_h} \times \ldots \times \mathrm{C}_{m_{h-s-1}/n_h},$$

che devono essere isomorfi in quanto quozienti di gruppi isomorfi per sottogruppi che si corrispondono nell'isomorfismo.

Ma per ipotesi induttiva, $h-r-1 = h-s-1$, quindi $r = s$, da cui $n_i = m_i$ per $i \geq h-r$. Inoltre $n_i/n_h = m_i/n_h$, per $i = 1, ..., h-r-1$ da cui $n_i = m_i$ per ogni $i$. L'enunciato è dimostrato. □

Il Teorema 5.12 è quindi dimostrato.

## 6. Struttura di alcuni gruppi finiti

### 6.1. **Gruppi di ordine** $8$**.**

**Lemma 6.1.** *Se $G$ è un gruppo abeliano di ordine $8$, allora è isomorfo a uno tra $\mathrm{C}_8$, $\mathrm{C}_4 \times \mathrm{C}_2$, $\mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$.*

*Dimostrazione.* Segue dal teorema di classificazione dei gruppi abeliani finitamente generati. □

Sia allora $G$ non abeliano, $|G| = 8$. $G$ non può avere elementi di ordine $8$, in quanto sarebbe ciclico e quindi abeliano. Inoltre deve possedere elementi di ordine $4$, poiché se ogni elemento $a \in G$ soddisfa $a^2 = e$, allora $G$ è nuovamente abeliano.

**Proposizione 6.2.** *Sia $G$ un gruppo non abeliano di ordine $8$, $x \in G$ un elemento di ordine $4$. Se $G$ possiede un elemento di ordine $2$ non contenuto in $(x)$, allora $G$ è isomorfo a $\mathrm{D}_4$.*

*Dimostrazione.* Ogni elemento $x \in G$ di ordine $4$ genera un sottogruppo $N$ di indice $2$, e quindi normale. Se esiste $a \notin (x)$ di ordine $2$ in $G$, allora $G$ è prodotto semidiretto di $H = (a) < G$ con $N = (x) \lhd G$. Se tale prodotto semidiretto fosse diretto, $G$ sarebbe necessariamente abeliano.

L'unico automorfismo non banale di $(x) \simeq \mathrm{C}_4$ manda $x$ nel suo inverso; di conseguenza, l'unico omomorfismo non banale $\phi : H \to \mathrm{Aut}(N)$ manda $a$ in tale automorfismo. Vi è pertanto un unico prodotto semidiretto (non diretto) a meno di isomorfimo, che deve essere isomorfo al gruppo diedrale $\mathrm{D}_4$. □

**Proposizione 6.3.** *Sia $G$ un gruppo non abeliano di ordine $8$, $x \in G$ un elemento di ordine $4$. Se $x^2$ è l'unico elemento di ordine $2$ in $G$, allora $G$ è isomorfo a $\mathrm{Q}_4$.*

*Dimostrazione.* Per ipotesi, ogni elemento di $G \setminus (x)$ ha ordine $4$. Infatti, $c = x^2$ è l'unico elemento di ordine $2$, e genera il centro $Z(G)$: $G$ è un $2$-gruppo finito, e quindi ha centro non banale, di ordine diverso da $2$; l'unica possibilità è che $|Z(G)| = 2$.

Sia $y \in G \setminus (x)$ un elemento di ordine $4$. Allora $(x, y) = G$. Il sottogruppo $(y)$ ha indice $2$ ed è quindi normale; l'elemento $xyx^{-1}$ è allora un generatore di $(y)$, che è diverso da $y$ altrimenti $x$ e $y$ commuterebbero, e $G = (x, y)$ sarebbe abeliano. Necessariamente, $xyx^{-1} = y^{-1}$ e quindi $xy = y^{-1}x$.

Questo determina tutta la struttura del gruppo: $(xy)^2 = xyy^{-1}x = x^2 = y^2 = c$. Quindi $z = xy$ ha lo stesso quadrato di $x$ e $y$ ed ha anch'esso ordine $4$. Inoltre $yz = y(xy) = yy^{-1}x = x$ e $zx = xyx = y^{-1}x^2 = y^{-1}c = y$; allo stesso modo $yx = cy^{-1}x = cxy = cz$, e quindi $zy = (xy)y = cx$, e $xz = x(xy) = cy$. In conclusione, $x \mapsto i, y \mapsto j, z \mapsto k, c \mapsto -1$ individuano un isomorfismo di $G$ con $\mathrm{Q}_4$. □

Possiamo riassumere quanto mostrato nel seguente

**Teorema 6.4.** *Ogni gruppo di ordine $8$ è isomorfo ad esattamente uno tra i gruppi $\mathrm{C}_8$, $\mathrm{C}_4 \times \mathrm{C}_2$, $\mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$, $\mathrm{D}_4$, $\mathrm{Q}_4$.*

### 6.2. **Gruppi di ordine** $12$**.** Sia $G$ un gruppo di ordine $12$.

**Lemma 6.5.** *$G$ possiede almeno un Sylow normale.*

*Dimostrazione.* Per il Teorema di Sylow, il numero dei $3$-Sylow è $1$ o $4$. Se il $3$-Sylow è unico, allora è normale in $G$; se invece $G$ possiede $4$ $3$-Sylow, allora contiene $8$ elementi di ordine $3$, e soltanto quattro elementi di ordine diverso da $3$: questi devono allora costituire l'unico $2$-Sylow. □

Se almeno uno dei sottogruppi di Sylow di $G$ è normale, $G$ è prodotto semidiretto del 2-Sylow e del 3-Sylow. I prodotti diretti sono tutti abeliani, e producono $\mathrm{C}_{12}$ e $\mathrm{C}_6 \times \mathrm{C}_2$. I gruppi non abeliani sono invece prodotti semidiretti non banali: elenchiamoli caso per caso.

**Proposizione 6.6.** *Un gruppo non abeliano di ordine* 12 *che abbia il* 2*-Sylow normale è isomorfo a* $\mathrm{A}_4$*.*

*Dimostrazione.* Sia $G$ un gruppo con le proprietà richieste, $P$ il suo 2-Sylow, e indichiamo con $Q$ uno dei 3-Sylow. Per quanto detto prima, $G$ è isomorfo a $P \rtimes_\phi Q$ per qualche omomorfismo $\phi : Q \to \mathrm{Aut}(P)$.

Innanzitutto, $P$ non può essere ciclico. In effetti, se $P \simeq \mathrm{C}_4$, allora $\mathrm{Aut}(P)$ contiene solo due elementi — l'identità e l'automorfismo che manda ogni elemento nel suo inverso. Ma allora l'unico omomorfismo $Q \to \mathrm{Aut}(P)$ è banale, e quindi l'unico prodotto semidiretto $P \rtimes Q$ è diretto, e quindi abeliano.

Allora, $P = \{e, a, b, c\}$ è isomorfo a $V_4 = \mathrm{C}_2 \times \mathrm{C}_2$. Gli automorfismi di $P$ permutano $a, b, c$ tra loro, ed ogni permutazione dà origine ad un automorfismo. Gli elementi di ordine 3 in $P$ permutano quindi ciclicamente gli elementi $a, b, c$.

Se $\phi : Q \to \mathrm{Aut}(P)$ è non banale, possiamo sempre scegliere $q \in Q$ in modo che $\phi(q)$ sia la permutazione ciclica $(a\,b\,c)$. Il prodotto semidiretto è allora univocamente determinato. □

**Proposizione 6.7.** *Sia* $G$ *un gruppo non abeliano di ordine* 12*, non isomorfo a* $\mathrm{C}_2 \times \mathrm{D}_3$*, e che abbia il* 3*-Sylow normale. Allora* $G$ *è unico a meno di isomorfismo.*

*Dimostrazione.* Sia $Q = (q)$ il 3-Sylow normale di $G$, e indichiamo con $P$ uno dei 2-Sylow di $G$. Allora $G$ è isomorfo a $Q \rtimes_\phi P$ per qualche omomorfismo $\phi : P \to \mathrm{Aut}(Q)$. L'omomorfismo $\phi$ deve essere non banale, altrimenti il prodotto è diretto e $G$ è abeliano.

