# Lezione 1 Algebra

Federico De Sisti

2024-10-01

# 1 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)

# 2 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*

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

**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) $SL_n(\mathbb{K}) = \{A \in Mat_{nn}(\mathbb{K}) | det(A) = 1\}$
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 i lgruppo di permutazioni su $n$ elementi)
Si chiama gruppo simmetrico

**Definizione 2** (Gruppo diedrale)
*$n \geq 3$ Consideriamo l'n-agono regoalre 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 $D_3$
**TODO INSERISCI DISEGNO gruppo diedrale**
**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 $g^n = e$ poniamo $ord(g) = +\infty$*

**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 cicliclo*

**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) Trvoare 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 nkn sono gruppi
$\cdot Mat_{n\times n}(\mathbb{K})$ con prodotto riche per colonne
$GL(\mathbb{K})$ con somma tra matrici
$\mathbb{Z}\mathbb{Q}\mathbb{R} conilprodotto$

**Proposizione 1**
*$(G, \cdot)$ gruppi finito, Allora ogni elemento ah ordine finito*

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

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

*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 $g^n = e \Rightarrow ord(g) \leq n < +\infty$* $\square$

**Definizione 8** (Sottogruppo)
*$(G, \cdot)$ gruppo $H \subseteq G$ sottosinsieme, 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 rispettto 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 alĺ 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* $h^{-1} = h^{ord(h)-1} = h \cdot \ldots \cdot h \in H \Rightarrow h^{-1} \in H$ $\square$

**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*

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

**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 $H \to gH \quad \forall g \in G$

# Lezione 2 Algebra 1

Federico De Sisti

2024-10-03

# 1 Nelle lezioni precedenti...

**Definizione 1**
*$(G, \cdot)$ gruppo $H \leq G$ $f, g \in G$ si dicono congruenti modulo $H$ se*
$f^{-1} \cdot g \in H$

# 2 Classi di equivalenza

**Notazione 1**
*classi di equivalenza:*

$$G/H.$$

**Esempi importanti**
$(G, \cdot) = (\mathbb{Z}, +)$ $H = (m) = \{am|a \in \mathbb{Z}\}$ con m fissato
$G/H = \mathbb{Z}/(m)$
**Attenzione**
potete definire $f = g \bmod H$ 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 2**
*Gli elementi di $G/H$ si chiamano laterali sinistri, quelli di $H \backslash G$ si chiamano laterali destri*

**Esercizio:**
$(G, \cdot)$ gruppo
$H \leq G$ $g \in G$ 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

$$g \equiv f \bmod H.$$

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 3**
*$(G, \cdot)$ 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

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

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

**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*

$$H \trianglelefteq G.$$

**Esercizio**
$H \leq G$ sottogruppo dimostrare che l'applicazione $\phi : H \to gH$
$g \to g \cdot h$
**Soluzione**
$\phi$ è suriettiva per definizione di $gH$
è anche iniettiva infatti se $h_1, h_1 \in H$ soddisfano

$$gh_1 = gh_2 \quad .$$

allora $h_1 = h_2$ (per la legge di cancellazione)
**Ossercazione**
$(G, \cdot)$ 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 4**
*$(G, \cdot)$ 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 1**
*$(G, \cdot)$ gruppo $H \leq G$ allora*

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

**Dimostrazione**
*Basta ricordare che la cardinalità di ciascun laterale sinistro è pari a $|H|$* $\square$
**Osservazione**
$H \subseteq G => [G : H] = \dfrac{|G|}{|H|}$

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

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

**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* $H = H$

$\square$

**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* $\square$

# 3 Operazioni fra sottogruppi

**Proposizione 2**
$(G, \cdot)$ *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* $\square$

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

**Definizione 5**
*Dati* $H, K \leq G$ *definiamo il* <u>*sottoinsieme*</u>

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

***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 6** (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**
$\cdot H, K \leq G$

