# Dispense Algebra I

Prima parte del corso

Federico De Sisti

2024-12-22

# Contents

# 1 Preambolo

Siamo giunti a un nuovo capitolo della nostra vita. A volte, per andare avanti, è necessario guardarsi un po' indietro; altre volte, per dimostrare un teorema, bisogna osare e andare oltre l'uso delle semplici ipotesi, arrivando persino a utilizzare la stessa tesi che vogliamo comprovare. L'algebra, in fondo, non è solo una raccolta di regole e teoremi, ma un modo per guardare il mondo con nuovi occhi e trovare connessioni inaspettate tra idee apparentemente lontane.

Questa dispensa non è solo un supporto didattico, ma un piccolo viaggio da percorrere insieme, fatto di curiosità, sfide e, perché no, qualche sorriso lungo il cammino. Alberto, con il suo cuore così grande, riesce a infondere a tutti noi un po' della sua energia: la stessa che distribuisce periodicamente nell'aula 1, per evitare che esploda di entusiasmo.

Un ringraziamento speciale va alla redazione, che con impegno e creatività ha reso tutto questo possibile: Marco (dai capelli lunghi, anche se, da quando hanno aperto un barbiere a Civita, un po' meno lunghi), Gabriel (sempre nel flusso, come un'equazione ben bilanciata), Fabio (compagno di merende a mensa, con cui ogni pausa si trasforma in un momento memorabile) e Simone (che, quando riesci a incontrarlo, sa sempre come strapparti un sorriso).

E infine, un augurio a Simone affinché possa finalmente avere la meglio sul suo nemico più temuto: LPC. Perché, in fondo, ogni battaglia può essere vinta con la giusta determinazione e un pizzico di algebra.

Buona lettura e buon viaggio in questo affascinante mondo che, come una funzione complessa, nasconde sempre qualcosa di meraviglioso appena dietro l'angolo.

P.S. Se non avete stampato queste dispense tramite l'autore siete un mucchio di stronzi.
P.P.S. Si ringrazia OpenAI per l'immensa saggezza nella formulazione di questo preambolo, con qualche dritta, sorprende sempre.

## 2 Cosa c'è su e-leaning di Francesco Mazzini

Date appelli
Esercizi settimanali
All'esame ti chiedono due esercizi delle schede scelti a caso
Ci sono 2 esoneri (primo 17 dicembre) (secondo ?? maggio)
**Libri**
M. Artin Algebra
IN. Hernstein: Algebra (difficile)

## 3 Gruppi

**Definizione 1** (Gruppo)
*Un gruppo è un dato di un insieme $G$ con un'operazione $\cdot$ tali che:*
*1) L'operazione è associativa*

$$f \cdot (gh) = (f \cdot g) \cdot h \qquad \forall f, g, h \in G$$

*2) Esistenza elemento neutro*

$$\exists e \in G \text{ tale che } g \cdot e = e \cdot g = g \quad \forall g \in G.$$

*3) esistenza degli inversi*

$$\forall g \in G \qquad \exists \quad g^{-1} \in G \quad \text{tale che } g^{-1} \cdot g = g \cdot g^{-1} = e.$$

**Nomenclatura 1** (notazione)
*$(G, \cdot)$ dato $g \in G$ denotiamo con:*
*1)* $g^0 = e$
2)$g^1 = g$
3)$g^n = g \cdot \ldots \cdot g$
4)$g^{-n} = (g^{-1})^n$

**Osservazione:**
Con questa notazione:

$$(g^n)^m = g^{nm}$$
$$g^n \cdot g^m = g^{n+m}$$

**Esempi**
1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$
2) $GL_n(\mathbb{K}) = \{A \in Mat_{n\times n}(\mathbb{K}) | det(A) \neq 0\}$ con prodotto
3) $SL_n(\mathbb{K}) = \in Mat_{nn}(\mathbb{K}) | det(A) = 1\}$
4) $X$ insieme

$$S_X = \{ \text{ funzioni } X \to X \text{ invertibili}\}$$

**Speciale** Se $X = \{1, \dots, n\}$
Allora chiamiamo

$$S_n = S_X.$$

(è il gruppo di permutazioni su $n$ elementi)
Si chiama gruppo simmetrico

**Definizione 2** (Gruppo diedrale)
$n \geq 3$ *Consideriamo l'n-agono regolare nel piano (3-agono, triangolo)*
$D_n$ *è l'insieme delle simmetrie del piano che preservano l' n-agono*
*Si chiama gruppo diedrale, l'operazione è la composizione*

**Esempio:**
Per $n = 3$ abbiamo $D_3 = \{e, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$
**Esercizio**
Determina gli inversi e tutti i possibili prodotti degli elementi di $D_3$

**Definizione 3** (Gruppo Abeliano)
$(G, )$ *gruppo si dice Abeliano se l'operazione è commutativa*

$$f \cdot g = g \cdot f$$

**Definizione 4** (Gruppo finito)
$(G, \cdot)$ *gruppo si dice finito se la sua cardinalità è finita*

$$|G| < +\infty$$

**Definizione 5** (Ordine del gruppo)
$L(G, \cdot)$ *gruppo, l'ordine di* $G$ *è* $|G|$

**Definizione 6** (Ordine di un elemento)
$ord(g) = \min\{n \in \mathbb{N} | g^n = e\}$
*se* $\nexists n \in \mathbb{N}$ *tale che* $g^n = e \quad$ *poniamo* $\quad ord(g) = +\infty$

**Definizione 7** (Gruppo ciclico)
$n \geq 3$ *consideriamo* $C_n$ *l'insieme delle isometrie del piano che preservano l' n-agono e preservano l'orientazione, questo si chiama gruppo ciclico.*

**Esempio**
Nel caso di $n = 3$ abbiamo solamente 3 elementi: identità, e le due rotazioni (ordine dispari)
**Esercizi**

1) si dimostri che l'elemento neutro in un gruppo è unico
2) si dimostri che ogni elemento in un gruppo ammette un unico elemento inverso
per casa
1) Trovare un'applicazione biunivoca $S_3 \to D_3$
2) Dimostrare che non esiste un'applicazione biunivoca $S_4 \to D_4$
3) Dimostrare che i seguenti non sono gruppi
$\cdot Mat_{n\times n}(\mathbb{K})$ con prodotto righe per colonne
$GL(\mathbb{K})$ con somma tra matrici
$\mathbb{Z}\mathbb{Q}\mathbb{R} conil prodotto$

**Proposizione 1**
*$(G,\cdot)$ gruppo finito, Allora ogni elemento ha ordine finito*

**Dimostrazione**
*$g \in G$ Considero il sottoinsieme*

$$A = \{g, g^2, g^3, \ldots\} \subseteq G.$$

*quindi $|A| < +\infty \Rightarrow \exists s,t \in \mathbb{N}, s > t$ tali che*

$$g^s = g^t.$$

*Moltiplico per $g^{-t}$ a destra*

$$g^s = g^t \quad \Rightarrow \quad g^s \cdot g^{-t} = g^t \cdot g^{-t} \quad \Rightarrow \quad g^{s-t} = e.$$

*Quindi $n = s - t \geq 1$ e $g^n = e \Rightarrow ord(g) \leq n < +\infty$* □

**Definizione 8** (Sottogruppo)
*$(G,\cdot)$ gruppo $H \subseteq G$ sottoinsieme, si dice che $H$ è un sottogruppo se $(H,\cdot)$ è un gruppo.*
*In tal caso scriveremo $H \leq G$*

**Osservazione**
$(G,\cdot)$ gruppo, $G \subseteq G$ sottoinsieme allora $H \leq G$se H è chiuso rispetto a $\cdot$
e $H$ è chiuso rispetto agli inversi
(se $g,h \in G \Rightarrow g \cdot h \in H$ e se $h \in H \Rightarrow h^{-1} \in H$)

**Proposizione 2**
*$(G,\cdot)$ gruppo $H \subseteq G$ sottoinsieme con $|H| < +\infty$ Allora:*
*1) $H \leq G$ se e solo se $H$ è chiuso rispetto a $\cdot$*

**Dimostrazione**
$(\Rightarrow)$ *ovvia*

($\Leftarrow$) *basta dimostrare che* $H$ *è chiuso rispetto all'inverso ovvero*
*se* $|H| < +\infty$
*e* $H$ *chiuso rispetto a* $\cdot$
*Allora* $H$ *è chiuso rispetto agli inversi*
*Sia* $h \in H$
$A = \{h, h^2, h^3, \ldots\} \subseteq H$
*Allora* $|A| < \infty$
*Ragionando come prima deduciamo* $ord(h) < +\infty$

$$h \cdot h^{ord(h)-1} = h^{ord(h)-1} \cdot h = e.$$

*Quindi* $h^{-1} = h^{ord(h)-1} = h \cdot \ldots \cdot h \in H \Rightarrow h^{-1} \in H$ □

**Esempi**
1)$C_n \leq D_n$
2) $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$
3) $(G, \cdot)$ gruppo $g \in G$

$$< g >= \{g^n \in G | n \in \mathbb{Z}\}.$$

Allora $< g > \leq G$

**Congruenze**
$(G, \cdot)$ gruppo $H \leq G$

**Definizione 9**
$f, g \in G$ *si dicono congruenti modulo* $H$ *se*

$$f^{-1}g \in H.$$

*In tal caso scriveremo*

$$f \equiv g \mod H \text{ oppure } f \equiv_H g.$$

**Esercizio**
Dimostrare che al congruenza modulo $H$ definisce una relazione di equivalenza su $G$
**Suggerimento**
$(f^{-1} \cdot g)^{-1} = g^{-1} \cdot (f^{-1})^{-1} = g^{-1} \cdot f$
e $H$ è chiuso rispetto agli inversi
**Esercizi:**
$(G, \cdot)$ è un gruppo $H \leq G$ Allora la classe di equivalenza di $g \in G$ modulo $H$ è il sottoinsieme

$$gH = \{g \cdot h | h \in H\}.$$

C'è una classe di equivalenza speciale in $G$ data da

$$e \cdot H = H.$$

l'unica ad essere un sottogruppo

---

Dimostrare che esiste un'applicazione biunivoca tra $H \to gH \quad \forall g \in G$

## 3.1 Classi di equivalenza

**Notazione 1**
*Sia $(G, \cdot)$ un gruppo e sia $H \leq G$ un sottogruppo:*

- *Dato $g \in G$ il sottoinsieme $gH$ si chiama laterale sinistro o "classe laterale sinistra"*
- *L'insieme dei laterali sinistri si indica con $G/H$*

**Esempi importanti**
$(G, \cdot) = (\mathbb{Z}, +)$
$H = (m) = \{am | a \in \mathbb{Z}\}$ con m fissato
$G/H = \mathbb{Z}/(m)$
**Attenzione**
potete definire $f = g \mod H$ tramite la condizione $f \cdot g^{-1}$
Le due definizioni non sono equivalenti [La chiameremo congruenza destra]

**Notazione 2**
*L'insieme delle classi di equivalenza destra si indica con*

$$H \backslash G.$$

**Definizione 10**
*Gli elementi di $G/H$ si chiamano laterali sinistri, quelli di $H\backslash G$ si chiamano laterali destri*

**Esercizio:**
$(G, \cdot)$ gruppo
$H \leq G \quad g \in G$ fissato
Allora il laterale sinistro a cui appartiene $g$ è

$$gH = \{g \cdot h | h \in H\}.$$

**Soluzione**
fisso $f \in G$ e osserviamo che

$$g \equiv f \mod H.$$

Se e solo se $g^{-1} \cdot f \in H$.
Questo è equivalente a

$$\exists h \in H \text{ tale che } g^{-1} \cdot f = h.$$

ovvero

$$\exists h \in H \text{ tale che } f = g \cdot h.$$

**Esercizio**
$H \leq G$
Allora $|G/H| = |H\backslash G|$
**Soluzione**
Basta eseguire un'applicazione biunivoca tra i due insiemi

**Definizione 11**
*$(G, \cdot)$ gruppo $H \leq G$ si dice sottogruppo normale se $gH = Hg \quad \forall g \in G$*

**Esempio**
$G = S_3$ ricordo che $S_3$ è il gruppo di permutazioni dell'insimee $\{1, 2, 3\}$
Quali sono gli elementi di $S_3$?

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (3, 2, 1)$$

scambio il 3 con l'uno , il 2 con il 2

(2,3,1)
(1,3)
(1,2)
Id

$$H_1 =< (1, 2) >= \{id, (1, 2)\}.$$

$$H_2 =< (3, 2, 1) >= \{id, (3, 2, 1), (2, 3, 1)\}.$$

**Esempio (Nuova) Notazione**
$G = S_3$ ricordo che $S_3$ è il gruppo di permutazioni dell'insimee $\{1, 2, 3\}$
Gli elementi sono $S_3 = \{Id, (12), (13), (23), (231), (321)\}$
Per la composizione usiamo la seguente notazione:
Per esempio leggiamo $(123)(231) = (213)$, quindi leggiamo i cicli da destra e permutiamo verso destra, quindi 2 va in 3, (mi sposto nel primo ciclo) 3 va in 1, quindi ottengo 2 va in 1, finisce quidni con 1 e controllo dove va, nel ciclo di destra, quindi 1 va in 2, cambio cilco, 2 va in 3, ottengo quindi (213)
**Esercizio**
Dimostrare che $H_1 \leq S_3$ non è normale, mentre $H_2 \leq S_3$ è normale

**Notazione 3**
*Se $H \leq G$ è normale scriveremo*

$$H \trianglelefteq G.$$

**Osservazione**
$(G, \cdot)$ gruppo
$H \leq G$ Allora

$$|gH| = |Hg| \quad \forall g \in G.$$

anche se $gH \neq Hg$ poiché hanno entrambi la stessa cardinalità di $H$
Inoltre tutti i laterali sinistri (e destri) hanno la stessa cardinalità

**Definizione 12**
*$(G, \cdot)$ gruppo, $H \leq G$ l'indice di $H$ in $G$ è*

$$[G : H] = |G/H|.$$

*dove $|G/H|$ è il numero di classi laterali sinistre*

**Osservazione**
$H \leq G$ sottogruppo
Se $G$ è abeliano allora $H \trianglelefteq G$
Il viceversa è falso! Possono esistere sottogruppi normali in gruppi non abeliani

**Proposizione 3**
*$(G, \cdot)$ gruppo $H \leq G$ allora*

$$|G| = [G : H]|H|.$$

**Dimostrazione**
*Basta ricordare che la cardinalità di ciascun laterale sinistro è pari a $|H|$* □

**Osservazione**
$H \leq G => [G : H] = \dfrac{|G|}{|H|}$

**Teorema 1** (Lagrange)
*$(G, \cdot)$ gruppo $H \leq G$ Allora l'ordine di $H$ divide l'ordine di $G$*

**Dimostrazione**
*Dall'osservazione segue* $\dfrac{|G|}{|H|} = [G : H] \in \mathbb{N}$ □

**Corollario 1**
*$(G, \cdot)$ gruppo di ordine primo (ovvero $|G| = p$ con $p$ primo)*
*Allora $G$ non contiene sottogruppi non banali (tutto il gruppo o il gruppo minimale)*

**Dimostrazione**
*Sia $H \leq G$ allora per Lagrange abbiamo*

$$|H| \text{ divide } p.$$

$\Rightarrow |H| = 1$ *quindi* $H = \{e\}$
*oppure* $\Rightarrow |H| = p$ *quindi* $H = H$

□

**Corollario 2**
$(G, \cdot)$ *gruppo (finito)*
*Dato* $g \in G$ *si ha* $ord(g)$ *divide l'ordine di* $G$

**Dimostrazione**
*Dato* $g \in G$ *considero*

$$< g >= \{e, g, g^2, \ldots, g^{n-1}\}$$
$$| < g > | = ord(g).$$

*La tesi segue ora da Lagrange* □

## 3.2 Operazioni fra sottogruppi

**Proposizione 4**
$(G, \cdot)$ *gruppo* $H, K \leq G$
*Allora* $H \cap K \leq G$

**Dimostrazione**
$H \cap K$ *è chiuso rispetto all'operazione e agli inversi poiché sia* $H$ *che* $K$ *che lo sono* □

**Esercizio**
Esibire due sottogruppi $H, K \leq G$ tali che $H \cup K$ non è un gruppo

**Definizione 13**
*Dati $H, K \leq G$ definiamo il sottoinsieme*

$$HK = \{h \cdot k | h \in H, k \in K\}.$$

***Attenzione*** *non è necessariamente un sottogruppo*

**Esercizio**
Dimostrare che $HK$ è un sottogruppo, di $G$ se e solo se

$$HK = KH.$$

**Soluzione**
Supponiamo che $HK$ sia un sottogruppo

$$HK = (HK)^{-1} = \{(h \cdot k)^{-1} | h \in H, k \in K\} = K^{-1}H^{-1} = KH.$$

Viceversa supponiamo che $HK = KH$
1) Dimostro che $KH$ è chiuso rispetto all'operazione.
$h_1k_1 \in HK$ e $h_2 \cdot k_2 \in HK$

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2) = h_1 \cdot (k_1 \cdot h_2) \cdot k_2 = h_1 \cdot h_3 \cdot k_3 \cdot k_2 = (h_1 \cdot h_3) \cdot (k_3 \cdot k_1).$$

2) $HK$ è chiuso rispetto agli inversi

$$h \cdot k \in HK \rightsquigarrow (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} = h_4 \cdot k_4 \in HK.$$

**Definizione 14** (Sottogruppo generato da un sottoinsieme)
*$(G, \cdot)$ gruppo $X \subseteq G$ sottoinsieme*
*Il sottogruppo generato da $X$ è*

$$< X >= \bigcap_{H \leq G, X \subseteq H} H.$$

**Notazione 4**
$\cdot H, K \leq G$

$$< H, K >:=< H \cup K > .$$

$\cdot g_1, \ldots, g_n \in G$

$$< g_1, \ldots, g_n >:=< \{g_1, \ldots, g_n\} > .$$

**Caso Speciale**
$(G, \cdot) = (\mathbb{Z}, +) \quad m \in \mathbb{Z}$
$(m) :=< m >$

## 3.3 Sottogruppi di $(\mathbb{Z}, +)$

**Ricordo**
dato $a \in \mathbb{Z}$ si ha $(a) \leq \mathbb{Z}$
**Obbiettivo**
non esisotno altri sottogruppi

**Teorema 2**
*$H \leq \mathbb{Z}$ allora esiste $m \in \mathbb{Z}$ tale che $H = (m)$*

**Dimostrazione**
*Distinguiamo due casi:*
*1) $H = (0)$ finito*
*2) $H \neq (0)$ allora $H$ contiene (almeno) un intero positivo, Definiamo*

$$m := \min\{n \in \mathbb{Z} | n \geq 1, n \in H\}.$$

*Vogliamo verificare che $H = (m)$ Sicuramente $(m) \subseteq H$ poich$H \leq \mathbb{Z}$*
*Viceversa supponiamo che $\exists n \in Hx(n)$.*
*Allora*

$$n = qm - r \text{ per qualche } q \in \mathbb{Z} \quad 0 < r < m.$$

$\rightarrow r = n - qm \in H$
*Ma $r > 0, r < m$ quindi otteniamo l'assurdo per minimalità di $m$*

□

**Proposizione 5**
*$a, b \in \mathbb{Z}$, Allora:*
$1)(a) \cap (b) = (m)$ *dove* $m := mcm\{a, b\}$
$2)(a) + (b) = (d)$ *dove* $d := MCD\{a, b\}$

**Osservazione**
$(a) + (b)$ è della forma $HK$ con $H = (a)$ e $K = (b)$
inoltre $(a) + (b) \leq \mathbb{Z}$ poich$(\mathbb{Z}, +)$ è abeliano
**Dimostrazione**
$1)(a) \cap (b)$ *è il sottogruppo dei multipli di $a$ e di $b$*
*Dunque* $(a) \cap (b) = (m)$
$2)a + b \leq \mathbb{Z} \Rightarrow (a) + (b) = (d')$ *per teorema*
*Dobbiamo verificare che $d' = d$*

$$(d') = (a) + (b) \supseteq (a) \Rightarrow d'|a \quad (d' \text{ divide } a).$$

$$\Rightarrow \begin{cases} d'|a \\ d'|b \end{cases} \Rightarrow d' \leq d$$

$d' \in (a) + (b) \Rightarrow \exists h, k \in \mathbb{Z}$ *tale che* $d' = ha + kb$

*Dunque:*

$$\begin{cases} d|a \\ d|b \end{cases} \Rightarrow d|d' => d \leq d'$$

*Allora* $d = d'$ □

## 3.4 Gruppi $D_n$ e $C_n$

**Ricordo**
$n \geq 3$
Fissiamo un $n - agono$
$D_n = \{$isometrie che preservano l'n-agono$\}$
$C_n = \{$isometrie che preserrvano l'n-agono e l'orientazione$\}$

**Teorema 3**
$n \geq 3$ *Allora*

$$|D_n| = 2n$$
$$|C_n| = n$$

**Dimostrazione**
*Fissiamo un lato l dell'n-agono. Un'isometria* $\varphi \in D_n$ *è univocamente determinata dall'immagine di* $\varphi(l)$
*Ho n scelte per il lato e per ogniuna di queste ho 2 scelte per le orientazione (mando il lato in se stesso? in quello dopo? in quello dopo ancora?, posso anche invertire la sua orientazione, i successivi lati vengono definiti da dove viene mandato il primo)*
*se non scegliamo l'orientazione, ci rimane il gruppo ciclico, e ciò conclude la dimostrazione* □

**Osservazione**
La dimostrazione prova che

$$C_n =< \rho > .$$

dove $\rho$ è la rotazione di angolo $\frac{2\pi}{n}$ attorno al centro dell'$n$-agono
Infatti $\rho \in C_n \Rightarrow < \rho > \subseteq C_n$ ma l'ordine di questa rotazione è $n$

$$| < \rho > | = ord(\rho) = n = |C_n| => C_n =< \rho > .$$

**Osservazione**
Dalla dimostrazione segue che $D_n$ è costituito da $n$ rotazioni
(della forma $\rho^i \quad i \in \{1, \ldots, n\}$
e $n$ riflessioni

**Proposizione 6**
*$n \geq 3$ Allora:*
1)$D_n =< \rho, \sigma >$
*Dove $\sigma$ è una simmetria qualsiasi ($\sigma \in D_n \setminus C_n$) e $\rho = \frac{2\pi}{n}$*
2)$\rho^i \sigma = \sigma \rho^{n-i}$

**Dimostrazione**
*1)Sicuramente* $< \rho, \sigma > \subseteq D_n$
$H =< \rho >= \{Id, \rho, \rho^2, \ldots, \rho^{n-1}\}$
$K =< \sigma >= \{Id, \sigma\}$
$H \cap K = \{Id\}$

$$|KH| = \frac{|H||K|}{|H \cap K|} = 2n.$$

$\Rightarrow HK \subseteq D_n$ *(In particolare HK è sottogruppo)* $\Rightarrow D_n = HK =< \rho, \sigma >$
$\rho\sigma$ *non preserva l'orientazione*
$\Rightarrow \rho^i \sigma$ *è riflessione*
$\Rightarrow ord(\rho^i \sigma) = 2$
$\Rightarrow \rho^i \sigma \rho^i \sigma = Id$
$\Rightarrow \rho^i \sigma \rho^i = \sigma$
$\Rightarrow \sigma \rho^i = \rho^{n-1} \sigma$ □

**Proposizione 7** (Caratterizzazzione dei sottogruppi normali)
*$(G, \cdot)$ gruppo, $N \leq G$*
*Le seguenti sono equivalenti:*
1)$gNg^{-1} \subseteq N \quad \forall g \in G$
2)$gNg^{-1} = N \quad \forall g \in G$
3)$N \trianglelefteq G$
4) *L'operazione* $G/N \times G/N \to G/N$
*è ben posta* $(fN, gN) \to fgN$
*o equivalentemente* $N\backslash G \times N\backslash G \to N\backslash G$
$(Nf, Ng) \to Nfg$

**Dimostrazione**
$1 \to 2$
*Verifichiamo che* $N \subseteq gNg^{-1}$
*Dato che* $n \in N \Rightarrow n = g(g^{-1}ng)g^{-1}$ *basta dimostrare che* $g^{-1}ng \in N$
*D'altra parte* $g^{-1}ng \in g^{-1}Ng \subseteq N$ *(per ipotesi 1)*
$2 \to 3$
$\forall g \in G \quad \forall n \in N$
$gng^{-1} \in N$ *(per ipotesi 2)*

$$\begin{cases} gn \in Ng \\ ng^{-1} \in g^{-1}N \end{cases} \Rightarrow \begin{cases} gN \subseteq Ng (1) \\ Ng^{-1} \subseteq g^{-1}N (2) \end{cases} .$$

*Il che è equivalente a dire che $gN = Ng$ la prima condizione mi dice $G/N \subseteq G/N$ e la seconda dell'arbitrarietà di g*
$G/N \subseteq G/N$
$3 \to 4$
*Dati $f$ e $g \in G$ abbiamo*

$$(Nf)(Ng) = (fN)(Ng) = fNg = (fN)g = (Nf)g = Nfg.$$

$4 \to 1$
*Per ipotesi 4 $(Nf)(Ng) = Nfg \quad \forall f, g \in G$ quindi*

$$nfn'g \in Nfg \quad \forall n, n' \in N.$$

*dall'arbitrarietà di g, scelgo $g = f^{-1}$, quindi*

$$nfn'f^{-1} \in N \quad \forall f \in G.$$

*Moltiplico (a sinistra) per $n^{-1}$ e ottengo*

$$fn'f^{-1} \in N \quad \forall f \in G.$$

*Dall'arbitrarietà di $n'$ otteniamo $fNf^{-1} \subseteq N \quad \forall f \in G$ che è la condizione (1)* □

**Osservazione**
$(G, \cdot)$ gruppo, la proposizione ci dice che un sottogruppo $H$ è normale se e solo se l'operazione indotta su $G/H$ è ben definita

**Teorema 4**
*$(G, \cdot)$ gruppo $N \trianglelefteq G$*
*Allora $(G/N, \cdot)$ è un gruppo (detto gruppo quoziente)*

**Dimostrazione**
*Associatività, ovvia*
*elemento neutro : $N = Ne$*
*elemento inverso di $Ng$ è $Ng^{-1} \quad \forall g \in G$* □

**Osservazione**
$(G, \cdot)$ gruppo e $H \leq G$ t.c. $[G : H] = 2$ Allora $H \trianglelefteq G$
Infatti esistono solo due laterali sinistri o destri: H, G/H

**Osservazione**
$(G, \cdot)$ gruppo abeliano $\Rightarrow$ ogni sottogruppo è normale
**<u>Non</u> vale sempre il viceversa**

**Esempio**
Dimostrare che $Q = \{\pm 1, \pm i, \pm j, \pm k\}$
è un gruppo (rispetto al prodotto) non abeliano in cui però tutti i sottogruppi sono normali

**Prodotti:**
$i^2 = k^2 = j^2 = -1$
$ij = k \quad jk = i \quad ki = j$
$ji = -k \quad kh = -i \quad ik = -j$

## 3.5 Omomorfismi tra gruppi

**Definizione 15**
*Siano* $(G_1, \cdot)$ *e* $(G_2, *)$ *gruppi*
*Sia* $\varphi$ *un'applicazione*
$\varphi : G_1 \to G_2$ *si dice omomorfismo se:*

$$\varphi(g \cdot f) = \varphi(g) * \varphi(f) \quad \forall g, f \in G_1.$$

**Osservazione**
Graficamente $\varphi$ è un omomorfismo se

$$\begin{array}{ccc} (g,f) & G_1 \times G_1 \xrightarrow{\cdot} G_1 & (g,f) \longrightarrow g \cdot f \\ \downarrow & \varphi\times\varphi \downarrow \quad \downarrow \varphi & \downarrow \\ (\varphi(g), \varphi(f)) & G_2 \times G_2 \xrightarrow{*} G_2 & \varphi(g \cdot f) \end{array}$$