Poiché $Q \simeq \mathrm{C}_3$, i suoi unici automorfismi sono l'identità e quello che manda ogni elemento nel suo inverso. $\mathrm{Aut}\, Q$ ha quindi ordine 2, ed è facile individuare tutti gli omomorfismi $\phi : P \to \mathrm{Aut}(Q)$.

- Se $P \simeq V_4 \simeq \mathrm{C}_2 \times \mathrm{C}_2$, allora dobbiamo costruire $\phi : V_4 \to \mathrm{Aut}(\mathrm{C}_3) \simeq \mathrm{C}_2$. Poiché $\phi$ è non banale, la sua immagine contiene due elementi, e quindi il suo nucleo è un sottogruppo di ordine 2 di $V_4$. A meno di rinominare gli elementi di $V_4$ possiamo supporre che $\ker \phi = (a)$, e che $\phi(b) = \phi(c)$ sia l'automorfismo non banale di $\mathrm{C}_3$. In questo caso, vi è quindi un unico prodotto semidiretto non banale. Si vede facilmente che $G$ è allora isomorfo a $\mathrm{C}_2 \times \mathrm{D}_3 = \mathrm{C}_2 \times \mathrm{S}_3$.
- Se $P$ è ciclico, dobbiamo costruire $\phi : \mathrm{C}_4 \to \mathrm{Aut}(\mathrm{C}_4) \simeq \mathrm{C}_2$. L'omomorfismo $\phi$ è determinato dall'immagine del generatore $x$ di $\mathrm{C}_4$: se $\phi(x) = 1$ si ottiene l'omomorfismo banale, che porta all'abelianità di $G$; l'unica altra possibilità è che $\phi(x)$ sia l'automorfismo non banale di $\mathrm{C}_3$, che scambia tra loro $q$ e $q^{-1}$. Questo caso conduce quindi a gruppi tra loro isomorfi.

□

In conclusione,

**Teorema 6.8.** *Ogni gruppo di ordine* 12 *è isomorfo ad uno tra i gruppi* $\mathrm{C}_{12}$*,* $\mathrm{C}_6 \times \mathrm{C}_2$*,* $\mathrm{S}_3 \times \mathrm{C}_2 = \mathrm{D}_3 \times \mathrm{C}_2 \simeq \mathrm{D}_6$ *oppure al gruppo di presentazione*

$$\langle x, q \mid x^4 = q^3 = e, xqx^{-1} = q^{-1} \rangle.$$

6.3. **Gruppi di ordine** $pq$**, con** $p < q$ **primi.** Siano $p < q$ numeri primi. Un gruppo $G$ di ordine $pq$ può sicuramente essere abeliano, ed è in tal caso ciclico. A volte, tuttavia, esistono anche gruppi non abeliani di ordine $pq$.

**Teorema 6.9.** *Siano* $p < q$ *numeri primi, e supponiamo che* $p | q - 1$*. Allora esiste un gruppo non abeliano di ordine* $pq$*, unico a meno di isomorfismo.*

*Se invece* $p$ *non divide* $q - 1$*, allora i gruppi di ordine* $pq$ *sono tutti abeliani.*

*Dimostrazione.* Il $q$-Sylow $Q$ è necessariamente unico, perché il numero dei $q$-Sylow è $\equiv 1 \mod q$ e divide $p < q$, e non può che essere 1. Se indichiamo con $P$ uno dei $p$-Sylow

di $G$, allora $G$ è isomorfo ad un prodotto semidiretto $Q \rtimes_\phi P$ per qualche omomorfismo $\phi : P \to \mathrm{Aut}(Q)$.

Poiché $Q \simeq \mathrm{C}_q \simeq \mathbb{Z}/(q)$, il gruppo $\mathrm{Aut}(Q)$ è isomorfo a $\mathrm{Aut}(\mathrm{C}_q) \simeq \mathbb{Z}/(q)^\times$ che è ciclico di ordine $q-1$, in quanto gruppo moltiplicativo del campo $\mathbb{F}_q$. Si tratta quindi di descrivere tutti gli omomorfismi $\mathrm{C}_p \to \mathrm{C}_{q-1}$.

Se $p$ non divide $q-1$, allora l'unico omomorfismo $\mathrm{C}_p \to \mathrm{C}_{q-1}$ è quello banale, in quanto $\mathrm{C}_{q-1}$ non contiene elementi di ordine $p$ tra i quali scegliere l'immagine del generatore di $\mathrm{C}_p$. In questo caso, $|G| = pq$ impone l'abelianità di $G$.

Se $p$ invece divide $q-1$, allora esistono anche omomorfismi non banali. In effetti, gli elementi di ordine $p$, assieme all'identità, costituiscono un sottogruppo ciclico di $\mathrm{Aut}(Q)$. Se $\phi : P \to \mathrm{Aut}(Q)$ è un omomorfismo non banale, comunque scegliamo un automorfismo $T$ di $Q$ di ordine $p$, la sua controimmagine tramite $\phi$ sarà un generatore ciclico di $P$. In conclusione, possiamo scegliere $x \in P$ tale che $P = (x)$ e $\phi(x) = T$. Questo mostra l'unicità di $G$, nel caso non abeliano, a meno di isomorfismo. □

6.4. **Risolubilità dei gruppi di ordine $< 60$.** Vogliamo far vedere che tutti i gruppi con meno di $60$ elementi sono risolubili. Per fare questo, è sufficiente mostrare che tali gruppi sono abeliani o possiedono un sottogruppo normale non banale

**Lemma 6.10.** *Sia $|G|$ dispari, minore di $60$, e non primo. Allora $G$ possiede un sottogruppo normale non banale.*

*Dimostrazione.* Abbiamo già visto che se $|G| = pq$, con $p < q$ primi, allora il $q$-Sylow è normale. Inoltre se $|G| = p^n$, con $p$ primo, $n > 1$, allora $G$ è un $p$-gruppo finito e possiede sottogruppi normali di ordine $p^h$ per qualsiasi $0 \leq h \leq n$. L'unico numero dispari minore di $60$ che non sia primo, né di queste forme, è $45 = 3^2 \cdot 5$. Ad ogni modo, se $|G| = 45$, allora il numero dei $5$-Sylow di $G$ divide $9$ ed è $\equiv 1 \mod 5$. Pertanto $G$ ha un solo $5$-Sylow, che è normale. □

*Osservazione* 6.11. Per quanto riguarda $45 = 3^2 \cdot 5$, avremmo potuto utilizzare un celebre teorema di Burnside che dimostra, utilizzando la teoria della rappresentazione dei gruppi finiti, che un gruppo il cui ordine abbia solo due fattori primi è sempre risolubile.

Il Lemma è comunque vero in maniera molto più forte: un gruppo finito di ordine dispari, non primo, possiede sempre un sottogruppo normale non banale! Questo fatto è un difficile e complicato teorema di Feit e Thompson, la cui dimostrazione eviteremo accuratamente.

**Lemma 6.12.** *Se $2 \neq |G| < 60$ è il doppio di un numero dispari, o quattro volte un numero primo, allora $G$ contiene un sottogruppo normale non banale.*

*Dimostrazione.* Abbiamo già visto, per mezzo dell'immersione di Cayley, come un gruppo di ordine $2d$, con $d$ dispari, abbia un sottogruppo di indice $2$, necessariamente normale.

Se $|G| = 4p$, con $p$ primo maggiore di $3$, allora il numero dei $p$-Sylow di $G$ divide $4$ ed è $\equiv 1 \mod p$. Poiché $p > 4$, $G$ ha un solo $p$-Sylow, necessariamente normale. Quando $|G| = 12$, possiamo invece fare ricorso alla classificazione che abbiamo fornito precedentemente. □

**Lemma 6.13.** *Se $|G| = 40, 56$, allora $G$ possiede un sottogruppo normale non banale.*

*Dimostrazione.* Se $|G| = 40$, il numero dei $5$-Sylow divide $8$ ed è $\equiv 1 \mod 5$. Pertanto $G$ possiede un unico $5$-Sylow, che è normale.