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

$\cdot g_1, , g_n \in G$

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

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

# 4 Sottogruppi di 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 $H = (m)$ Sicureamente $(m) \subseteq H$ poich$H \leq \mathbb{Z}$*
*$Viceversa supponiamo che \exists n \in H x (n).$*
*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 3**
*$a, b \in \mathbb{Z}$, Allora:*
$1)(a) \cap (b) = (n)$ *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 $d' = d$*

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

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

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

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

*Allora $d = d'$* □

# 5 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 4**
$n \geq 3$ *Allora:*
1)$D_n = < \rho, \sigma >$
*Dove $\sigma$ è una rotazione qualsiasi ($\sigma \in D_n \setminus C_n$)*
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*

$\Rightarrow ord(\rho^i\sigma) = 2$

$\Rightarrow \rho^i\sigma\rho^i\sigma = Id$

$\Rightarrow \rho^i\sigma\rho^i = \sigma$

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

# Lezione 3 Algebra I

Federico De Sisti

2024-10-08

# 1 Altra roba sui gruppi

**Proposizione 1** (Caratterizazzione 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* $\qquad (fN, gN) \to fgN$
*o equivalentemente* $N\backslash G \times n\backslash G \to n\backslash G$
$\qquad\qquad (Nf, Ng) \to Nfg$

**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)*
$2 \to 3$
$\forall g \in G \ \ \forall n \in N$
$gng^{-1} \in N$ *(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* $\to 4$
*Datifeg*$\in G$ *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)*
$\square$

**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 1**
*$(G, \cdot)$ 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:**
$i^2 = k^2 = j^2 = -1$
$ij = k \quad jk = i \quad ki = j$
$ji = -k \quad kh = -i \quad ik = -j$

**Definizione 1**
*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

$$\begin{tikzcd} (g,f) \arrow[d] \\ (\varphi(g), \varphi(f)) \end{tikzcd} \qquad \begin{tikzcd} G_1 \times G_1 \arrow[r, "\cdot"] \arrow[d, "\varphi \times \varphi"'] & G_1 \arrow[d, "\varphi"] \\ G_2 \times G_2 \arrow[r, "*"] & G_2 \end{tikzcd} \qquad \begin{tikzcd} (g,f) \arrow[r] & g \cdot f \arrow[d] \\ & \varphi(g \cdot f) \end{tikzcd}$$

**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
$\pi : G \to G/N$
$g \to gN$
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 2**
*$\varphi : G_1 \to G_2$ 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 $H_1 \trianglelefteq G_1 \Rightarrow \varphi(H_1) \trianglelefteq \varphi(G_1)$
1) Se $H_2 \leq G_2 \Rightarrow \varphi^{-1}(H_2) \leq G_1$
se $H_1 \trianglelefteq G_2 \Rightarrow \varphi^{-1}(H_2) \trianglelefteq \varphi(G_1)$

# Lezione 4 Algebra I

Federico De Sisti

2024-10-10

# 1 Altre informazioni sugli omomorfismi

**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
**Soluzione di un esercizio passato**
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 $\varphi^{-1}(H_2) \trianglelefteq G_1$
**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 $H_1 = G_1 \leq G_1$
$\Rightarrow Im(\varphi) = \varphi(G_1) \leq G_2$

# 2 Parte figa della lezione

**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)*
$n \in N$
$\Rightarrow \pi(n) = N \to \pi(h)\pi(e) = \pi(ne)$
$\pi(e) = N \qquad = \pi(n) \in \pi H$ $\square$

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

**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* $\pi^{-1}(\pi(H)) \subseteq HN$

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

*segue (1)* $\square$

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

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

$\square$

**Dimostrazione** (3)
*Segue dal fatto che* $\pi \grave{e} unomomorfismosuriettivo$

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

$\square$

**Teorema 1**
$(G, \cdot)$, $n \trianglelefteq G$
*Allora esistono due corrispondenze biunivoche*

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

**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 2** (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.* $\bar{\varphi} \circ \pi = \varphi$

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] \arrow[d, "\pi"] & G_2 \\ G_1/N \arrow[ur, dashed, "\exists!\bar{\varphi}"] & \end{tikzcd}$$

*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 1**
$(G, \cdot)$, $N \trianglelefteq G$
*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 1**
$\varphi : G_1 \to G_2$
*omomorfismo si dice isomorfismo se è invertibile*