**Esempi:**
$(\mathbb{R}, +)$ gruppo additivo reali
$(\mathbb{R}_{>0}, \cdot)$ gruppo moltiplicativo reali positivi
**Allora**
$exp : \mathbb{R} \to \mathbb{R}_{>0}$
$x \to e^x$
è un omomorfismo infatti: $\forall x, y \in \mathbb{R}$

$$e^{x+y} = e^x \cdot e^y.$$

**Esempio**
$ln : \mathbb{R}_{>0} \to \mathbb{R}$
$x \to ln(x)$
è un omomorfismo, infatti $\ln(x \cdot y) = \ln(x) + \ln(y) \quad \forall x, y \in \mathbb{R}_{>0}$
**Osservazione:**
$l^0 = 1 \quad ln(1) = 0$
0 è l'elemento neutro in $(\mathbb{R}, +)$
1 è l'elemento neutro in $(\mathbb{R}_{>0}, \cdot)$
**Osservazione:**
$e^{-x} = \frac{1}{e^x}$
Inverso di $x$ in $(\mathbb{R}, +)$
è invero di $e^x$ in $(\mathbb{R}_{>0}, \cdot)$
$\ln(\frac{1}{x}) = -\ln(x)$
**Esercizio**
$\varphi : G_1 \to G_2$ omomorfismo. Dimostrare
1)$\varphi(e_1) = e_2$
2)$\varphi(g^{-1}) = \varphi(g)^{-1} \quad \forall g \in G_1$
**Soluzione:**
$\varphi(e_1) = \varphi(e_1 \cdot e_2) = \varphi(e_1) * \varphi(e_1)$
moltiplico per $\varphi(e_1)^{-1}$
$\Rightarrow e_2 = \varphi(e_1)^{-1} * \varphi(e_1) = \varphi(e_1)^{-1} * (\varphi(e_1) * \varphi(e_1)) = \varphi(e_1)$

**Esempio**
$(G, \cdot)$ gruppo, $N \trianglelefteq G$
Allora
$\pi : G \to G/N$
$\quad g \to gN$
è un omomorfismo
**Esempio**
$det : GL_n(\mathbb{K}) \to \mathbb{K}^*$
dove $\mathbb{K}$ campo
$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ è un gruppo rispetto l prodotto
allora $det$ è un omomorfismo
infatti:

$$\forall A, B \in GL_n(\mathbb{K}) \quad det(AB) = det(A)det(B).$$

in particoalre:
$det(Id) = 1$
$det(A^{-1}) = \frac{1}{det(A)} \quad \forall A \in GL_n(\mathbb{K})$

**Definizione 16**
*$\varphi : G_1 \to G_2$ omomorfismo*
*il nucleo di $\varphi$ è $ker(\varphi) := \{g \in G_1 | \varphi(g) = e\}$*
*L'immagine di $\phi$ è*
$Im(\varphi) = \{h \in H_2 | \exists g \in G_1 : \varphi(g) = h\}$

**Esercizio:**
$\varphi : G_1 \to G_2$ omomorfismo
Allora $ker(\varphi) \trianglelefteq G_1$)
**Soluzione**
Chiamo $H : ker(\varphi)$
vorrei verificare che $gHg^{-1} \subseteq H \quad \forall g \in G_1$
scegliamo $h \in H$ (ovvero $\varphi(g) = e_2$)
$\Rightarrow \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) =$ per esercizio $= \varphi(g)\varphi(h)\varphi(g)^{-1} = e_2$
$\Rightarrow ghg^{-1} \in H \forall h \in H, \forall g \in G \Rightarrow gHg^{-1} \subseteq H$
**Osservazione**
$(G, \cdot)$ gruppo, $H \leq G$. Allora $HG$ se e solo se esiste $\varphi : G_1 \to G_2$ omomorfismo tale che $H = ker(\varphi)$

**Dimostrazione**
*Resta solo l'implicazione $\Rightarrow$*
*Sia $H \trianglelefteq G$. considero l'omomorfismo*
$\pi : G \to G/H$
$\quad g \to gH$
*chi è $ker(\pi)$*
$ker(\pi) = \{g \in G | gH = H\} = \{g \in G | g \in H\} = H$ □

**Esempio**
$det : GL_n(\mathbb{K}) \to K^*$
$ker(det) := \{A \in GL_n(\mathbb{K}) | det(A) = 1\} = SL_n(\mathbb{K})$
*quindi*
$\mathrm{SL}_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$
**Esercizio**
$(G, \cdot)$ gruppo $g \in G$ fissato
$\varphi : \mathbb{Z} \to G$
$\quad n \to g^n$
è un omomorfismo
determinare $ker\varphi$ e $Im\varphi$
**Esercizio**
Sia $\varphi : G_1 \to G_2$ omomorfismo
1) Se $H_1 \leq G_1 \Rightarrow \varphi(H_1) \leq G_2$
se $H_1 \trianglelefteq G_1 \Rightarrow \varphi(H_1) \trianglelefteq \varphi(G_1)$
2) Se $H_3 \leq G_2 \Rightarrow \varphi^{-1}(H_2) \leq G_1$
se $H_1 \trianglelefteq G_2 \Rightarrow \varphi^{-1}(H_2) \trianglelefteq \varphi(G_1)$
**Soluzione**
1)Se $H_1 \subseteq G_1$ dimostriamo che $\varphi(H_1) \trianglelefteq \varphi(G_1)$
Verifichiamo che

$$f\varphi(H_1)f^{-1} \subseteq \varphi(H_1) \quad \forall f \in (G_1).$$

Quindi basta dimostrare che
$\forall h \in H_1 \quad \forall g \in G_1$ abbiamo
$\varphi(g)\varphi(h)\varphi(g)^{-1} \in \varphi(H_1)$
Questo è equivalente a richiedere che

$$\varphi(g \cdot h \cdot g^{-1})\varphi(H_1).$$

Ma $ghg^{-1} \in gH_1g^{-1} = H_1$ dato che $H_1 \trianglelefteq G_1$

$$\exists \tilde{h} \in H_1 \text{ t.c } g \cdot h \cdot g^{-1} = \tilde{h}$$
$$\varphi(ghg^{-1}) = \varphi(\tilde{h}) \in \varphi(H_1)$$

2) Se $H_2 \trianglelefteq G_2$ dimostriamo che $\varphi^{-1}(H_2) \trianglelefteq G_1$
Ho due omomorfismi,
li compongo:

$$\psi : G_1 \underset{\varphi}{\to} G_2 \underset{\pi}{\to} G_2/H_2.$$

Studia il $\ker(\psi)$
$\ker(\psi) := \{g \in G_1 | \psi(g) = H_2\} = \{g \in G_1 | \varphi(g)H_2 = H_2\}$
$ker(\psi) = \{g \in G | \varphi(g) \in H_2\} = \varphi^{-1}(H_2)$
Quindi $\varphi^{-1}(H_2)$ è il nucleo di un omomorfismo $\psi : G_1 \to G_2/H_2$ e dunque $\varphi^{-1}(H_2) \trianglelefteq G_1$

**Esercizio**
Sia $\varphi : G_1 \to G_2$ omomorfismo dei gruppi
$ker\varphi = \{g \in G_1 | \varphi(g) = e_2\}$
Dimostrare che
$\varphi$ è iniettivo $\Leftrightarrow ker(\varphi) = \{e_1\}$
soluzione:
supponiamo che $ker(\varphi) = \{e_1\}$
Allora dati $g, h \in G_1$ t.c $\varphi(g) = \varphi(h)$
dobbiamo mostrare che $g = h$
moltiplico per $\varphi(h)^{-1}$

$$\Rightarrow \varphi(h)^{-1} * \varphi(g) = e_2$$
$$\Rightarrow \varphi(h^{-1}) * \varphi(g) = e_2$$
$$\Rightarrow \varphi(h^{-1} \cdot g) = e_2$$
$$\Rightarrow h^{-1} \cdot g \in ker\varphi$$
$$\Rightarrow h^{-1} \cdot g = e_1$$
$$\Rightarrow g = h$$

Il viceversa è lasciato al lettore come esercizio
**Osservazione:**
Se $\varphi : G_1 \to G_2$
omomorfismo di gruppi
$H_2 = \{e_2\} \trianglelefteq G_2$
l'esercizio (2) ci dice che $\ker(\varphi) = \varphi^{-1}(\{e_2\}) \trianglelefteq G_1$
**Osservazione**
Dalla parte (1) segue che
$H_1 \leq G_1 \Rightarrow \varphi(H_1) \leq G_2$
Quindi se scelgo $H_1 = G_1 \leq G_1$
$\Rightarrow Im(\varphi) = \varphi(G_1) \leq G_2$

**Lemma 1**
*$(G, \cdot)$ gruppo*
*$N \trianglelefteq G, H \trianglelefteq G$ sottogruppi normali*
*$\pi : G \to G/N$*
*Allora $\pi(H) = \pi(HN)$*

**Dimostrazione**
*$H \subseteq HN$ poiché $e \in N$ ogni elemento di $H$ lo scrivo come lui stesso $e \Rightarrow$ $\pi(H) \subseteq \pi(HN)$*
*Viceversa dimostriamo che $\pi(HN) \subseteq \pi(H)$*
*infatti:*
$\forall h \in H \quad \forall n \in N$

$\pi(hn) = \pi(h)\pi(n)$ *(omomorfismo)*
$n \in N$
$\Rightarrow \pi(n) = N \rightarrow \pi(h)\pi(e) = \pi(ne)$
$\pi(e) = N \quad = \pi(n) \in \pi H$ □

**Lemma 2**
$(G, \cdot)$ *gruppo*
$\cdot H \trianglelefteq G$
$\cdot N \trianglelefteq G$
$\cdot \pi \rightarrow G/N$
*Allora:*
1)$\pi^{-1}(\pi(H)) = HN$
2) *se* $N \subseteq H \rightarrow \pi^{-1}(\pi(H)) = N$
3)$\bar{H} \leq G/N \rightarrow \pi(\pi^{-1}(\bar{H})) = \bar{H}$

**Dimostrazione** (1)
$\pi^{-1}(\pi(H)) =?$
*osserviamo che dal lemma 1*
$\pi(H) = \pi(HN) = HN$
*dato che* $\pi(hn) = \pi(h)\pi(n) = hn$
$\Rightarrow \pi^{-1}(\pi(H)) = \pi^{-1}(\pi(HN)) = \pi^{-1}(HN) \supseteq HN$
*Resta da verificare che* $\pi^{-1}(\pi(H)) \subseteq HN$

$$\begin{aligned}
\pi^{-1}(\pi(H)) &:= \{g \in G | \pi(g) \in \pi(H)\} \\
&= \{g \in G | \exists g \in H : \pi(g) = \pi(h)\} \\
&= \{g \in G | \exists h \in H : \pi(h)^{-1}\pi(g) = N\} \ N = \text{elemento neutro in } G \\
&= \{g \in G | \exists h \in H : \pi(hg) = N\} \\
&= \{g \in G | \exists h \in H : h^{-1}g \in N\} \\
&= \{g \in G | \exists h \in H : g \in hN \acute{r} brace \subseteq HN
\end{aligned}$$

*segue (1)* □

**Dimostrazione** (2)
*È un caso particolare del punto 1, infatti se*

$$N \subset H \Rightarrow HN = H.$$

□

**Dimostrazione** (3)
*Segue dal fatto che* $\pi$ *è un omomorfismo suriettivo*

$$\pi(\pi^{-1}(\bar{H})) = \pi(G) \cap \bar{H} = \bar{H}.$$

□

**Teorema 5**
$(G,\cdot)$, $n \trianglelefteq G$
*Allora esistono due corrispondenze biunivoche*

$$\{\textit{sottogruppi } H \leq G \;\; t.c. \;\; N \supseteq H\} \to \{\textit{sottogruppi di } G/N\}$$
$$H \to \pi(H)$$
$$\pi^{-1} \leftarrow \bar{H}$$
$$\{ \textit{ sottogruppi normali } H \trianglelefteq G \; t.c \; N \subseteq H\} \to \{ \textit{ sottogruppi normali } G/N\}$$
$$H \to \pi(H)$$
$$\pi^{-1}(\bar{H}) \to \bar{H}$$

**Dimostrazione**
*Il lemma 2 (punti 2 e 3) garantisce che le due applicazioni* $H \to \pi(H)$ $\pi^{-1}(H) \to \bar{H}$
*sono una l'inversa dell'altra* □
**Osservazione:**
Per la seconda corrispondenza osserviamo che per la suriettività di $\pi$ e l'esercizio di oggi

$$H \trianglelefteq G \to \pi(H) \trianglelefteq G/N.$$

**Teorema 6** (Teorema di omomorfismo)
$\varphi : G_1 \to G_2$ *omomorfismo*
$\cdot N \trianglelefteq G_1$
$\pi : G_1 \to G/N$
*Allora:*
*1) esiste unico omomorfismo*
$\bar{G}/N \to G_2$
*t.c.* $\bar{\varphi} \circ \pi = \varphi$

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \exists!\bar{\varphi}} & \\ G_1/N & & \end{array}$$

*2)* $Im(\bar{\varphi}) = Im(\varphi)$
*3)* $\bar{\varphi}$ *è iniettivo* $\Leftrightarrow ker\varphi = N$

**Dimostrazione**
*La condizione* $\bar{\varphi} \cdot \pi = \varphi$
*Significa*
$\forall g \in G_1$ *si ha*
$\bar{\varphi} \cdot \pi(g) = \varphi(g)$
*ovvero*

$\bar{\varphi}(gN) = \varphi(g)$
*Dobbiamo verificare:*
$\cdot$ *Unicità (segue da* $\bar{\varphi} \cdot \pi = \varphi$*)*
$\cdot\bar{\varphi}$ *è ben definita*
$\cdot\bar{\varphi}$ *è un omomorfismo*
*significa che se* $gN = fN$ *per qualche* $g, f \in G_1$*, allora* $\varphi(g) = \varphi(f)$
*Verifichiamo:*
$gN = fN \to g \equiv f mod N$
$\Rightarrow \exists n \in N$ *t.c.* $g^{-1}f = n$
$\Rightarrow f = gn \Rightarrow \varphi(f) = \varphi(gn)$
$\Rightarrow \varphi(f) = \varphi(g)\varphi(n) = \varphi(g)$
*dato che* $\varphi(n) = e_2$ *ovvero* $N \subseteq \ker\varphi$
***Mostriamo adesso che*** $\bar{\varphi}$ ***è un omomorfismo***
*Significa che* $\forall f, g \in G$

$$\bar{\varphi}((fN) \cdot (gN)) = \bar{\varphi}(fN) \cdot \bar{\varphi}(gN).$$

*Per definizione*

$$\bar{\varphi}((fN)(gN)) = \bar{\varphi}(fgN) = \varphi(fg) = \varphi(f)\varphi(g).$$

2)$\bar{\varphi} \circ \pi = \varphi$
*dalla suriettività del* $\pi$ *segue che* $Im(\bar{\varphi}) = Im(\varphi)$
3)$\bar{\varphi}$ *è iniettivo* $\Leftrightarrow ker\bar{\varphi} = \{N\}$
$ker\bar{\varphi} = \{gN \in G_1/N | \bar{\varphi}(gN) = e_2\}$
$= \{gN \in G_1/N | \varphi(g) = e_2\}$
$= \{gN \in G_1/N | g \in ker(\varphi)\}$ □

**Corollario 3**
$(G, \cdot)$, $N \trianglelefteq G$
*Allora esiste una corrispondenza biunivoca*

$$\{omomorfismi\ \varphi : G \to G'\ t.c.\ N \subseteq ker(\varphi)\} \to \{omomorfismi\ G/N \to G'\}$$
$$\varphi \to \bar{\varphi}$$
$$\pi \leftarrow \bar{\varphi}$$

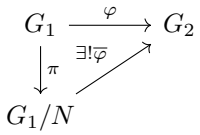
**Dimostrazione**
*basta osservare che*
*dato* $\bar{\varphi} : G/N \to G'$ *la composizione*
$\bar{\varphi} \circ \pi : G \to G'$ *è un omomorfismo*
*tale che* $ker(\bar{\varphi} \circ \pi) \supseteq N$
*segue* $\pi(N) = N$ *che è l'elemento neutro di* $G/N$
$\Rightarrow \bar{\varphi} \circ \pi(N) = e'$ *che è l'elemento neutro di* $G'$

□

**Definizione 17**
$\varphi : G_1 \to G_2$
*omomorfismo si dice isomorfismo se è invertibile*

**Teorema 7** (Primo teorema di isomorfismo)
$\varphi : G_1 \to G_2$
*Allora:*
$Im(\varphi) \cong G_1/ker(\varphi)$
*Dove* $\cong$ *(isomorfo) significa che esiste un isomorfismo tra i due gruppi*

**Dimostrazione**




*scelgo* $N - ker\varphi$
*il teorema di isomorfismo fornisce un omomorfismo iniettivo*

$$\bar{\varphi} : G_1/\ker\varphi \to G_2.$$

*Allora mi restringo all'immagine di* $\bar{\varphi}$ *così diventa suriettiva*

$$G/ker\varphi \cong Im(\bar{\varphi}) \cong Im(\varphi).$$

*la prima tramite* $\bar{\varphi}$ *la seconda per il teorema di isomorfismo*

□

**Applicazione:**
det: $GL_n(\mathbb{K}) \to (\mathbb{K}^*, \cdot) = (\mathbb{K} \setminus \{0\}, \cdot)$
$\ker(det) = SL_n(\mathbb{K})$ matrici con det 1
$\Rightarrow GL_n(\mathbb{K})/SL_n(\mathbb{K}) \cong (\mathbb{K}^*, \cdot)$

## 3.6 Teoremi di isomorfismo

**Teorema 8** (Secondo teorema di isomorfismo)
$(G, \cdot)$ *gruppo*
$H, N \trianglelefteq G$ *tali che* $N \subseteq H$ *Allora*

1. $H/M \trianglelefteq G/N$
2. $G/N/H/N \cong G/H$

**Dimostrazione**


$\pi_H$ *proiezione sul quoziente* $H$

$N \subseteq H = ker(\varphi)$
*Inoltre* $Im(\bar{\varphi}) = Im(\varphi) = G/H$
***Idea:*** *applicare il primo teorema di isomorfismo*
*suriettiva* $\bar{\varphi} : G/N \to G/H$
*basta quindi dimostrare che* $ker(\bar{\varphi}) = H/N$
*Studiamo*

$$ker(\bar{\varphi}) = \{gN \in G/N | \bar{\varphi}(gN) = H\}.$$
$$\{gN \in G/N | gH = H\}.$$
$$\{gN \in G/N | g \in H\} = H/N.$$

□

**Corollario 4**
*In* $(\mathbb{Z}, +)$ *gruppo abeliano*
$a, n \in \mathbb{Z}$ *interi non nulli*
*Denotiamo con*

$$[a] = a + (n) \in \mathbb{Z}/(n) = \{[0], [1], [2], \ldots, [n-1]\}.$$

*Allora* $ord_{\mathbb{Z}/(n)}([a]) = \frac{n}{MCD(a,n)}$

**Nota:**
se $MCD(n, a) = 1$ allora a genera il gruppo ciclico $\mathbb{Z}/(n)$
**Dimostrazione**
*Consideriamo* $G = \mathbb{Z}$ $H = (a) + (n)$ $N = (n)$
*Dal II Teorema di isomorfismo*

$$\mathbb{Z}/(n) \Big/ ([a]) \cong \mathbb{Z}/(n) \Big/ (a) + (n)/(n) \cong G/N \Big/ H/N \cong G/N \cong \mathbb{Z}/(MCD(a, n)).$$

□

Confrontiamo le cardinalità

$$MCD(a,n) = |\mathbb{Z}/(MCD(a,n))|.$$
$$= |{}^{\mathbb{Z}/(n)}\Big/_{([a])}|$$

.

$$\frac{|Z/(n)|}{([a])} = \frac{n}{ord([a])}.$$
$$ord([a]) = \frac{n}{MCD(a,n)}.$$

**Lemma 3**
*$a, bg \in Z$ non nulli*
*tali che $a|b$ (allora $(b) \subseteq (a)$*
*Allora*

$$|(a)/(b)| = \frac{b}{a}.$$

**Dimostrazione**
*Studiamo $(a)/(b)$*
*Per definizione è l'insieme dei laterali*

$$(a)/(b) = \{ta + (b) | t \in \mathbb{Z}\}.$$

*dobbiamo capire quanti laterali distinti esistono*
*Dati $t, s \in \mathbb{Z}$ tali che*

$$ta + (b) = sa + (b).$$
$$\Leftrightarrow ta \equiv sa \ mod(b).$$
$$\Leftrightarrow -ta + sa \in (b).$$

*Allora*

$$(a)/(b) = \{ta + (b) | tt \in \{1, \ldots, \frac{b}{a}\}\}.$$

□

**Teorema 9** (III teorema di isomorfismo)
$(G, \cdot)$ *gruppo*

- $N \trianglelefteq G$
- $H \leq G$

*Allora*

1. $H \cap N \trianglelefteq H$
2. $H/_{H \cap N} \cong HN/N$

**Dimostrazione**
$\pi_N : G \to G/N$
$g \to gN$
*consideriamo la restrizione*

$$\begin{gathered}\pi_N|_H : H \to G/H \\ h \to hN \\ ker(\pi_N|_H) = \{h \in H | \pi_N|_H(h) = N\} \\ = \{h \in H | hN = N\} \\ = \{h \in H | h \in N\} \\ = H \cap N\end{gathered}$$

*Deduciamo che* $H \cap N \trianglelefteq N$
*Idea: Applicare il I teorema di isomorfismo all'omomorfismo*

$$\varphi = \pi_N|_H : H \to G/N.$$

*Avremo* $Im(\varphi) \cong H/ker(\varphi) = H/H \cap N$
*Studiamo* $Im(\varphi)$

$$Im(\varphi) = Im(\pi_N|_H) = \pi_N(H) = \pi_N(HN) = HN/N.$$

*Il penultimo passaggio deriva da un lemma già visto a lezione* □

**Corollario 5**
*$a, b \in \mathbb{Z}$ non nulli*
*Allora* $mcm(a,b) = \frac{ab}{MCD(a,b)}$

**Dimostrazione**
$G = \mathbb{Z}$
$H = (a)$
$N = (b)$
$H + N = (MCD(a,b))$
$H \cap N = (mcm(a,b))$
*Dal III teorema di isomorfismo*

$$(a) \Big/ (mcm(a,b)) \cong H /_{H \cap N} \cong HN /_N \cong (MCD(a,b)) \Big/ (b).$$

*Confrontiamo la cardinalità*
*Per il lemma*

$$\frac{mcm(a,b)}{a} = |(a)(mcm(a,b))| = |(MCD(a,b)) \Big/ (b)| = \frac{b}{MCD(a,b)}.$$

*Quindi*

$$mcm(a,b) = \frac{ab}{MCD(a,b)}.$$

□

## 3.7 Classificazione di gruppi di ordine "piccolo" a meno di isomorfismo

**Ordine 1**
Se $|G| = 1 \quad \Rightarrow \quad G = \{e\}$
**Ordine p primo:**
Abbiamo mostrato che se $|G| = p$ allora $G$ non ammette sottogruppi non banali
Sia $g \in G$ tale che $g \neq e \Rightarrow ord(g) = p \ \Rightarrow G =< g >$

$$\varphi : G \to G_p =< p >$$
$$g \to p$$

**Obiettivo:** classificare a meno di isomorfismo i gruppi di ordine 4 e di ordine 6

**Definizione 18** (Klein,1884)
*Il gruppo di Klein, $K_4$ è il gruppo delle isometrie del piano che preservano un rettangolo fissato.*

**Esercizio**
Verificare che $K_4 = \{id, \rho, \sigma, \rho\sigma\}$
dove $\rho$ = rotazione di angolo $\pi$
e dove $\sigma$ = riflessione rispetto ad un lato
**Osservazione**
tutti gli elementi in $K_4$ hanno ordine $\leq 2$ Quindi $K_4 \neq C_4$

**Notazione 5**
*Dato che* $K_4 =< \rho, \sigma >$
*denoteremo anche*

$$K_4 = D_2 \text{ (gruppo diedrale).}$$

**Esercizio**
$(G, \cdot)$ gruppo in cui ogni elemento ha ordine $\leq 2$ (equivalentemente ogni elemento è inverso di se stesso)
1) Dimostrare che $G$ è abeliano
2) Se $|G| = 4$ dimostrare che $G \cong K_4$
**Svolgimento** 1) Dati $f, g \in G$
$fg = (fg)^{-1} = g^{-1}f^{-1} = gf$
2) Sia $|G| = 4$
Scelgo $g, f \in G$ distinti tali che $\begin{cases} g \neq e \\ f \neq e \end{cases}$
Considero $H =< g, h >$
Per Lagrange
$H \geq 3$
$\Rightarrow H = H$
$\Rightarrow G = \{e, f, g, fg\}$
abeliano
Costruisco l'isomorfismo esplicito con $K_4$

$$\varphi : G \to K_4 =< \rho, \sigma >$$
$$e \to e$$
$$f \to \rho$$
$$g \to \sigma$$
$$fg \to \rho\sigma$$

che è chiaramente biunivoca ed è un omomorfismo $\Rightarrow \varphi$ è un isomorfismo

## 3.8 Teoremi sulla cardinalità dei gruppi

**Teorema 10**
*$(G, \cdot)$ gruppo. Se $|G| = 6$ allora*
*$G \cong C_6$ (abeliano) oppure $G \cong D_3$ (non abeliano)*

**Dimostrazione**
*Se $G$ contiene un elemento di ordine 6 allora $G \cong C_6$*
*Se invece $G$ non contiene elementi di ordine 6, per l'esercizio (2) esistono elementi $r, s \in G$ t.c. $ord(r) = 3$ e $ord(s) = 2$*
*Definisco:*

$$G :=< r >= \{e, r, r^2\} \qquad k :=< s >= \{e, s\}.$$
$$H \cap K = \{e\}.$$
$$|HK| = \frac{|H||K|}{|H \cap K|} = 6 = |KH|.$$

$\Rightarrow HK = G = KH$
***Esplicitamente:***
$HK = \{e, r, r^2, s, rs, r^2 s\}$
$KH = \{e, r, r^2, s, sr, sr^2\}$
***Dobbiamo considerare 2 casi:***
*I caso: $rs = sr$*
*studiamo $ord(rs)$*
$(rs)^2 = r^2 s^2 = r^2 \neq e \Rightarrow ord(rs) \neq 2$
$(rs)^3 = r^3 s^3 = s^3 = s \neq e$
***Per Lagrange***
*necessariamente $ord(rs) = 6$*
$\Rightarrow G$ *è cicliclo* $\Rightarrow$ *Assurdo*
*II caso:* $\begin{cases} rs = sr^2 \\ r^2 s = sr \end{cases}$
*Costruiamo l'isomorfismo*

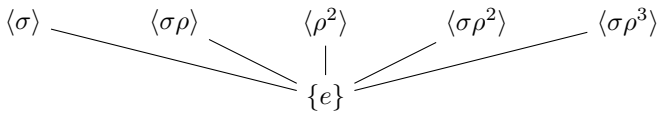
$$G \to D_3 :=< \rho, \sigma >$$
$$e \to Id$$
$$r \to \rho$$
$$r^2 \to \rho^2$$
$$s \to \sigma$$
$$sr \to \sigma\rho$$

□

**Definizione 19**
*Dato un gruppo $(G, \cdot)$ il reticolo dei sottogruppi $T_G$ è un grafo definito come*

- *esiste un vertice in $T_G$ per ogni sottogruppo $H \leq G$*
- *esiste un lato $H_1$ — $H_2$ se e solo se $H_1 \subseteq H_2$ e $\nexists K \leq G$ t.c. $H_1 \subset K \subset H_2$*

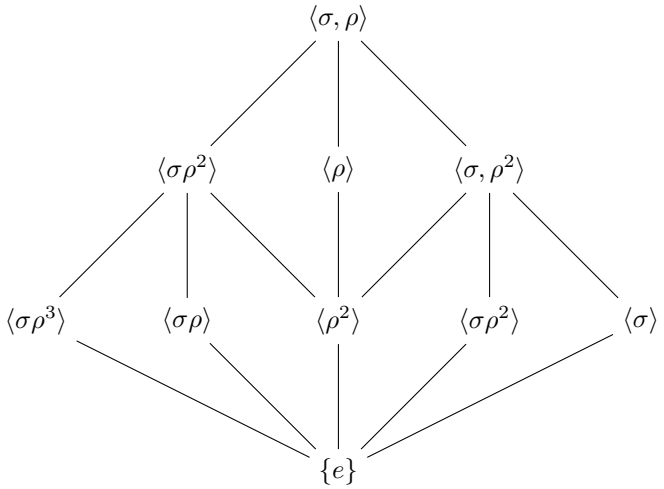
**Esempio:**
$T_{D_4}$
Ricordiamo che $D_4 =< \sigma, \rho >$ $\quad |D_4| = 8$
studiamo i sottogruppi di $D_4$
**ordine 1:** L'unico sottogruppo è $H = \{e\}$
**ordine 2:** Sono tutti e soli quelli generati da un elemento di ordine 2 in $D_4$



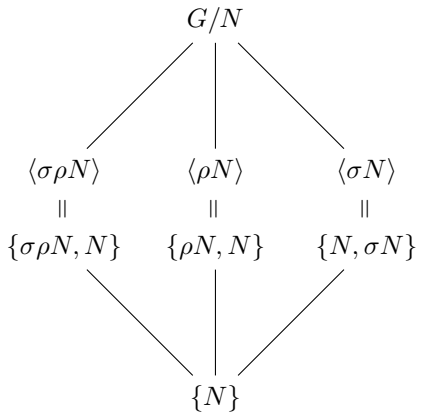

**ordine 4:** per la classificazione sono ciclici ($C_4$) oppure di Klein ($K_4$) altre al ciclico $< p >$ esistono altri sottogruppi

$$\langle \rho^2, \sigma \rangle = \{e, \sigma, \rho^2, \sigma\rho^2\}.$$
$$\rangle \rho^2, \sigma\rho \rangle = \{e, \sigma\rho, \rho^2, \sigma\rho^3\}.$$

Ordine 8: $D_4$



**Esempio:**
$G = D_4$
$N =< \rho^2 > \trianglelefteq G$
Vogliamo $T_{G/N}$
studiamo $G/N = D_4/ < rho^2 >$
$|G/N| = [G : N] = \dfrac{|G|}{|N|} = \dfrac{8}{2} = 4$
chi sono i laterali?
$IdN = N < \rho^2 >= \{Id, \rho^2\}$
$\rho N = \{\rho, \rho^3\}$
$\sigma N = \{\sigma, \sigma\rho^2\}$
$\sigma\rho N = \{\sigma\rho, \sigma\rho^3\}$
**Ricordo:**
Abbiamo una corrispondenza biunivoca tr ai sottogruppi di $G/N$ e i sottogruppi di $G$ contenenti $N$.