Se $|G| = 56$, il numero dei $7$-Sylow di $G$ divide $8$ ed è $\equiv 1 \mod 7$. Se $G$ possiede un unico $7$-Sylow, abbiamo finito. Se invece ne possiede $8$, allora contiene $48$ elementi di ordine $7$; gli $8$ elementi rimanenti devono formare l'unico $2$-Sylow, che è quindi normale. □

**Lemma 6.14.** *Se $|G| = 24, 36, 48$, allora $G$ possiede un sottogruppo normale non banale.*

*Dimostrazione.* Se $|G| = 36$, si vede facilmente che il numero dei 3-Sylow è $1$ oppure $4$. Se $G$ possiede un unico 3-Sylow, questo è allora normale. Se invece $G$ ne possiede $4$, allora la sua azione per coniugio sui $4$ 3-Sylow induce un omomorfismo $\rho : G \to \mathrm{S}_4$, che non può essere iniettivo per questioni di cardinalità. $\ker \rho$ è allora un sottogruppo normale $G$, ed è non banale poiché l'azione di coniugio di $G$ sui 3-Sylow è transitiva.

Se $|G| = 24, 48$, allora il numero dei 2-Sylow è $1$ oppure $3$. Se $G$ possiede un unico 2-Sylow, allora è normale. Altrimenti, $G$ ne possiede $3$, e la sua azione per coniugio sui $3$ 2-Sylow induce un omomorfismo $\phi : G \to \mathrm{S}_3$. Ora si procede come prima. □

**Proposizione 6.15.** *I gruppi con meno di* $60$ *elementi sono tutti risolubili.*

*Dimostrazione.* Se un gruppo $G$ possiede un sottogruppo normale risolubile $N$ tale che $G/N$ è risolubile, allora $G$ è necessariamente risolubile. Inoltre, ogni gruppo abeliano è risolubile.

Se $|G| < 60$ non è primo, abbiamo già dimostrato che $G$ possiede un sottogruppo normale non banale. Se invece $|G|$ è primo, allora $G$ è ciclico, e quindi abeliano. Possiamo allora procedere con una facile induzione: se $|G|$ è primo, allora $G$ è abeliano, e quindi risolubile. Se $|G|$ non è primo, allora esiste $N \lhd G$ tale che $N$ e $G/N$ hanno ordine inferiore a quello di $G$, e sono quindi risolubili per ipotesi induttiva. □

6.5. **Semplicità di** $\mathrm{A}_n, n \geq 5$**.** Dimostrerò ora, con qualche variazione rispetto alla lezione, la semplicità del gruppo alterno $\mathrm{A}_n$ quando $n \geq 5$. Un gruppo $G$ è semplice quando non ammette sottogruppi normali non banali. Questo vuol dire che l'immagine di ogni omomorfismo $G \to \bar{G}$ è isomorfa a $G$, oppure è composta dalla sola identità. Il nome di *semplice* allude esattamente a questo: possiamo vedere l'immagine di un gruppo $G$ attraverso un omomorfismo come una versione "semplificata" di $G$, in cui dimentichiamo alcune informazioni sulla struttura del gruppo $G$, mantenendone altre. Ad esempio, l'omomorfismo $\mathbb{Z} \to \mathrm{C}_2$ che manda i soli numeri pari nell'identità trattiene solo l'informazione sulla parità del numero, e sulla parità della somma tra due numeri, mentre dimentica tutto il resto. Per un gruppo semplice questo non è possibile: o trascuriamo tutte le informazioni, o le tratteniamo tutte.

Per quanto riguarda i gruppi abeliani, gli unici gruppi semplici sono quelli ciclici di ordine primo, come abbiamo già visto. La classificazione dei gruppi semplici non abeliani è invece di una difficoltà colossale. Mi limiterò qui solamente a mostrare una delle famiglie infinite di gruppi semplici finiti non abeliani: quella dei gruppi alterni.

6.5.1. *Prima dimostrazione.*

**Lemma 6.16.** *Sia* $(e) \neq H \lhd \mathrm{A}_n$*. Allora* $H$ *contiene almeno un* $3$*-ciclo o un prodotto di due trasposizioni disgiunte.*

*Dimostrazione.* Il sottogruppo normale $H$ contiene almeno un elemento $\sigma$ diverso dall'identità. Esprimiamo la permutazione $\sigma$ come prodotto di cicli disgiunti:

$$\sigma = (a_1\, a_2\, \ldots\, a_m)(a_{m+1}\, a_{m+2}\, \ldots\, a_n)(a_{n+1} \ldots) \ldots$$

La permutazione $\tau = (a_1 a_2 a_3)^{-1} \sigma (a_1 a_2 a_3)$ è coniugata a $\sigma$ ed appartiene quindi anch'essa ad $H$. Il prodotto $\sigma\tau^{-1}$ si calcola facilmente ed è uguale ad $(a_1 a_m a_3)$ se $m > 2$ o ad $(a_1 a_3)(a_2 a_n)$ se $m = 2$. □

**Lemma 6.17.** *Sia* $(e) \neq H \lhd \mathrm{A}_n, n \geq 5$*. Allora* $H$ *contiene almeno un* $3$*-ciclo.*

*Dimostrazione.* Basta mostrare che se $H$ contiene un prodotto di due trasposizioni disgiunte, allora contiene anche un 3-ciclo. Ora, se $H$ contiene l'elemento $\phi = (a_1\, a_2)(a_3\, a_4)$, scegliamo un elemento $a_5$ distinto da ciascuno degli elementi $a_1, a_2, a_3, a_4$. Allora $H$ dovrà contenere anche il coniugato

$$\psi = (a_3\, a_4\, a_5)^{-1} \cdot (a_1\, a_2)(a_3\, a_4) \cdot (a_3\, a_4\, a_5) = (a_1\, a_2)(a_4\, a_5).$$

Ma allora $\phi\psi = (a_3\, a_5\, a_4)$ è anch'esso un elemento di $H$. □

**Lemma 6.18.** *Sia* $n \geq 5$*. Se* $H \lhd \mathrm{A}_n$ *contiene un* $3$*-ciclo, allora li contiene tutti.*

*Dimostrazione.* Facciamo vedere che se $(a_1\,a_2\,a_3) \in H$ allora anche $(a_1\,a_2\,b) \in H$ per ogni possibile scelta di $b$. In effetti, scegliamo $c$ distinto da ciascuno degli elementi $a_1, a_2, a_3, b$. Allora, coniugando si ottiene: $(a_3\,b\,c)^{-1}(a_1\,a_2\,a_3)(a_3\,b\,c) = (a_1\,a_2\,b)$, che deve essere un elemento di $H$. Questo mostra che cambiando uno degli elementi permutati da un 3-ciclo in $H$ otteniamo ancora un 3-ciclo contenuto in $H$. Ma allora:

$$(a_1\,a_2\,a_3) \in H \Rightarrow (a_1\,a_2\,b_3) \in H \Rightarrow (a_1\,b_2\,b_3) \in H \Rightarrow (b_1\,b_2\,b_3) \in H,$$

per qualsiasi scelta di $b_1, b_2, b_3$. □

**Lemma 6.19.** *Se un sottogruppo $H < \mathrm{A}_n$ contiene tutti i 3-cicli, allora $H = \mathrm{A}_n$.*

*Dimostrazione.* Sia $(a_1\,a_2 \ldots a_m)$ un ciclo contenuto in $\mathrm{A}_n$. Allora $m$ è dispari, e possiamo scrivere

$$(a_1\,a_2 \ldots a_m) = (a_1\,a_2\,a_3)(a_1\,a_4\,a_5)\ldots(a_1\,a_{m-1}\,a_m).$$

Allo stesso modo, se $h, k$ sono numeri pari, allora il prodotto

$$(a_1\,a_2 \ldots a_h)(b_1\,b_2 \ldots b_k)$$

è un elemento di $\mathrm{A}_n$, che possiamo ottenere come

$$(a_1\,a_2\,a_3)\ldots(a_1\,a_{h-2}\,a_{h-1})(a_1\,b_1\,a_h)(a_h\,b_2\,b_1)(b_1\,b_3\,b_4)\ldots(b_1\,b_{k-1}\,b_k).$$[11]