**Teorema 3** (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**

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] \arrow[d, "\pi"] & G_2 \\ G_1/N \arrow[ur, "\exists!\overline{\varphi}"] & \end{tikzcd}$$

*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*
$\Rightarrow GL_n(\mathbb{K})/SL_n(\mathbb{K}) \cong (\mathbb{K}^*, \cdot)$ $\square$

# Lezione 5 Algebra I

Federico De Sisti

2024-10-15

# 1 Teoremi di isomorfismo

**Teorema 1** (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**

$$\begin{tikzcd} G \arrow[r, "\varphi=\pi_H"] \arrow[d, "\pi"'] & G/H \\ G/N \arrow[ur, dashed, "\exists!\overline{\varphi}"] & \end{tikzcd}$$

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

*$N \subseteq H = ker(\varphi)$*
*Inoltre $Im(\bar{\varphi}) = Im(\varphi) = G/H$*
***Idea:** applicare il primo teorema di isomorfismo*
*<u>suriettiva</u> $\bar{\varphi} : G/N \to G/H$*
*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 1**
*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*

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

$\square$

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 1**
*$a, bg \in Z$ 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 <u>distinti</u> 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*

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

$\square$

**Teorema 2** (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 2**
$a, b \in \mathbb{Z}$ *non nullli*
*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*

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

□

# 2 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 1** (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 $K_4 \neq C_4$
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 $K_4$

$$\begin{gathered} \varphi : G \to K_4 =< \rho, \sigma > \\ e \to e \\ f \to \rho \\ g \to \sigma \\ fg \to \rho\sigma \end{gathered}$$

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

# Lezione 6 Algebra I

Federico De Sisti

2024-10-21

## 1 Teoremi sulla cardinalità dei gruppi

**Teorema 1**
*$(G,\cdot)$ 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:***
$HK=\{e,r,r^2,s,rs,r^2s\}$
$KH=\{e,r,r^2,s,sr,sr^2\}$
***Dobbiamo considerare 2 casi:***
*I caso: $rs=sr$*
*studiamo $ord(rs)$*
$(rs)^2=r^2s^2=r^2\neq e\Rightarrow ord(rs)\neq 2$
$(rs)^3=r^3s^3=s^3=s\neq e$
***Per Lagrange***
*necessariamente $ord(rs)=6$*
*$\Rightarrow G$ è cicliclo $\Rightarrow$ Assurdo*
*II caso:* $\begin{cases} rs=sr^2 \\ r^2s=sr \end{cases}$
*Costruiamo l'isomorfismo*

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

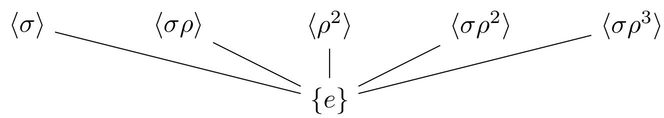
$\square$

**Definizione 1**
*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. $H_1 \subset K \subset H_2$*

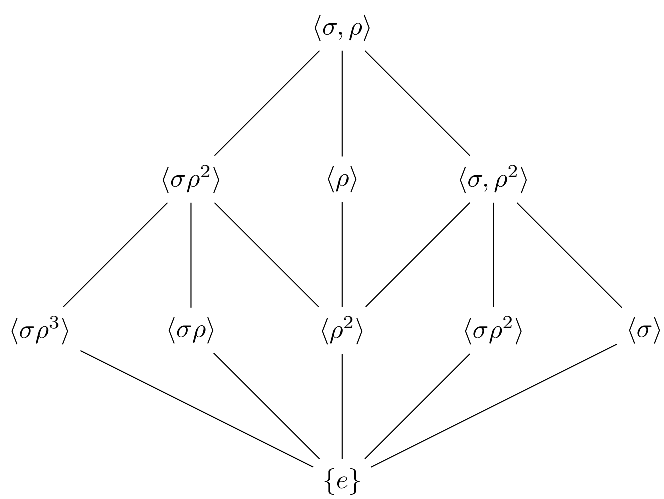
**Esempio:**
$T_{D_4}$
Ricordiamo che $D_4 =< \sigma, \rho > \quad |D_4| = 8$
studiamo i sottogruppi di $D_4$
**ordine 1:** L'unico sottogruppo è $H = \{e\}$
**ordine 2:** Sono tutti e soli quelli generati da un elemento di ordine 2 in $D_4$