**Obiettivo: studiare** $S_n$
**Ricordo:**
$X := \{1, \ldots, n\}$
$S_n := S_X = \{$ applicazioni biunivoche $X \to X\}$
$S_n$ gruppo di permutazioni
**Osservazione:**
$|S_n| = n!$
**Osservazione:**
se $n = 3 \to |S_3| = 6$
$\Rightarrow S_3 \cong D_3$
**Osservazione**
$S_n \cong D_n \quad \forall n \geq 4$
Infatti $n! > 2n \quad \forall n \geq 4$

## 3.9 notazioni in $s_n$

$\sigma = (123)(47)$
$\tau = (23456)$
$\sigma\tau = \sigma \circ \tau = (123)(46)(23456)(12)(36)(45)$
$\tau \circ \sigma = (23456)(123)(46) = (13)(24)(56)$

**Lemma 4**
*Data $\sigma \in S_n$ allora $\sigma$ partizione $X = \{1, \dots, n\}$ in sottoinsiemi permutati ciclicamente e disgiunti tra loro*

**Dimostrazione**
*Definiamo la relazione d'equivalenza $i \sim j \Leftrightarrow \exists k \in \mathbb{Z}$ t.c. $\sigma^k(i) = j$*
*È una relazione d'equivalenza!*
***studiamo le classi di equivalenza***
*fissato $i \in X$*
*la sua clase*

$$X_i = \{\sigma^k(i) | k \in \mathbb{Z}\} \subseteq X.$$

*quindi $\exists \ \ k_1, k_2 \in \mathbb{Z}$ distinti t.c. $\sigma^{k_1}(i) = \sigma^{k_2}(i)$*
$\Rightarrow i = \sigma^{k_2 - k_1}(i)$
$\Rightarrow m := min\{k \in \mathbb{Z}_{>0} | \sigma^k(i) = i\}$
$\Rightarrow X_i = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{n-1}(i)\}$ □

**Proposizione 8**
*Data $\sigma \in S_n$, allora $\sigma$ può essere rappresentata come composizione di cicli disgiunti*

**Obiettivo:** Definire un omomorfismo

$$sgn : S_n \to (\{\pm 1\}, \cdot).$$

Questo ci permetterà di definire il sottogruppo alterno $A_n \trianglelefteq S_n$
$A_n := ker(sgn)$

**Notazione 6**
*Dato un polinomio*
$f \in \mathbb{Q}[x_1, \dots, x_n]$
*e data* $\sigma \in S_n$
*Definiamo*

$$f^\sigma(x_1, \dots, x_n) := f(x_{\sigma(1),\dots,x_{\sigma(n)}\}}.$$

*Ci sta un polinomio speciale:*

- $\Delta(x_1, \dots, x_n) = \prod_{1 \le i < j \le n}(x_i - x_j)$
- $\Delta^\sigma(x_1, \dots, x_n) = \prod_{1 \le i < j \le n}(x_{\sigma(i)} - x_{\sigma(j)})$

**Definizione 20**
$\sigma \in S_n$
$sgn(\sigma) := \frac{\Delta^\sigma}{\Delta} \in \{\pm 1\}$

**Osservazione**
$sgn : S_n \to \{\pm 1\}$
è un omomorfismo

**Dimostrazione**
*In generale*
$(f^\sigma)^\tau = f^{\sigma\tau}$
$(fg)^\sigma = f^\sigma g^\sigma$

$$sgn(\sigma\tau) = \frac{\Delta^{\delta\tau}}{\Delta} = \frac{((\Delta^\sigma)^\tau)}{\Delta} = \frac{\Delta^\sigma}{\Delta}\frac{(\Delta^\sigma)^\tau}{\Delta^\sigma} = sgn(\sigma)\frac{\Delta^\tau}{\Delta} = sgn(\delta)sgn(\tau) \qquad \square$$

## 3.10 Il sottogruppo alterno

**Definizione 21**
*Sia* $n \in \mathbb{Z}$ *un intero positivo. Il* sottogruppo alterno $A_n \trianglelefteq S_n$ *è definito da*

$$A_n := \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}.$$

*Una permutazione* $\sigma \in S_n$ *si dice* pari *se* $\sigma \in A_n$ *e si dice* dispari *altrimenti.*

**Osservazione**
Dal momento che $\mathrm{sgn} : S_n \to \{\pm 1\}$ è un omomorfismo di gruppi per l'osservazione precedente, abbiamo che $A_n = \ker(\mathrm{sgn}) \le S_n$, ed è un sottogruppo normale (Esercizio passato).

**Proposizione 9**
*Sia $n \geq 2$ un intero. Allora:*

- $[S_n : A_n] = 2$,
- $[H : A_n \cap H] = 2$ *per ogni sottogruppo* $H \leq S_n$ *tale che* $H \not\subseteq A_n$.

**Dimostrazione**
*Chiaramente è sufficiente dimostrare la seconda parte dell'enunciato. Sia dunque* $H \leq S_n$. *Due permutazioni* $\sigma, \tau \in S_n$ *sono congruenti modulo* $A_n$ *se e solo se* $\sigma^{-1}\tau \in A_n$, *ovvero se e solo se*

$$\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) = 1,$$

*dove abbiamo sfruttato l'osservazione anche per dedurre* $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$. *Pertanto esistono solo due laterali sinistri dati da*

$$H \cap A_n \quad e \quad H \setminus (H \cap A_n) = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = -1\}.$$

□

**Esercizio 7.4** (Sottogruppi di $A_4$).
Consideriamo il sottogruppo alterno $A_4 \trianglelefteq S_4$.

1. Determinare tutti gli elementi di $A_4$.
2. Dimostrare che il sottoinsieme $V := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \subseteq A_4$ è un sottogruppo di $A_4$ isomorfo al gruppo di Klein $K_4$.
3. Dimostrare che $A_4$ non contiene sottogruppi di ordine 6.

**Soluzione.** Procediamo per passi.

1. Dalla Proposizione 7.3 segue che $|A_4| = 12$ poiché $|S_4| = 4! = 24$. I suoi elementi sono:

   - ordine 1: id,
   - ordine 2: $(12)(34), (13)(24), (14)(23)$,
   - ordine 3: $(123), (132), (124), (142), (134), (143), (234), (243)$.

   Il fatto che gli otto 3-cicli siano elementi di $A_4$ segue dall'Esercizio 6.21.

2. Osserviamo che $V$ è chiuso rispetto all'operazione poiché

   $$(12)(34) \cdot (13)(24) = (14)(23),$$
   $$(13)(24) \cdot (14)(23) = (12)(34),$$
   $$(14)(23) \cdot (12)(34) = (13)(24).$$

   Dunque $V$ è un sottogruppo. Inoltre, gli elementi di $V$ hanno tutti ordine 1 o 2. Dalla classificazione dei gruppi di ordine 4 si ha dunque $V \cong K_4$ (si veda l'Esercizio 6.4).

3. Dal momento che $A_4$ non contiene elementi di ordine 6 non può contenere sottogruppi isomorfi a $C_6$. Dunque un sottogruppo $H \leq A_4$ di ordine 6 è necessariamente isomorfo a $D_3$ (si veda Teorema 6.7); pertanto $H$ contiene 3 elementi di ordine 2 e due elementi di ordine 3. Ne segue che $V \subset H$, da cui l'assurdo per il Teorema 2.14 di Lagrange.

**Esercizio 7.5** (Sottogruppi di $S_4$). Consideriamo il gruppo simmetrico $S_4$.

1. Determinare il numero di sottogruppi di $S_4$ di ordine 2 e di ordine 3.
2. Determinare tutti i sottogruppi di $S_4$ non ciclici e di ordine 4.
3. Determinare tutti i sottogruppi di $S_4$ di ordine 6.
4. Determinare tutti i sottogruppi di $S_4$ di ordine 8.
5. Determinare tutti i sottogruppi di $S_4$ di ordine 12.

**Soluzione.** Procediamo per punti.

1. Ogni sottogruppo di ordine 2 è generato da un elemento di ordine 2; pertanto è sufficiente contare gli elementi di ordine 2 in $S_4$. Abbiamo: $\binom{4}{2} = 6$ trasposizioni e i 3 elementi non banali del sottogruppo $V \subseteq A_4$ (si veda l'Esercizio 7.4). In totale esistono dunque 9 sottogruppi di ordine 2 in $S_4$.

   Ogni sottogruppo di ordine 3 è generato da un elemento di ordine 3; pertanto è sufficiente contare gli elementi di ordine 3 in $S_4$, ovvero i 3-cicli. Questi sono $2 \cdot \binom{4}{3} = 8$, ed esistono 8 sottogruppi di ordine 3 in $S_4$.

2. Sia $H \leq S_4$ un sottogruppo non ciclico tale che $|H| = 4$. Ora, se $H \leq A_4$ abbiamo necessario che $H = V$, poiché $V$ contiene tutti gli elementi di $A_4$ di ordine divide 4. Se invece $H \not\leq A_4$, allora abbiamo $|H \cap A_4| = 2$ per la Proposizione 7.3. Ne deduciamo che $H$ contiene un solo prodotto di trasposizioni disgiunte $(i_1 i_2)(i_3 i_4)$ con $\{i_1, i_2, i_3, i_4\} = \{1, 2, 3, 4\}$ Ne segue necessariamente che

   $$H = \{\mathrm{id}, (i_1 i_2), (i_3 i_4), (i_1 i_2)(i_3 i_4)\}.$$

   poichè il prodotto di un'altra traposizione con l'elemento $(i_1 i_2)(i_3 i_4)$ fornisce come risultato un 4-ciclo. Concludiamo che i sottogruppi non ciclici di oridne 4 di $S_4$ sono

   $$H_1 = \{id, (12), (34), (12)(34)\} \quad H_2 = \{id, (13), (24), (13)(24)\}.$$

   $$H_3 = \{id, (14), (23), (14)(23)\} \quad V = \{id, (12)(34), (13)(24), (14)(23)\}.$$

3. Dal momento che $S_4$ non contiene elementi di ordine 6, non può contenere sottogruppi isomorfi a $C_6$. Dunque un sottogruppo $H \leq S_4$ di ordine 6 è necessariamente isomorfo a $D_3$ (si veda il Teorema 6.7); pertanto $H$ contiene 3 elementi di ordine 2 e 2 elementi di ordine di 3, ovvero $H$ contiene

necessariamente due 3-cicli che saranno uno l'inverso dell'altro. Ora, ricordiamo che dall'Esercizio 7.4 segue che $A_4$ non contiene sottogruppi di ordine 6, dunque $|H \cap A_4| = 3$ per la Proposizione 7.3. Ne deduciamo che i restanti tre elementi di ordine 2 in $H$ devono necessariamente avere segno $-1$, dunque sono trasposizioni.

Si noti infine che la scelta delle trasposizioni da inserire nel sottogruppo $H$ è univocamente determinata dai 3-cicli contenuti in $H$. Infatti, se $(i_1 i_2 i_3) \in H$ allora il prodotto

$$(i_1 i_4)(i_1 i_2 i_3) = (i_1 i_2 i_3 i_4)$$

fornisce un 4-ciclo in $H$, contraddicendo il Corollario 2.15. Ne segue che se $(i_1 i_2 i_3) \in H$, allora

$$H = \{\mathrm{id}, (i_1 i_2), (i_1 i_3), (i_2 i_3), (i_1 i_2 i_3), (i_1 i_3 i_2)\}.$$

I sottogruppi di ordine 6 in $S_4$ sono allora:

$$H_1 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}, \quad H_2 = \{\mathrm{id}, (12), (14), (24), (124), (142)\},$$

$$H_3 = \{\mathrm{id}, (13), (14), (34), (134), (143)\}, \quad H_4 = \{\mathrm{id}, (23), (24), (34), (234), (243)\}.$$

4. Sia $H \leq S_4$ un sottogruppo di ordine 8. Dal momento che $8 \nmid 12$, dalla Proposizione 7.3 deduciamo che $|H \cap A_4| = 4$. Dall'Esercizio 7.4 segue dunque che $V = H \cap A_4$, poiché i 3-cicli contenuti in $A_4$ hanno ordine 3 e non possono dunque appartenere ad $H$ per il Corollario 2.15.

   Supponiamo ora che $H$ contenga una trasposizione $(i_1 i_2) \in H$. Abbiamo

   $$(i_1 i_2)(i_1 i_2)(i_3 i_4) = (i_3 i_4) \in H,$$

   e

   $$(i_1 i_2)(i_1 i_3)(i_2 i_4) = (i_1 i_3 i_2 i_4) \in H,$$

   da cui si deduce che

   $$H = V \cup \{(i_1 i_2), (i_3 i_4), (i_1 i_3 i_2 i_4), (i_1 i_4 i_2 i_3)\}.$$

   D'altra parte, assumendo che $H$ contiene un 4-ciclo, si deduce facilmente che $H$ contiene una trasposizione e dunque $H$ è ancora della forma precedente. Concludiamo che i sottogruppi di ordine 8 di $S_4$ sono:

   $$H_1 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\},$$

   $$H_2 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\},$$

   $$H_3 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (14), (23), (1234), (1342)\}.$$

5. Sia $H \leq S_4$ un sottogruppo di ordine 12. Dalla Proposizione 7.3 deduciamo che

   $$|H \cap A_4| = 6 \quad \text{oppure} \quad |H \cap A_4| = 12.$$

   Dall'Esercizio 7.4 segue dunque che $H = A_4$.

## 3.11 Prodotto diretto tra gruppi

**Definizione 22**
*Siano* $(G_1, \cdot)$, $(G_2, *)$ *gruppi il loro prodotto diretto risulta l'insieme* $(G_1 \times G_2)$ *dotato dell'operazione:*

$$(g_1, g_2) \cdot (f_1, f_2) = (g_1 \cdot f_1, g_2 * f_2) \quad \forall g_1, f_1 \in G_1, \quad \forall g_2, f_2 \in G_2.$$

*e lo indichiamo con* $(G_1 \times G_2)$

**Proposizione 10**
$(G_1 \times G_2, \cdot)$ *è un gruppo*

**Dimostrazione**
*L'associatività segue da quella di* $\cdot$ *e* $*$ *l'elemento neutro è* $(e_1, e_2)$
*l'inverso di* $(g, f)$ *con* $g \in G_1$ *e* $f \in G_2$ *risulta* $(g^{-1}, f^{-1})$ □

**Esercizio**
$(G_1, \cdot)$ e $(G_2, *)$ gruppi
Dimostrare: 1) $|G_1 \times G_2| = |G_1||G_2|$
2) $G_1 \times G_2$ è abeliano se e solo se $G_1$ e $G_2$ sono entrambi abeliani
3) Dati due sottogruppi $H \leq G_1$ e $K \leq G_2 \Rightarrow H \times K \leq G_1 \times G_2$
4) Dati $H \trianglelefteq G_1$ e $K \trianglelefteq G_2 \Rightarrow H \times K \trianglelefteq G_1 \times G_2$
5) Dati $H \trianglelefteq G_1$ e $K \trianglelefteq G_2$

$$G_1/H \times G_2/H \cong G_1 \times G_2 \,/ H \times K\,.$$

**Dimostrazione** (4,5)

$$\begin{array}{ccc} G_1 \times G_2 & \xrightarrow{\varphi} & \frac{G_1}{H} \times \frac{G_2}{K} \\ \downarrow & \overset{\exists!\bar{\varphi}}{\nearrow} & \\ \frac{(G_1 \times G_2)}{ker\varphi} & & \end{array}$$

*dove*

$$\varphi(g_1, g_2) = (g_1 H, g_2 K)$$

*Dal primo teorema di isomorfismo*

$$Im\varphi \cong \frac{G_1 \times G_2}{ker\varphi}.$$

$\cdot \varphi$ *suriettiva poichè* $\pi_H e \pi_K$ *sono suriettive*
$\cdot$ $ker\varphi = \{(g_1, g_2) \in G_1 \times G_2 | \varphi(g_1, g_2) = (H, K)\}$
$= \{(g_1, g_2) | g_1 H = H \text{ e } g_2 K = K\}$
$\{(g_1, g_2) | g_1 \in H, g_2 \in K\} = H \times K$
*quindi* $H \times K \trianglelefteq G_1 \times G_2$

$$\frac{G_1 \times G_2}{H \times K} \cong G_1/H \times G_2/K.$$

□

**Esercizio (importante)**
$(G_1, \cdot)$ e $(G_2, *)$ gruppi
$H, K \trianglelefteq G_1 \times G_2$ tali che $H \cap K = \{\tilde{e}\}$ dove $\tilde{e} = (e_1, e_2)$
Dimostrare che ogni elemento di $H$ commuta con ogni elemento di K.
**Dimsotrazione**
Consideriamo $h \in H, k \in K$ e verifichiamo che $hk = kh$
**Idea:**
Dimostrare che $hkh^{-1}k^{-1} = e$
Data l'ipotesi $H \cap K = \{e\}$ è sufficiente dimostrare che $hkh^{-1}k^{-1} \in H \cap K$
**Sfruttare la normalità di H e K**
**Esercizio**
$(G_1, \cdot)$, $(G_2, *)$ gruppi

$$H := G_1 \times \{e_2\} = \{(g, e_2) | g \in G_1\} \leq G_1 \times G_2.$$

$$H := e_1 \times G_2\} = \{(e_1, g) | g \in G_2\} \leq G_1 \times G_2.$$

Verificare che $H$ e $K$ soddisfano le ipotesi dell'esercizio precedente

**Definizione 23**
*$(G, \cdot)$ gruppo $H, K \leq G$*
*Diremo che $G$ è*
*Prodotto diretto interno di $H$ e $K$ se:*
*1) $H, K \trianglelefteq G$*
*2) $H \cap K = \{e\}$*
*3) $HK = G$*

**Teorema 11**
*$(G, \cdot)$ gruppo*
*1) Se $G$ è un prodotto diretto interno di $H, K \leq G$ allora $G \cong H \times K$*
*2) Se $G \cong G_1 \times G_2$ allora esistono $H, K \leq G$ tali che $G$ sia prodotto diretto interno di $H$ e $K$ e inoltre $H \cong G_1, K \cong G_2$*

**Dimostrazione** (1)
$\psi : H \times K \to G$
$(h, k) \to hk$
*Dobbiamo verificare che $\psi$ sia isomorfismo*
*1)$\psi$ è suriettiva perchè ogni elemento di $G$ si scrive come $hk$ quindi $Im(\psi) = G$*

*2)È anche iniettiva infatti se* $\psi(g_1, k_1) = \psi(h_2, k_1)$

$$\Rightarrow h_1 k_1 = h_2 k_2$$
$$\Rightarrow h_2^{-1} h_1 k_1 = k_2$$
$$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K = \{e\}$$
$$\Rightarrow \begin{cases} h_2^{-1} h_1 = e \\ k_2 k_1^{-1} = e \end{cases} \Rightarrow (h_1, k_1) = (h_2, k_2)$$
$$\Rightarrow \psi \text{ iniettiva}$$

*Bisogna in fine dimostrare che* $\psi$ *è un omomorfismo, ovvero che*

$$\psi(h_1 h_2, k_1 k_2) = \psi(h_1, k_1)\psi(h_2, k_2).$$

*dunque*

$$\psi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 (h_2 k_1) k_2 = h_1 (k_1 h_2) k_2 = \psi(h_1, k_1)\psi(h_2, k_2).$$

*Ricordando che tutti gli elementi di* $H$ *commutano con quelli di* $K$ □

**Dimostrazione** (2)
*Per ipotesi esiste un isomorfismo* $\varphi : G_1 \times G_2 \to G$
$(g_1, g_2) \to \varphi(g_1, g_2)$
*considero*
$H := \varphi(G_1, \{e_2\})$
$K := \varphi(\{e_1\} \times G_2)$
*Abbiamo visto che*
$\cdot G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2 \to H \trianglelefteq G$
$\cdot \{e_1\} \times G_2 \trianglelefteq G_1 \times G_2 \to K \trianglelefteq G$

$$H \cap K = \varphi((G_1 \times \{e_2\}) \cap (\{e_1\} \times G_2)) = \{e\}.$$

$$HK = \varphi((G_1 \times \{e_2\})(\{e_1\} \times G_2)) = G.$$

*Le opportune restrizioni di* $\varphi$ *forniscono gli isomorfismi*

$$H \cong G_1 \times \{e_2\} \cong G_1.$$

$$K \cong \{e_1\} \times G_2 \cong G_2.$$

□

**Esempio:**
Siano $n, m \in \mathbb{Z}_{>0}$ t.c.
$MCD(n, m) = 1$
Consideriamo $C_{nm} =< p >$

dove $ord(p) = nm$
Considero

$$H =< \rho^m > \quad K =< \rho^n > .$$

$|H| = ord(\rho^m) = n$
$|K| = ord(\rho^n) = m$
Verifichiamo che

$$C_{nm} \cong H \times K.$$

Dobbiamo mostrare:

1. $H, KC_{nm}$
2. $H \cap K = \{Id\}$
3. $HK = C_{nm}$

1) $C_{nm}$ abeliano, quindi $H, KC_{nm}$
2) $H \cap K =?$
sia $\rho^h \in H \cap K$
Allora

$$\begin{cases} \rho^h = (\rho^m)^{t_1} \\ \rho^h = (\rho^h)^{t_2} \end{cases} \qquad \begin{cases} m|h \\ n|h \end{cases} .$$

Ma $h \geq mcm(m,n) = mn \Rightarrow h = mn \Rightarrow \rho^h = Id \Rightarrow H \cap K = \{Id\}$

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{nm}{1}.$$

$\Rightarrow HK$ è tutto chiuso quindi è $C_{nm}$

**Definizione 24** (Automorfismo)
$(G, \cdot)$ *gruppo*
*Un automorfismo di* $G$ *è un isomorfismo* $\varphi : G \to G$

**Osservazione**
$(G, \cdot)$ gruppo
$\Rightarrow Aut(G) = \{$automorfismi di $G\}$
è un gruppo (rispetto alla composizione)
**Esempio:**
$(G, \cdot)$ gruppo
Fissato $g \in G$ definiamo
$I_g : G \to G$

$f \to gfg^{-1}$

$I_g$ si dice automorfismo interno
$Int(G) = \{$automorfismi interni di $G\}$

**Proposizione 11**
$Int(G) \trianglelefteq Aut(G)$

**Dimostrazione**
$If_G = I_e \in Int(G)$
*dato* $g \in G$ *allora*

$$I_{g^{-1}} = I_g^{-1} \to \begin{cases} I_g \in Aut(G) \\ Int(G) \text{ è chiuso rispetto agli inversi} \end{cases} .$$

$I_{g_2} \cdot I_{g_1}(f) = g_3 g_2 f g_2^{-1} g_2^{-1} = (g_2 g_1) f (g_2 g_1)^{-1} = I_{g_2 g_1}(f)$
$I_{g_2} \cdot I_{g_1} = I_{g_2 g_1}$
*quindi* $Int(G)$ *è chiuso rispetto alla composizione*
*Quindi* $Int(G) \leq Aut(G)$
*Basta verificare che:*
$\varphi \circ Int(G) \circ \varphi^{-1} \subseteq Int(G) \quad \forall \varphi \in Aut(G)$
*ovvero dato* $g \in G$

$$\varphi \circ I_g \circ \varphi^{-1} \in Int(G).$$

$\forall f \in G$
$\varphi \circ I_g \circ \varphi^{-1}(f) = \varphi(g\varphi^{-1}(f)g^{-1}) =$
$\varphi(g)\varphi(\varphi^{-1}(f))\varphi(g^{-1}) =$
$= \varphi(g) f \varphi(g) =$
$= I_{\varphi(g)}(f)$
$\Rightarrow \varphi \circ I_g \circ \varphi^{-1} = I_{\varphi(g)} \in Int(G)$ □

**Definizione 25** (Centro di un gruppo)
$(G, \cdot)$ *gruppo*
*Il centro di* $G$ *è*

$$Z(G) := \{g \in G | gf = fg \quad \forall f \in G\}.$$

**Osservazione**
$Z(G) \trianglelefteq G$
**Osservazione:**
$(G, \cdot)$ gruppo
Definiamo un omomorfismo
$\varphi : G \to Int(G)$
$g \to I_g$
· $\varphi$ è suriettiva
· $\varphi$ è omomorfismo
$\varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1)$
$I_{g_2 g_1} = I_{g_2} \circ I_{g_1}$
Chi è il $ker(\varphi)$

$ker(\varphi) = \{g \in G | \varphi(g) = Id\} =$
$= \{g \in G | I_g = Id\} =$
$= \{g \in G | \forall f \in G : I_g(f) = Id(f)\} =$
$= \{g \in G | \forall f \in G : gfg^{-1} = f\} = Z(G)$
Dal I teorema di isomorfismo si ha che

$$Int(G) \cong G/Z(G).$$

## 3.12 Prodotto semidiretto

Consideriamo due gruppi
$(N, \cdot)$ e $(H, *)$
Fissiamo un omomorfismo
$\phi : H \to Aut(N)$
$h \to \varnothing_n$

**Definizione 26** (Prodotto semidiretto)
*il prodotto semidiretto di $N$ e $H$ tramite $\varnothing$ è l'insieme $N \times H$ dotato dell'operazione*

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \varnothing_{h_1}(n_2), h_1 * h_2).$$

$\forall n_1, n_2 \in N \quad \forall h_1, h_2 \in H$

**Notazione 7**
*Indichiamo il prodotto semidiretto tra $N$ e $H$ con il simbolo $N \rtimes_{\varnothing} H$*

**Proposizione 12**
*$N \rtimes_{\varnothing} H$ è un gruppo*

**Dimostrazione**
*Dato $(n, h) \in N \rtimes_{\varnothing} H$*
*l'inverso è dato da $(\varnothing_{h^{-1}}(n^{-1}), h^{-1})$* □

**Definizione 27**
$(G, \cdot)$ *gruppo*
$N, H \leq G$ *Diremo che*
$G$ *è prodotto semidiretto interno di* $N$ *e* $H$ *se*

- $N \trianglelefteq G$
- $N \cap H = \{e\}$
- $NH = G$

**Esempio**
$D_n =< \rho, \sigma >$ $N =< \rho > \trianglelefteq D_n$
$H =< \sigma > \leq D_n$. Allora $D_n$ è prodotto semidiretto interno di $N$ e $H$
**Osservazione:**
$h_1 \in H$, $\phi_{h_1} \in Aut(N)$ $\phi_{h_1}(n_2) \in N$
**Esempio**
Scegliendo
$\phi : H \to Aut(N)$
$h \to \phi_h$
con $\phi_n := Id_N$ $\forall h \in H$
Abbiamo:

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot n_2, h_1 * h_2).$$

Quindi il prodotto diretto è un caso particolare del prodotto semidiretto

## 3.13 Prodotto semidiretto interno:

Un gruppo $G$ si dice *prodotto semidiretto interno* di $N$ e $H \leq G$ se:

1. $N \trianglelefteq G$,
2. $N \cap H = \{e\}$,
3. $NH = G$.

