Capitolo 1: Teoria dei gruppi:

Definizione (Gruppo):

È un insieme G munito di un'operazione binaria $*$, ossia $f: G \times G \to G \mid f(a,b) = a * b$ che rispetti le seguenti proprietà:

1- Associativa: $(a * b) * c = a * (b * c)\ \forall a, b, c \in G$
2- $\exists\ e$ elemento neutro$\mid e * x = x * e = x\ \forall x \in G$
3- $\forall x \in G\ \exists\ x^{-1}$ inverso$\mid x^{-1} * x = x * x^{-1} = e$

Se vale $a * b = b * a\ \forall a, b \in G$ il gruppo si dice Abeliano.

Definizione (Sottogruppo):

È un sottoinsieme H di G che è un gruppo con l'operazione indotta da G. Si indica con $H < G$.

Teorema:
$H < G \leftrightarrow 1.\ H \neq \emptyset\ \ 2.\ a, b \in H \to a * b \in H\ \ 3.\ a \in H \to a^{-1} \in H$

Proposizione:
Se $H, K < G$ allora $H \cup K < G \leftrightarrow H \subseteq K$ o $K \subseteq H$.

Definizione (Sottogruppo generato da S):

È il più piccolo sottogruppo che contiene S. Si indica con $< S >$.

Definizione (Gruppo ciclico):

Un gruppo G si dice ciclico se $\exists x \in G \mid G =< x >$

Teorema: (Corollario del primo T. di O. per G.)
Ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/_{n\mathbb{Z}}$

Teorema:
Sia G un gruppo ciclico di ordine m ($G \cong \mathbb{Z}/_{m\mathbb{Z}}$), allora per ogni $d \mid m\ \exists!\ H < G \mid |H| = d$

Definizione (Ordine di un elemento):

Se G è un gruppo finito. L'ordine di x ($\mathrm{ord}(x)$) è il minimo esponente $h \mid x^h = e$.
L'ordine di un gruppo invece è il # dei suoi elementi o cardinalità, si indica con $|G|$.

Teorema di Lagrange:
L'ordine di un sottogruppo di un gruppo finito è un divisore dell'ordine del gruppo.

Definizione (Classi laterali di un sottogruppo):

$xH = \{y = xh \mid h \in H\}$ (Classe laterale sinistra). $Hx = \{y = hx \mid h \in H\}$ (Classe laterale destra).

Teorema:

Tutte le classi laterali hanno la stessa cardinalità.

Definizione (Indice):

È il numero delle classi laterali (Sinistre o destre) di H in G.

Osservazione:

Essendo classi di equivalenza le classi laterali formano una partizione e vale la relazione:
$|G| = \text{indice}(H) \cdot \dim Classi\ laterali$

Proposizione:

Se $H < G$ ha indice 2 → Normale

Definizione (Sottogruppi normali):

$H \lhd G \leftrightarrow xH = Hx\ \forall x \in G$

Osservazione:

Ciclico→Abeliano→Tutti i sottogruppi sono normali.

Osservazione:

Per dimostrare che $H \lhd G$ basta provare che $xhx^{-1} \in H\ \forall x \in G, \forall h \in H$.

Proposizione:

Sfruttando il fatto che le classi di coniugio hanno tutte lo stesso numero di elementi ci basta mostrare che l'orbita di H contiene solo H.
Quindi se H è l'unico sottogruppo di ordine dato → $H \lhd G$

Definizione (Gruppo quoziente):

È l'insieme delle classi laterali di $H \lhd G$. Si indica con G/H ed è un gruppo con l'operazione indotta:
$xH \cdot yH = (x \cdot y)H$

Definizione (Omomorfismo di gruppi):

Dati $(G,*)$ e $(G',*')$ una funzione $f: G \to G'$ si dice un omomorfismo se:

$f(x * y) = f(x) *' f(y)\ \forall x, y \in G$

Esempio importante:

La proiezione canonica $\pi: G \to {}^{G}/_{H} \mid \pi(x) = xH$ e $H \lhd G$

Proprietà:

$f(e) = e'$

$f(x^{-1}) = f(x)^{-1}$

$H < G \to f(H) < G'$

$H' < G' \to f^{-1}(H') < G$

$H' \lhd G' \to f^{-1}(H') \lhd G$

Se f è un omomorfismo surgettivo: $H \lhd G \to f(H) \lhd G'$

Un omomorfismo iniettivo e surgettivo si dice **isomorfismo**

Osservazione:

Dato $f: G \to G'$ se assegno i generatori di G ho completamente descritto l'omomorfismo.

