Lezione 06

Gruppi di Trasformazioni

I gruppi di natura geometrica, detti **gruppi di trasformazioni** hanno un'importanza notevole, dato che i gruppi (astratti) sono nati come gruppi di trasformazioni.

Sia X un insieme. Consideriamo l'insieme $S(X)$, insieme di tutte le trasformazioni o corrispondenze biunivoche di X in X. Se indichiamo con $\circ$ il *prodotto operatorio* (la funzione composta), ossia se $(f \circ g)(x) = f(g(x))$, è facile vedere che $(S(X), \circ)$ è un gruppo:

1. **Associatività**: Per ogni $f, g, h \in S(X)$ e per ogni $x \in X$, abbiamo $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)$.
2. **Elemento neutro**: L'identità $id_X : X \to X$ definita da $id_X(x) = x$ per ogni $x \in X$ è un elemento di $S(X)$ e agisce come un elemento neutro per l'operazione $\circ$, perché per ogni $f \in S(X)$ e per ogni $x \in X$, abbiamo $(id_X \circ f)(x) = id_X(f(x)) = f(x)$ e $(f \circ id_X)(x) = f(id_X(x)) = f(x)$.
3. **Inversi**: Per ogni $f \in S(X)$, poiché f è una trasformazione biunivoca, esiste un'inversa $f^{-1} : X \to X$ tale che $f^{-1}(f(x)) = x$ e $f(f^{-1}(x)) = x$ per ogni $x \in X$. Quindi, $f^{-1} \in S(X)$ e $(f \circ f^{-1})(x) = f(f^{-1}(x)) = x = id_X(x)$ e $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = id_X(x)$ per ogni $x \in X$.

Quindi $(S(X), \circ)$ è un gruppo.

Teorema di Cayley - Mappa iniettiva in un gruppo G che preserva le operazioni.

Sia $(G, \star)$ un gruppo. Allora esiste una mappa iniettiva $\Phi(G, \star) \longrightarrow (S(G), \circ)$ che preserva le operazioni, cioè $\Phi(a \star b) = \Phi(a) \circ \Phi(b)$.

Dimostrazione:

Definiamo la seguente applicazione:

$$\begin{aligned} T_a : G &\longrightarrow G \\ x &\longrightarrow ax, \quad \forall x \in G \end{aligned}$$

T_a è la moltiplicazione sinistra per a. Si tratta di una corrispondenza biunivoca di G in sé.
Infatti:
1. $ax = ay \implies x = y$, cioè T_a è iniettiva.
2. Per ogni $y \in G$ esiste $x \in G$ tale che $y = ax$: basta prendere $x = a^{-1}y$, quindi T_a è suriettiva.

Quindi T_a è biunivoca, pertanto appartiene all'insieme delle funzioni biunivoche di G in sé stesso: $T_a \in S(G)$.

Definiamo adesso l'applicazione:

$$\begin{aligned}\Phi : (G, \cdot) &\longrightarrow (S(G), \circ) \\ a &\longrightarrow T_{a.}\end{aligned}$$

1. Φ conserva l'operazione: dobbiamo dimostrare che $\Phi(ab) = \Phi(a) \circ \Phi(b)$, cioè $T_{ab} = T_a \circ T_b$.

$$T_{ab}(x) = ab \cdot x = a(bx) = a(T_b(x)) = T_a(T_b(x)) = T_a \circ T_b(x), \quad \forall x \in G$$

2. Φ è iniettiva. Infatti se $\Phi(a) = \Phi(b)$, cioè $T_a = T_b$,

$$T_a = T_b \implies T_a(x) = T_b(x) \implies ax = bx \implies a = b$$

   in particolare:

$$a = T_a(e) = T_b(e) = b \implies a = b$$

   Chiaramente tale applicazione non è suriettiva, perché se confrontiamo le cardinalità di G e di $S(G)$ sono rispettivamente n e $n!$. Tuttavia l'immagine di Φ, cioè $\Phi(G) \overset{def}{=} \{T_a | a \in G\}$ è un sottogruppo di $S(G)$ risulta quindi isomorfo a G.

Questo teorema viene utilizzato nella dimostrazione del teorema di **Cayley**, che afferma che ogni gruppo (G) è isomorfo ad un sottogruppo di $(S(G))$.

Il teorema che abbiamo appena dimostrato fa vedere che per ogni gruppo esiste un **omomorfismo** (approfondiremo questo concetto più avanti) **iniettivo canonico**

Gruppo Simmetrico S_n

Ora, nel caso in cui l'insieme X sia finito e ha cardinalità n ($X = \{x_1, x_2, \ldots, x_n\}$) il gruppo $S(X)$ si indica con S_n e prendi il nome di **gruppo simmetrico** (o **di permutazioni**) di g n (o su n elementi).

Sia $X = \{1, 2, \ldots, n\}$. Ogni elemento σ di S_n, in quanto corrispondenza biunivoca di X in sé, rappresenta una *permutazione* di $\{1, 2, \ldots, n\}$. Quindi la cardinalità di S_n è $n!$ (fattoriale)

Prendiamo per esempio $n = 6, X = \{1, 2, 3, 4, 5, 6\}$ e sia σ la seguente corrispondenza biunivoca:

$$\begin{aligned}\sigma : X &\longrightarrow X \\ 1 &\longrightarrow 5 \\ 2 &\longrightarrow 1 \\ 3 &\longrightarrow 4 \\ 4 &\longrightarrow 6 \\ 5 &\longrightarrow 2 \\ 6 &\longrightarrow 3.\end{aligned}$$

Possiamo scrivere σ come una matrice 2×6 :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 2 & 3 \end{pmatrix}$$

Notiamo che nella seconda riga vi sono tutti gli elementi di X anche se in ordine diverso. In generale quindi un elemento di S_n verrà indicato con la matrice $2 \times n$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ i_1 & i_2 & i_3 & i_4 & \dots & i_n \end{pmatrix}$$

(la prima riga è sempre la stessa, la seconda è data dalle varie permutazioni).