**Esercizio**
Sia $\phi : H \to Aut(N)$ un omomorfismo
Dimostrare:
1)$|N \rtimes_\phi H| = |N||H|$
2)$N \rtimes_\phi H$ è abeliano $\Leftrightarrow N, H$ abeliani
3)$\tilde{H} \leq H, \tilde{N} \leq N$ (sottogruppo caratteristico)

$$\tilde{N} \rtimes_\phi \tilde{H} := \{(n, h) \in N \rtimes_\phi H | n \in \tilde{N}, n \in \tilde{H}\}.$$

è un sottogruppo di $N \rtimes_\phi H$

**Definizione 28** (Sottogruppo caratteristico)
*$\tilde{N} \leq N$ sottogruppo caratteristico se*
*$\varphi(n) \in \tilde{N} \quad \forall n \in N \quad \forall \varphi \in Aut(N)$*

**Teorema 12**
*Sia $G$ un gruppo.*
*1) Se $G$ è prodotto semidiretto di $N$ e $H \leq G$, allora esiste un omomorfismo $\phi : H \to Aut(N)$ tale che $G \cong N \rtimes_\phi H$*
*2) Se $G \cong \tilde{N} \rtimes_\phi \tilde{H}$ allora esistono $N, h \leq G$ t.c.*

- *$G$ sia prodotto semidiretto interno di $N$ e $H$*
- *$N \cong \tilde{N}, h \cong \tilde{H}$*

**Dimostrazione** (1)
*Definiamo l'applicazione*
$\phi : H \to Aut(N)$
$h \to \phi_n$
*dove* $\phi_h(n) := (hnh^{-1}) \in hNh^{-1} = N \quad \forall n \in N$
*Dato che abbiamo assunto $N$ normale*
*Abbiamo verificato la volta scorsa che è un omomorfismo.*
*Definiamo l'applicazione*
$\psi : N \rtimes_\phi H \to G$
$(n, h) \to nh$
*$\psi$ è suriettiva poiché* $N \cdot H = G$
*$\psi$ è iniettiva poichè*

$$n_1 h_1 = n_2 h_2 \to n_2^{-1} h_1 = h_2 h_1^{-1} \in H \cap N = \{e\}$$
$$\Rightarrow \begin{cases} n_2^{-1} n_1 = e \\ h_2 h_1^{-1} = e \end{cases} \to (n_1, h_1) = (n_2, h_2)$$

*$\psi$* ***è omomorfismo:***
$\psi((n_1, h_1) \cdot (n_2, h_2)) =$
$= \psi((n_1 \phi_{h_1}(n_2), h_1 h_2))$
$= n_1 \phi_{h_1}(n_2) h_1 h_2$
$= n_1 h_1 n_2 h_1^{-1} h_1 h_2 = \psi(n_1, h_1) \cdot \psi(n_2, h_2)$
*Omomorfismo biunivoco* □

**Dimostrazione** (2)
*Dato un isomorfismo*
$\psi : \tilde{N} \rtimes_{\phi} \tilde{H} \to G$
*definiamo:*
$N := \psi(\tilde{N} \rtimes_{\phi} \{e_{\tilde{H}}\}) \trianglelefteq G$
$H := \psi(\{e_n\} \rtimes_{\phi} \tilde{H})$
*Osserviamo che:*
$\cdot \tilde{N} \cong \tilde{N} \rtimes_{\phi} \{e_{\tilde{H}}\} \cong N$
$\cdot \tilde{H} \cong \{e_{\tilde{H}}\}_{\rtimes_{\phi} \tilde{H} \cong H}$
$\cdot N \cap H = \{e\}$
$\cdot NH = e$
*(analogo alla dimostrazione per prodtto diretto)* □

# 4 Numeri primi e aritmetica

**Definizione 29** (Numero primo)
*Un intero* $\rho > 1$ *si dice primo se* $\forall a, b \mathbb{Z}$

$$\rho | ab \to \rho | a \text{ oppure } \rho | b.$$

**Definizione 30** (Numero irriducibile)
*Un intero* $\rho > 1$ *si dice irriducibile se i suoi unici divisori positivi sono* $1$ *e* $\rho$

**Esercizio:**
Dimostrare che $\rho$ è primo $\Leftrightarrow$ è irriducibile

**Teorema 13** (Fondamentale dell'aritmetica)
$n > 1$ *intero. Allora* $n$ *si scrive in modo unico come*

$$n = \rho_1^{k_1} \cdot \ldots \cdot \rho_r^{k_r} \qquad \textit{(forma canonica)}$$

*dove* $k_i > 0 \quad \forall i \in \{1, \ldots, r\}$
*e* $\rho_1 < \rho_2 < \ldots < \rho_r$
*e* $\rho_i$ *è primo* $\forall i \in \{1, \ldots, r\}$

**Teorema 14**
$\rho$ *primo. Allora*
$\sqrt{\rho}$ *è irrazionale (ovvero* $\sqrt{\rho} \ni \mathbb{Q}$*)*

**Dimostrazione** (Per assurdo)
$\exists a, b \in \mathbb{Z}$ *t.c.* $\sqrt{\rho} = \frac{a}{b}$ *con* $MCD(a, b) = 1$

*Allora:*
$(a) + (b) = (MCD(a,b)) = (1)$
$\to 1 \in (a)) + (b)$
$\exists r, s, \in$ , *t.c.* $1 = ra + sb$ *(identità di Bezout)*
*ora:* $\begin{cases} a = \sqrt{\rho} b \\ b\rho = a\sqrt{\rho} \end{cases}$
*Quindi:* $\sqrt{\rho} = \rho \cdot 1 = \sqrt{\rho} \cdot (ra + sb)$
$(\sqrt{\rho}a)r + (\sqrt{\rho}b)s$
$= \rho br + as \in \mathbb{Z}$
$\Rightarrow \sqrt{\rho} \in \mathbb{Z}$ *quindi* $\sqrt{\rho}$ *è un intero che divide* $\rho$ *e* $1 < \sqrt{\rho} < \rho$ □

**Teorema 15** (Euclide)
*Esistono infiniti numeri primi*

**Dimostrazione**
*Supponiamo per assurdo che* $\exists$ *un numero finito di primi* $\rho_1, \ldots, \rho_r$
*Definiamo:* $N := (\rho_1 \cdot \ldots \cdot \rho_r) + 1 > 1$
$\Rightarrow \exists \rho_k$ *primo tale che* $\rho_k | N$
$\Rightarrow \begin{cases} \rho_k | N \\ \rho_k | N - 1 \end{cases} \Rightarrow \rho_k | N - (N-1) \Rightarrow \rho_k | 1$, *assurdo* □

**Definizione 31** (Primi di Euclide)
*Sia* $\rho$ *primo*

$$\rho^{\#} := \left( \prod_{q \in \rho, q \text{ primo}} q \right) + 1.$$

$\rho^{\#} + 1$ *si dice numero di Euclide*

**Congettura**
Esistono infiniti primi di euclide

## 4.1 Svolgimento esercizi

**Ossercazione:**
Quali sono gli elementi di oridne 21 in $S_{13}$?
Ricordo che in $S_4$, gli elementi $(12)(34), (13)(24), (14)(23)$ hanno ordine 2
gli elementi di ordine 21 sono $(3-ciclo)(7-ciclo)$ sono $\frac{13!}{126}$
$(3-ciclo)(3-ciclo)(7-ciclo)$ sono $\frac{13!}{126}$
Nelle note del corso trovi soluzioni degli esercizi
**Esercizi:**
1) $(\mathbb{Z}, +) \quad Aut(\mathbb{Z}) =?$
**Osservazione**

Per definire un omomorfismo è sufficiente definirlo sui generatori.
Se inoltre vogliamo un automorfismo $\phi(1)$ deve generare $\mathbb{Z} \Rightarrow \phi(1) = 1$ o $-1$
$\Rightarrow Aut(\mathbb{Z}) = \{Id, -Id\} \cong C_2$
2) Dimostrare che $D_n \cong C_n \rtimes_\phi C_2$ dovea
$\phi : C_2 \to Aut(C_n) =< \rho >$ e $\phi(\rho) = \rho^{-1}$ SOluzione:
$\sigma \to \phi_\sigma$
$N =< \rho > \trianglelefteq D_n$ $[D_n : N] = 2$
$H :=< \sigma > \leq D_n$
Verifichiamo che $D_n$ è prodotto semidiretto interno di $N$ e $H$
$\cdot N \cap H = \{Id\}$
$\cdot |NH| = \frac{|N||H|}{|N \cap H|} = 2n \Rightarrow NH = D_n$
Ora dal teorema segue che $D_n = N \rtimes_\phi H$
dove $\phi : H \to Aut(N)$ $H = \{Id, \sigma\}$
$h \to h$
$\cdot \phi_{Id} = Id_N$
$\cdot_\sigma(\rho) = \sigma\rho\sigma^{-1} = \sigma\rho\sigma = \sigma\sigma\rho^{n-1} = p^{n-1} = p^{-1}$
dove abbiamo usato il fatto che $\rho^i\sigma = \sigma\rho^{n-i}$
Infine $H \cong C_2$ $N \cong C_n$
**Osservazione**
Se avessimo scelto $\phi : C_2 \to Aut(C_n)$
$\sigma \to \phi_\sigma$
con $\phi_\sigma(\rho) = \rho$ Avremmo $C_n \rtimes_\phi C_2 = C_n \times C_2$ è abeliano $\Rightarrow$ non isomorfo a $D_n$ $\forall n \geq 3$
3)$G = C_5 \cong \mathbb{Z}/(5)$
$Aut(C_5)$
Cerchiamo le immagini di $\varphi(\rho)$
$\mathbb{Z}/(5) = \{[0], [1], [2], [3], [4]\}$ ricordo che $ord_{\mathbb{Z}/(n)}([a]) = \frac{n}{MCD(a,n)}$
$ord([1]) = ord([2]) = ord([3]) = ord([4])$
$ord([0]) = 1 \Rightarrow |Aut(\mathbb{Z}/(5))| = 4$
**Osservazione**
In generale denotiamo con $U_n$ il gruppo delle classi in $\mathbb{Z}/(n)$ $U_n = \{[a] \in \mathbb{Z}/(n) | MCD(a, n) = 1\}$
**Esercizio**
$U_n$ è un gruppo rispetto $U_n \times U_n \to U_n$
$([a], [b]) \to [a \cdot b]$
Si dice gruppo degli invertibili
**Esercizi**— $\cdot Aut(C_n) \cong U_n$
$\cdot Aut(K_4) = S_3$

**Teorema 16** (Cinese del resto)
*$C_{nm} \cong C_n \times C_m$ per ogni coppia di interi tale che $MCD(m, n) = 1$*

**Dimostrazione**
*Già dimostrato* □

**Teorema 17** (Piccolo teorema di Fermat)
*$p$ primo, $a \geq 1$ $MCD(a,p) = 1 \Rightarrow a^{p-1} \equiv_p 1$*

**Dimostrazione**
$A := \{a, 2a, 3a, \ldots, (p-1)a\}$ *sono* $p-1$ *interi.*
*Mi chiedo se* $[ra] = [sa]$ *in* $\mathbb{Z}/(p)$
*Sappiamo che esistono* $1 \leq r < s \leq p-1$ *tali che* $[ra] = [sa]$ *in* $\mathbb{Z}/(p) \Rightarrow$ *Assurdo poiché*
$[r] \neq [s]$ *in* $\mathbb{Z}/(p)$
*Quindi le classi definite dagli elementi di A sono tutte distinte e non banali* $\Rightarrow$
$\{[a], [2a], \ldots, [(p-1)a]\} = \{[1], [2], \ldots, [p-1]\}$
*Consideriamo il prodotto* $a \cdot 2a \cdot \ldots \cdot (p-1)a_p 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$
$\Rightarrow a^{p-1}(p-1)! \equiv_p (p-1)$ *Dato che* $MCD(p,(p_1)) = 1$ *abbiamo* $a^{p-1} \equiv_p 1$ □

**Corollario 6**
*$a \geq 1$ $p$ primo* $\Rightarrow a^p \equiv_p a$

**Dimostrazione**
*Se* $MCD(a,p) = 1$ *segue dal piccolo teorema di Fermat*
· *Se* $MCD(a,p) \neq 1 \Rightarrow p|a \Rightarrow [a] = [0]$ *in* $\mathbb{Z}/(p) \Rightarrow a^p \equiv_p 0 \equiv_p a$
□

**Obbiettivo**
Cosa succede al piccolo teorema di Fermat senza $p$ primo?

**Definizione 32** (Funzione di Eulero)
*$n \geq 1 \Rightarrow \phi(n) = |U_n|$ ovvero $\phi(n)$ è il numero di interi positivi minori o uguali ad $n$ coprimi con $n$*

**Esempio**
$p$ primo $\Rightarrow \phi(p) = p-1$; $\phi(1) = 1$
**Esercizio**
Mostrare che se $p$ è primo $\Rightarrow \phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
**Soluzione:**
$MCD(a,p) = 1 \Leftrightarrow p|a$ Quindi gli elementi inclusi sono $p, 2p, 3p, \ldots, (p^{k-1})p$ tutti i multipli di $p \leq p^k$
Sono $p^{k-1}$ elementi $\Rightarrow \phi(p^k) = p^k - p^{k-1}$

**Definizione 33**
*Una funzione* $f : \mathbb{Z}_{>0} \to \mathbb{Z}$ *si dice moltiplicativa se* $f(n \cdot m) = f(n) \cdot f(m)$ *se* $MCD(n, m) = 1$

**Obiettivo**
Dimostrare che $\phi$ è moltiplicativa
**Esercizio**
$a, b, c \in \mathbb{Z}$

$$MCD(a, b, c) = 1 \Leftrightarrow \begin{cases} MCD(a, b) = 1 \\ MCD(a, c) = 1 \end{cases}$$

**Teorema 18** (Eulero)
$\phi : \mathbb{Z}_{>0} \to \mathbb{Z}$ *di Eulero è moltiplicativa*

**Dimostrazione**
*Per il teorema cinese del resto se* $MCD(n, m) = 1 \Rightarrow$
$\psi : \mathbb{Z}/(nm) \to \mathbb{Z}(n) \times \mathbb{Z}(m)$
$[a]_{nm} \to ([a]_n, [a]_m)$ *Consideriamo la restrizione* $\psi|_{U_{nm}} : U_{nm} \to Z/(n) \times \mathbb{Z}/(m)$ *è una funzione iniettiva*
*Studiamo* $Im(\psi|_{U_{nm}}) = U_n \times U_m$ *(esercizio)*
$\Rightarrow |U_{nm}| = |U_n| \times |U_m| \Rightarrow \phi(nm) = \phi(n)\phi(m)$ □
**Osservazione** (Formula generale)
$n > 1$ intero con fattorizzazione canonica

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \Rightarrow \phi(n) = \phi(p_1^{k_1}) \cdot \ldots \cdot \phi(p_r^{k_r})$$

$$= (p_1^k - p_1^{k_1 - 1}) \cdot \ldots \cdot (p_r^{k_r} - p_r^{k_r - 1}) = \left(1 - \frac{1}{p_1^{k_1}}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r^{k_r}}\right).$$

**Osservazione**
$|Aut(C_n)| = \phi(n)$ dato che $Aut(\mathbb{Z}/(n)) \cong U_n$
**Osservazione**
Se $n \geq 2 \Rightarrow \phi(n)$ è pari

- Se $n = 2^k \Rightarrow \phi(n) = 2^k - 2^{k-1} = 2^{k-1}$
- $n > 2 \Rightarrow k > 1 \Rightarrow k - 1 > 0 \Rightarrow 2|\phi(n)$
- Se $n \neq 2^k \Rightarrow \exists p$ primo e dispari tale che $p|n \Rightarrow n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ con $p = p_j$ per qualche $j \leq r \Rightarrow \phi(p_j^{k_j})|\phi(n)$. Ma $\phi(p_j^{k_j}) = p^{k_j} - p^{k_j - 1} = p^{k_j - 1}(p - 1)$ $\Rightarrow (p_j - 1)|\phi(p_j^{k_j})$.Ma $p_j$ è dispari $\Rightarrow 2|(p_j - 1) \Rightarrow 2|\phi(n)$

**Teorema 19** (Waring 1770, Lagrange 1771)
*Se $p$ è un numero primo* $\Rightarrow (p-1)! \equiv_p (p-1)$

**Dimostrazione**
*Studiare le soluzioni di* $x^2 - 1 \equiv_p 0$
$(x^2-1) \equiv_p (x-1)(x+1) \equiv_p 0$
*Quindi* $x - 1 \equiv_p 0$ *oppure* $x + 1 \equiv_p 0$
*ovvero deduciamo che gli unici elementi in* $U_p$ *di ordine* $\leq 2$ *sono* $[1]$ *e* $[p-1]$
*Nel prodotto* $[(p-1)!]$ *compaiono tutti gli elementi di* $U_p \Rightarrow$ *ogni elemento di* $U_p$ *diverso da* $1$ *e* $p-1$ *oppure con il suo inverso ("moltiplicativo")* □

## 4.2 funzione di Eulero

$\phi : \mathbb{Z}_{>0} \to \mathbb{Z}$
$\quad n \to |U_n|$
**Ricordo:**
$\phi(1) = 1$
$\phi(\rho) = \rho - 1$
$\phi(\rho^k) = \rho^k - \rho^{k-1}$
$\phi(n \cdot m) = \phi(n)\phi(m) \quad$ se $MCD(n,m) = 1$

**Lemma 5**
$n > 1, a \in \mathbb{Z}$ *t.c.* $MCD(n,a) = 1$
*sia* $\{a_1, \ldots, a_{\phi(n)}\}$ *l'insieme dei numeri positivi minori di* $n$ *coprimi con* $n$ *distinti fra loro.*
*Allora* $\{[a_1], \ldots, [a_{\phi(n)}] = \{[aa_1], \ldots, [aa_{\phi(n)}]\}$ *(Classi in* $Z/(n)$*)*

**Dimostrazione**
*Basta verificare che gli elementi delle classi* $[aa_i] \;\; \forall\, 0 < i < \phi(n)$
*Siano tutte distinte tra loro e* $aa_i$ *sia coprimo con* $n \; \forall\, 0 < i < \phi(n)$
*Se per assurdo* $[aa_i] = [aa_j] \;\; i \neq j \Rightarrow aa_i \equiv aa_j \; mod(n) \Rightarrow a \equiv a_j \; mod(n)$
*Assurdo perché* $1 \leq a_i, a_j < n$ *per ipotesi e dunque* $a_i - a_j \notin (n)$
$\begin{cases} MCD(a,n) = 1 \\ MCD(a_i, n) = 1 \end{cases} \Rightarrow MCD(a, a_i) = 1$

□

**Teorema 20** (Eulero 1760)
$n > 1, a \in \mathbb{Z}$ *tale che* $MCD(a,n) = 1$
*Allora*

$$a^{\phi(n)} \equiv 1 \; mod(n).$$

**Nota**
Se $n$ è primo ritroviamo il piccolo teorema di Fermat
**Dimostrazione**
*Considero la situazione del lemma:*
$A = \{a_1, \ldots, a_{\phi(n)}\}$
*Insieme degli interi positivi minori di n e coprimi con n distinti tra loro*
*Dal lemma segue che*

$$a_1 \cdot \ldots \cdot a_{\phi(n)} \equiv (aa_1) \cdot \ldots \cdot (aa_{\phi(n)}) \ mod(n).$$

$$\equiv a^{\phi(n)} \cdot a_1 \cdot \ldots \cdot a_{\phi(n)} \ mod(n).$$

*Dal momento che* $MCD(a_i, n) = 1$
*abbiamo:* $1 \equiv a^{\phi(n)} \ mod(n)$ □
**Esempio**
Se volessi calcolare le ultime 3 cifre di $2024^{2025}$ Studiamo la congruenza

$$x \equiv 2024^{2025} \ mod(1000)$$

È equivalente al sistema (Teorema cinese del resto):

$$\begin{cases} x \equiv 2024^{2025} \ mod(2^3) \\ x \equiv 2024^{2025} \ mod(5^3) \end{cases}$$

Alternativamente mi accorgo che la prima equazione è equivalente a

$$x \equiv 24^{2025} \ mod(1000).$$

$\phi(1000) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$
$\Rightarrow 24^{400} \equiv 1 mod(n)$
Ma questo implica che la congruenza che devo studiare è:

$$\Rightarrow x \equiv 24^{2025} mod(1000).$$

$$\Rightarrow \begin{cases} x \equiv 24^{2025} \ mod(8) \\ x \equiv 24^{2025} \ mod(125) \end{cases} \Rightarrow \begin{cases} x \equiv 0 \ mod(8) \\ x \equiv 24^{2025} \ mod(125) \end{cases}.$$

Dove nell'ultimo passaggio abbiamo utilizzato il fatto che $8|24$ e $24^{\phi(125)} \equiv 24^{100} \equiv 1 \ mod(125)$
Alla fine dovremmo ricostruire la soluzione in $\mathbb{Z}/(1000)$ che sarà unica per il teorema cinese del resto

## 4.3 Teorema cinese del resto

**Problema**
Dato un sistema di congruenze
$\begin{cases} x \equiv= a_1 \ mod(n_1) \\ \vdots \\ x \equiv= a_r \ mod(n_r) \end{cases}$
con $MCD(n_i, n_j) = 1 \ \ \forall i \neq j$
Come ricostruire l'unica soluzione $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \ldots \cdot n_r)$
$\bar{x} \equiv a_i \ mod(n_i) \ \forall i \in \{1, \ldots, r\}$
**Idea**
Definiamo:
$n := n_1 \cdot n_r$
$N_i := \frac{n}{n_i}$
$\bar{x} := a_1 N_1^{\phi(n_1)} + \ldots + a_r N_r^{\phi(n_r)}$
Ora $\bar{x} \equiv a_i N^{\phi(n)} \ mod(n) \Rightarrow \bar{x} = a_i mod(n_i) \ \ \forall i$

**Teorema 21** (TCR)
*Dato il sistema*
$\begin{cases} x \equiv a_1 \ mod(n) \\ \ldots x \equiv a_r \ mod(n_r) \end{cases}$
*con* $MCD(n_i, n_j) = 1 \ \ \forall i \neq j$
*Allora esiste un'unica classe* $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \ldots \cdot n_r)$ *tale che*
$\bar{x} \equiv a_i \ mod(n_i) \ \ \forall i \in \{1, \ldots, r\}$

**Dimostrazione** (Alternativa al teorema di Eulero)
$n := n_1 \ldots \cdot n_r$
$N_i = \frac{n}{n_i}$
$\bar{x} := a_1 N_1 m_1 + \ldots a_r N_r m_r$
*dove gli* $m_i$ *sono univocamente determinati dalla condizione* $N_i m_i \equiv 1 mod(n_i)$
*Infatti*

$$\bar{x} \equiv a_i N_i m_i \ mod(n_i) \Rightarrow \bar{x} \equiv a_i mod(n_i).$$

*Osserviamo che* $MCD(N_i, n_i) = 1$ *Per ipotesi*
*Quindi* $[N_i] \in U_{n_i}$ *e* $[m_i]$ *è l'unico inverso di* $[N_i]$ *in* $U_{n_i}$ □
**Osservazione**
Per risolvere i sistemi di congruenze "basta" saper trovare gli inversi degli elementi in gruppi $U_{n_i}$
**Esercizi dalle schede**
**Esercizio (Gauss)**
Dato un intero $n > 1$ dimostrare che $n = \sum_{d|n} \phi(d)$ (somma di tutti i divisori positivi di $n$
**Dimostrazione**
$S_d := \{m \in \mathbb{Z} | MCD(m, n) = d, 1 \leq m \leq n\}$

*Osserviamo che*
$\{1, \dots, n\} = \bigcup_d S_d$
$\Rightarrow n = \sum_{d|n} |S_d|$
$MCD(m, n) = d \Leftrightarrow MCD(\frac{m}{d}, \frac{n}{d}) = 1$
*Quindi* $|S_d| = \phi(\frac{n}{d})$
$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d)$

□

**Esempio**
$n = 15$
Voglio ripetere la dimostrazione per ottenere $15 = \sum_{d|15} \phi(d)$
$S_1 = \{1, 2, 4, 7, 8, 11, 13, 14\} \Rightarrow \phi(15/1) = 8$
$S_3 = \{3, 6, 9, 12\} \Rightarrow \phi(15/3) = 4$
$S_5 = \{5, 10\$ \Rightarrow \phi(15/5) = 2$
$S_{15} = \{15\} \Rightarrow \phi(15/15) = 1$
**Esempio**
$n.1$ Allora la somma di tutti gli interi positivi minori di $n$ coprimi con $n$ vale $\frac{1}{2} n\phi(n) \in \mathbb{Z}$
**Dimostrazione**
*Chiamiamo* $a_1, \dots, a_{\phi(n)}$ *tali interi:*
*Studio* $\sum_{i=1}^{\phi(n)} a_i$
*Osserviamo che* $MCD(a, n) = 1 \Leftrightarrow MCD(n - a_i, n) = 1$
*Quindi*
$\{a_1, \dots, a_{\phi(n)}\} = \{n - a_1, \dots n - a_{\phi(n)}\}$
$\Rightarrow \sum_{i=1}^{\phi(n)} a_i = \sum_{i=1}^{\phi(n)} (n - a_i) = n\phi(n) - \sum_{i=1}^{\phi(n)} a_i \Rightarrow 2\sum_{i=1}^{\phi(n)} a_i = n\phi(n)$ □

## 4.4 Teorema di Wilson/Lagrange

Ricordo

**Teorema 22** (Wilson)
*p primo. Allora*
$(p-1)! \equiv (p-1)\ mod(p)$

**Teorema 23** (Lagrange)
$m > 1$ *intero tale che*
$(m-1)! \equiv (m-1)\ mod(m)$
*Allora m è primo*

**Dimostrazione**
*Per assurdo, se m non è primo allora esiste un intero* $d|m$ *tale che* $1 < d < m$
*Osserviamo che:*
$d < m \Rightarrow d|(m-1)!$
*dall'ipotesi segue che*

$$m|(m-1)! + 1.$$

$\Rightarrow d|(m+1)!+1$

$Quindi \begin{cases} d|(m-1)! \\ d|(m-1)!+1 \end{cases} => d|1 \ che \ è \ un \ assurdo$ □