Osservazione:

$x \in G \to \mathrm{ord}\big(f(x)\big) \mid \mathrm{ord}(x)$

Conclusione:

Se stiamo costruendo gli omomorfismi iniettivi bisogna imporre che per ogni generatore x valga: $ord(x) = ord\big(f(x)\big)$

Definizione (Nucleo):

$\ker f = \{x \in G \mid f(x) = e'\}$; vale $\ker f \lhd G$

Teorema:

I sottogruppi normali sono tutti e soli i nuclei degli omomorfismi.

Ossia sia $H \lhd G \to \exists f: G \to G'$ omomorfismo $\mid \ \ker f = H$

Proposizione:

$f: G \to G'$ un omomorfismo surgettivo induce una corrispondenza biunivoca tra:

1. Sottogruppi di G che contengono $\ker f$
2. Sottogruppi di G'

Proposizione:

$H \lhd G \leftrightarrow N(H) = G$

Primo teorema di omomorfismo per gruppi:

Sia $f: G \to G'$ un omomorfismo di gruppi → ∃! omomorfismo $\varphi: \frac{G}{\ker f} \to G' \mid f = \varphi \circ \pi$.

φ è iniettivo. φ è surgettivo ↔ f surgettivo.

Secondo teorema di omomorfismo per gruppi:

G gruppo; $H \subseteq K$; $H, K \lhd G \to {}^{(G/H)}\big/_{(K/H)} \cong {}^{G}\big/_{K}$

Terzo teorema di omomorfismo per gruppi:

G gruppo; $H < G$; $K \lhd G \to {}^{H}\big/_{H \cap K} \cong {}^{HK}\big/_{K}$

Proprietà pratica importante:

G finito → $|H||K| = |H \cap K||HK|$

Osservazione:
Questa proprietà è insiemistica, ossia è valida a prescindere dal fatto che HK, detto **Prodotto di Frobenius** sia un gruppo.

Teorema di Cayley:

Sia G un gruppo finito → $\exists n \in \mathbb{N} \mid G$ è isomorfo ad un sottogruppo di S_n

Definizione (Automorfismo):

È un isomorfismo da un gruppo in sé.

Osservazione:
$(\mathrm{Aut}(G), \circ)$ è un gruppo.

Definizione (Automorfismi interni):

$\mathrm{Int}(G) = \{\varphi \in \mathrm{Aut}(G) \mid \exists g \in G \text{ con } \varphi(x) = gxg^{-1}\ \forall x \in G\}$

Osservazione:
$\varphi_g(x) = gxg^{-1}$ è un automorfismo interno (**Coniugio**)
Si può definire una relazione di equivalenza $x \sim y \leftrightarrow \exists g \in G \mid gxg^{-1} = y$
Le classi per questa relazione di equivalenza (Orbite per gli automorfismi interni) si dicono **Classi di Coniugio**.

Proposizione:
$\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$

Osservazione (Automorfismi di prodotti diretti):

Ragionare su come sia possibile assegnare i generatori: $\mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5) = (5^2 - 1)(5^2 - 5)$

Definizione (Centro di un Gruppo):

$Z(G) = \{x \in G \mid xy = yx \ \forall y \in G\}$

Proposizione:

$\mathrm{Int}(G) \cong {}^{G}/_{Z(G)}$ in quanto $Z(G) \lhd G$

Proposizione:

G non abeliano $\rightarrow {}^{G}/_{Z(G)}$ non ciclico

Proposizione:

G abeliano $\leftrightarrow Z(G) = G$

Formula delle classi (Legata al coniugio):