**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 $N$.

$$\begin{tikzcd}[arrows=dash]
 & G/N \arrow[dl] \arrow[d] \arrow[dr] & \\
\begin{matrix}\langle\sigma\rho N\rangle \\ \parallel \\ \{\sigma\rho N, N\}\end{matrix} \arrow[dr] & \begin{matrix}\langle\rho N\rangle \\ \parallel \\ \{\rho N, N\}\end{matrix} \arrow[d] & \begin{matrix}\langle\sigma N\rangle \\ \parallel \\ \{N, \sigma N\}\end{matrix} \arrow[dl] \\
 & \{N\} &
\end{tikzcd}$$

**Obiettivo: studiare $S_n$**
**Ricordo:**
$X := \{1, \dots, n\}$
$S_n := S_X = \{$ 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 $n! > 2n \quad \forall n \geq 4$

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

**Proposizione 1**
*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 1**
*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 2**
$\sigma \in S_n$
$sgn(\sigma) := \frac{\Delta^\sigma}{\Delta} \in \{\pm 1\}$

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

**Dimostrazione**
*In generale*
$(f^\sigma)^\tau = f^{\sigma\tau}$
$(fg)^\sigma = f^\sigma g^\sigma$
$sgn(\sigma\tau) = \dfrac{\Delta^{\delta\tau}}{\Delta} = \dfrac{(\Delta^\sigma)^\tau)}{\Delta} = \dfrac{\Delta^\sigma}{\Delta}\dfrac{(\Delta^\sigma)^\tau}{\Delta^\sigma} = sgn(\sigma)\dfrac{\Delta^\tau}{\Delta} = sgn(\delta)sgn(\tau)$ $\square$

# Lezione 7 Algebra I

Federico De Sisti

2024-10-22

# 1 parte da recuperare

# 2 Seconda ora

# Lezione 8 Algebra I

Federico De Sisti

2024-10-26

# 1 Prodotti tra gruppi

## 1.1 Prodotto diretto di gruppi

**Definizione 1**
*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 1**
*bold $(G_1 \times G_2, \cdot)$ 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 $(g^{-1}, f^{-1})$* $\square$
**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)

$$\begin{tikzcd}
G_1 \times G_2 \arrow[r, "\varphi"] \arrow[d] & \frac{G_1}{H} \times \frac{G_2}{K} \\
\frac{(G_1 \times G_2)}{ker\varphi} \arrow[ur, dotted, "\exists! \bar{\varphi}"] &
\end{tikzcd}$$

*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*
$\cdot \quad ker\varphi = \{(g_1, g_2) \in G_1 \times G_2 | \varphi(g_1, g_2) = (H, K)\}$
$= \{(g_1, g_2) | g_1 H = H \ e \ g_2 K = K\}$

$\{(g_1, g_2)|g_1 \in H, g_2 \in K\} = H \times K$
*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. **dimo**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**
Per l'esercizio sotto chiedi a Marco
**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 2**
*$(G, \cdot)$ 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 1**
*$(G, \cdot)$ 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* $\psi(g_1, k_1) = \psi(h_2, k_1)$

$$\Rightarrow h_1k_1 = h_2k_2$$
$$\Rightarrow h_2^{-1}h_1k_1 = k_2$$
$$\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$$
$$\Rightarrow \begin{cases} h_2^{-1}h_1 = e \\ k_2k_1^{-1} = e \end{cases} \Rightarrow (h_1, k_1) = (h_2, k_2)$$
$$\Rightarrow \psi \text{ iniettiva}$$