## 4.5 Divisione Euclidea

**Teorema 24**
$a, b \in \mathbb{Z} \ con \ b \neq 0 \ allora \ \exists q, r \in \mathbb{Z} \ tale \ che$
$\cdot a = qb + r$
$\cdot \ 0 \leq r < |b|$

**Dimostrazione**
*Procediamo per passi*
$1) a, b \in \mathbb{Z}_{>0}$

$$A = \{k \in \mathbb{Z} | kb > a\}.$$

*Osserviamo che* $A \neq \emptyset$
*Infatti* $(a+1)b = ab + b > ab \geq a \Rightarrow a+ \in A$
*Per il principio del buon ordinamento di* $\mathbb{N}$

$$\Rightarrow \exists m := min\{k\} \in \mathbb{Z}^+.$$

*Definiamo*

$$q := m - 1 \in \mathbb{Z}^+.$$

$q \notin A \ e \ q+1 \in A$
$qb \leq a < (q+1)b = qb + b$
$\Rightarrow 0 \leq a - qb < b$
*Definiamo* $r = a - qb \ e \ otteniamo:$
$0 \leq r < b$
$a = qb + r$
*2)* $a \in \mathbb{Z} \ b > 0$
*Se* $a \geq 0$ *(ok per 1)*
*Se* $a < 0 \Rightarrow -a > 0$
$\Rightarrow -a = qb + r \ con \ 0 \leq r < b$
$\Rightarrow a = (-q)b - r$
*Se* $r = 0$ *abbiamo finito*
*Se invece* $0 < r < b$
*definiamo* $r' = b - r \Rightarrow 0 < r' < b$
$a = (-q)b - b + \frac{b-r}{r'}$
$\Rightarrow a = (-q-1)b + r' = q'b + r'$
*3)* $a \in \mathbb{Z}, b < 0$
$\Rightarrow -b > 0$
$a = q(-b) + r \ con \ 0 \leq r < -b$
$\Rightarrow a = (-q)b + r \quad 0 \leq r < |b|$ □

## 4.6 Esercizi delle schede

$\begin{cases} x \equiv 50 \ mod(110) \\ x \equiv 47 mod(73) \end{cases}$
Dal teorema cinese del resto sappiamo che esiste un'unica soluzione modulo il prodotto $mod(110 * 73) = mod(8030)$
Come lo costruisco?
$\bar{x} = 50 \cdot 73 \cdot m_1 + 47 \cdot 110 \cdot m_2$
L'idea è di infilare al posto di $m_1$ l'inverso di 73 $mod(110)$

$$\begin{cases} 73 \cdot m_1 \equiv 1 \ (110) \\ 110 \cdot m_2 \equiv 1 \ (73) \end{cases} .$$

Bisogna determinare $m_1, m_2$
**Idea:** Sfruttare l´identità di Bezoit: $(n_1) + (n_2) = (MCD(n_1, n_2)) = (1)$
obiettivo: $n_1 \cdot r + n_2 \cdot s = 1$
Nel nostro caso cerco $110 \cdot r + 73 \cdot s = 1 \quad r, s \in \mathbb{Z}$
Perché è importante $110 \cdot r \equiv 1 \ mod(73)$
$73 \cdot s \equiv 1 \ mod(110)$
Il nuovo obiettivo è determinare $r, s$
Procedo con la divisione euclidea tra 110 e 73

$$\begin{aligned} 110 &= 73 + 37 \\ 73 &= 2 \cdot 37 - 1 \\ \Rightarrow 1 &= 2 \cdot 37 - 73 \\ \Rightarrow 2 \cdot (110 - 73) - 73 &= 1 \\ \Rightarrow 2 \cdot 110 - 3 \cdot 73 & \end{aligned}$$

Quindi:
$1 = 2 \cdot 110 - 3 \cdot 73$
da cui

$$\begin{aligned} m_1 &= -3 \\ m_2 &= 2 \end{aligned}$$

$$\bar{x} \equiv 5 - \cdot 73 \cdot (-3) + 47 \cdot 110 \cdot (2) \equiv -620 \ mod(8030).$$

8==========D
**Nuovo Esercizio**
$\begin{cases} x \equiv_6 2 \\ x \equiv_{10} 3 \end{cases}$ Non possiamo sfruttare il teorema cinese del resto

$$x \equiv_6 2$$
$$\Updownarrow$$
$$x = 2 + 6k \quad k \in \mathbb{Z}$$
$$\Updownarrow$$
$$x = 2(1 + 3k)$$

$$x \equiv_{10} 3$$
$$\Updownarrow$$
$$x = 3 + 10h \quad h \in \mathbb{Z}$$
$$\Updownarrow$$
$$x = 2(5h + 1) + 1$$

Dunque dalla prima congruenza segue

$$x \equiv_2 0.$$

dalla seconda

$$x \equiv_2 1.$$

Quindi concludiamo che è impossibile 8==========
**Nuovo Esercizio**
$\begin{cases} 3x \equiv_{15} 6 \\ 7x \equiv_9 2 \end{cases}$
Non posso usare $TCR$ studio $3x \equiv_{15} 6$

$$3x \equiv 6 + 15k$$
$$\Updownarrow$$
$$3x = 3(2 + 5k)$$
$$\Updownarrow$$
$$x = 2 + 5k$$

$\begin{cases} x \equiv_5 2 \\ 7x \equiv_9 2 \end{cases}$
Ora $MCD(3, 9) = 1$ Vorrei sfruttare TCR, per farlo dobbiamo eliminare i coefficienti
Noto che 7 e 9 sono coprimi $\Rightarrow [7] \in U_9$ (invertibili modulo 9)
Cerchiamo l'inverso moltiplicativo di $[7] \in U_9$
ovvero cerco $s \in \mathbb{Z}$ tale che $7s \equiv_9 1$

Utilizzo la divisione euclidea

$$\begin{gathered} 9 = 7 + 2 \\ 7 = 3 \cdot 2 + 1 \\ \Rightarrow 1 = 7 - 3 \cdot 2 \\ \Rightarrow 1 = 7 - 3 \cdot (9 - 7) \\ \Rightarrow 1 = 4 \cdot 7 - 3 \cdot 9 \end{gathered}$$

Quindi $s = 4$

$$\begin{gathered} 7x \equiv_9 2 \\ \Updownarrow \\ 4 \cdot 7 \equiv_9 4 \cdot 2 \\ \Updownarrow \\ x \equiv_9 8 \end{gathered}$$

Il sistema è quindi equivalente a

$$\begin{cases} x \equiv_5 2 \\ x \equiv_9 8 \end{cases}$$

Applico TCR
La soluzione esiste ed è unica modulo (45)
Soluzione:

$$\bar{x} \equiv_{45} 2 \cdot 9 \cdot m_1 - 1 \cdot 5 \cdot m_2.$$

Dove : $\begin{cases} 5m_2 \equiv_9 1 \\ 9m_1 \equiv_5 1 \end{cases}$ Divisione euclidea

$$\begin{gathered} 9 = 5 + 4 \\ 5 = 4 + 1 \\ 1 = 5 - 4 \\ 1 = 5 - (9 - 5) \\ 1 = 2 \cdot 5 - 9 \end{gathered}$$

$\Rightarrow m_2 = 2 \;\; m_1 = -1$

$$\bar{x} \equiv_{45} -18 - 10 \equiv_{45} -28.$$

# 5 Azioni di gruppi

**Definizione 34**
*Un'azione di un gruppo* $(G, \cdot)$ *su un insieme* $X$ *è un'applicazione*

$$G \times X \to X$$
$$(g, x) \to g.x$$

*tale che*
*1)* $e.x = x$
*2)* $(f \cdot g).x = f(g.x) \quad \forall f, g \in G \quad \forall x \in X$

**Esempi:**
1)$(G, *)$ gruppo scelgo $X = G$ agisce per moltiplicazione sinistra

$$G \times X \to X$$
$$(g, x) = g *_{\cdot} x$$

2) $G = S_n \quad X = \{1, \ldots, n\}$

$$\mathrm{S}_n \times X \to X$$
$$(\sigma, x) \to \sigma(x)$$

3) $n, m \in \mathbb{Z}^+$
$G := GL_n(\mathbb{R}) \times GL_n(\mathbb{R})$
$X = Mat_{n,m}(\mathbb{R})$

$$G \times X \to X$$
$$(AB, C) \to BCA^{-1}$$

4) $G = GL_n(\mathbb{R}) \quad X = \mathbb{R}^n$

$$\mathrm{G} \times X \to X$$
$$(\mathrm{A}, \mathrm{v}) \to Av$$

5) $G = GL_n(\mathbb{R}) \quad X = Mat_{n,m}(\mathbb{R})$

$$G \times X \to X$$
$$(A, C) \to ACA^{-1}$$

6) $(G, \cdot)$ gruppo $X = G$

$$G \times X \to X$$
$$(g, x) \to g * x * g^{-1}$$

**Definizione 35**
*Data un'azione di un gruppo $G$ su un insieme $X$ si dice transitiva se*

$$\forall x, y \in X \ \exists g \in G \text{ tale che } g.x = y.$$

**Definizione 36**
*Un'azione si dice semplicemente transitiva se*

$$\forall x, y \in X \ \ \exists! g \in G \text{ tale che } g.x = y.$$

**Esercizio:**
1) Dimostrare che gli esempi dati sono azioni
2) stabilire quali degli esempi sono semplicemente transitivi, transitivi o nessuna delle due

**Notazione 8**
*Scriveremo $G \curvearrowright X$ per indicare che il gruppo $G$ agisce sull'inseme $X$*

**Definizione 37**
*$G \curvearrowright X$, Dato $x \in X$ definiamo:*
*· l'orbita di $x$ come il sottoinsieme*

$$O_x = \{g.x | g \in G\} \subseteq X.$$

*lo stabilizzatore di $x$ il sottogruppo:*

$$Stab_x = \{g \in G | g.x = x\} \subseteq G.$$

**Esercizio:**
Dimostra che lo stabilizzatore di ogni elemento è sempre un sottogruppo (non necessariamente normale
**Esercizio:**
Sia $G$ gruppo finito ($|G| < +\infty$) con $G \curvearrowright X$, per ogni $x \in X$ si ha:
1) $|Stab_x| < +\infty$ (banale)
2) $|O_x| < +\infty$
3) $|G| = |O_x||Stab_x|$
**Suggerimento:**
2) Abbiamo un'applicazione suriettiva

$G \to O_x$

$g \to g.x$

3) L'idea è di dimostrare che esiste una corrispondenza biunivoca fra gli elementi dell'orbita e i laterali sinistri dello stabilizzatore, poi concludete ricordando che $[G : Stab_x] = \frac{|G|}{|Stab_x|}$ (numero di laterali sinistri)

**Idea**(per la corrispondenza biunivoca)

Verificare che $\forall g, f \in G$

$$g \equiv f mod(Stab_x)$$
$$\Updownarrow$$
$$g.x = f.x$$

**Teorema 25** (Cauchy)
*Sia $G$ un gruppo finito, Sia $p$ primo tale che $p \mid |G|$*
*Allora esistono (almeno) $p-1$ elementi di ordine $p$ in $G$*

**Dimostrazione**

*1) In generale se $G \curvearrowright X$ allora $X$ è unione disgiunta di orbite*
*Definiamo la relazione di equivalenza su$X$come$x\tilde{y} \Leftrightarrow g \in G$ tale che $g.x = y$.*
Basta dimostrare che è una relazione d'equivalenza

2) $X = \{(g_1, \ldots, g_n) \in G \times \ldots \times G | g \cdot \ldots \cdot g_p = e\}$

Vogliamo definire un'azione del gruppo ciclico $C_p =< p >$ su $X$

$$C_p \times X \to X$$
$$\rho.(g_1, \ldots, g_p) \to (g_2, g_3, \ldots, g_p, g_1)$$

Verifichiamo che l'azione sia ben definita ovvero che
$\rho.(g_1, \ldots, g_p) \in X \quad \forall (g_1, \ldots, g_p) \in X$

$$g_2 \cdot \ldots \cdot g_p g_1 = (g_1^{-1} g_1)(g_2 \cdot \ldots \cdot g_p) g_1 = g_1^{-1}(g_1 \cdot \ldots \cdot g_p) g_1 = g_1^{-1} g_1 = e.$$

3) Studio $|X|$ abbiamo $|X| = |G|^{p-1}$ infatti:
$\forall (g_1, \ldots, g_{p-1}, g_p) \in X$ dove $_p = (g_1, \ldots, g_{p-1})^{-1} \Rightarrow$ in particolare $p||X|$
4)Studiamo le orbite dell'azione $C_p \curvearrowright X$, Sappiamo che $|C_p| = |O_x||Stab_x| \; \forall x \in X$
Quindi $|O_x| = 1 \quad \vee \quad |O_x| = p$
5) Dato che $X$ è unione disgiunta di orbite e $p||X|$
Allora il numero di orbite formate da $(x)$ unico elemento è un multiplo di $p$
6) Studio tali orbite
L'orbita $O_{(g_1,\ldots,g_p)}$ è formata da un singolo elemento se e solo se
$g_1 = g_2 = \ldots = g_p$ □

Dunque abbiamo una corrispondenza biunivoca

$$\{O_x : \; |O_x| = 1\} \; \leftrightarrow \; \{g \in G | g^p = e\}.$$

Quindi $p$ divide $|\{g \in G | g^p = e\}|$
d'ora in poi $A = \{g \in G | g^p = e\}$
7)$A \neq \emptyset$ poiché $e \in A$

$$A = \{e\} \cup \{g \in G | ord(g) = p\}.$$

Quindi modulo $(p)$ abbiamo

$$0 \equiv_p 1 + |\{g \in G | ord(g) = 1\}|.$$

Quindi l'insieme di elementi di ordine $p$ in $G$ è non uvoto e

$$|\{g | ord(g) = p\} \equiv_p p - 1.$$

Deduciamo

$$|\{g \in G | ord(g) = p\} = kp - 1 \geq p - 1.$$

con $k \in Z^+$

## 5.1 Torniamo alle schede

$\begin{cases} 3x \equiv_{15} 6 \\ 21x \equiv_{49} 13 \end{cases}$ La prima congruenza è equivalente a $x \equiv_5 2$
$MCD(21, 49) = 7$
La seconda congruenza significa

$$21x = 13 + 49k \quad k \in \mathbb{Z}.$$

$$21x - 49k = 13$$
$$7(3x - 7k) = 13$$

**Osservazione:**
Se $MCD(a, n) \not| b$
allora $ax \equiv_n b$ non ammette soluzioni
Infatti: $d = MCD(a, n)$
con $d \not| b$ allora
con $d$ divide il membro di sinistra ma non quello di destra
**Esercizio**
$G$ gruppo $g \in G \quad ord(g) = n$
Allora, $g^h = g^k$ se e solo se $h \equiv_n k$
**Soluzione**
Assumiamo che $g^h = g^k$ Divisione Euclidea
$h - k = qn + r$ con $0 \leq r < n$

Assurdo se $0 < r < n \;\; r = 0$
$h - k = qn \Rightarrow h \equiv_n k$
**Esercizio**
per quali $n, m \in \mathbb{Z}$ si ha $2^n + 2^m$ divisibile per 9
**Soluzione**
Studio

$$\begin{gathered} 2^n + 2^m \equiv_9 0 \\ \Updownarrow 2^n \equiv_9 -2^m \\ \Updownarrow \\ 2^{n-m} \equiv_9 -1 \\ \Updownarrow \\ 2^{n-m} \equiv_9 8 \\ \Updownarrow \\ 2^{n-m} \equiv_9 2^3 \end{gathered}$$

Sfruttiamo l'esercizio precedente con $G = U_9$
La congruenza è verificata se e solo se

$$n - m \equiv 3 \; mod(ord_{U_9}([2])).$$

$$\begin{gathered} 2 \\ 2^2 = 4 \\ 2^3 = -1 \\ 2^4 = -2 \\ 2^5 = -4 \\ 2^6 = 1 \end{gathered}$$

quindi $ord([2]) = 6$
Soluzione: $n - m \equiv_6 3$

## 5.2 Azione di coniugio

**Definizione 38**
*Se $G$ gruppo e $a, b, g \in G$ tali che:*

$$a = gbg^{-1}.$$

*diremo che $a, b$ sono coniugati*

**Definizione 39**
*G gruppo. Allora G agisce su se stesso tramite l'azione di coniugio*
$G \times G \to G$
$g.f = gfg^{-1}$

**Esercizio**
Verificare che è un'azione

**Teorema 26**
*G gruppo*
1) *elementi coniugati hanno lo stesso ordine*
2) $|O_a| = [G : C(a)]$ *dove*
$C(a) := \{g \in G | ga = ag\} \leq G$ *(centralizzatore di a)*
3) *equazione delle classi*
$$|G| = |Z(G)| + \sum_{O_a \not\subseteq Z(G)} \frac{|G|}{|C(a)|}$$

**Dimostrazione**
*1) Siano* $a, b, g \in G$ *tali che* $a = gbg^{-1}$ *supponiamo che* $b^k = e \quad k \in \mathbb{Z}$
*Allora* $a^k = (gbg^{-1}) \cdot \ldots \cdot (gbg^{-1}) = gb^k g^{-1} = e$
*Quindi* $ord(a) \leq ord(b)$.
*Per simmetria* $b = g^{-1}ag \Rightarrow ord(b) \leq ord(a)$
*Allora* $ord(a) = ord(b)$
*2)Osserviamo che*
$C(a) = \{g \in G | ga = ag\}$
$= \{g \in G | gag^{-1} = a\}$
$= Stab_a$
*Ricordiamo che :*
$|O_a| \cdot |Stab_a| = |G|$
$\Rightarrow |O_a| = \frac{|G|}{|Stab_a|} = [G : C(a)]$
*3) se* $a \in Z(G)$ *allora* $O_a = \{a\}$ *poiché*
$\forall g \in G$ *si ha* $ga = gag^{-1} = agg^{-1} = a$
*Ricordiamo che G ammette una partizione in G-orbite*

$$|G| = |Z(G)| + \sum_{O_a \not\subseteq Z(G)} |O_a|.$$

*Dal punto (2)* $\Rightarrow |O_a| = \frac{|G|}{|C(a)|}$

$$|G| = |Z(G)| + \sum_{a \mid O_a \not\subseteq Z(G)} \frac{|G|}{|C(a)|}.$$

***Esempio*** *(dalla nuova scheda)*
$n \geq 3$ *intero dispari* $G = D_n$

$Z(D_n) = \{Id\}$ *infatti* $\rho^i\sigma = \sigma\rho^{n-i}$
*Quindi*
1)$O_\sigma = \{Id\}$
2)$O_{\rho^i} =?$
*Idea* $|O_{\rho^i}| = [D_n : C(\rho^i)]$
$C(\rho') = \{\rho^i | i = 0, \ldots, n-1\}$
$\Rightarrow |C(\rho^i)| \geq n$
*Dato che* $C(\rho^i) \leq D_n$ *allora* $|C(\rho^i)| = n$ *oppure* $|C(\rho^i) = 2n$
*Ma* $\sigma\rho^i = \rho^{n-i}\sigma \neq \rho^i\sigma \quad \forall 0 < i < n$
$\Rightarrow |O(\rho^i)| = n$
*Quindi*
$O_{\rho^i} = [D_n : C(\rho^i)] = \frac{2n}{n} = 2$
*Basta ora trovate un altro elemento coniugato a* $\rho^i \quad (0 < i < n)$

$$\sigma\rho^i\sigma^{-1} = \rho^{n-i}\sigma\sigma^{-1} = \rho^{n-i}.$$

*quindi* $O_{\rho^i} = \{\rho^i, \rho^{n-i}\} \quad \forall 0 < i < n$
3)$O_\sigma = \{\sigma, ?\}$
*Studiamo* $C(\sigma)$
$\sigma$ *non commuta con* $\rho^i \quad \forall 0 < i < n$
*Se* $\sigma$ *commuta con* $\sigma\rho^i \quad con 0 < i < n$
*Allora* $\sigma$ *commuta anche con il prodotto* $\sigma(\sigma\rho^i) = \rho^i$ *assurdo*
$C(\sigma) = \{Id, \sigma\}$
*Quindi* $|O|_\sigma| = [D_n : C(\sigma)] = \frac{2n}{2} = n$
$\Rightarrow O_\sigma = \{\sigma\rho^i | 0 \leq i < n\}$
*Equazione delle classi.*
$|D_n| = |Z(D_n)| + \sum_{O_a \not\subseteq Z(D_n)} |O_a|$

$$2n = 1 + 2 + \ldots + 2 + n.$$

□

**Teorema 27**
*G gruppo tale che* $|G| = p^k \quad p$ *primo* $k > 0$.
*Allora:*
*1)* $Z(G) \neq \{e\}$
*2)* $[G : Z(G)] \neq p$

**Dimostrazione**
*1)* ***IDEA*** *equazioni delle classi*

$$|G| - |Z(G)| = \sum_{O_a \not\subseteq Z(G)} \frac{|G|}{C(a)}.$$

*modulo* $(p)$ *avremmo*

$$|Z(G)| \equiv_p 0.$$

$|Z(G)| \neq 1 \Rightarrow Z(G) \neq \{e\}$
*Attenzione,* $\frac{|G|}{C(a)} = 1 \Rightarrow C(a) = G \Rightarrow a \in Z(G) \Rightarrow O_a = \{a\} \subseteq Z(G)$
*Supponiamo per assurdo che*
$[G : Z(G)] = p$
$\Rightarrow \frac{|G|}{|Z(G)|} = p \Rightarrow |Z(G)| = p^{k-1}$
*Consideriamo* $g \setminus Z(G)$
$\Rightarrow C(g) \supseteq Z(G) \cup \{g\}$
$\Rightarrow\Rightarrow |C(g) = p^{k-1} + 1$
$\Rightarrow |C(g)| = p^k \Rightarrow C(g) = G$
$\Rightarrow g \in Z(G)$ *assurdo* □

**Corollario 7** (Classificazione dei gruppi di oridine $p^2$)
*$G$ gruppo tale che $|G| = p^2$ con $p$ primo.*
*Allora $G \cong C_{p^2}$ oppure $G \cong C_p \times C_p$*

**Dimostrazione**
***IDEA CHIAVE*** *Se $|G| = p^2$ allora $G$ è abeliano.*
*Infatti dal teorema:*
$\cdot$ $Z(G) \neq \{e\}$
$\cdot |Z(G)| \neq p$ *perché avremmo* $[G : Z(G)] = p$
*allora per Lagrnage*
$|Z(G)| = p^2 \Rightarrow Z(G) = G \Rightarrow G$ *abeliano*
*Ora se* $\exists g \in G$ *tale che* $ord(g) = p^2$ *allora* $G \sim G_{p^2}$
*Se invece non esistono elementi di ordine $p^2$ allora tutti gli elementi $(\neq e)$ in $G$ hanno ordine $p$*
*Sia* $h \in G$ *tale che* $h \neq e \Rightarrow H :=< h >$ *con* $|H| = p$
*Sia* $k \in G \setminus H$
$\Rightarrow K :=< k >$ *con*$|K| = p$
*Verifichiamo che $G$ è prodotto diretto interno di $H$ e $K$*
$\cdot H \trianglelefteq G$ *e* $K \trianglelefteq G$ *(poiché $G$ abeliano)*
$H \cap K = \{e\}$ *Infatti:*

$$\begin{cases} H \cap KK \\ H \cap K \neq K \end{cases} \Rightarrow |H \cap K| = 1.$$

$HK =?$
$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^2}{1} = p^2$
$\Rightarrow HK = G$
*Allora* $G \cong H \times K \cong C_p \times C_p$

□

**Osservazione** (per $p = 2$ )
$G = C_4$ oppure $G \cong K_4 \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$
**Osservazione**
$p = 3$ $|G| = 0$ allora

$G \cong C_9$ oppure $G \cong C_3 \times C_3$

## 5.3 Classi coniugate in $S_n$

**Teorema 28** (Fondamentale)
*Due permutazioni in $S_n$ sono coniugate se e solo se hanno la stessa struttura ciclica*

**Dimostrazione**
$\tau = (a_1, \dots, a_n) \in S_n$ *un k-ciclo* $\sigma \in S_n$
*Studio ora* $\sigma\tau\sigma^{-1}$ *e la sua azione sull'insieme* $\{\sigma(1), \dots, \sigma(n)\}$
*Se* $\tau(j) = j$
$\Rightarrow \sigma\tau\sigma^{-1}(\sigma(j)) = \sigma\tau(j) = \sigma(j)$
*Se* $j = a_i$ *per qualche* $1 \leq i \leq k \Rightarrow \tau(j) = \tau(a_i) = a_{i+1 \ mod(k)}$
$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(a_i) = \sigma(a_{i+1 \ mod(k)})$
*Allora*
$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k))$
*Da questo abbiamo dedotto che date* $\sigma, \tau \in S_n$ *qualsiasi, allora:*
$\sigma\tau\sigma^{-1}$ *ha la stessa struttura ciclica di* $\tau$
$\cdot$ *Vogliamo ora dimostrare il viceversa, ovvero: Date* $\tau, \omega \in S_n$ *vogliamo costruire* $\sigma$ *tale che* $\sigma\tau\sigma^{-1} = \omega$ *(* $\tau, \omega$ *con la stessa struttura ciclica)*
*Per ipotesi,* $\tau = \tau_1 \dots tau_h$ *e* $\omega = \omega_1 \dots \omega_h$ *dove* $h \geq 1, \tau_i, \omega_i$ *sono* $k_i - cicli$
*Denotiamo* $\tau_i = (a^{i\,i}_{1\,k_i}), \omega = (b^i_1 \dots b_{k_i})$
*Possiamo definire* $\sigma$ *esplicitamente*
*Infatti*
$\sigma\tau_i\sigma^{-1} = (\sigma(a^i_1) \dots \sigma(a^i_{k_i})$
*Quindi*
*Definiamo* $\sigma := \{\sigma(a^i_j) = b^i_j \ \ \forall i \in \{1, \dots, h\}, j \in \{1, \dots, k\}, \sigma(t) = t \ se \ t \neq a^i_j\}$
*Allora* $\sigma\tau_i\sigma^{-1} = \omega_i \ \ \forall i = h$
$\Rightarrow \sigma\tau\sigma^{-1} = \sigma\tau_1 \dots \tau_h\sigma^{-1}$
$= (\sigma\tau_1\sigma^{-1}) \dots (\sigma\tau_h\sigma^{-1})$
$= \omega_1 \dots \omega_h = \omega$ □

**Osservazione**
Dato che la dimostrazione è costruttiva, è molto utile per risolvere gli esercizi.

## 5.4 Il gruppo p-Sylow

**Idea**
Prendiamo un gruppo finito.
Esistono sottogruppi di un dato ordine (divisore di $|G|$)?
Il risultato parziale che abbiamo è dato dal Teorema di Cauchy:
Se $\exists p$ primo e divide $|G|$, allora:
$\exists H \leq G$ t.c. $|H| = p$
Sylow, va avanti secondo questo filone:

**Definizione 40**
*Sia $G$ gruppo finito, $p, r, m \in \mathbb{Z}_{>0} t.c.$*
$\cdot |G| = p^r \cdot m$
$\cdot p$ *primo* *(ogni gruppo finito ha queste caratteristiche)*
$\cdot MCD(p, m) = 1$
*Un sottogruppo di ordine $p^r$ in $G$ si chiama $p - Sylow$*
*L'insieme dei $p - Sylow$ si denota con $Syl_p(G)$*

**Teorema 29** (I Teorema di di Sylow (1862-1872))
*Se $G$ gruppo finito, $p$ primo che divide $|G|$, Allora:*
$Syl_p(G) \neq \emptyset$