Quindi tutti i cicli di lunghezza dispari, e tutti i prodotti di due cicli disgiunti di lunghezza pari giacciono in $H$, in quanto prodotto di 3-cicli. Poiché ogni elemento $g \neq e$ di $\mathrm{A}_n$ si scrive come prodotto di cicli di lunghezza dispari e di un numero pari di cicli di lunghezza pari, abbiamo mostrato che $\mathrm{A}_n \subset H$, e quindi che $H = \mathrm{A}_n$. □

Ricapitolando:

**Teorema 6.20.** *Sia $n \geq 5$. Il gruppo $\mathrm{A}_n$ è semplice.*

*Dimostrazione.* Sia $(e) \neq H \lhd \mathrm{A}_n$. Abbiamo visto che $H$ contiene almeno un 3-ciclo, quindi contiene tutti i 3-cicli, quindi contiene tutto $\mathrm{A}_n$. □

I casi in cui $n < 5$ sono facili da analizzare. Se $n = 1, 2$ il gruppo $\mathrm{A}_n$ contiene un solo elemento. $\mathrm{A}_3$ ha ordine 3 ed è quindi ciclico di ordine 3. $\mathrm{A}_4$ possiede 12 elementi, che sono 3-cicli o prodotto di due trasposizioni disgiunte, oltre all'identità. Il suo unico sottogruppo normale non banale è $\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

6.5.2. *Seconda dimostrazione con il principio di inclusione-esclusione.*

6.6. **Gruppi semplici di ordine 60.** Abbiamo visto come $\mathrm{A}_5$ sia un gruppo semplice di ordine 60. In effetti, ogni gruppo con tali proprietà è necessariamente isomorfo ad $\mathrm{A}_5$. Sia $G$ un gruppo semplice di ordine 60.

**Lemma 6.21.** *$G$ possiede esattamente 6 5-Sylow.*

*Dimostrazione.* Il numero dei 5-Sylow divide 12 ed è $\equiv 1 \mod 5$. Tuttavia, non può essere 1, in quanto l'unicità del 5-Sylow garantisce la sua normalità e contraddice la semplicità di $G$. L'unica altra possibilità è che i 5-Sylow siano 6. □

**Proposizione 6.22.** *$G$ è isomorfo ad un sottogruppo di $\mathrm{A}_6$.*

*Dimostrazione.* Sappiamo dal Teorema di Sylow che i 5-Sylow di $G$ sono tutti coniugati tra loro. L'azione di $G$ per coniugio su questi sei sottogruppi produce[12] un omomorfismo $\rho : G \to \mathrm{S}_6$ il cui nucleo è un sottogruppo normale di $G$ contenuto nel normalizzatore di ciascuno dei 5-Sylow. A causa della semplicità di $G$, $\rho$ deve essere iniettivo, e realizza $G$ come sottogruppo di $\mathrm{S}_6$. E' importante osservare che se $\rho(G)$ non fosse interamente contenuto in $\mathrm{A}_6$, allora la sua intersezione con $\mathrm{A}_6$ sarebbe un sottogruppo di indice 2, quindi normale. Poiché $G$ non possiede sottogruppi normali non banali, $\rho$ immerge $G$ dentro $\mathrm{A}_6$. □

[11] Questa espressione va intesa in modo che $(a_1\,a_2)(b_1\,b_2 \ldots b_k) = (a_1\,b_1\,a_2)(a_2\,b_2\,b_1)\ldots(b_1\,b_{k-1}\,b_k)$ e che $(a_1\,a_2)(b_1\,b_2) = (a_1\,b_1\,a_2)(a_2\,b_2\,b_1)$.

[12] dopo aver numerato i 5-Sylow.

**Teorema 6.23.** *$G$ è isomorfo ad $\mathrm{A}_5$.*

*Dimostrazione.* Abbiamo già identificato $G$ con un sottogruppo di $\mathrm{A}_6$, di indice $|\mathrm{A}_6|/|G| = 360/60 = 6$. Il gruppo $\mathrm{A}_6$ agisce allora per moltiplicazione sinistra sull'insieme $X = \mathrm{A}_6/G$ dei sei laterali di $G$. Tale azione induce un omomorfismo $\phi : \mathrm{A}_6 \to \mathrm{S}_X$ il cui nucleo è un sottogruppo normale di $\mathrm{A}_6$ contenuto in $G$, ed è quindi banale per semplicità di $\mathrm{A}_6$. L'omomorfismo $\phi$ è allora iniettivo, e l'immagine di $\phi$ è un sottogruppo di indice $2$ in $\mathrm{S}_X$, che coincide quindi con $\mathrm{A}_X$.

Ora, se $g \in G \subset \mathrm{A}_6$, allora $gG = G$, e quindi la permutazione $\phi(g) \in \mathrm{S}_X$ fissa il laterale $G$; $\phi$ identifica allora $G$ con elementi di $\mathrm{A}_X$ che fissano un dato elemento di $X$. Poiché $X$ possiede $6$ elementi, $\phi$ identifica $G$ con un sottogruppo di $\mathrm{A}_{X\setminus\{G\}} \simeq \mathrm{A}_5$. Ma $G$ possiede $60$ elementi, pertanto $G \simeq \mathrm{A}_5$. □

6.7. **Semplicità di $\mathrm{GL}(3,\mathbb{F}_2)$.** Il gruppo $\mathrm{GL}(3,\mathbb{F}_2)$ possiede esattamente $168$ elementi, e poche classi di coniugio, tutte di cardinalità relativamente grande. Se ne può quindi dimostrare la semplicità facendo vedere che gli unici sottoinsiemi che sono unione di classi di coniugio, contengono l'identità e hanno ordine che divide $|G|$ sono $(\mathrm{id})$ e $G$, in analogia con quanto abbiamo già visto per $\mathrm{A}_5$ nel Paragrafo 6.5.2.

Il modo più facile per calcolare la cardinalità delle classi di coniugio è utilizzare la forma canonica razionale (primaria), studiata alla fine del corso di Algebra 1. Vi ricordo che ogni endomorfismo $T$ di uno spazio vettoriale di dimensione finita sul campo $\mathbf{k}$, può essere messo in forma diagonale a blocchi, in modo che ogni blocco è a sua volta un *blocco di Jordan generalizzato* rispetto ad un polinomio irriducibile a coefficienti in $\mathbf{k}$. Nel caso in cui $\mathbf{k}$ sia algebricamente chiuso, si riottiene la forma canonica di Jordan.

Nel caso in questione, abbiamo a che fare con matrici $3 \times 3$ a coefficienti di $\mathbf{k} = \mathbb{F}_2$, che si guarda bene dall'essere algebricamente chiuso. I polinomi irriducibili in $\mathbb{F}_2[x]$ di grado al più $3$ sono:

- $x, x+1$ di grado $1$;
- $x^2 + x + 1$ di grado $2$;
- $x^3 + x + 1, x^3 + x^2 + 1$ di grado $3$.

Ricordiamo che gli elementi di $\mathrm{GL}(3,\mathbb{F}_2)$ sono invertibili, e quindi il loro polinomio minimo non può avere $x$ come fattore. I blocchi irriducibili della forma canonica razionale primaria sono:

- $(1)$ per il polinomio $x+1$;
- $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ per il polinomio $x^2 + x + 1$;
- $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ per il polinomio $x^3 + x + 1$;
- $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ per il polinomio $x^3 + x + 1$;

e più in generale

$$Q = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

per il polinomio irriducibile $q(x) = x^n + a_n x^{n-1} + \cdots + a_1 x + a_0$. Ricordiamo anche che la matrice associata ad un blocco di Jordan superiore, relativo ad una potenza

$q(x)^m, m > 1$ dell'irriducibile $q(x)$ è la seguente matrice a $m$ blocchi $n \times n$

$$\begin{pmatrix} Q & 0 & 0 & \dots & 0 \\ J & Q & 0 & \dots & 0 \\ 0 & J & Q & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & J & Q \end{pmatrix}$$

dove $J$ è la matrice quadrata con tutti coefficienti uguali a $0$ tranne quello nell'angolo in alto a destra, che è uguale ad $1$. Poiché le matrici coinvolte sono $3 \times 3$, non possono esserci blocchi di Jordan superiori relativi a irriducibili di grado maggiore di $1$, perché già due blocchi $2 \times 2$ richiederebbero matrici almeno $4 \times 4$. Gli unici blocchi di Jordan superiori sono quindi

- $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ per il polinomio $(x+1)^2$;
- $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ per il polinomio $(x+1)^3$,

e quindi ogni elemento di $\mathrm{GL}_3(\mathbb{F}_2)$ è coniugato ad esattamente una delle seguenti matrici:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Ci proponiamo ora di calcolare la cardinalità di ciascuna di tali sei classi di coniugio.