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

$$\psi(h_1h_2, k_1k_2) = \psi(h_1, k_1)\psi(h_2, k_2).$$

*dunque*

$$\psi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1(h_2k_1)k_2 = h_1(k_1h_2)k_2 = \psi(h_1, k_1)\psi(h_2, k_2).$$

*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 3** (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 2**
$Int(G) \trianglelefteq Aut(G)$

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

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

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

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

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

**Definizione 4** (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
$\varphi : G \rightarrow Int(G)$
$\quad g \rightarrow I_g$
$\cdot$ $\varphi$ è suriettiva
$\cdot$ $\varphi$ 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 $ker(\varphi)$

$$
\begin{aligned}
ker(\varphi) &= \{g \in G | \varphi(g) = Id\} = \\
&= \{g \in G | I_g = Id\} = \\
&= \{g \in G | \forall f \in G : I_g(f) = Id(f)\} = \\
&= \{g \in G | \forall f \in G : gfg^{-1} = f\} = Z(G)
\end{aligned}
$$

Dal I teorema di isomorfismo si ha che

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

## 1.2 Prodotto semidiretto

Consideriamo due gruppi
$(N, \cdot)$ e $(H, *)$
Fissiamo un omomorfismo
$\phi : H \to Aut(N)$
$\quad h \to \text{ø}_n$

**Definizione 5** (Prodotto semidiretto)
*il prodotto semidiretto di $N$ e $H$ tramite ø è l'insieme $N \times H$ dotato dell'operazione*

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \text{ø}_{h_1}(n_2), h_1 * h_2).$$

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

**Notazione 1**
*Indichiamo il prodotto semidiretto tra $N$ e $H$ con il simbolo $N \rtimes_{\text{ø}} H$*

**Proposizione 3**
*$N \rtimes_{\text{ø}} H$ è un gruppo*

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

**Definizione 6**
*$(G,\cdot)$ 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**
$D_n =< \rho, \sigma > \quad N =< \rho > \trianglelefteq D_n$
$H =< \sigma > \leq D_n$. Allora $D_n$ è prodotto semidiretto interno di $N$ e $H$

# Lezione 9 Algebra I

Federico De Sisti

2024-10-30

# 1 Ricapitolando

Siano $(N, \cdot), (H, *)$ gruppi.

**Definizione 1**
*Il prodotto semidiretto di $N$ e $H$ tramite un omomorfismo $\theta : H \to Aut(N)$ è l'insieme $N \times H$ dotato dell'operazione*

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

**Osservazione:**
$h_1 \in H, \quad \o_{h_1} \in Aut(N) \quad \o_{h_1}(n_2) \in N$
**Esempio**
Scegliendo
$\o : H \to Aut(N)$
$\quad h \to \o_h$
con $\o_n := Id_N \quad \forall h \in H$
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

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

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

è un sottogruppo di $N \rtimes_{\o} H$

**Definizione 2** (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 1**
*Sia $G$ un gruppo.*
*1) Se $G$ è prodotto semidiretto di $N$ e $H \leq G$, allora esiste un omomorfismo $\varnothing : H \to Aut(N)$ tale che $G \cong N \rtimes_{\varnothing} H$*
*2) Se $G \cong \tilde{N} \rtimes_{\varnothing} \tilde{H}$ 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*
$\varnothing : H \to Aut(N)$
$h \to \varnothing_n$
*dove* $\varnothing_h(n) := (hnh^{-1}) \in hNh^{-1} = N \quad \forall n \in N$
*Dato che abbiamo assunto $N$ normale*
*Abbiamo verificato la volta scorsa che è un omomorfismo.*
*Definiamo l'applicazione*
$\psi : N \rtimes_{\varnothing} H \to G$
$(n, h) \to nh$
*$\psi$ 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:***
$\psi((n_1, h_1) \cdot (n_2, h_2)) =$
$= \psi((n_1 \varnothing_{h_1}(n_2), h_1 h_2))$
$= n_1 \varnothing_{h_1}(n_2) h_1 h_2$
$= n_1 h_1 n_2 h_1^{-1} h_1 h_2 = \psi(n_1, h_1) \cdot \psi(n_2, h_2)$
*Omomorfismo biunivoco* $\square$

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