G gruppo finito; R insieme di rappresentanti per le classi di coniugio (Non elementi del centro);

$|G| = |Z(G)| + \sum_{x \in R} \frac{|G|}{|Z(x)|}$

Conseguenza 1:

G p-gruppo non banale $\rightarrow Z(G) \neq \{e\}$

Conseguenza 2:

$|G| = p^2 \rightarrow G$ abeliano

Conseguenza 3:

G p-gruppo; $\{e\} \neq H \lhd G \rightarrow H \cap Z(G) \neq \{e\}$

Proposizione:

G p-gruppo; $H < G$; $H \neq G$ allora $N(H) \supsetneq H$

Teorema di Cauchy:

G gruppo finito; p primo tale che $p \mid |G| \rightarrow \exists x \in G \mid \mathrm{ord}(x) = p$

Proposizione:

In un p-gruppo ci sono sottogruppi ∀ divisore dell'ordine del gruppo.

Definizione (Prodotto diretto):

È un gruppo definito sul prodotto cartesiano $G = G_1 \times G_2 = \{(x_1, x_2) \mid x_i \in G_i\}$ definendo l'operazione di gruppo come: $(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$

Lemma (Due gruppi commutano)

$H, K \lhd G$ e $H \cap K = \{e\} \rightarrow hk = kh \; \forall h \in H \; \forall k \in K$

Teorema (Condizione per prodotto diretto):

G gruppo, $H, K \lhd G$; $H \cap K = \{e\}$; $HK = G \rightarrow G \cong H \times K$

Teorema di Struttura dei Gruppi Abeliani:

Ogni gruppo abeliano finito è isomorfo ad un prodotto diretto di gruppi ciclici.

Proposizione:

Sia G un gruppo abeliano di ordine $m \cdot n$ con $(m, n) = 1 \rightarrow G \cong G_m \times G_n$

Notazione:

$G_n = \{x \in G \mid nx = 0\}$; $\forall n \in \mathbb{N} \; G_n < G$

Definizione (Prodotto semidiretto):

Siano A, B gruppi. Un prodotto semidiretto tra A e B è dato dall'insieme $A \times B$ e da un omomorfismo $\varphi: B \rightarrow \mathrm{Aut}(A)$.

Su $G = A \rtimes_\varphi B$ definiamo la seguente operazione: $(a_1, b_1)(a_2, b_2) \coloneqq \left(a_1 \varphi_{b_1}(a_2), b_1 b_2\right)$

Osservazione:

Il p. diretto è un caso specifico del prodotto semidiretto con $\varphi_b(a) = a \;\; \forall a \in A \; \forall b \in B$

Osservazione:

Se $G = A \rtimes_\varphi B$ allora: $\tilde{A} \lhd G$ mentre $\tilde{B}$ non è detto che sia normale.

Notazione:

$\tilde{A} = A \times \{e_b\}$

Teorema (Condizione per prodotto semidiretto):

Siano G gruppo e $H, K < G \mid$

1- $H \lhd G$
2- $H \cap K = \{e\}$
3- $HK = G$

Allora $G \cong H \rtimes_\varphi K$ con $\varphi: K \rightarrow \mathrm{Aut}(H)$ l'omomorfismo che associa ad ogni $k \in K$ l'automorfismo interno $\varphi_k: \varphi_k(h) = khk^{-1}$

Osservazione pratica (Centro di un prodotto semidiretto:
Se abbiamo $K \rtimes_{\varphi_1} H$ e $K \rtimes_{\varphi_2} H$ e vogliamo capire se non sono isomorfi un modo può essere studiare i rispettivi centri (Se non coincidono come dimensioni non possono essere isomorfi).
Ricordiamo che $(k,h) \in Z\left(K \rtimes_{\varphi_i} H\right) \leftrightarrow h \in \ker \varphi_i$
Non è necessario studiare gli automorfismi di K ma basta cercare il ker dell'omomorfismo nel gruppo ad esso isomorfo (Se stiamo studiando $\varphi: H \to \mathrm{Aut}(\mathbb{Z}_{11})$ è come studiare $\bar{\varphi}: H \to \mathbb{Z}_{10}$