- La prima matrice è l'identità, e fa classe di coniugio a sé.
- La seconda matrice ha polinomio minimo $(x+1)^2 = x^2 + 1$ e ha quindi ordine $2$. Per calcolare il numero dei suoi coniugati, dobbiamo contare il numero delle matrici con cui commuta. Si ha:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ d+g & e+h & f+i \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} a & b+c & c \\ d & e+f & f \\ g & h+i & i \end{pmatrix}.$$

  Imporre la commutazione fornisce le condizioni: $c = d = f = 0, e = i$. Il centralizzatore contiene quindi le matrici della forma:

$$\begin{pmatrix} a & b & 0 \\ 0 & e & 0 \\ g & h & e \end{pmatrix}$$

  che hanno determinante $ae^2 \neq 0$, da cui $a = e = 1$. I coefficienti $b, g, h \in \mathbb{F}_2$ si possono scegliere liberamente, e quindi il centralizzatore possiede $8$ elementi. La cardinalità di questa classe di coniugio è quindi $168/8 = 21$.
- La terza matrice ha polinomio minimo $(x+1)^3$ e soddisfa $(x+1)^4 = x^4 + 1 = 0$; la sua quarta potenza è quindi uguale all'identità, mentre il suo quadrato non lo è: ha quindi ordine $4$. Calcoliamo il centralizzatore:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ a+d & b+e & c+f \\ d+g & e+h & f+i \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b+c & c \\ d+e & e+f & f \\ g+h & h+i & i \end{pmatrix},$$

e quindi la commutazione impone $b = c = f = 0$, $a = e = i, d = h$. Il centralizzatore contiene le matrici della forma

$$\begin{pmatrix} a & 0 & 0 \\ d & a & 0 \\ g & d & a \end{pmatrix}.$$

L'invertibilità impone $a = 1$, e rimangono due parametri $d, h \in \mathbb{F}_2$ liberi. L'ordine del centralizzatore è $4$, e la cardinalità della classe di coniugio è $168/4 = 42$.

- La quarta matrice ha polinomio minimo $(x+1)(x^2+x+1) = x^3+1$ e ha quindi ordine $3$. Calcoliamo il centralizzatore:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ g & h & i \\ d+g & e+h & f+i \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} a & c & b+c \\ d & f & e+f \\ g & i & h+i \end{pmatrix},$$

e quindi la commutazione impone $b = c = 0$, $d = g = 0$, $f = h$, $e + f = i$. Il centralizzatore contiene le matrici della forma

$$\begin{pmatrix} a & 0 & 0 \\ 0 & e & f \\ 0 & f & e+f \end{pmatrix}.$$

L'invertibilità impone $a = 1$ and $e(e+f) + f^2 = 1$. Per il piccolo Teorema di Fermat, si ha $a^2 = a$ per ogni $a \in \mathbb{F}_2$, quindi $e^2 + ef + f^2 = 1$ è equivalente a $(e+1)(f+1) = ef+e+f+1 = 0$. Quindi almeno uno dei fattori $e+1, f+1$ si annulla, e quindi $e, f$ non possono essere entrambi zero. L'ordine del centralizzatore è $2^2 - 1 = 3$, e la cardinalità della classe di coniugio è $168/3 = 56$.

- Le ultime due matrici hanno polinomio minimo $x^3+x+1$ e $x^3+x^2+1$ rispettivamente, e generano quindi un sottoanello di $\mathrm{End}(\mathbb{F}_2^3)$ isomorfo a $\mathbb{F}_8$: annullano quindi $x^8 - x$, ed essendo invertibili, anche $x^7 - 1$. Hanno quindi entrambe ordine $7$.

  Il calcolo del centralizzatore è simile, e lo svolgiamo soltanto in uno dei due casi.

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} g & h & i \\ a+g & b+h & c+i \\ d & e & f \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} b & c & a+b \\ e & f & d+e \\ h & i & g+h \end{pmatrix},$$

e quindi la commutazione impone $b = g, c = d = h, a + b = e, e = i, b + c = f$. Il centralizzatore contiene le matrici invertibili della forma

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

che sono al più $8$. Possiede come sottogruppo le sette potenze della matrice, e quindi il suo ordine deve essere un multiplo di $7$. Pertanto, contiene solamente tali $7$ elementi, e l'ordine della classe coniugata è $168/7 = 24$.

In conclusione, abbiamo sei classi di coniugio, di cardinalità $1, 21, 42, 56, 24, 24$. E' facile vedere che le uniche somme che contengono l'addendo $1$ e dividono $168$ sono $1$ e $168$. Pertanto, i sottogruppi normali di $G$ sono solo quelli banali.

Osserviamo che $G$ contiene $21$ elementi di ordine $2$, $42$ di ordine $4$, $56$ di ordine $3$ e $48$ di ordine $7$. Incontreremo queste informazioni anche nel prossimo paragrafo.

6.8. **Gruppi semplici di ordine** $168$**.** In questo paragrafo mostreremo che esiste un unico gruppo semplice di ordine $168$ a meno di isomorfismo. La strategia dimostrativa sarà lievemente contorta: innanzitutto mostrerò che ogni gruppo semplice $G$ di ordine $168$ è isomorfo a $\mathrm{PSL}_2(\mathbb{F}_7)$ esibendo dei generatori di $G$ la cui azione per coniugio sui 7-Sylow è isomorfa all'azione di $\mathrm{PSL}_2(\mathbb{F}_7)$ sulla retta proiettiva $\mathbb{P}^1_{\mathbb{F}_7}$. Questo mostra che SE esistono gruppi semplici di ordine $168$, allora devono essere isomorfi a $\mathrm{PSL}_2(\mathbb{F}_7)$, ma lascerebbe aperta la possibilità che questo gruppo non sia semplice e che quindi non vi siano gruppi semplici di ordine $168$. Tuttavia, abbiamo già dimostrato che $\mathrm{GL}_3(\mathbb{F}_2)$ ha ordine $168$ ed è semplice; pertanto i gruppi $\mathrm{GL}_3(\mathbb{F}_2)$ e $\mathrm{PSL}_2(\mathbb{F}_7)$ sono isomorfi ed entrambi semplici.

In tutto ciò che segue, $G$ sarà un gruppo semplice di ordine $168$.

**Lemma 6.24.** *$G$ possiede esattamente $8$ 7-Sylow, e li coniuga fedelmente.*

*Dimostrazione.* Il numero dei 7-Sylow è $\equiv 1 \mod 7$ e divide $168/7 = 24$. Gli unici numeri che soddisfano tali condizioni sono $1$ e $8$, ma $G$ è semplice e non può possedere un unico 7-Sylow, che sarebbe in tal caso normale.

L'azione per coniugio di $G$ sull'insieme $X$ dei 7-Sylow è transitiva, e quindi il corrispondente omomorfismo $\rho : G \to \mathrm{S}_X$ non può mandare ogni elemento nell'identità. Ma allora, per semplicità di $G$, $\rho$ deve essere iniettivo, e l'azione di $G$ su $X$ è quindi fedele. □

Poiché le intersezioni di due 7-Sylow distinti sono banali, $G$ possiede esattamente $8 \cdot (7-1) = 48$ elementi di ordine 7.

**Corollario 6.25.** *Se $P$ è un 7-Sylow di $G$, allora il suo normalizzatore $N(P)$ è un gruppo non abeliano di ordine $21$.*

*Dimostrazione.* L'indice di $N(P)$ è uguale al numero di 7-Sylow. Da $|G|/|N(P)| = [G : N(P)] = 8$ si ottiene $|N(P)| = 168/8 = 21$. Se $N(P)$ fosse abeliano, allora sarebbe necessariamente ciclico; tuttavia, $\rho$ immerge $G$ in $\mathrm{S}_8$, che non contiene elementi di ordine $21$, □

Nel gruppo $N(P)$, il 7-Sylow $P$ è normale, e i $14$ elementi di $N(P) \setminus P$ sono tutti di ordine $3$.