**Dimostrazione**
*Sia* $X := \{S \subseteq G : \ |S| = p^r\}$
*Definisco un azione*
$G \times X \to X$
$(g, s) \to gS = \{gs | s \in S\}$
*Dalle osservazioni* $\Rightarrow p \not| \ |X|$
*D'altra parte, $x$ si decompone in $G$-orbite*
*Inoltre* $|O_S| \cdot |Stab_S| = |G| = p^r \cdot m$
$\Rightarrow \exists$ *almeno un elemento* $\underline{S} \in X t.c. \ |\underline{S}| \not\equiv_p 0$
*Allora*

$$\frac{|O_{\underline{S}}|}{|O_{\underline{S}}|} \cdot |Stab_{\underline{S}}| = \frac{p^r \cdot m}{|O_{\underline{S}}|} \in \mathbb{Z}.$$

*Da cui segue che* $|Stab_{\underline{S}}| \equiv_{p^r} 0$
$p^r \leq |Stab_{\underline{S}}|$
*L'idea ora è di dimostrare che* $Stab_{\underline{S}} \in Syl_p(G)$
*Essendo uno stabilizzatore, è sicuramente un sottogruppo, quindi basta dimostrare che* $|Stab_{\underline{S}}| \leq p^r$
***Osservazione/Esercizio***
$\exists$ *applicazione iniettiva,* $Stab_{\underline{S}} \to p$ *definita fissando un elemento qualsiasi* $\underline{s} \in S$
$Stab_{\underline{S}} \to \underline{S}$
$g \to g\underline{s}$
*dimostrare che questa funzione è iniettiva, questo porta alla conclusione che* $|Stab_{\underline{S}}| \leq |\underline{S}| = p^r$ *dato che* $\underline{S} \in X$ □

**Esempio**
Sia $|G| = 12 = 2^2 \cdot 3 = 3 \cdot 4$
Dal I Teorema di Sylow segue:
$\cdot Syl_2(G) \neq 0 \Rightarrow \exists H \leq G : |H| = 4$
$\cdot Syl_3(G) \neq 0 \Rightarrow \exists H \leq G : |H| = 3$

**Osservazione**
$\cdot X = O_{S_1} \circ O_{S_2} \circ \ldots \circ O_{S_r}$
$\Rightarrow |X| = \sum_{j=1}^{r} |O_{S_j}|$ Ma $|X| \not\equiv_p 0$

**Idea**
$G$ gruppo, $|G| = p^r$
$MCD(p, m) = 1, p$ primo, $p, r, m \in \mathbb{Z}_{>0}$
Per il I teorema sappiamo che (1)$Syl_p(G) \neq 0$.
il II Teorema ci dirà che (2) Tutti i $p - Sylow$ sono tra loro coniugati.
Il (3) ci dice che $\rightarrow$ Un $p$-Sylow è normale se e solo se è l'unico $p$-Sylow.
Quanti sono i $p$-Sylow? Analogamente $n_p := |Syl_p(G)| =?$

**Teorema 30** (II Teorema di Sylow)
*Dati* $H_1, H_2 \in Syl_p(G), \exists g \in G$ *t.c.* $\quad gH_1g^{-1} = H_2$

**Dimostrazione**
*L'enunciato è equivalente a dimostrare che la seguente azione è transitiva.*

$$\begin{aligned} G \times Syl_p(G) &\rightarrow Syl_p(G) \\ (g, H) &\rightarrow gHg^{-1} \end{aligned}$$

*o equivalentemente, che esiste un'unica orbita.*
*Per assurdo supponiamo che esistano due orbite distinte,* $O_H^G$ *e* $O_K^G$.
***Passo 1***
*Denotiamo con* $Stab_H^G$ *lo stabilizzatore di* $H$ *rispetto a questa azione*

$$\begin{cases} |G| = |O_H^G| \cdot |Stab_H^G| = |O_H^G| \cdot [Stab_H^G : H] \cdot |H| \\ H \leq Stab_H^G \end{cases} .$$

*Quindi* $p \nmid |O_H^G|$
***Passo 2***
*Restringiamo l'azione*

$$\begin{aligned} K \times O_H^G &\rightarrow O_H^G \\ (k,S) \quad & S\ k^{-1} \end{aligned}$$

*Rispetto a questa azione abbiamo orbite diverse.*
*In particolare*
$|O_H^G| = O_{H_1}^K \cup \ldots \cup O_{H_r}^K$

$$\begin{aligned} \Rightarrow |O_H^G| &= \sum_{i=1}^{r} |O_{H_i}^K| \\ &= \sum_{i=1}^{r} \frac{|K|}{|Stab_{H_i}^K|} \\ &= \sum_{i=1}^{r} \frac{p^r}{|Stab_{H_i}|} \end{aligned}$$

*Dato che* $p \not| |O_H^G|$ *deduciamo che* $\exists H_i$ *t.c.* $|O_{H_i}^K| = 1$
$\Rightarrow 1 = |O_{H_i}^K| = [K : Stab_{H_i}^G]$
*Quindi* $K$ *stabilizza* $H_i$
$\Rightarrow kH_ik^{-1} = H_i \quad \forall k \in K$
$\Rightarrow KH_i = H_iK$
***Passo 3*** $KH_i = H_iK \Rightarrow KH_i \leq G$
$|KH_i| = \dfrac{|K| \cdot |H_i|}{|K \cap H_i|} = \dfrac{p^{2r}}{p^s}$ *con* $s < r$ *(poichè altrimenti* $K = H_i$*)*
$|KH_i| = p^{2r-s} = p^{r+t}$ *con* $t > r$
*Ma* $|KH_i|$ *divide* $|G| = p^r m$ *per Lagrange (assurdo)*

**Corollario 8**
*p primo che divide* $|G|$ *allora* $H \in Syl_p(G)$ *è normale se e solo se* $n_p = |Syl_p(G)| = 1$

***Osservazione***
*è importante sapere se* $n_p = 1$ *perché l'esistenza di sottogruppi normali spesso permette di realizzare un gruppo come prodotto semidiretto*

**Teorema 31** (III teorema di Sylow)
*G gruppo finito*

- $|G| = p^r m$
- $r, p, m \in \mathbb{Z}_{>0}$
- $p$ *primo*
- $MCD(p, m) = 1$

*Allora:*
*1)* $n_p = [G : N_G(H)]$ *dove* $H \in Syl_p(G)$
*2)* $m \equiv_{n_p} 0$
*3)* $n_p \equiv_p 1$

*Prima della dimostrazione vogliamo estendere la nozione di centralizzatore (o centralizzante)*

**Definizione 41** (Normalizzatore)
*$G$ gruppo $S \subseteq G$ sottoinsieme*
*1)Il centralizzatore di $S$ in $G$ è*

$$C(S) = \{g \in G | gs = sg \quad \forall s \in S\}.$$

*2) Il normalizzatore di $S$ in $G$ è*

$$N_G(S) = \{g \in G | gS = Sg\}.$$

***Esercizio:***
*Dimostrare che*
*1) Se $S \subseteq G \Rightarrow C(S) \leq G$*
*2) $S \subseteq G \Rightarrow N_G(S) \leq G$*
*3) $S \leq G \Rightarrow S \leq N_G(S)$*

**Dimostrazione**
*Considero l'azione*
$G \times Syl_p(G) \to Syl_p(G)$
$(g, H) \to g.H := gHg^{-1}$
*Allora* $\forall H \in Syl_p(G)$
$p^r m = |G| = [G : Stab_H] \cdot |Stab_H|$
$= [G : N_G(H)] \cdot |N_G(H)|$ *(dato che $Stab_h = N_G(H)$)*
$= [G : B_G(H)][N_G(H) : H]|H|$ *(dato che $H \leq N_G(H)$)*
*Deduciamo che* $m = [G : N_G(H)] \cdot [N_G(H) : H]$
*Ora:*
$n_p = |Syl_p(G)| = |O_H^G|$ *(II Teorema di Sylow)*
$= [G : Stab_H]$
*Quindi abbiamo dimostrato* (1) *e* (2)
*Resta da dimostrare* (3)
*di un fissato* $K \in Syl_p(G)$

$$K \times Syl_p(G) \to Syl_p(G).$$
$$(k, H) \to k.H := kHk^{-1}.$$

*Questa azione avrà $r + 1$ orbite (con $r \geq 0$)*
$O_K^K, O_{H_1}^K, \ldots, O_{H_r}^K$
*Abbiamo una decomposizione in orbite disgiunte*

$$Syl_p(G) = O_K^K \cup O_{H_1}^K \cup \ldots \cup O_{H_r}^K.$$

$$\Rightarrow n_p = |Syl_p(G)| = |O_K^K| + \sum_{j=1}^{r} |O_{H_j}^K|$$

$$= |O_K^K| + \sum_{j=1}^{r} [K : Syl_{H_j}^K].$$

$$= |O_K^K| + \sum_{j=1}^{r} [K : N_K(H_j)].$$

***Idea***
*Basta ora verificare che*

- $|O_K^K| = 1$
- $O_{H_j}^K \equiv_p 0 \quad \forall 1 \leq j \leq r$

*Abbiamo:*

$$O_K^K = [K : N_K(K)] = 1.$$

*Dato che* $H \leq N_G(H) \leq G \Rightarrow N_K(K) = K$

$$|O_{H_j}^K| = [K : N_K(H_j)] = \frac{|K|}{|N_K(H_j)|} = \frac{p^r}{|N_K(H_j)|}.$$

*dato che* $K \in Syl_p(G)$
*Quindi resta da escludere il caso* $N_K(H_j) = K$
*Ma questo è equivalente a* $KH_j = H_jK$

$$\Rightarrow \begin{cases} KH_j \leq G \\ |KH_j| = \frac{|K||H_j|}{|K \cap H_j|} = \frac{p^{2r}}{p^{s_j}} \end{cases} .$$

*dove* $0 \leq s_j < r$ *dato che* $H_j \neq K_j$
*Ma* $p^{2r-s_j} \nmid p^r m$ *da cui l'assurdo per Lagrange* □

## 5.5 Applicazioni di Sylow

Possiamo (ri)-dimostrare un vecchio risultato

**Teorema 32** (Cauchy)
*G gruppo finito, p primo che divide* $|G|$ *allora* $\exists g \in G$ *tale che* $ord(g) = p$

**Dimostrazione**
*Da Sylow I segue che esiste* $H \in Syl_p(G)$
*Scegliamo* $h \in H$ *tale che* $h \neq e$
*Ora* $ord(h) = p^s$ *per qualche* $s > 0$
*Definiamo* $f = h^{p^{s-1}}$
$f = h^{p^{s-1}} \neq e \Rightarrow ord(h) \neq 1$
$f^p = (h^{p^{s-1}})^p = h^{p^s} = e \Rightarrow ord(f) = p$ □

**Teorema 33** (Wilson)
*$p$ primo allora* $(p-1)! \equiv_p p-1$

**Dimostrazione**
*Scelgo* $G = S_p$ *Studio* $n_p$
*I p-Sylow in* $S_p$ *hanno ordine p*
$\Rightarrow$ *sono tutti i sottogruppi ciclici di ordine p in* $S_p$
$\cdot$ *Gli unici elementi di ordine p in* $S_p$ *sono i p-cicli.*
*fissato il primo elemento, abbiamo* $p-1$ *scelte per il secondo,* $p-2$ *per il terzo e così via*
*quindi i p-cicli sono* $(p-1)!$
*Quindi i sottogruppi di* $S_p$ *di ordine p sono* $\frac{(p-1)!}{(p-1)} = (p-2)!$ *perché in ogni tale sottogruppo appaiono* $p-1$ *p-cicli*
$\Rightarrow (p-2)! = n_p \equiv_p 1 \quad \Rightarrow \quad (p-1)! \equiv_p p-1$ $\square$

**Teorema 34** (Classificazione dei gruppi $pq$)
*$G$ gruppo finito,* $p, q > 1$ *tali che*
$\cdot p, q$ *primi*
$\cdot p < 1$
$\cdot |G| = pq$
*Allora*
*1) Se* $p \nmid q-1$ *allora* $G \cong C_{pq}$
*2) Se* $p | q-1$ *allora* $G \cong C_q \rtimes_\phi C_p$

**Dimostrazione**
*Studio* $n_q$
$$\begin{cases} p = m \equiv_{n_q} 0 \\ n_q \equiv_q 1 \end{cases}$$
$$\Rightarrow \begin{cases} n_q = 1 \text{ oppure } n_q = p \\ \text{seconda esclude } n_q = p \text{ perchè } p < q \end{cases}$$
$\Rightarrow n_q = 1$
$\Rightarrow \exists! Q \in Syl_p(G)$
$\Rightarrow Q \trianglelefteq G$ *e* $|G| = q \Rightarrow Q \cong C_q$
*Studio* $n_p$ *nel caso* $p \nmid q-1$
$$\begin{cases} q\text{-}m \equiv_{n_p} 0 \\ n_p \equiv_p 1 \end{cases} \Rightarrow n_p = 1 \text{ oppure } n_p = q$$
$\Rightarrow n_p \neq q$ *perché*
$q \not\equiv_p 1$ *per ipotesi*
$n_p = 1 \Rightarrow \exists! P \in Syl_p(G)$
$\Rightarrow PG$ *e* $|P| = p \Rightarrow P \cong C_p$
*Ora abbiamo due sottogruppi normali* $P, Q \trianglelefteq G$
*tali che*

$\cdot P \cap Q = \{e\}$ *perchè* $|P \cap Q|$ *divide sia* $|P| = p$ *che* $|Q| = q$
$\cdot PQ| = \frac{|P||Q|}{|P|} = pq = |G|$
$\Rightarrow G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$
*Resta il caso* $p|q-1$
$\cdot \exists! Q \in Syl_p(G) \rightsquigarrow Q \trianglelefteq G$
$\cdot \exists P \in Syl_p(G) \rightsquigarrow P \leq G$
*Ora*
$\cdot P \cap Q = \{e\}$ *come prima*
$PQ = G$ *come prima*
*Quindi* $G$ *prodotto semidiretto interno*
$\Rightarrow G \cong Q \rtimes_\phi P \Rightarrow C_q \rtimes_\phi C_p$
*per qualche omomorfismo* $\phi : C_p \to Aut(C_q)$ □
**Esercizio:**
Classificare i gruppi di ordine $2q$ con $q > 2$ primo □

## 5.6 Ricordo:

**Teorema 35**
$p < q$ *primi* $G$ *gruppo finito di ordine* $pq$
*Allora:*
$\cdot$ *se* $p \not| q+1$ *allora* $G \cong C_{pq}$
$\cdot$ *se* $p|q+1$ *allora* $G \cong C_q \rtimes_\phi C_p$

**Osservazione**
Il professore ha costruito una tabella fino all'ordine 9

**Corollario 9**
$q > 2$ *primo,* $G$ *gruppo di ordine* $2q$
*Allora* $G \cong C_{2q}$ *oppure* $G \cong D_q$

**Dimostrazione**
*Dal teorema basta studiare gli omomorfisimi*

$$\begin{aligned} \phi : & C_2 \to Aut(G) \\ & s \to (\phi_s : r \to s) \end{aligned}$$

*Affinchè* $\phi$ *sia un omomorfismo, dato che* $ord_{C_2}(s) = 2$
*dobbiamo imporre che* $ord_{Aut(G)}(\phi_s) \in \{1, 2\}$
*Se è uguale a 1* $\phi_s = Id \Rightarrow \phi$ *omomorfismo banale*
$\Rightarrow$ *il prodotto è diretto*
$\Rightarrow G \cong C_q \times C_2 \cong C_{2q}$
*Nell'altro caso* $ord_{Aut(G)}(\phi_s) = 2$
$\Rightarrow \phi_s \circ \phi_s = Id_{C_q} \Rightarrow \phi_s(\phi_s(r)) = r$
$\phi_s(r^k) = r$

$\Rightarrow k^2 \equiv_{ord_{C_1}(r)} 1 \Rightarrow k^2 \equiv_q 1$
$\Rightarrow (k-1)(k+1) \equiv_q 0$
$\Rightarrow k \equiv_q \pm 1$
*Se* $k \equiv_q 1$
$\Rightarrow \phi_s = Id_{C_q} \Rightarrow G \equiv C_{2q}$
*Se* $k \equiv_q -1$
$\Rightarrow \phi_s(r) = r^{-1}$
$\Rightarrow G \cong C_q \rtimes_\phi C_2 \cong D_q$ *(già visto)*

□

## 5.7 Gruppi di ordine 12

Studiamo $G$ tramite i teoremi di Sylow
$\cdot Syl_2(G) \neq \emptyset$
$\cdot Syl_3(G) \neq \emptyset$
Dal Sylow III abbiamo

$$\begin{cases} n_2 \equiv_2 1 \\ 3 \equiv_{n_2} 0 \end{cases} .$$

$\Rightarrow n_2 = 1$ oppure $n_2 = 3$
Dal Sylow II

$$\begin{cases} n_3 \equiv_3 1 \\ 4 \equiv_{n_3} 0 \end{cases} .$$

$n_3 = 1$ oppure $n_3 = 4$
**Osservazione:**
Esiste un sottogruppo normale in $G$
**Dimostrazione**
*se* $n_3 = 4$
*Allora in G esistono 4 sottogruppi di ordine 3*
*Ognuno dei quali contenente due elementi di ordine 3.*
*Quindi G contiene 8 elementi di ordine 3.*
*Quindi i restanti 3 elementi di ordine diverso da 3 formano necessariamente l'unico* 2*-Sylow* □
**Esercizio:**
Se $|G| = 12$ e $n_3 = 4$ allora esiste un omomorfismo iniettivo $G \to S_4$
**Nota**
Da questo segue che $G \cong A_4$ perchè $A_4$ è l'unico sottogruppo di ordine 12 in $S_4$
**Dimostrazione**
$G \times Syl_3(G) \to Syl_3(G)$
$(g, H) \to gHg^{-1}$
$n_3 = 4$
$\Rightarrow Syl_3(G) = \{H_1, H_2, H_3, H_4\}$
*Definiamo*
$\psi : G \to S_4$

$g \to \tau_g$
$\tau_g(i) = j \Leftrightarrow gHg^{-1} = H_j$ *con* $i \in \{1,2,3,4\}$ *(Questa è l'idea da utilizzare negli esercizi delle schede*
*Verifiche:*
1)$\psi$ *è ben definita, Infatti* $\tau_g$ *è invertibile con inversa* $\tau_{G^{-1}}$
2) $\psi$ *è un omomorfismo, ovvero*

$$\psi(gf) = \psi(g)\psi(f).$$

$\tau_{gf}(i) = j$
$\Leftrightarrow (gf)H(gf)^{-1} = H_j$
$\Leftrightarrow g(fHf^{-1})g^{-1} = H_j$
$\Leftrightarrow \tau_g(\tau_f(i)) = j$
*3)* $\psi$ *iniettiva*
*supponiamo che* $\tau_g = \tau_f$
$gHg^{-1} = fHf^{-1} \quad \forall H \in Syl_3(G)$
$\Rightarrow (f^{-1}g)H(f^{-1}g)^{-1} = H \quad \forall H \in Syl_3(G)$
$\Rightarrow f^{-1}g \in N_G(H) \quad \forall H \in Syl_3(G)$
$\Rightarrow f^{-1}g \in \bigcap_{H \in Syl_3(G)} N_G(H)$
$\Rightarrow f^{-1}g \in \bigcap_{H \in Syl_3(G)} H = \{e\} \Rightarrow f^{-1}g = 3 \Rightarrow f = g$
*Resta da verificare che* $H = N_G(H)$
$4 = n_3 = [G : N_G(H)] = \dfrac{|G|}{|N_G(H)|} = \dfrac{12}{N_G(H)} \Rightarrow |N_G(H)| = 3$
*Ma* $H \leq N_G(H) \Rightarrow H = N_G(H)$ □

## 5.8 Studiare gruppi di ordine 12 in cui $n_3 = 1$

Da Sylow III Segue che $\exists! Q \in Syl_3(G) \Rightarrow Q \trianglelefteq G$
Esiste in $G$ almeno un 2-Sylow $P \leq G$
Ora:
$\cdot G \trianglelefteq G, \quad P \leq G$
$\cdot Q \cap P = \{e\}$ (perchè l' $MCD(|Q|, |P|) = 1$
$\cdot |QP| = \dfrac{|Q||P|}{|Q \cap P|} = \dfrac{3 \cdot 4}{1} = 12$
$\Rightarrow QP = G$
Allora $G \cong Q \rtimes_\phi P$ per qualche
$\phi : P \to Aut(Q) \cong C_2$
Quindi studiamo i possibili omomorfismi
$\phi : P \to Aut(C_3)$ se $P \cong C_4$
$C_4 =< \gamma > \qquad C_3 =< r >$
$\phi :< \gamma > \to Aut(C_3)$
$\gamma \to (\phi_\gamma : r \to r^k$ con k $\pm$ 1) nel csao $k = 1$ abbiamo $\phi$ banale

$\Rightarrow$ prodotto diretto
$\Rightarrow G \cong C_3 \times C_4 \cong C_{12}$
nel caso $k = -1$
abbiamo $G \cong C_3 \rtimes_\phi C_4 \cong Dic_3$
dove
$\phi : C_4 \to Aut(C_3)$

$\gamma \to (\phi_\gamma : r \to r^{-1})$
$P \cong K_4$
$\phi : K_4 \to Aut(C_3)$

$\{Id, a, b, ab\}$

$a \to (\phi_a : r \to r^{\pm 1})$

$b \to (\phi_b : r \to r^{\pm 1})$

$ab \to (\phi_{ab} : r \to r^{\pm 1})$
Se $\phi$ è banale
$\Rightarrow$ prodotto diretto
$\Rightarrow G \cong C_3 \times K_4$

$\cong C_3 \times C_2 \times C_2$

$\cong C_6 \times C_2$
Se $\phi$ è non banale, a meno di rinominare gli elementi $\{a, b, ab\}$ avremo che

$\phi_a r \to r$

$\phi_b r \to r^{-1}$ Grazie (!) a Esercizio 1 di scheda 7 tutti i restanti prodotti

$\phi_{ab} r \to r^{-1}$
semidiretti sono isomorfi
$G \cong C_3 \rtimes_\phi K_4 \cong D_6$
Infatti $|D_6| = 12$
$D_6$ non è isomorfo ad alcuno dei precedenti casi
1)$C_2$ è ciclico
2)$C_6 \times C_2$ è abeliano, ma non ciclico
3)$A_4$ unico caso in cui $n_3 = 4$
4)$Dic_3$ non è abeliano e contiene elementi di ordine 4
5)$D_6$ non è abeliano e non contiene elementi di ordine 4 ($C_4$)

## 5.9 Radici primitive

**Definizione 42** (Radice primitiva modulo (n))
*Un intero a si definisce radice primitiva modulo (n) se* $ord_{U_n}([a]) = \phi(n)$

**Osservzaione:**
Per teorema di Eulero

$$a^{\phi(n)} \equiv_n 1.$$

$\Rightarrow ord_{U_n}([a]) = \phi(n)$
**Osservazione**
$a$ radice primitiva mod (n) significa che $U_n =< [a] >$
**Obiettivo** (Scheda 7)
Dimostrare che se $p > 1$ primo allora $\exists$ radice primitiva modulo $(p)$
**Esempi**
Non esistono radici primitive mod(8)
Studio $U_8 = \{[1], [3], [5], [7]\}$

$$\phi(8) = 2^3 - 2^2 = 4.$$

$1^2 \equiv_8 1$

$3^2 \equiv_8 1$

$5^2 \equiv_8 1$

$7^2 \equiv_8 1$
**Es(ercizio esempio)**
3 è radice primitiva mod(7)
**Svolgimento:**
$3^1 \equiv_7 3$
$3^2 \equiv_7 2$
$3^3 \equiv_7 1$
$3^4 \equiv_7 3$
$3^5 \equiv_7 2$
$3^6 \equiv_7 1$

---

2 è radice primitiva mod(9)
**Da fare**
**Esercizio**(Scheda 7)
Dimostrare che
$Aut(C_p) \cong C_{p-1}$
**Soluzione**
Sappiamo che
$Aut(C_p) \cong U_p \cong C_{\phi(p)} \cong C_{p-1}$
**Esercizio**
$p$ primo
$f(x) = a_n x^n + \ldots + a_1 x + a_0$
$f(x) \equiv_p 0$ ammette al più $p$ soluzioni distinte in $\mathbb{Z}/(p)$

**Dimostrazione**
*per induzione su n*
*se* $n = 1 \Rightarrow a_1 x \equiv_p -a_0$
$\Rightarrow x \equiv_p = -a \cdot a_1^{-1}$ $a_1$ *invertibile in* $\mathbb{Z}/(p)$ *per ipotesi*
$n > 1$
*Se* $f(x) \equiv_p 0$
*non ammette soluzioni ok*

*Se invece $a$ è soluzione dividiamo*
$f(x) = (x-a)q(x) + r$
$\Rightarrow f(x) \equiv_p (x-a)q(x) + r$
*Valuto in $a$:*
$\Rightarrow 0 \equiv_p f(a) \equiv_p (a-a)q(a) + r$
$\Rightarrow f(x) \equiv_p (x-a)q(x)$
*Sia $b \not\equiv_p a$ tale che $f(b) \equiv_p 0$*
$0 \equiv_p f(b) \equiv_p (b-a)q(b)$
$\mathbb{Z}/(p)$ *dominio d'integrità*
$q(b)_p 0$
*Ma per induzione $q(x) \equiv_p 0$*
*ammette al più $n-1$ soluzioni distinte*
$\Rightarrow f(x) \equiv_p 0$ *ammette al più $n$ soluzioni*

□

## 5.10 Ricordo (Lagrange)

$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ tale che $a_n \not\equiv_p 0$ con $p > 1$ primo
Allora $f(x) \equiv_p 0$ ammette al più $n$ soluzioni

**Corollario 10**
*Dimostrare che se $p$ primo e $d|(p-1)$ allora $x^d - 1 \equiv_p 0$ ammette esattamente $d$ soluzioni*

**Dimostrazione** (Soluzione)
*Abbiamo che se $d(p-1)$ allora $(x^d-1)|(x^{p-1}-1)$*
$\Rightarrow x^{p-1} = (x^d-1)f(x)$
*dove $f$ è di grado $(p-1-d)$*
*Ora $x^{p-1} \equiv_p 1$ ammette $p-1$ soluzioni distinte per il piccolo teorema di Fermat.*
*Le soluzioni sono $1, 2, \ldots, p-1$*
*Se una di tali soluzioni non risolve $f(x) \equiv_p 0$ allora risolve $x^d - 1 \equiv_p 0$ (Sto usando il fatto che $\mathbb{Z}/(p)$ è un dominio d'integrità [prodotto commutativo e se il prodotto tra due numeri è 0 allora o uno o l'altro sono 0])*
*Dato che $f(x) \equiv_p 0$ ammette al più $p-1-d$ soluzioni distinte deduciamo che $x^d - 1 \equiv_p$ ammette almeno $d = (p-1) - (p-1-d)$ soluzioni distinte in $\mathbb{Z}/(p)$.*
*D'altra parte per l'esercizio precedente ne ammette al più $d$, e quindi segue la tesi.* □

**Corollario 11** (Esercizio)
*$p > 1$ primo, $d|(p-1)$ Allora, esistono esattamente $\phi(d)$ interi, distinti in $U_p$, di ordine $d$ in $U_p$*