Il gruppo dei commutatori (Derivato):

Dato un gruppo G, $\forall a, b \in G \ \exists x \mid ab = bax$
Questo $x = a^{-1}b^{-1}ab$ è detto commutatore di a e b.
Il commutatore si indica con $[a,b]$

Osservazione (Unità):
L'unità è un commutatore in quanto $1 = [a,a] \ \forall a \in G$

Osservazione:
Due elementi $a, b \in G$ commutano $\leftrightarrow [a,b] = [b,a] = 1$
Un gruppo G è abeliano $\leftrightarrow G' = \{1\}$
Più elementi ha il gruppo dei commutatori meno il gruppo G è abeliano.

Osservazione (Inverso):
L'inverso di un commutatore è un commutatore:
$[a,b]^{-1} = [b,a]$

Definizione (Derivato):
Il derivato è il gruppo generato dai commutatori, si indica con:
$G' = [G,G] \coloneqq \langle [a,b] \mid a, b \in G \rangle$

Osservazione:
Dobbiamo prendere il gruppo generato perché il prodotto di due commutatori non è necessariamente un commutatore.

Teorema (Gruppo abelianizzato):
Vale $G' <_{\mathrm{car}} G$, dunque si può definire:
G/G' che è abeliano che è detto Gruppo abelianizzato di G

Teorema:
$N < G \,;\, G' \subseteq H \to H \lhd G$

Gruppo di Klein:

Viene chiamato gruppo di Klein ed indicato con Kl il gruppo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Questo gruppo è abeliano e ha 3 elementi di ordine 2 e l'identità.

Un esempio di gruppo di Klein è $\{\mathrm{Id}, \text{riflessione su x}, \text{riflessione su y}, \text{rotazione di } 180°\}$ sottogruppo delle isometrie di $\mathbb{R}^2$.

Approfondimento azioni:

Definizione (Azione di un gruppo su di un insieme):

G gruppo; X insieme; $S(X) = \{\text{permutazioni di } X\}$; un'azione di G su X è un omomorfismo $\varphi: G \to S(X)$

Definizione (Stabilizzatore):

Data un'azione di G su X ; $\mathrm{Stab}(x) = \{g \in G \mid \varphi_g(x) = x\}$; $\mathrm{Stab}(x) < G$

Proposizione:

$\varphi_g(x) = \varphi_h(y) \leftrightarrow g\mathrm{Stab}(x) = h\mathrm{Stab}(x)$

Definizione (Orbita):

Data un'azione di G su X ; ; $\mathrm{Orb}(x) = \{\varphi_g(x) \mid g \in G\}$; $\mathrm{Orb}(x) \subseteq X$

Osservazione:

Si può definire una relazione di equivalenza $x \sim y \leftrightarrow \exists g \in G \mid gxg^{-1} = y$ (**Relazione di Coniugio**)

In questo caso le Orbite sono le classi di equivalenza.

Definizione (Normalizzatore):

$H \subseteq G$; $\mathrm{N}(H) = \mathrm{Stab}(H) = \{\varphi_g \in \mathrm{Int}(G) \mid \varphi_g(H) = H\}$

Equivalente nel caso $H < G$: $\mathrm{N}(H)$ è il più grande sottogruppo di $G \mid H \lhd N(H)$

Osservazione:

$H \lhd G \leftrightarrow N(H) = G$

Per parlare di normalizzatore dobbiamo sfruttare come insieme il gruppo con cui lavoriamo.