**Lemma 6.26.** *Siano $P, P', P''$ elementi distinti di $X$. Allora $N(P) \cap N(P')$ ha ordine $3$, mentre $N(P) \cap N(P') \cap N(P'')$ ha ordine $1$.*

*Dimostrazione.* Innanzitutto, $|N(P)N(P')| = 21^2/|N(P) \cap N(P')|$ mostra che $N(P) \cap N(P') \neq (\mathrm{id})$. Inoltre, $P$ è l'unico 7-Sylow di $N(P)$ e pertanto l'intersezione $N(P) \cap N(P')$ non può contenere un sottogruppo di ordine 7. Di conseguenza, $|N(P) \cap N(P')|$ è necessariamente uguale a $3$.

Per mostrare che solo l'identità normalizza tre 7-Sylow distinti, identifichiamo $G$ con la sua immagine $\rho(G) \subset \mathrm{S}_X$. Se $x$ è un generatore di $P \in X$, allora $x$ permuta ciclicamente gli altri sette 7-Sylow. Dopo averli numerati, possiamo scrivere: $x = (P_0P_1P_2P_3P_4P_5P_6)$. Se $a \in N(P) \cap N(P_0)$, allora $a$ coniuga $P$ non identicamente. A meno di sostituire $a$ con $a^{-1}$, possiamo allora supporre che $axa^{-1} = x^2$. Poiché $a$ fissa sia $P$ che $P_0$, l'unica possibilità è che sia $a = (P_1P_2P_4)(P_3P_6P_5)$. Poiché i 3-Sylow di $G$ sono tutti coniugati tra loro, ogni elemento di ordine $3$ in $G$ è coniugato ad $a$ o ad $a^{-1} = (P_1P_4P_2)(P_3P_5P_6)$. Pertanto, ogni elemento di ordine $3$ normalizza esattamente due 7-Sylow. □

**Lemma 6.27.** *$G$ possiede esattamente $56$ elementi di ordine $3$, e il normalizzatore di un 3-Sylow possiede $6$ elementi.*

*Dimostrazione.* Ogni elemento di ordine $3$ normalizza esattamente due 7-Sylow, e vi sono $14$ elementi di ordine $3$ che normalizzano ciascun 7-Sylow. Pertanto, $G$ possiede $14 \cdot 8/2 = 56$ elementi di ordine $3$, e di conseguenza $28$ 3-Sylow. Se $Q$ è un 3-Sylow di $G$, allora $N(Q)$ ha indice $28$ in $G$, e quindi $|N(Q)| = 168/28 = 6$. □

**Corollario 6.28.** *Se $Q$ è un 3-Sylow di $G$, allora $N(Q)$ non è abeliano.*

*Dimostrazione.* Con le stesse notazioni del Lemma 6.26, possiamo supporre che $Q$ sia generato da $a = (P_1P_2P_4)(P_3P_6P_5)$, che normalizza $P$ e $P_0$. Se $N(Q)$ è abeliano, allora è isomorfo a $\mathrm{C}_6$ e contiene esattamente $2$ elementi $b, b^{-1}$ di ordine $6$, che non possono normalizzare nessun $7$-Sylow. Tuttavia, le uniche permutazioni pari, senza punti fissi, di ordine $6$ in $\mathrm{A}_8$ sono prodotto disgiunto di un $6$-ciclo e di una trasposizione, e quindi l'azione per coniugio di $b$ su $X$ scambia $P_0$ con $P$ e permuta ciclicamente gli altri sei $7$-Sylow. Possiamo ripetere questa costruzione per ogni scelta di due $7$-Sylow di $G$. Otteniamo, in totale, almeno $2 \cdot \binom{8}{2} = 56$ elementi di ordine $6$.

Ricapitolando, sappiamo che $G$ possiede $48$ elementi di ordine $7$, $56$ elementi di ordine $3$ e almeno $56$ elementi di ordine $6$. Rimangono al più $168 - (48 + 56 + 56) = 8$ elementi di ordine diverso da $3, 6, 7$; poiché ogni $2$-Sylow ha ordine $8$ e l'ordine di ogni suo elemento è una potenza di $2$, dobbiamo concludere che $G$ possiede un $2$-Sylow unico, e quindi normale, il che contraddice la semplicità di $G$. □

Il nostro obiettivo è ora quello di identificare $X$ con la retta proiettiva $\mathbb{P}^1_{\mathbb{F}_7}$ e osservare che l'azione di $G$ su $X$ e quella di $\mathrm{PSL}_2(\mathbb{F}_7)$ su $\mathbb{P}^1_{\mathbb{F}_7}$ si corrispondono in questa identificazione. Ricordiamo che $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}_7} = \{0, 1, 2, 3, 4, 5, 6, \infty\}$, e che l'azione di $\mathrm{PSL}_2(\mathbb{F}_7)$ su $\mathbb{P}^1$ è data da applicazioni lineari fratte, cioè della forma

$$t \mapsto \frac{at + b}{ct + d},$$

per qualche scelta di

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_7).$$

Utilizzando le notazioni del Lemma 6.26, identifichiamo $X$ on $\mathbb{P}^1$ associando ad ogni $P_i, i = 0, \ldots, 6$ il corrispondente $i$, e a $P$ il punto improprio $\infty$. Allora l'azione di $x = (P_0P_1P_2P_3P_4P_5P_6)$ è data da

$$t \mapsto t + 1 = \frac{1 \cdot t + 1}{0 \cdot t + 1},$$

mentre quella di $a$ è data da

$$t \mapsto 2t = \frac{3 \cdot t + 0}{0 \cdot t + 5},$$

che sono entrambe trasformazioni lineari fratte indotte da matrici di determinante $1$. Tuttavia $a$ e $x$ generano soltanto $21$ dei $168$ elementi di $G$, mentre dobbiamo mostrare che ogni elemento di $G$ agisce per mezzo di una trasformazione lineare fratta.

**Proposizione 6.29.** *Siano $x \in P$, $a \in N(P) \cap N(P_0)$, come nel Lemma 6.26. Allora l'elemento $b = (P_0P)(P_1P_6)(P_2P_3)(P_4P_5)$ appartiene a $G$ e normalizza il $3$-Sylow $Q = (a)$.*

*Dimostrazione.* Sappiamo che $N(Q)$ ha sei elementi e non è abeliano. Pertanto $N(Q)$ è isomorfo a $\mathrm{S}_3$ e possiede esattamente $3$ elementi di ordine $2$, che coniugano $b$ in $b^{-1}$.

Possiamo calcolare esplicitamente tutti gli elementi di ordine $2$ senza punti fissi di $\mathrm{S}_8$ che coniugano $b$ in $b^{-1}$: sono le tre permutazioni $(P_1P_3)(P_2P_5)(P_4P_6)(P_0P)$, $(P_1P_5)(P_2P_6)(P_3P_4)(P_0P)$ e $(P_1P_6)(P_2P_3)(P_4P_5)(P_0P)$. Trattandosi di soli tre elementi, devono essere tutti e soli quelli di ordine $2$ che appartengono a $N(Q)$. In particolare $b \in N(Q)$. □

Si noti che l'azione di $b$, attraverso l'identificazione di $X$ con $\mathbb{P}^1$, è data dall'applicazione lineare fratta

$$t \mapsto -1/t = \frac{0 \cdot t - 1}{1 \cdot t + 0}.$$

**Teorema 6.30.** *L'azione di $G$ su $X$ si identifica all'azione di $\mathrm{PSL}_2(\mathbb{F}_7)$ su $\mathbb{P}^1$. Pertanto, $G$ è isomorfo a $\mathrm{PSL}_2(\mathbb{F}_7)$.*

*Dimostrazione.* L'azione per coniugio degli elementi $x$ e $bxb^{-1}$ sull'insieme $X$ fissa $P$ e $P_0$ rispettivamente. Poiché un elemento di ordine $7$ normalizza precisamente il $7$-ciclo che genera, otteniamo che $x$ genera $P$ e $bxb^{-1}$ genera $P_0$. L'intersezione $P \cap P_0$ è banale, e quindi il sottogruppo $H = \langle P, P_0 \rangle$ possiede almeno i $49$ elementi contenuti nel

sottoinsieme $PP_0$. Ma allora $H$ ha indice $[G : H] \leq 168/49 < 4$; tuttavia, i sottogruppi di indice $< 4$ in $G$ devono essere necessariamente normali, e quindi $H = G$ per semplicità di $G$. In conclusione, $\langle x, b\rangle \supset \langle P, P_0\rangle = G$.