**Dimostrazione** (Soluzione)
*Introduco $S_d = \{k \in \mathbb{Z} | ord_{U_p}([k]) = d, \quad 1 \leq k \leq p-1\}$*

*La tesi è equivalente a dimostrare che* $|S_d| = \phi(d)$
*Abbiamo una partizione* $\{1, \dots, p-1\} = \bigcup_{d|p-1} S_d$
*Quindi* $p - 1 = \sum_{d|(p-1)} |S_d|$
*Ricordo:*
$n = \sum_{d|n} \phi(d)$ *(esercizio delle vecchie schede)*
*Scegliendo* $n = p - 1$ *deduciamo*
$\sum_{d|p-1} |S_d| = \sum_{d|p-1} \phi(d)$
*Basta allora dimostrare che* $|S_d| \leq \phi(d) \quad \forall d | p-1$
*Se* $S_d = \emptyset \Rightarrow |S_d| = 0 \leq \phi(d)$
*Se* $S_d \neq \emptyset \Rightarrow \exists a \in S_d$
$\Rightarrow \{a, a^2, a^3, \dots, a^d\}$ *sono tutti distinti* $mod(p)$ *infatti*

$$a^i \equiv_p a^k$$
$$\Updownarrow$$
$$i \equiv_d j$$

*Quindi* $a, a^2, \dots, a^n$ *sono tutte e sole le soluzioni di* $x^d - 1 \equiv_p 0$ *Quindi gli elementi di ordine* $d$ *in* $U_p$ *sono della forma* $a^j$ *per qualche* $j \in \{1, \dots, j\}$
*Ma* $ord([a^j]) = \frac{d}{MCD(j,d)}$ *(esercizio di una riga)*
*Quindi* $|S_d| = \phi(d)$

□

**Corollario 12** (Esercizio)
$p > 1$ *primo:*
*Allora esistono esattamente* $\phi(p-1)$ *radici primitive distinte*

**Dimostrazione** (Soluzione)
*Basta applicare l'esercizio precedente, scegliendo* $d = p - 1$ □

---

**Esercizio**
$p > 1$ primo
dimostrare che $Aut(C_p) \cong C_{p-1}$
**Soluzione:**
Sappiamo che $Aut(C_p) \cong U_p \cong C_{p-1}$
Dove la prima congruenza la sappiamo da teoremi precedenti, la seconda viene data dal precedente corollario

**Congettura 1** (Gauss, 1801)
*Esistono infiniti primi per cui* 10 *è una radice primitiva*

**Congettura 2** (E. Artin, 1927)
$a \in \mathbb{Z}$, $a \neq \pm 1$
*Assumiamo che a non sia un quadrato perfetto, Allora esistono infiniti primi per cui a è una radice prima*

**Osservazione**
Oggi sappiamo che la congettura di Artin è vera per infiniti interi $a$, ma non è noto quali
**Esercizio:** $p > 1$ primo
Sia $a = x^2$ con $x \in \mathbb{Z}$
Dimostrare che se $[a] \in U_p$
allora $ord_{U_p}([a]) \neq p - 1$
**Esercizio** [classificazione dei gruppi di ordine $pq$]
Dimostrare che tutti i gruppi non ciclici di ordine $pq$ con $p \neq q$ primi, sono fra loro isomorfi e non abeliani
**Soluzione**
Dato $G$ tale che $|G| = pq$ Avevamo dimostrato che $\exists! Q \in Syl_q(G) \ \Rightarrow \ Q \trianglelefteq G$
Inoltre $\exists P \in Syl_p(G) \Rightarrow P \leq G$
Abbiamo verificato che:
$\cdot P \cap Q = \{e\}$
$\cdot |PQ| = |G| \Rightarrow PQ = G$
$\Rightarrow G \cong Q \rtimes_\phi P \cong C_q \rtimes_\phi C_p$
dove $\phi : C_p \to AutC_q \cong C_{q-1}$
cot se $p \not| q - 1 \Rightarrow \phi$ è banale $\Rightarrow G \cong C_q \times C_p \cong C_{pq}$
$\cdot$ se $p|q - 1 \Rightarrow \phi$ potrebbe essere non banale $\Rightarrow ord_{Aut(C_q)}(\phi_P) = p \Rightarrow Im(\phi) \subseteq Aut(C_q) \cong C_{q-1}$ con $|Im(\phi)| = p$
Sappiamo che $C_{q-1}$ contiene un unico sottogruppo di ordine $p \Rightarrow Im(\phi)$ non dipende da $\phi$ (a meno che $\phi$ non banale)
$\Rightarrow$ A meno di "precomporre" $\phi$ con un automorfismo di $C_q$ la mappa $C_p \to Aut(C_q) \cong C_{q-1}$ è univocamente determinata
**Concretamente:**
Dati $\phi, \phi' : C_p \to Aut(C_q)$ non banali $\Rightarrow$ esiste $B \in Aut(C_p)$ tale che $\phi' = \phi \cdot B \Rightarrow C_q \rtimes_\phi C_p \cong C_q \rtimes_\phi C_p$ quindi esiste un'unica classe d'isomorfismo non ciclica

## 5.11 Successioni esatte corte

**Esercizi [Scheda 9]**

**Definizione 43**
*Una successione esatta corta di gruppi è una coppia di omomorfismi* $H \xrightarrow{r} G \xrightarrow{\pi} K$ *dove* $r$ *iniettivo* $\pi$ *suriettivo e* $Im(r) = ker(\pi)$

- $G$ *si dice estensione di* $K$ *tramite* $H$
- *la successione spezza se* $\exists S : K \to G$ *omomorfismo tale che* $\pi \circ S = Id$
- $S$*, se esiste, si chiama sezione*

**Esempi**
Costruire una successione esatta corta (SEC) di $Q_8$ che estende $K_4$ tramite $C_2$
**Soluzione**

$$\{Id, \rho\} = C_2 \xrightarrow{r} Q_8 \xrightarrow{\pi} K_4$$

$r$ per essere iniettiva deve mandare $\rho$ che è di ordine 2 in un elemento di ordine 2.
$ord(r(\rho)) = 2 \Rightarrow r(\rho) = -1$ $\begin{matrix} Id \to 1 \\ \rho \to -1 \end{matrix}$
Considero la proiezione al quoziente $Q_8 \to Q_8/\{\pm 1\} \cong K_4$
$\Rightarrow$ basta prendere $\pi : Q_8 \to Q_8/\{\pm 1\} \cong K_4$
2) Non spezza!:
Se spezzasse dato che una sezione è necessariamente iniettiva (esercizio), ma non esistono omomorfismi iniettivi da $K_4$ in $Q_8$
$\mathrm{Z} \xrightarrow{r} \mathbb{R} \to S^1 \leq C^*$
3) $\mathrm{n} \to 2\pi n$
$\theta \to e^{i\theta}$
è una SEC che non spezza

**Definizione 44** (Spezza)
*Una successione esatta corta* $H \to G \to K$ *spezza se* $\exists S : K \to G$ *omomorfismo t.c.* $\pi \circ S = Id_K$

**Osservzione**
Una sezione è iniettiva
**Esempio:**
$H, K$ gruppi $G := H \rtimes_\phi K$
per qualche $\phi : K \to Aut(H) \Rightarrow$
$\mathrm{H} \xrightarrow{r} H \rtimes_\phi K \xrightarrow{\pi} K$
$h \to (h, e_K)$ è una SEC che spezza
$(h, k) \to k$

$\cdot r$ è iniettiva
$\cdot \pi$ è suriettiva
$\cdot Im(r) = \{(h, e_K) | h \in H\} = ker(\pi)$
$\cdot$ spezza perchè S: $K \to H \rtimes_\phi K \quad k \to (e_K, k)$
è una sezione:

$$(\pi \cdot S)(k) = \pi(e_H, k) = k \quad \forall k \in K.$$

**Esercizio scheda 9**
Data una SEC $H \xrightarrow{r} G \xrightarrow{K}$ con $S : K \to G$ che spezza $\Rightarrow GH \rtimes_\phi K$
**Soluzione:**
Osservo che:
$\cdot r(H) \leq G \rightsquigarrow \cdot r(H) = ker(\pi)G$
$\cdot S(K) \leq G \rightsquigarrow \cdot r(H) \cap S(K) = \{e_G\}$
$\Rightarrow$ Sia $x \in r(H) \cap S(K) \Rightarrow \exists h \in H, \exists k \in K$
$t.c. x = r(h) = S(k)$
Applicando $\pi$ :
$e_K = \pi(r(h)) = \pi(S(k)) = k \ \Rightarrow \ x = S(k) = S(e_K) = e_G$
$\cdot r(H) \cdot S(K) = G$
$g \in G \rightsquigarrow \pi(g) \in K \rightsquigarrow f = S(\pi(g)) \in S(K) \leq G$
Vorremmo ora scrivere $g$ come un'elemento in $r(H)$ per $f$
Basta quindi mostrare che $gf^{-1} \in Im(r)$ ma $Im(r) = ker(\pi)$
Applicando $\pi$ : $\pi(gf^{-1}) = \pi(g)\pi(f^{-1}) = \pi(g)\pi(S(\pi(g^{-1}))) = \pi(g) \cdot (\pi \circ S)(\pi(g^{-1})) = \pi(gg^{-1}) = e_K$
Sapendo che $f^{-1} = (S(\pi(g)))^{-1}$ e che $(\pi \circ S) = Id_K$
Quindi $gf^{-1} \in ker(\pi) = Im(r) \Rightarrow \exists h \in H$ t.c. $gf^{-1} = r(h) \Rightarrow g = r(h)g = r(h)S(\pi(g))$
$\quad \cap \qquad \cap$
$Im(r) \ Im(S)$
$\cdot$ Deduciamo che $G \cong r(H) \rtimes_\phi S(K) \cong H \rtimes_\phi K$
poiché $r$ e $S$ iniettive $\Rightarrow H \cong r(H)$ e $K \cong S(K)$

## 5.12 Quaternioni

$i^2 = j^2 = k^2 = ijk = -1$
$\mathbb{H} = \{a + bi + cj + dk | i^2 = j^2 = k^2 = -1, ijk = -1, a, b, c, d \in \mathbb{R}\}$
è uno spazio vettoriale di dimensione 4.
Dalla scheda 9 segue che $\mathbb{H}^* = \mathbb{H} \setminus \{0\}$ è un gruppo moltiplicativo.

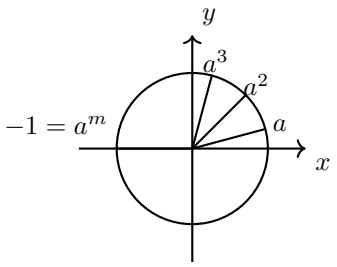
**Definizione 45**
$n \geq 2 \quad Dic_n :=< a, j > \leq \mathbb{H}^*$ *dove* $a = \cos(\frac{\pi}{n}) + i \sin(\frac{\pi}{n}) \in \mathbb{H}^*$

**Osservazione**
$(a)$ è un gruppo ciclico di ordine $2n$
**Osservazione**

$n = 2 \rightsquigarrow a = \cos(\frac{\pi}{2}) + i\sin(\frac{\pi}{2}) = i \quad \Rightarrow \quad Dic_2 =< i, j >= \{\pm 1, \pm i, \pm j, \pm k\} = Q_8$

## 5.13 Gruppi diciclici

$Dic_n =< a, j > \leq \mathbb{H}^*$
1) $ord(a) = 2n \quad ord(j) = 4$
2) Mostrare $j^2 a^m = a^m + n = a^m j^2$
**Soluzione**
$j^2 = -1$ e $a^n = -1$ tutti i membri delle uguaglianze sono quindi $-a^m$
3) Mostrare $j^{\pm 1} a^m = a^{-m} j^{\pm 1}$
**Soluzione**
$j^-1 = -j$
$ja^m = j(cos(\frac{m\pi}{n}) + i\sin(\frac{m\pi}{n}) = \cos(\frac{m\pi}{n})) = \cos(\frac{-m\pi}{n}) + i\sin(-\frac{m\pi}{n}) = a^{-m} j$
$\Rightarrow ja^m - a^{-m} j \Rightarrow -ja^m = a^{-m}(-j) \Rightarrow j^{-1} a^m = a^{-m} j^{-1}$
6) Mostrare che ogni elemento in $Dic_n$ può scriversi come $a^m j^k$ con $0 \leq m < 2n$
$0 \leq j \leq 1$ segue dalle relazioni precedenti $\Rightarrow Dic_n = \{a^m | 0 \leq m < 2n\} \cup \{a_j^m | 0 \leq m < 2n\}$
$\Rightarrow (6) : |Dic_n| = 4n$
8) Mostrare che esiste una SEC
$C_{2n} \xrightarrow{r} Dic_n \to \pi C_2$
$\rho \to a$
$\cdot r(\rho)L = a \Rightarrow r$ iniettiva
$\cdot \pi : Dic_n \to C_2$
Vorrei verificare proiezione al quoziente.
In effetti $r(C_{2n}) =< a > \trianglelefteq Dic_n$ perchè
$\pi : Dic_{m2} =< \sigma >$
$[Dic_n :< a >] = 2 \qquad a^m \to e \qquad$ 9) Mostrare che <u>non</u> si spezza
$a^m j \to \sigma$
**Soluzione**
Mi chiedo se esiste una sezione $S : C_2 \to Dic_n$
Se $S$ esiste allora $S(\sigma) = a^m j$ per qualche $0 \leq m < 2n$
$ord(a^m j) = 4 \rightsquigarrow (a^m j)(a^m j) = a^{m-m} j = j^2 = -1$
$\Rightarrow ord(S(\sigma)) \neq ord(\sigma) \Rightarrow$ assurdo
10) Mostrare che esiste unna SEC
$C_n \xrightarrow{r} Dic_n \xrightarrow{\pi} C_4$ ds n dispari:




$C_n =< \rho > \xrightarrow{r} Dic_n$
$\rho \to a^2$

$\pi : Dic_n \to C_4 =< r > \quad \pi(a^m) = \begin{cases} Id & \text{se } m \equiv_2 0 \\ r^2 & \text{se } m \equiv_2 1 \end{cases}$

$\pi(a^m j) = \begin{cases} rm & \text{se } m \equiv_2 0 \\ r^3 m & \text{se } m \equiv_2 1 \end{cases}$

**Osservazione**

$r^2 = \pi(j^2) = \pi(a^n) = \begin{cases} Id & \text{se } n \text{ pari} \\ r^2 & \text{se } n \text{ pari} \end{cases}$

2) $n \geq 3$ dispari
Dimosrtare che $Dic_n \cong C_n \rtimes_\phi C_4$ per qualche $\phi : C_4 \to Aut(C_n)$
**Soluzione:**
Costruiamo $S : C_4 \to Dic_n$
· dobbiamo solo definire $S(r) = j$
· $S$ omomorfismo
·$\pi \circ S(r) = \pi(j) = r$

**Definizione 46**
*Un gruppo $G$ si dice semplice se i suoi unici sottogruppi normali sono $\{e\}$ e $G$*

**Esempio:**
·$Q_8$ non è semplice
·$A_3 \cong C_3$ è semplice
·$A_4$ non è semplice;
Ricordo:
per $A_4$ sia ha $n_3 = 4$ e $n_2 = 1 \Rightarrow A_4$ contiene un unico 2-Sylow ("sottogruppo di oridne 4") che quindi è normlae

$$V = \{Id, (12)(34), (13)(24), (14)(23)\} \rightsquigarrow V \trianglelefteq A_4.$$

**Proposizione 13**
*$A_n$ è semplice $\forall n \geq 5$*

· Strategia: Vogliamo procedere per passi dimostrando che:
1) $\{e\} \neq H \trianglelefteq A_n \Rightarrow H$ contiene un 3-ciclo
2) Se $H$ contiene un 3-ciclo $\Rightarrow$ li contiene tutti
3) $A_n$ con $n \geq 5$ è generato dai 3-cicli

**Lemma 6**
*$\{e\} \neq H \trianglelefteq A_n$ Allora*
*$H$ contiene almeno un 3-ciclo oppure (almeno un prodtotto di trasposizioni disgiunte)*

**Dimostrazione**
*Sia* $\sigma \in H, \sigma \neq Id \Rightarrow \sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_k$
*con* $\sigma_i$ *cicli disgiunti.*
*Caso I:* $\sigma_1$ *è* $m$ *ciclo con* $m \geq 4$ $\sigma_1 = (a_1 a_2 a_3 \ldots)$
$:= (a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1} \in H \Rightarrow \sigma\tau^{-1} \in H$
$\Rightarrow \sigma\tau^{-1} = \sigma(a_1 a_2 a_3 a)\sigma^{-1}(a_1 a_2 a_3)^{-1} = (\sigma(a_1)\sigma(a_2)\sigma(a_3))$
$= (a_2 a_3 a_4)(a_1 a_3 a_2) = (a_1 a_4 a_2)(a_3) \in H$
*Caso II* $m = 3$ *per casa*
*Caso I :* $m = 2$ *per casa* □

## 5.14 Gruppi semplici

**Definizione 47** (Gruppo Semplice)
*Un gruppo di dice semplice se gli unici sottogruppi normali sono banali*

**Obiettivo**
Dimostrare $A_n$ è semplice per $n \geq 5$
**Osservazione:**
$A_4$ non è semplice
$A_2$ e $A_3$ sono semplici
**Strategia**
$n \geq 5$
1) $\{Id\} \neq H \trianglelefteq A_n$ allora $H$ contiene almeno un 3-ciclo
2) $\{Id\} \neq H \trianglelefteq A_n$ se $H$ contiene un 3-ciclo allora li contiene tutti
3) $A_n$ è generato dai suoi 3-cicli
Ricordo:

**Lemma 7**
$n \geq 3 \ \ \{Id\} \neq H \trianglelefteq A_n$
*Allora $H$ contiene almeno un 3-ciclo oppure un prodotto di trasposizioni disgiunte*

**Proposizione 14**
$n \geq 5, \ \ \{Id\} \neq H \trianglelefteq A_n$ *allora $H$ contiene almeno un 3-ciclo*

**Dimostrazione**
*Basta verificare che se $\sigma = (a_1 a_2)(a_3 a_4) \in H$, allora esiste un e-ciclo in $H$.*
*Dato che $H \trianglelefteq A_n$ abbiamo*

$$gHg^{-1} \subseteq H \ \ \forall g \in A_n.$$

*Definiamo $a_5 \notin \{a_1, a_2, a_3, a_5\}$*
$\tau := (a_3 a_4 a_5)\sigma(a_3 a_4 a_5)^{-1} \in H$
$\Rightarrow \sigma\tau^{-1} \in H$ *Studiamo* $\sigma\tau^{-1}$
$\Rightarrow \sigma\tau^{-1} = \sigma(a_3 a_4 a_5)\sigma^{-1}(a_3 a_4 a_5)^{-1}$
*Dove* $\sigma(a_3 a_4 a_5) = (\sigma(a_3)\sigma(a_4)\sigma(a_5))$
$\sigma\tau^{-1} = (a_4 a_3 a_5)(a_3 a_5 a_4) = (a_3 a_4 a_5) \in H$ □

**Teorema 36**
$n \geq 5 \ \{Id\} \neq H \trianglelefteq A_n$
*Allora $H$ contiene tutti i 3-cicli*

**Dimostrazione**
*Basta verificare che dato*
$\sigma = (a_1 a_2 a_3) \in H$
*Allora $H$ contiene tutti i 3-cicli*
*Sfruttiamo $H \trianglelefteq A_n$*
$\Rightarrow \tau = (a_3 a_4 a_5)\sigma(a_3 a_4 a_5)^{-1}$
$\tau \in H$
*dove* $a_4, a_5 \notin \{a_1, a_2, a_3\}$
*Studiamo* $\tau$ :
$\tau = (a_3 a_4 a_5)(a_1 a_2 a_3)(a_3 a_4 a_5)^{-1} = (a_1 a_2 a_4) \in H$
*Abbiamo dimostrato che se* $(a_1 a_2 a_3) \in H$ *allora* $(a_1 a_2 a_4) \in H \ \ \forall a_4 \notin \{a_1, a_2\}$
*Dunque mostriamo che il 3-ciclo arbitrato* $(b1, b_2, b_3) \in H$ *per qualunqe* $b_1, b2, b_3$
$(a_1 a_2 a_3) \in H$
$\Rightarrow (a_1 a_2 a_3) \in H$
$\Rightarrow (b_1 b_2 b_3) \in H$

□

**Corollario 13**
*$n \geq 5$ $A_n$ è semplice*

**Dimostrazione**
*Sia $\{e\} \neq H \trianglelefteq A_n$, dimostriamo che $H = A_n$*
*Per il teorema $H$ contiene tutti i 3-cicli, quindi basta verificare che $A_n$ è generato dai 3-cicli, Sia $\sigma \neq Id, \sigma \in A_n \subseteq S_n$*
*Ricordando che $S_n$ è generato da trasposizioni*
$\Rightarrow \sigma = \tau_1\tau_2 \dots \tau_{2i-1}\tau_{2i} \dots \tau_{2k-1}$
*L'idea è verificare che $\tau_{2i-1}\tau_{2i}$ si ottiene come prodotto di 3-cicli $\forall i \in \{1, \dots, k\}$*
*Caso 1 $\tau_{2i-1} = \tau_{2i}$*
$\tau_{2i-1}\tau_{2i} = Id = (123)(132)$
*Caso 2 $\tau_{2i-1} = \tau_{2i}$*
*hanno un indice in comune*
*Allora:*
$\tau_{2i-1} = (ab)$
$\tau_{2i} = (bc)$
$\Rightarrow \tau_{2i-1}\tau_{2i} = (ab)(bc) = (abc)$
*Caso 3:*
$\tau_{2i-1}, \tau_{2i}$ *non hanno indici in comune.*
$\Rightarrow \tau_{2i-1} = (ab),\ \tau_{2i} = (cd)$
$\tau_{2i-1}\tau_{2i} = (ab)(cd)$
*Ma*
$(abc)(bcd) = (ab)(cd)$
*Quindi: $\tau_{2i-1}\tau_{2i} = (abc)(bcd)$*
*Allora $\sigma$ è prodotto di 3-cicli $\Rightarrow \sigma \in H \Rightarrow H = A_n$* □

**Esercizio**
$n \geq 5$ dimostrare che gli unici sottogruppi normali di $S_n$ sono $\{e\}, A_n, S_n\{e\}, A_n, S_n$

**Soluzione**
Osserviamo che se $H \trianglelefteq S_n$ allora $H \cap A_n \trianglelefteq A_n$ poichè $H \trianglelefteq S_n$ significa
$gHg^{-1} \subseteq H \quad \forall g \in S_n$
Quindi $\{Id\} \neq H \trianglelefteq S_n$
Studio $H \cap A_n$
1) $H \subseteq A_n$
$\Rightarrow H = H \cap A_n \trianglelefteq A_n$
$\xrightarrow{A_n \text{semplice}} H = \{Id\}$ oppure $H = A_n$
2) $H \not\subseteq A_n$
$\Rightarrow [H : H \cap A_n] = 2$ e $H \cap A_n \trianglelefteq A_n$
$A_n$ semplice$H \cap A_n = \{Id\}$ oppure $H \cap A_n = A_n$
Se $H \cap A_n = \{Id\}$
$\Rightarrow [H : H \cap A_n] = 2$
$\Rightarrow |H| = 2$
$\Rightarrow H = \{Id, \sigma\}$ con $ord(\sigma) = 2$

Se tale $H$ fosse normale allora avremmo

$g^{-1} = \sigma \quad \forall g \in S_n$
$\Rightarrow$ Assurdo perchè $\sigma$ è coniugato a tutti gli elementi con la sua stessa struttura ciclica. $\cdot$ Allora $H \cap A_n = A_n$.
$\Rightarrow [H : H \cap A_n] = 2$
$\Rightarrow |H| = n! \Rightarrow H = S$
ricordando che $H \cap A_n = A_n$

## 5.15 Classi di coniugio in $\mathbf{A}_n$

Obiettivo:
Studiare le azioni

$$\begin{array}{l|l} S_n \times A_n \to A_n & A_n \times A_n \to A_n \\ (\tau, \sigma) \to \tau\sigma\tau^{-1} & (\tau, \sigma) \to \tau\sigma\tau^{-1} \end{array}$$

**Ricordo:**
Data $\sigma \in A_n$
$O_\sigma^{S_n} = \{$ permutazioni con la stessa struttura ciclica di $\sigma\}$
Domanda: $O_\sigma^{A_n} = ?$
A priori abbiamo $O_\sigma^{A_n} \subseteq O_\sigma^{S_n}$
**Esempio:** n = 3
$O_{(123)}^{S_3} = \{(123), (132)\}$
infatti $(23)(123)(23)^{-1} = (132)$
$A_3 = \{Id, (123), (132)\}$
$O_{123}^{A_3} = \{(123)\}$
**Ricordo:**
Data $\sigma \in A_n$
$\cdot C_{A_n}(\sigma) = \{\tau \in A_n | \tau\sigma\tau^{-1}\} = Stab_\sigma^{A_n}$
$\cdot C_{S_n}(\sigma) = \{\tau \in S_n | \tau\sigma\tau^{-1} = \sigma\} = Stab_\sigma^{S_n}$
**Osservazione**
$C_A = (\sigma) = C_{S_n}(\sigma) \cap A_n$

**Teorema 37**
*$n \geq 2 \quad \sigma \in A_n$*
*1) Se $C_{S_n}(\sigma) \not\subseteq A_n$ allora $O_\sigma^{A_n} = O_\sigma^{S_n}$*
*2) $C_{S_n}(\sigma) \subseteq A_n$ allora $|O_\sigma^A n| = \frac{1}{2}|O_\sigma^{S_n}$*

**Dimostrazione**
*Supponiamo che $C_{S_n}(\sigma) \not\subseteq A_n$*
*Allora $C_{S_n}(\sigma) \leq S_n$*
$|C_{S_n}(\sigma) : C_{S_n}(\sigma) \cap A_n] = 2$
*notando che $C_{S_n}(\sigma) \cap A_n = C_{A_n}(\sigma)$*
$\Rightarrow |C_{A_n}(\sigma)| = \frac{1}{2}|O_{S_n}(\sigma)|$
$\Rightarrow \begin{cases} n! = |S_n| = |C_{S_n}(\sigma)| \cdot |O_\sigma^{S_n}| \\ \frac{n!}{2} = |A_n| = |C_{A_n}(\sigma)| \cdot |O_\sigma^{A_n} \end{cases}$

$\Rightarrow |O_\sigma^{S_n}| = |O_\sigma^{A_n}$
$\Rightarrow O_\sigma^{S_n} = O_\sigma^{A_n}$
*2) Se* $C_{S_n}(\sigma) \subseteq A_n$
$\Rightarrow C_{S_n}(\sigma) = C_{A_n}(\sigma)$
$\Rightarrow \begin{cases} n! = |S_n| = |C_{S_n}(\sigma)| \cdot |O_\sigma^{S_n}| \\ \frac{n!}{2} = |A_n| = |C_{A_n}(\sigma)| \cdot |O_\sigma^{A_n}| \end{cases}$
$\Rightarrow |O_\sigma^{A_n}| = \frac{1}{2}|O_\sigma^{S_n}|$

□

**Esempio:**
$\sigma = (123) \quad n = 5$
$\Rightarrow O_{(123)}^{S_n} = O_{(123)}^{A_n}$
perché $(45) \in C_{S_n}(\sigma)$ MA $(45) \notin A_5$
**Esercizio**
$\sigma = \sigma_1, \ldots, \sigma_k \in S_n$ disgiunti.
$\sigma_i$ è $m_i$-ciclio
1) se $\sum_{i=1}^{k} m_i \leq n - 2$
allora $O_\sigma^{S_n} = O_\sigma^{A_n}$
**IDEA:**
dall'ipotesi segue che $\exists a, b \in \{1, \ldots, n\}$ tali che $\sigma(a) = a, \sigma(b) = b$
$\Rightarrow (ab) \in C_{S_n}(\sigma)$ e $sgn(ab) = -1$

# 6 Gli anelli

**Definizione 48**
*Un anello* $(R, +, \cdot)$ *è un insieme* $R$ *dotato di due operazioni,* $+, \cdot$ *che soddisfano le seguenti:*

1. $(R, +)$ *è un gruppo abeliano*
2. *L'operazione* $\cdot$ *è associativa* $(a \cdot b \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R)$
3. $\exists 1 \in R$ *tale che* $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$ *(*$R$ *è unitario)*
4. *Vale la legge distributiva*
   $(a + b) \cdot c = a \cdot c + b \cdot c$
   $c \cdot (a + b) = c \cdot a + c \cdot b \quad \forall a, b, c \in R$

***Nota***
*Artin richiede anche la commutatività*

**Definizione 49**
*Un anello* $(\mathbb{R}, +, \cdot)$ *si dice commutativo se*

$$a \cdot b = b \cdot a \quad \forall a, b \in R.$$

**Esempi**
1)$(\mathbb{Z}, +, \cdot)$ è un anello commutativo
2)$Mat_{2\times 2}(\mathbb{Q})$ è un anello non commutativo

**Definizione 50** (Dominiio d'integrità)
*Un dominio d'integrità è un anello commutativo tale che*

1. $0 \neq 1$
2. $\forall a, b \in R$ *tale che* $a \cdot b = 0$ *si ha* $a = 0$ *oppure* $b = 0$

$0$ *denota l'elemento neutro del gruppo* $(R, +)$
*Si dice che* $R$ *non ha divisori dello* $0$

**Esempio:**
$R = \{e\}$
$e + e = e$
$e \cdot e = e$
$(R, +, \cdot)$ è un anello che soddisfa $0 = 1$
Si chiama Anello Banale (Zero Ring)
**Esercizio**
$(R, +, \cdot)$ anello
1) dimostrare che

$$a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in R$$

2) dimostrare che

$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$$

3) se $0 = 1$ allora $R$ è l'anello banale (ovvero $|R| = 1$)

**Definizione 51**
$(R, +, \cdot)$ *anello.*
*Un sottoanello di* $R$ *è un sottoinsieme* $A \subseteq R$ *tale che:*

1. $(A, +) \leq (R, +)$
2. $1 \in A$
3. $A$ *è chiuso rispetto all'operazione* $\cdot$

**Esempi**
$M \geq 2$ intero
$(\mathbb{Z}/(m), +)$ gruppo abeliano
$(\mathbb{Z}/(m), +, \cdot)$ è un anello commutativo
IN generale non è un dominio d'integrità.