Definizione (Caratteristico):

$K < G$ si dice caratteristico in G se $\forall \varphi \in \mathrm{Aut}(G)$ vale $\varphi(K) = K$

Proposizione pratica:

G finito $\to |\mathrm{Orb}(x)||\mathrm{Stab}(x)| = |G|$

Osservazione (Coniugio):

$|\mathrm{Cl}(x)||\mathrm{Z}(x)| = |S_n|$

Esercizi ed esempi

Esempio 1 (Classi di coniugio):

Sia G il gruppo delle $f: \mathbb{Z}_7 \to \mathbb{Z}_7 \mid f(x) = ax + b \; ; a \in \mathbb{Z}_7^* \; ; b \in \mathbb{Z}_7$
Dato $H = \{f \in G \mid f(x) = 2^t x + b \text{ con } t \in \mathbb{Z}\}$
Determinare le classi di coniugio su G e su H di $f(x) = x + 1 \; ; g(x) = 2x + 1$ e le loro cardinalità.

Consideriamo l'elemento $h = ax + b \; ; h^{-1} = a^{-1}x - a^{-1}b$ per il quale vogliamo coniugare:
$h^{-1}fh(x) = a^{-1}\big((ax + b) + 1\big) - a^{-1}b = x + a^{-1}$
Quindi in G vale $\mathrm{Cl}\big(f(x)\big) = \{f = x + a \text{ con } a \in \mathbb{Z}_7^*\} \to \big|\mathrm{Cl}\big(f(x)\big)\big| = 6$
Su H siccome a può valere solamente 2^t varrà $\mathrm{Cl}\big(f(x)\big) = \{x + 2 \; ; \; x + 4 \; ; \; x + 1\}$

Per $g(x)$ invece:
$h^{-1}gh = 2x + a^{-1}(b + 1)$ e siccome $b + 1$ può assumere ogni valore di $\mathbb{Z}_7$ sia in G che in H ed esiste un $a \mid a^{-1} = 1$ per entrambi, allora $\mathrm{Cl}\big(g(x)\big) = \{2x + a \text{ con } a \in \mathbb{Z}_7\} \to \big|\mathrm{Cl}\big(g(x)\big)\big| = 7$

Esempio 2 (Sottogruppi caratteristici):

Sia $G = \mathbb{Z}_8 \times \mathbb{Z}_2$
a. Determinare il numero dei sottogruppi di G di ogni possibile ordine.
b. Dimostrare che i sottogruppi di ordine 4 sono caratteristici.

a.
L'ordine di un sottogruppo divide l'ordine del gruppo, dunque esistono solo di ordine $2,4,8$
I sottogruppi di ordine 2 sono tutti e soli quelli generati da un elemento di ordine 2.
Sono dunque $\langle(4,0)\rangle \; ; \; \langle(4,1)\rangle \; ; \; \langle(0,1)\rangle$
I gruppi di ordine 4 esistono di due tipi:
Isomorfi a $\mathbb{Z}_4 \to$ Ciclo$\to$ ce ne sono $\frac{\#\text{elementi di ordine } 4}{\Phi(4)} = 2$ e sono $\langle(2,0)\rangle \; ; \; \langle(2,1)\rangle$
Isomorfi a $\mathbb{Z}_2 \times \mathbb{Z}_2$, di questo ce ne è uno solo perché un gruppo del genere contiene (ed è caratterizzato) da 3 elementi di ordine 2. Siccome in G ci sono esattamente 3 elementi di ordine 2 ce ne sarà uno solo. Il sottogruppo di ordine 4 è: $\{(0,0) \; ; (0,1) \; ; (4,0) \; ; (4,1)\}$
I sottogruppi di ordine 8 possono essere:
Isomorfi a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, assurdo in quanto non sono presenti in G 7 elementi di ordine 2.
Isomorfi a $\mathbb{Z}_4 \times \mathbb{Z}_2$ che come prima è unico ed è:
$\{(0,0) \; ; (4,0) \; ; (0,1) \; ; (4,1) \; ; (2,0) \; ; (6,0) \; ; (2,1) \; ; (6,1)\}$
Isomorfi a $\mathbb{Z}_8 \to$ Ciclici $\to$ ce ne sono $\frac{\#\text{elementi di ordine } 8}{\Phi(8)} = 2$ e sono $\langle(1,0)\rangle \; ; \; \langle(1,1)\rangle$

b.
I tre gruppi sono caratteristici perché quello isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ può andare solo in se stesso mentre se gli altri si scambiassero mediante l'automorfismo di G φ
Avremmo che $\varphi\big((1,0)\big) = (a, b)$ mi descrive il comportamento di ogni elemento fra cui $(2,0)$ generatore del primo gruppo, ma $\varphi\big((2,0)\big) = (2a, 2b) = (2a, 0) \neq (2,1); (6,1)$ i generatori del secondo. Quindi non si possono scambiare.