Per mostrare che ogni elemento di $G$ agisce su $X$ per trasformazioni lineari fratte (sotto l'identificazione con $\mathbb{P}^1$ che abbiamo costruito) è allora sufficiente controllarlo per gli elementi $x$ e $b$. Ma abbiamo già visto che tali elementi agiscono per mezzo delle trasformazioni fratte $t \mapsto t + 1, t \mapsto -1/t$, che appartengono entrambe a $\mathrm{PSL}_2(\mathbb{F}_7)$. Pertanto l'omomorfismo $\rho : G \to \mathrm{S}_X \simeq \mathrm{S}_{\mathbb{P}^1}$ ha immagine contenuta in $\mathrm{PSL}_2(\mathbb{F}_7)$, che ha ordine $168$, ed è iniettivo per semplicità di $G$. Di conseguenza $\rho$ fornisce un isomorfismo $G \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. □

### 6.9. **Struttura di** $\mathbb{Z}/(n)^\times$**.** Scrivi meglio

Per il teorema cinese del resto, posso separare i primi l'uno dall'altro. Quindi basta capire come sia fatto $\mathbb{Z}/(p^h)^\times$ per $p$ primo e $h > 0$. Il caso $h = 1$ è facile perché è ciclico per il teorema dell'elemento primitivo.

Se $p$ dispari, $h > 1$, allora trovo in $\mathbb{Z}/(p^h)^\times$ un sottogruppo di ordine $p - 1$ (sollevo il generatore di $\mathbb{Z}/(p)^\times$ e ne prendo un'opportuna potenza), e trovo un sottogruppo di ordine $p^{h-1}$ ciclico (quello generato da $1 + p$ va benissimo).

Il caso $p = 2$ è più delicato $3 = 1 + 2$ genera un sottogruppo ciclico di ordine $2^{h-2}$, purtroppo. Ottengo prodotto diretto con $(-1)$. La struttura è $\mathrm{C}_2 \times \mathrm{C}_{2^{h-2}}$, $h > 2$.

Conseguenza: $\mathbb{Z}/(n)^\times$ è ciclico solo quando $n = p^h, 2p^h$, $p$ primo dispari.

## 7. Automorfismi di $\mathrm{S}_n$

Iniziamo ricordando alcuni fatti che utilizzeremo in seguito:

- Se $n \geq 5$, l'unico sottogruppo normale non banale di $\mathrm{S}_n$ è il sottogruppo alterno $\mathrm{A}_5$.
- Due elementi di $\mathrm{S}_n$ sono coniugati se e solo se hanno la stessa struttura in cicli.
- L'ordine di una permutazione di $\mathrm{S}_n$ è il minimo comune multiplo delle lunghezze dei suoi cicli.
- Se $\phi$ è un automorfismo di un gruppo $G$, allora $\phi(g)$ ha lo stesso ordine di $g \in G$. Inoltre $g, h \in G$ sono coniugati se e solo se $\phi(g), \phi(h)$ lo sono.
- Ogni automorfismo di $\mathrm{S}_n$ mappa biunivocamente la classe coniugata delle trasposizioni in una classe coniugata di elementi di ordine $2$, ovvero di prodotti di trasposizioni disgiunte.

### 7.1. **Gli automorfismi di** $\mathrm{S}_n, n \neq 6$ **sono tutti interni.**

**Proposizione 7.1.** *Il numero delle permutazioni di* $\mathrm{S}_n$ *che si scrivono come prodotto di esattamente* $k$ *trasposizioni disgiunte,* $1 \leq k \leq n/2$*, è pari a*

$$\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2} = \frac{n!}{k!2^k(n-2k)!}.$$

*Dimostrazione.* E' un conto già svolto in precedenza. □

**Proposizione 7.2.** *Se* $n \neq 6$*, il numero di permutazioni di* $\mathrm{S}_n$ *che si scrivono ocme prodotto di esattamente* $k$ *trasposizioni disgiunte,* $1 < k \leq n/2$ *non è mai uguale al numero delle trasposizioni.*

*Al contrario, il gruppo* $\mathrm{S}_6$ *contiene* $15$ *trasposizioni, e* $15$ *prodotti di tre trasposizioni disgiunte.*

*Dimostrazione.* Se $1 < k \leq n/2$ è tale che

$$\frac{n!}{k!2^k(n-2k)!} = \frac{n!}{2(n-2)!} \tag{7.1}$$

allora

$$k!2^k(n-2k)! = 2(n-2)! \tag{7.2}$$

da cui

$$\binom{n-2}{2k-2} = \frac{k!2^{k-1}}{(2k-2)!} = \frac{k(2k-2)!!}{(2k-2)!} = \frac{k}{(2k-3)!!}. \tag{7.3}$$

Ora, il coefficiente binomiale a primo membro è sempre intero, mentre $k/(2k-3)!!$ è intero solo per $k = 2, 3$. Se $k = 2$, la (7.3) diventa $\binom{n-2}{2} = 2$, e quindi $(n-2)(n-3) = 4$ che non ha soluzioni intere. Se invece $k = 3$ allora da (7.3) segue $\binom{n-2}{4} = 1$ che conduce necessariamente a $n = 6$. □

**Corollario 7.3.** *Se $n \neq 6$, ogni automorfismo di $\mathrm{S}_n$ associa a ciascuna trasposizione una trasposizione.*

*Dimostrazione.* Abbiamo già visto che un automorfismo $\phi$ di $\mathrm{S}_n$ applica le trasposizioni in elementi di ordine $2$. Inoltre, dal momento che le trasposizioni sono tutte coniugate, $\phi$ mapperà le trasposizioni biunivocamente in un'unica classe coniugata di elementi di $\mathrm{S}_n$ di ordine $2$. Ma abbiamo osservato nella proposizione precedente che non vi sono altre classi di coniugio di elementi di ordine $2$ che possiedono la stessa cardinalità della classe che contiene le trasposizioni. Pertanto, $\phi$ applica trasposizioni in trasposizioni. □

**Teorema 7.4.** *Se $n \neq 6$, ogni automorfismo di $\mathrm{S}_n$ è interno.*

*Dimostrazione.* Sia $\phi$ un automorfismo di $\mathrm{S}_n, n \neq 6$. Sappiamo per la proposizione precedente che $\phi$ manda trasposizioni in trasposizioni. Indichiamo con $s_i$ la trasposizione $(i, i+1)$. E' immediato verificare che $s_i$ commuta con $s_j$ a meno che $|i-j| = 1$. Questo vuol dire che se $|i-j| > 1$ allora $\phi(s_i)$ e $\phi(s_j)$ sono trasposizioni che agiscono su elementi distinti, mentre $\phi(s_i)$ e $\phi(s_{i+1})$ non commutano, ed hanno in comune esattamente un elemento sul quale agiscono non banalmente. E' allora possibile trovare indici $\sigma_1, \sigma_2, \dots \sigma_n$ tutti distinti in modo che $\phi(s_i) = (\sigma_i, \sigma_{i+1})$.

Ma allora l'azione di $\phi$ sulle trasposizioni coincide con quella dell'automorfismo interno indotto dalla permutazione $\sigma(i) := \sigma_i$. Dal momento che le trasposizioni generano $\mathrm{S}_n$, $\phi$ coincide con l'automorfismo interno indotto da $\sigma$ su tutto $\mathrm{S}_n$. □

Rimane il problema di stabilire se anche per $\mathrm{S}_6$ gli automorfismi siano tutti interni. Da quello che abbiamo visto, rimane aperta la possibilità che esistano automorfismi (non interni) di $\mathrm{S}_6$ che scambiano le trasposizioni con i prodotti di $3$ trasposizioni disgiunte.