Ad esempio se $m = 6$
$[2][3] = [6] = [0]$
quindi $[2]$ e $[3]$ sono divisori di $[0]$ in $\mathbb{Z}/(6)$

**Proposizione 15**
*$m \geq 2$ è intero allora $\mathbb{Z}/(m)$ è un dominio d'integrità se e solo se $m$ è primo*

**Dimostrazione**
*Se $m$ non è primo allora esistono $1 < a, b < m$ tali che $m = ab$*
*Allora $[a] \cdot [b] = [m] = [0]$ e $[a]$ è un divisore dello zero*
*Viceversa se $m$ è primo dobbiamo dimostrare che non esistono zero divisori*
*Considero $[a] \in \mathbb{Z}/(m)$ con $[a] \neq [0]$*
*Assumo che $0 < a < m$*
*Allora $MCD(a, m) = 1$*
$\Rightarrow (a) + (m) = (1) = \mathbb{Z}$
$\Rightarrow \exists k, h \in \mathbb{Z}$ *tali che* $ka + hm = 1$
$\Rightarrow [k] \cdot [a] = [1] \in \mathbb{Z}/(m)$
*Ora se esiste $[b] \in \mathbb{Z}/(m)$ tale che*
$[a] \cdot [b] = [0]$
$\Rightarrow [k] \cdot [a] \cdot [b] = [k] \cdot [0]$
$\Rightarrow [b] = [0]$
$\Rightarrow [a]$ *non è zero divisore* □

**Osservazione**
Abbiamo dimostrato che se $a \in R$ ammette un inverso moltiplicativo allora $R$ è un dominio d'integrità (assumendo "solo" che $R$ sia anello commutativo)

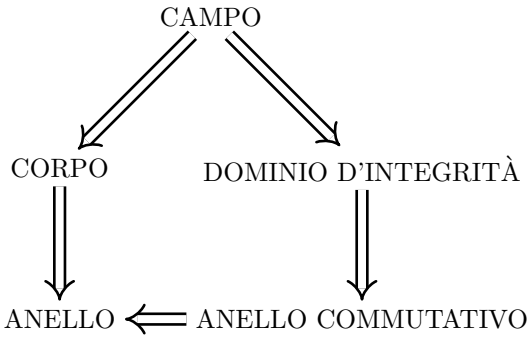
**Definizione 52**
*Un anello $(R, +, \cdot)$ si dice corpo se*
$0 \neq 1$
$\forall a \in R,\ \exists a^{-1} \in R$ *t.c.*
$a^{-1} \cdot a = a \cdot a^{-1} = 1$
$a^{-1}$ *si dice inverso moltiplicativo*

**Definizione 53**
*Un campo è un corpo commutativo*

**Osservazione**
Se $(R, +, \cdot)$ anello $a \in R$ che ammette inverso moltiplicativo $a^{-1} \in R$ Allora $a$ non è zero divisore
Infatti se $\exists b \in R$ t.c. $a \cdot b = 0$
$0 = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot a \cdot b = (a^{-1} \cdot a) \cdot b = b$
$1 \cdot b = 0 \Rightarrow b = 0$
$\Rightarrow a$ non è divisore di 0

**Corollario 14**
*Ogni campo è un dominio d'integrità*

**Dimostrazione**
$\forall a \in R$ *esiste* $a^{-1} \Rightarrow R$ *dominio d'integrità* □
**Osservazione**




**Esempio:** 1) $\mathbb{H}$ quaternioni è un corpo
infatti $i^2 = j^2 = k^2 = ijk = -1$ $q \in \mathbb{H}$
$\rightsquigarrow q = x + yi + zj + wk \in \mathbb{H}, \quad x, y, z, w \in \mathbb{R}$
$\rightsquigarrow \overline{q} := x - yi - zj - wk$ (coniugato)
$\rightsquigarrow |q|^2 = q\overline{q} = x^2 + y^2 + z^2 + w^2$
$\rightsquigarrow q \cdot \frac{\overline{q}}{|q|^2} = 1$ quindi tutti invertibili (tranne 0) $\Rightarrow \mathbb{H}$ è un corpo

**Proposizione 16**
*Ogni dominio d'integrità finito è un campo*

**Dimostrazione**
$(R, +, \cdot)$ *dominio finito. Dato* $a \in R \setminus \{0\}$ *vogliamo dimostrare che esiste* $a^{-1}$
***Idea:***
*considero la funzione* $\begin{matrix} \varphi_a : R \to R \\ b \to a \cdot b \end{matrix}$ $\varphi_a$ *è iniettiva. Infatti* $\varphi_a$ *è un omomorfismo di gruppi*
$(R, +) \to (R, +)$ *per la distributività*
*Inoltre*
$ker(\varphi_a) = \{b \in R | \varphi_a(b) = 0\} = \{b \in R | a \cdot b = 0\} = \{0\}$ *(dato che* $R$ *è dominio)*
$\Rightarrow \varphi_a$ *è iniettiva*
*Ora dato che* $|R| < +\infty$ $\varphi_a$ *è biunivoca*
*Quindi nell'immagine di* $\phi_a$ *abbiamo* 1
$\Rightarrow b \in R$ *tale che* $\varphi_a(b) = 1$ *ovvero* $a \cdot b = 1$
$\Rightarrow b$ *è l'inverso moltiplicativo di* $a$ □

**Definizione 54**
*Dati* $(R_1, +, \cdot)$ *e* $(R_2, \oplus, \odot)$ *anelli, un omomorfismo di anelli è una funzione* $f : R_1 \to R_2$ *tale che*

1. $f(a+b) = f(a) \oplus f(b)$
2. $f(a \cdot b) = f(a) \odot f(b)$
3. $f(1_{R_1}) = 1_{R_2} \quad \forall a, b \in R_1$

## 6.1 Idee per gli esercizi

1)$(R, +, )$ anello $a \in R$
$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$
$\Rightarrow -(0 \cdot a) + (0 \cdot a) = -(0 \cdot a) + (0 \cdot a) + (0 \cdot a)$
$\Rightarrow 0 = 0 \cdot a$
2) $a, b \in R$
$0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$
Sommando $-(a \cdot b)$ ad entrambi i membri ottengo:
$-(ab) = -(a)b$
**Esercizi Schede**
$G = GL_2(\mathbb{C})$
$X = Mat_{2\times 2}(\mathbb{C})$
G$\times X \to X$
$(A, B) \to A \cdot B$ è un'azione tra gruppi
Studiare le orbite
**Soluzione**
$O_{\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)} = \{\begin{pmatrix}0&0\\0&0\end{pmatrix}\}$
$O_{Id} = \{$ matrici invertibili$\}$
Restano da studiare solo i casi di matrici non invertibili e non nulle
Se $det(B) = 0$ allora $B = \begin{pmatrix}x&y\\ \lambda x&\lambda y\end{pmatrix} \quad x, y, \lambda \in \mathbb{C}$
$O_B =?$
**Caso 1**
Se $x = 0 \Rightarrow y \neq 0$
$\Rightarrow B = \begin{pmatrix}0&y\\0&\lambda y\end{pmatrix}$
Allora scelgo
$A = \begin{pmatrix}\frac{1}{y}&?\\?&1\end{pmatrix}$
$AB = \begin{pmatrix}\frac{1}{y}&0\\-\lambda&1\end{pmatrix} \cdot \begin{pmatrix}0&y\\0&\lambda y\end{pmatrix} = \begin{pmatrix}0&1\\0&0\end{pmatrix}$
Dove ho messo al posto dei punti interrogativi numeri appositi per arrivare alla matrice $e_{12}$
Quindi se $x \neq 0 \Rightarrow O_B = O_{\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)}$

**Caso II**
Se $x \neq 0$
Scelgo $A = \begin{pmatrix} \frac{1}{x} & 0 \\ ? & 1 \end{pmatrix}$
$AB = \begin{pmatrix} \frac{1}{x} & 0 \\ -\lambda & 1 \end{pmatrix} \begin{pmatrix} x & y \\ \lambda x & \lambda y \end{pmatrix} = \begin{pmatrix} 1 & \frac{y}{x} \\ 0 & 0 \end{pmatrix}$
$O_B = O_{\left(\begin{smallmatrix} 1 & \frac{y}{x} \\ 0 & 0 \end{smallmatrix}\right)}$
La matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Scambia le righe di $B$
$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
$AB = \begin{pmatrix} c & b \\ a & b \end{pmatrix}$

## 6.2 Ideali

**Definizione 55** (Ideali)
$(R, +, \cdot)$ *anello*
*Un ideale è un sottogruppo* $(I, +) \leq (R, +)$ *tale che*

1. $\forall a \in I \quad \forall x \in R$
   $\Rightarrow x \cdot a \in I$ *[Ideale Sinistro]*
2. $\forall a \in I \quad \forall x \in R$
   $\Rightarrow a \cdot x \in I$ *[Ideale Destro]*
3. $\forall a \in I, \forall x \in R$
   $\Rightarrow \begin{cases} x \cdot a \in I \\ a \cdot x \in I \end{cases}$ *[Ideale bilatero]*

**Osservazione**
Se $R$ è commutativo allora un sottogruppo (additivo) $I \leq R$
è ideale sinistro $\Leftrightarrow$ è un ideale destro $\Leftrightarrow$ è un ideale bilatero.

**Notazione 9**
*$R$ anello $I$ ideale bilatero lo chiameremo semplicemente* ***ideale***

**Osservazione**
$R$ anello $\Rightarrow (R, +)$ è un gruppo abeliano
$\Rightarrow I \subseteq R$ ideale è un sottogruppo additivo normale
**Esercizio:**
$R$ anello $I \subseteq R$ ideale $\Rightarrow (R/I, +)$ gruppo abeliano.
Dimostrare che l'operazione
$\cdot \; : \; R/I \times R/I \to R/I$
(aI,bI) $\to$ $(ab)I$

è ben definita e dedurre che $(R/I, +, \cdot)$ è un anello.
**Esempio**
$(\mathbb{R}, +, \cdot)$ è un anello
$(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
$(\mathbb{Z}, +, \cdot)$ è un sottoanello
$(\mathbb{Z}, +, \cdot)$ non è un ideale in $(\mathbb{R}, +, \cdot)$
Infatti $\sqrt{2} \cdot 1 \notin \mathbb{Z}$
**Esempi**
$R$ anello
$\Rightarrow I = \{0\}$ è un ideale
$\Rightarrow I = R$ è un ideale

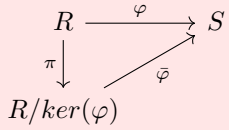
**Definizione 56**
*$R$ anello commutativo. $I \subseteq R$ ideale*
*$I$ si dice primo se $I \neq R$ e $ab \in I \Rightarrow a \in I$ oppure $b \in I$*

**Esercizio**
$R = (\mathbb{Z}, +, \cdot)$
Determinare tutti gli ideali primi di $R$
**Esercizio:**
$R$ anello $I \subseteq R$ ideale
Dimostrare che le seguenti sono equivalenti

1. $R/I$ è un dominio d'integrità
2. Se $a \cdot b \in I \Rightarrow a \in I$ oppure $b \in I$

**Teorema 38** (Omomorfismo per anelli)
*Dato $\varphi : R \to S$ un omomorfismo di anelli abbiamo*

1. *$ker(\varphi) \subseteq R$ è un ideale*
2. *esiste un unico omomorfismo di anelli $\bar{\varphi} : R/ker(\varphi) \to S$ tale che*




3. *Esiste un isomorfismo di anelli $R/ker(\varphi) \cong Im(\varphi)$*

**Dimostrazione** (Esercizio)

*1) Basta verificare che se $x \in ker(\varphi)$ e $y \in R$ allora* $\begin{cases} x \cdot y \in ker(\varphi) \\ y \cdot x \in ker(\varphi) \end{cases}$

$x \in ker(\varphi) \Rightarrow \varphi(x) = 0$
*Quindi*
$\cdot\ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
$= 0 \cdot \varphi(y)$
$= 0$
$\Rightarrow x \cdot y \in Ker(\varphi)$
$\cdot\ \varphi(y \cdot x) = \varphi(y) \cdot \varphi(x)$
$= \varphi(y) \cdot 0$
$= 0$
$\Rightarrow y \cdot x \in ker(\varphi)$ □

## 6.3 Caratteristica

Voglio associare ad ogni anello un numero intero che ci possa dare qualche informazione su di esso.

**Definizione 57**
$(R, +, \cdot)$ *anello.*
*Considero l'omomorfismo di anelli*
$\psi : \mathbb{Z} \to R$
$1 \to 1_R$
$n \to (1_R + \ldots + 1_R)$

*Osserviamo che* $\psi$ *è un omomorfismo di anelli*

$$\psi(nm) = \psi(n) \cdot \psi(m).$$

*Infatti*
$\psi(n) \cdot \psi(m) =$
$= (1_R + \ldots + 1_R)(1_R + \ldots + 1_R)$
$\quad n$ *volte* $\quad m$ *volte*
$= 1_R(1_R + \ldots + 1_R) + \ldots + 1_R(1_R + \ldots + 1_R)$
$\quad m$ *volte* $\quad m$ *volte*
$= \psi(n \cdot m)$
*Allora* $ker(\psi) = (m) \subseteq \mathbb{Z}$ *per qualche* $m \geq 0$
$m$ *si dice caratteristica di* $R$.

**Osservazione**
Supponiamo che $R$ abbia caratteristica positiva $m > 0$ allora $m = ord_{(R,+)}(1_R)$
**Esercizio:**
$(R, +, \cdot)$ campo
Dimostrare che la caratteristica $R$ è 0 oppure un numero primo
**Esempi:**
$\mathbb{R}, \mathbb{Q}, \mathbb{C}$
sono campi di caratteristica 0
Mentre $\mathbb{Z}/(p)$ è un campo di caratteristica $p$ (con p primo)
**Esercizio**
Un anello commutativo è un campo se e solo se non possiede ideali non banali
**Soluzione**
Supponiamo che $R$ sia un campo e sia $I \subseteq R$ un ideale $I \neq \{0\}$
Allora dobbiamo mostrare che $I = R$.
Se $a \in I \neq \{0\}$ considero $a^{-1} \in R$
$a^{-1} \cdot a = 1 \in I$ [Dato che è un ideale]
Dato $b \in R$ :
$b = b \cdot 1 \in I$ [Dato che 1 è nell'ideale ]
Viceversa:
dato $a \in R \setminus \{0\}$ dobbiamo verificare che esiste $b \in R$ tale che $a \cdot b = 1$
Definiamo $I := \{a \cdot r | r \in R\} \subseteq R$

$I$ è un ideale. Inoltre $I \neq \{0\}$ poiché $a \in I$
$\Rightarrow I = R \Rightarrow 1 \in I$ [Per ipotesi]
Quindi esiste $b \in R$ tale che $a \cdot b = 1$
**Osservazione**
Se $R$ campo e $\psi : R \to S$ è un omomorfismo di anelli, allora $\psi$ è iniettivo oppure $\psi$ è l'omomorfismo nullo.
Abbiamo verificato che $ker(\psi)$ è un ideale in $R$.
Quindi:

- $ker(\psi) = \{0\}$
  $\Rightarrow$ iniettivo
- $ker(\psi) = R$
  $\Rightarrow \psi(r) = 0 \quad \forall r \in R$

## 6.4 Esercizi delle schede

**Esercizio 0.1**
$(A, +, \cdot)$ tale che

1. 1) $(A, +)$ gruppo, "non necessariamente abeliano"
2. 2) $\cdot$ è associativa ed esiste $1 \in A$ tale che $1 \cdot a = a \cdot 1 = a$
3. Valgono le proprietà distributive

Dimostrare che $(A, +, \cdot)$ è un anello
**Soluzione**
$x, y \in A \;\; 1 + 1) \cdot (x + y) =?$
Primo caso:

$$(1 + 1)(x + y) = 1(x + y) + 1(x + y) = x + y + x + y.$$

Secondo caso:

$$(1+1)(x+y) = (1+1)(x)+(1+1)(y) = 1 \cdot x+1 \cdot x+1 \cdot y+1 \cdot y = x+x+y+y.$$

$\Rightarrow x + y + x + y = x + x + y + y$ sommando a sinistra l inverso additivo di $x$ e a destra l'inverso di $y$ otteniamo $y + x = x + y \Rightarrow (A, +)$ abeliano.
**Esercizio 0.2**
Sia $(A, +, \cdot)$ anello con $x^2 = x \;\; \forall x \in A \quad \Rightarrow A$ è commutativo
**Soluzione**
Studiamo $(a + a)^2$ :
$a \in A \Rightarrow a + a \in A \Rightarrow (a + a)^2 = (a + a)$
ma $(a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a \Rightarrow a + a = a + a + a + a \Rightarrow a + a = 0 \Rightarrow a = -a$
Siano ora $a, b \in A \Rightarrow (a + b) = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b \Rightarrow 0 = ab + ba \Rightarrow ab = -ba = ba$
**Esercizio 0.3**

$A$ anello tale che $(x \cdot y)^2 = x^2 \cdot y^2 \quad \forall x, y \in A \Rightarrow A$ è commutativo
**Soluzione**
Notazione: $[x, y] := x \cdot y - y \cdot x$ "Braket di Lie"
Dati $x, y \in A$ vogliamo dimostrare $[x, y] = 0$
$(x \cdot y)^2 = x^2 y^2$ ovvero $x \cdot y \cdot x \cdot y = x^2 \cdot y^2$
$\Rightarrow x^2 \cdot y^2 - x \cdot y \cdot x \cdot y = 0 \Rightarrow x \cdot (xy - y \cdot x) \cdot y = 0$
$\Rightarrow xx \cdot [x, y] \cdot y = 0$
**Osservazione:**
$[1, y] = 0$ e $[x, y] = 0$
La relazione precedente è verificata per $x + 1, y \in A \Rightarrow (x + 1) \cdot [x, y] \cdot y = 0 \Rightarrow$ $x \cdot [x, y] \cdot y + 1 \cdot [x, y] \cdot y = 0 \Rightarrow [x, y] \cdot y = 0 \quad \forall x, y \in A \Rightarrow$ tale relazione è verificata per $x, y + 1 \in A \Rightarrow [x, y + 1] \cdot (y + 1) = 0 \Rightarrow [x, y] \cdot y + [x, y] \cdot 1 = 0$
**Esercizio 0.4**
$A$ anello $I \subseteq A$, ideale, $1 \in I$ dimostrare che $I = A$
**Soluzione:**
$a \in A \Rightarrow a = a \cdot 1 \in I$
**Esercizio**
$A \in M_{2\times 2}(\mathbb{Q})$ anello non commutativo $\Rightarrow$ gli unici ideali bilateri di $A$ sono $\{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\}$ e $A$
**Soluzione**
Sia $I \subseteq A$ un ideale bilatero tale che $I \neq \{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\} \Rightarrow \exists \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in I \neq \{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\}$ .
Vogliamo che $g \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) g^{-1} \in I \quad \forall g \in GL_2(\mathbb{Q}) \in A$
$\Rightarrow$ possiamo assumere $a \neq 0$
$\Rightarrow$ considero $\left(\begin{smallmatrix} 1/a & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in I \Rightarrow \left(\begin{smallmatrix} 1 & b/a \\ 0 & 0 \end{smallmatrix}\right) \in I \Rightarrow \left(\begin{smallmatrix} 1 & b/a \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I$
$\Rightarrow \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I$, basta dimostrare che $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in I \Rightarrow \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \Rightarrow \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in I$
$\Rightarrow \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in I \Rightarrow \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in I$
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in I \Rightarrow I \in A$

**Definizione 58**
*$A \subseteq R$ sottoanello di un anello $R, b \in R$*
$A[b] = \{a_0 + a_1 b + a_2 b^2 + \ldots + a_n b^m | a_i \in A, n \in \mathbb{Z}_{>0}\}$

**Osservazione**
Se $b \in A \Rightarrow A = A[b]$
$\cdot$ in generale $A \subseteq A[b]$
**Esempi:**
$A = \mathbb{Z}; \; R = \mathbb{C}$
$\mathbb{Z}[i] = \{a_0 + a_1 i + \ldots + a_n i^n | a_j \in \mathbb{Z}, n \in \mathbb{Z}_{>0}\} = \{m + ni | m, n \in \mathbb{Z}\}$
**Esercizio**
$(\mathbb{Z}, +, \cdot)$ anello
$\mathbb{Z}[i] = \{m + ni | m, n \in \mathbb{Z}\} \subseteq \mathbb{C}$
Mostrare:
1)$\mathbb{Z}[i]$ è un sottoanello di $\mathbb{C}$
**Soluzione**
$(\mathbb{Z}[i], +)$ è un sottogruppo, $Z[i]$ è chiuso rispetto a $\cdot$ per distributività
2)$A \subseteq Z[i]$ sottoanello, dimostrare che $A = \mathbb{Z} \vee \exists l \in \mathbb{Z}_{>0}$ tale che $A = \{m +$

$nki|m, n \in \mathbb{Z}\}$
**Soluzione**
Un sottoanello $A \subseteq \mathbb{Z}[i]$ contiene $1 = 1 + 0_i \Rightarrow Z \subseteq A$
Quindi $A = \mathbb{Z} \vee \exists x + yiA$ con $y \neq 0$
$(A, +)$ sottogruppo di $\mathbb{Z}[i] \Rightarrow -x - yo \in A$
Quindi possiamo assumere $y > 0 \Rightarrow y \cdot i \in A$
con $y > 0$, infatti $\mathbb{Z} \subset A \Rightarrow -x + (x + iy) \in A$,
$k := \min\{y \in \mathbb{Z}_{>0} | y_i \in A\} \Rightarrow$ considero $a+bi \in A$ vogliamo che $k|b \Rightarrow b = qk+r$ con $0 \leq r < k$
Moltiplichiamo per $i \Rightarrow b_i = qk_i + r_i$
$\Rightarrow r_i = b_i - qk_i \in A \Rightarrow k \leq r$ oppure $r = 0$ poiché $r|k$
$\Rightarrow k|b \Rightarrow b = nk \Rightarrow A \subseteq \{m + nki | m, n \in \mathbb{Z}\}$
Il viceversa è facile

- $Z \subseteq A$
- $K_i A \Rightarrow nk_i \in A \ \ \forall n \in \mathbb{Z} \Rightarrow m + nk_i \in A \forall m, n \in \mathbb{Z}$

**Osservazione**
$(\mathbb{Q}, +\cdot)$ anello
$S :=$ insieme di numeri primi $\mathbb{Z}_S := \{\frac{m}{n} \in \mathbb{Q} |$ i fattori primi di $n$ sono in $S\}$
$\mathbb{Z}_S = Z[\frac{1}{p} | p \in S] \subseteq \mathbb{Q}$
**Esercizio**
1) Dimostrare che $\mathbb{Z}_S$ è un sottoanello di $\mathbb{Q}$
$\cdot(\mathbb{Z}_S, +)$ è un sottogruppo di $\mathbb{Q}$

$$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{n_2 m_1 + n_1 m_2}{n_1 n_2} \in \mathbb{Z}_S \text{ ed è chiuso rispetto agli opposti.}$$

$\cdot$ $Z_S$ è chiuso rispetto a $\cdot$

$$m_1 n_1 \cdot \frac{m_2}{n_2} = \frac{m_1 \cdot m_2}{n_1 n_2} \in \mathbb{Z}_S.$$

$\cdot 1 \in \mathbb{Z}_S$
2) Dimostrare che ogni sottoanello di è di tale forma per qualche insieme $S$
$A \subseteq Q$ sottoanello quindi $1 \in A \Rightarrow A \subseteq A \Rightarrow A = Z = Z_\phi \vee \mathbb{Z} \subsetneq A$
$\Rightarrow$ se $\mathbb{Z} \subsetneq A \Rightarrow \exists r \in A \setminus \mathbb{Z} \Rightarrow r\frac{m}{n} \in \mathbb{Q}$
con $n > 1$ e possiamo assumere che $MCD(m, n) = 1$
$\Rightarrow 1 = mx + ny$ con $x, y \in \mathbb{Z}$ (Bezout)
Dividiamo per $n : \frac{1}{n} = rx + y$ Ora:
$x, y \in \mathbb{Z} \subseteq A$ e $r \in A \Rightarrow \frac{1}{n} = ex + y \in A \Rightarrow \frac{a}{n} = a \cdot \frac{1}{n} \in A \ \ \forall a \in \mathbb{Z}$
$\Rightarrow n > 1 \Rightarrow n \cdot p_1 \cdot \ldots \cdot p_k$
Scelgo $a = p_2 \cdot \ldots \cdot p_k \in \mathbb{Z} \Rightarrow \frac{1}{p_1} = \frac{a}{n} \in A$
$\Rightarrow \frac{1}{p_j} \in A \ \ \forall j = 1, \ldots, k.$
Chiamo $S = \{p \in Z | p$ primo tale che $\frac{1}{p} \in A\}$
$Z_S = Z[\frac{1}{p} | p \in S] = A$

**Definizione 59**
$(A,+,\cdot)$ *anello commutativo* $I,J \subseteq A$ *ideali di* $A$.
$I \cdot J = \{\sum_{\alpha=1}^{n} a_\alpha \cdot b_\alpha | a_\alpha \in I, b_\alpha \in K, n \in \mathbb{Z}_{>0}\}$

**Esercizio:**
1)Dimostrare che $I \cdot J$ è un ideale.
**Soluzione**
$I \cdot J$ è un sottogruppo additivo inoltre $\forall x \in A \quad x \cdot \sum_{finita} a_\alpha b_\alpha = \sum (x a_\alpha) b_\alpha = \sum a'_\alpha \cdot b_\alpha$
2)$I \cap J$ è un ideale di $A$
**Soluzione**
$\cdot I \cap J$ è un sottogruppo di $(A,+)$ perchè intersezione di sottogruppi
$\cdot x \in A$ e $b \in I \cap J \Rightarrow \begin{cases} x \cdot b \in I \\ xb \in K \end{cases} \Rightarrow x \cdot b \in I \cap J$
3)$I \cdot J \subseteq I \cap J$
$\begin{cases} a \in I \\ b \in J \end{cases} \Rightarrow a \cdot b \in I \cap J$ ora $I \cap J$ è un sottogruppo di $(A,+) \Rightarrow \sum_{finita} a_\alpha b_\alpha \in I \cap J$