Esempio 3 (<u>Formula delle classi</u>):
Dimostrare che un gruppo di ordine p^4 ha sempre un sottogruppo abeliano di ordine p^3.

Sappiamo che $Z(G) < G \rightarrow |Z(G)| \in \{1, p, p^2, p^3, p^4\}$
Nel caso in cui $|Z(G)| = p^4 \rightarrow G$ abeliano ed esiste sempre un sottogruppo di ordine p^3 per il teorema di Sylow, in quanto sottogruppo di abeliano è abeliano.
$|Z(G)| = p^3$ allora proprio $Z(G)$ è il sottogruppo che stavamo cercando.
$|Z(G)| = p^2$ basta prendere un elemento $x \notin Z(G)$ e considerare $Z(x)$, questo gruppo contiene il centro ed $x \rightarrow$ ha cardinalità maggiore di p^2 ma minore di p^4 in quanto altrimenti $x \in Z(x)$.
Questo gruppo è abeliano in quanto $\{\{x\}, Z(x)\} \subseteq Z\big(Z(x)\big) \rightarrow$ il suo centro ha cardinalità maggiore di $p^2 \rightarrow = p^3$ ossia è tutto
$|Z(G)| = p$ applicando la formula delle classi otteniamo che $p^4 = p + \sum \frac{p^4}{|Z(x)|}$ se tutte le $Z(x)$ avessero cardinalità minore di p^2 avremmo un assurdo (p sarebbe divisibile per p^2) $\rightarrow$ uno degli $Z(x)$ ha cardinalità p^3 ed era il sottogruppo che stavamo cercando.
$|Z(G)| = 1$ Assurdo per il corollario della formula delle classi che afferma che ogni *p*-gruppo ha centro non banale.

Esempio 4 (<u>Omomorfismi</u>):
Dati A, B, C gruppi abeliani. Dimostrare che:
a. $\mathrm{Hom}(A \oplus B, C) \cong \mathrm{Hom}(A, C) \oplus \mathrm{Hom}(B, C)$
b. G abeliano di ordine $n \rightarrow G \cong \mathrm{Hom}(G, \mathbb{Z}_n)$

a.
Definiamo la funzione $\varphi(f, g) = h$ con $h(x) = \begin{cases} f(x) \text{ se } x \in A \\ g(x) \text{ se } x \in B \end{cases}$. Questa è una buona definizione ed è banalmente iniettiva e surgettiva.
Rimane da dimostrare che è un omomorfismo.
$\varphi(f + f', g + g') = \varphi(f, g) + \varphi(f', g')$ che si riduce a facili calcoli.
b.
Se il gruppo è abeliano (Per il teorema di struttura) $G \cong \bigoplus \mathbb{Z}_i$ con $\mathbb{Z}_i$ abeliani.
Per il risultato a. vale $\mathrm{Hom}(G, \mathbb{Z}_n) \cong \bigoplus \mathrm{Hom}(\mathbb{Z}_i, \mathbb{Z}_n)$
Ci basta dunque dimostrare che $\mathrm{Hom}(\mathbb{Z}_i, \mathbb{Z}_n) \cong \mathbb{Z}_i$
Siccome ogni omomorfismo è completamente determinato (Essendo gruppi ciclici) dall'assegnazione del generatore con l'unica condizione che $\mathrm{ord}\big(f(1)\big) \mid \mathrm{ord}(1) = i \rightarrow$ Stiamo semplicemente immergendo $\mathbb{Z}_i$ nella copia contenuta in $\mathbb{Z}_n$ e questo si può fare in i modi $\rightarrow$ $\mathrm{Hom}(\mathbb{Z}_i, \mathbb{Z}_n) \cong \mathbb{Z}_i$