7.2. **Un automorfismo esterno di $\mathrm{S}_6$.** Il sottogruppo $\Gamma = \langle (1\,2\,3\,4), (3\,4\,5\,6) \rangle < \mathrm{S}_6$ ci permetterà di costruire un automorfismo non interno di $\mathrm{S}_6$. Per comprendere la struttura di $\Gamma$ è utile notare che

**Lemma 7.5.** *L'azione di $\Gamma$ sull'insieme $X$ di tutte le partizioni di $\{1,2,3,4,5,6\}$ in tre sottoinsiemi di due elementi possiede un'orbita di cinque elementi.*

*Dimostrazione.* E' sufficiente esibire l'orbita:

$$\{\{1,2\},\{3,5\},\{4,6\}\}, \qquad \{\{1,3\},\{2,4\},\{5,6\}\}, \qquad \{\{1,4\},\{2,5\},\{3,6\}\},$$
$$\{\{1,5\},\{3,4\},\{2,6\}\}, \qquad \{\{1,6\},\{2,3\},\{4,5\}\}.$$

La verifica che l'azione dei generatori $(1\,2\,3\,4)$ e $(3\,4\,5\,6)$ stabilizza questi cinque elementi è immediata. □

*Osservazione* 7.6. Vale la pena di notare che l'azione dei due generatori di $\Gamma$ su tali cinque elementi induce nuovamente due $4$-cicli.

**Lemma 7.7.** $\Gamma \neq \mathrm{S}_6, \mathrm{A}_6$.

*Dimostrazione.* Innanzitutto, $\Gamma$ non è il sottogruppo alterno in quanto contiene la permutazione $(1\,2\,3\,4)$, che è dispari. $\Gamma$ non coincide neanche con $\mathrm{S}_6$, perché altrimenti agirebbe transitivamente sull'insieme $X$. □

**Proposizione 7.8.** *L'azione di $\Gamma$ su $\{1,2,3,4,5,6\}$ è $3$-transitiva.*

*Dimostrazione.* Immaginiamo i numeri da $1$ a $6$ disposti su sei caselle, opportunamente numerate anch'esse da $1$ a $6$, che vengono permutate tra loro per mezzo dei $4$-cicli $(1\,2\,3\,4)$ e $(3\,4\,5\,6)$. Per mostrare la $3$ transitività di $\Gamma$ è sufficiente far vedere come sia sempre possibile riportare, a partire da qualsiasi configurazione iniziale, i numeri $1, 2, 3$ nelle prime tre posizioni eseguendo in un'opportuna sequenza i due $4$-cicli. Questo non è difficile.

In effetti, se $1$ si trova nelle prime $4$ posizioni, è sufficiente eseguire $(1\,2\,3\,4)$ alcune volte per riportarlo in prima posizione. Se si trova nelle ultime due posizioni, dobbiamo dapprima eseguire $(3\,4\,5\,6)$ due volte in modo da riportarlo tra le prime quattro posizioni.

Una volta portato $1$ in prima posizione, è necessario sistemare $2$ in seconda. Se si trova già lì, non c'è nulla da fare. Altrimenti, possiamo supporre che si trovi nell'ultima posizione: in caso contrario, è sufficiente eseguire alcune volte $(3\,4\,5\,6)$ fino a portarvelo. Con $1$ in prima posizione, e $2$ in ultima, la composizione $(1\,2\,3\,4)^{-1} \circ (3\,4\,5\,6) \circ (1\,2\,3\,4)$ riordina $1$ e $2$ nelle prime $2$ posizioni. A questo punto è sufficiente eseguire $(3\,4\,5\,6)$ finché $3$ non giunge in terza posizione. □

**Corollario 7.9.** *$\Gamma$ possiede almeno $120$ elementi. Pertanto $[\mathrm{S}_6 : \Gamma] \leq 6$.*

*Dimostrazione.* $\Gamma$ agisce transitivamente sui sottoinsiemi di tre elementi dell'insieme $\{1, 2, 3, 4, 5, 6\}$, che sono appunto $120$. □

Consideriamo ora l'azione di $\mathrm{S}_6$ sui laterali destri di $\Gamma$ data per moltiplicazione sinistra. Se $n = [\mathrm{S}_6 : \Gamma]$, tale azione fornisce, dopo aver numerato gli elementi di $\mathrm{S}_6/\Gamma$, un omomorfismo $\phi : \mathrm{S}_6 \to \mathrm{S}_n$.

**Lemma 7.10.** $\ker \phi \subset \Gamma$.

*Dimostrazione.* Se $\gamma \in \ker \phi$, allora in particolare $\gamma\Gamma = \Gamma$, e quindi $\gamma \in \Gamma$. □

A questo punto tutto diventa immediatamente chiaro.

**Proposizione 7.11.** *L'omomorfismo $\phi$ è un isomorfismo. $\Gamma$ possiede esattamente $120$ elementi, ed è isomorfo a $\mathrm{S}_5$.*

*Dimostrazione.* $\ker \phi$ è un sottogruppo normale di $\mathrm{S}_6$. Essendo contenuto in $\Gamma$, non può essere né $\mathrm{S}_6$, né il sottogruppo alterno. L'unica altra possibilità è che $\ker \phi = (e)$, da cui l'iniettività di $\phi$.

Essendo $\phi$ iniettiva, l'ordine di $\mathrm{S}_n$ è almeno $720$. Ma allora $n = [\mathrm{S}_6 : \Gamma] \geq 6$. Sapevamo già che $n \leq 6$, e quindi $n = 6$, il che mostra come $\phi$ sia un isomorfismo, e l'ordine di $\Gamma$ sia $120$.

Inoltre, se $\gamma \in \Gamma$, allora $\gamma\Gamma = \Gamma$, e quindi $\phi(\gamma)$ è una permutazione sull'insieme dei laterali di $\Gamma$ che lascia fisso il laterale $\Gamma$. Questo mostra che $\phi(\Gamma)$ è contenuto nel sottogruppo di $\mathrm{S}_6$ che lascia fisso $\Gamma$, che è isomorfo al gruppo delle permutazioni sui cinque laterali residui. Per iniettività, concludiamo che $\Gamma \simeq \mathrm{S}_5$. □

$\phi : \mathrm{S}_6 \to \mathrm{S}_6$ è l'automorfismo esterno cercato. Per convincersene basta osservare che

**Lemma 7.12.** *L'automorfismo $\phi$ non conserva la struttura ciclica degli elementi di $\mathrm{S}_6$.*

*Dimostrazione.* $\Gamma$ contiene $\gamma = (1\,2\,3\,4)(3\,4\,5\,6) = (1\,2\,3)(4\,5\,6)$. Ma sappiamo che $\phi(\gamma)$ è una permutazione dei sei laterali di $\Gamma$ che ne fissa almeno uno. Non può quindi essere un prodotto di due $3$-cicli. □

**Teorema 7.13.** *Il gruppo $\mathrm{Aut}\,\mathrm{S}_6 \,/\, \mathrm{Int}\,\mathrm{S}_6$ degli automorfismi esterni di $\mathrm{S}_6$ ha ordine due.*

*Dimostrazione.* Gli automorfismi non interni di $\mathrm{S}_6$ devono necessariamente mandare le trasposizioni in prodotti di tre trasposizioni disgiunte e viceversa. Ma allora se $\phi$ e $\psi$ sono automorfismi non interni, $\phi \circ \psi^{-1}$ conserva la struttura in cicli, ed è quindi un automorfismo interno. Questo dimostra che $\mathrm{Int}\,\mathrm{S}_6$ ha indice due in $\mathrm{Aut}\,\mathrm{S}_6$. □

*Osservazione* 7.14. Incidentalmente, l'omomorfismo $\rho : \Gamma \to \mathrm{S}_5$ descritto nel Lemma 7.5 è anch'esso un isomorfismo. In effetti, sappiamo che $\rho(\Gamma)$ contiene almeno quattro elementi; possedendo adesso l'informazione che $\Gamma$ è isomorfo ad $\mathrm{S}_5$ si escludono immediatamente le possibilità che il nucleo di $\rho$ sia tutto $\mathrm{S}_5$, oppure il suo sottogruppo alterno. Ma allora $\rho$ è iniettiva, ed è allora anche suriettiva per una questione di cardinalità.

*E-mail address*: dandrea@mat.uniroma1.it