Proposizione - Se $n \geq 3$ allora S_n non è abeliano

S_n non è abeliano se $n \geq 3$. Per dimostrarlo, analizziamo il caso in cui $n = 2$ e $n = 3$.

- $n = 2$
  Nel caso di S_2, che è il gruppo simmetrico su un insieme di due elementi, ci sono solo due possibili permutazioni: l'identità, che lascia entrambi gli elementi al loro posto, e la trasposizione, che scambia i due elementi. Chiamiamo l'identità e e la trasposizione τ. Quindi abbiamo:

  $$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

  Ora, se calcoliamo le composizioni $e \circ \tau$ e $\tau \circ e$, otteniamo:

  $$e \circ \tau = \tau, \quad \tau \circ e = \tau.$$

  E se calcoliamo $\tau \circ \tau$, otteniamo e. Quindi, in S_2, la composizione di qualsiasi coppia di permutazioni è commutativa, cioè $\sigma \circ \tau = \tau \circ \sigma$ per ogni $\sigma, \tau \in S_2$. Questo è il motivo per cui S_2 è un gruppo commutativo (o abeliano).
- $n = 3$
  Nel caso di S_3, che è il gruppo simmetrico su un insieme di tre elementi, supponiamo che σ sia la permutazione che scambia 1 e 2, e τ sia la permutazione che scambia 2 e 3. Quindi abbiamo:

  $$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

  Calcoliamo ora le composizioni $\sigma \circ \tau$ e $\tau \circ \sigma$:

  $$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

  Notiamo che $\sigma \circ \tau \neq \tau \circ \sigma$, il che dimostra che S_n non è commutativo per $n \geq 3$.

Congruenze - L'anello $\mathbb{Z}_n$

La **relazione di congruenza modulo** n (un intero positivo) è una relazione che identifica in $\mathbb{Z}$ se la differenza tra due elementi è multiplo di n.

Sia $n \geq 2$. Si dice *relazione di congruenza modulo* n la relazione su $\mathbb{Z}$:

$$a\ \rho_n\ b, \text{ ovvero } a \equiv b(\text{mod } n) \iff a - b = nh, \text{ per qualche } h \in \mathbb{Z}.$$

Ovvero che a e b hanno lo stesso resto se divisi per n. Ogni intero a è *congruo modulo* n ad un intero b tale che $0 \leq b < n$. In luogo di $a \equiv b \pmod n$ si può anche scrivere $a \equiv b(n)$ oppure $a \equiv_n b$.

Esempio di modulo nella vita reale

Un esempio che può rendere l'idea è dato dalle lancette dell'orologio. Quando sono le ore $16:00$ molto spesso diciamo che sono le $4:00$. Se dalle ore 00:00 voglio che passino 72 ore (quindi 3 giorni), non saranno le $72:00$, ma sempre le $00:00$ (ogni 12 ore il ciclo ricomincia).

Osservazione 1 - la congruenza è una relazione di equivalenza

Sia $n > 0$ un intero fissato. La *relazione di congruenza modulo* n è una *relazione di equivalenza*. Risulta infatti:

- $a \equiv a \pmod n, \forall a \in \mathbb{Z}$;
- $a \equiv b \pmod n \implies b \equiv a \pmod n$;
- $a \equiv b \pmod n, b \equiv c \pmod n \implies a \equiv c \pmod n$;

Osservazione 2 - estensione ai casi specifici

La definizione di congruenza può essere estesa anche ai casi $n = 1, n = 0, n < 0$:

1. $a \equiv b \pmod 1 \iff 1|a - b \iff a - b \in \mathbb{Z}$. Dunque $\equiv_1$ è la relazione **caotica**, perché *tutti i numeri sono equivalenti fra loro.* b diviso 1 dà b con resto zero, perciò tutti gli a sono **equivalenti** a $(b \bmod 1) = 0$.
2. $a \equiv b \pmod 0 \iff 0|a - b \iff a - b = 0$. Dunque $\equiv_0$ è la relazione **identica,** perché *ogni numero è uguale a sé stesso.* b diviso 0 (in algebra) è uguale a 0 con resto b, ciò implica che a è **equivalente** a b se e solo se $a = b$.
3. Sia $n < 0$. $a \equiv b \pmod n \iff |n|\ |a - b$. Dunque $\equiv_n$ coincide con $\equiv_{|n|}$, in quanto, se divido per un numero negativo, *il resto rimane invariato.*

Con $\mathbb{Z}_n$ si definisce l'insieme quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo n:

$$\boxed{\mathbb{Z}_n \overset{def}{=} \mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}}$$

I suoi elementi sono detti **classi resto modulo** n. Per ogni $a \in \mathbb{Z}$ la classe resto di a modulo n è denotata $\bar{a}$ (oppure$[a]$). Risulta:

$$\bar{a} = a + n\mathbb{Z} = \{a + nt, \forall t \in \mathbb{Z}\}.$$

Dove $\bar{a}$ equivale agli interi che divisi per n danno resto a.

Osservazione 3 - insiemi delle classi di equivalenza in $\mathbb{Z}_n$

Ricordando la proprietà che lega classi di equivalenza e relazioni di equivalenza, con la relazione $a \sim_n b$ valida se $a - b$ è divisibile per n, notiamo che nell'insieme delle classi di equivalenza

$$\mathbb{Z}_n = \{[0], [1], [2], [n-1], [n], [n+1], [n+2]\}$$

alcune classi di equivalenza coincidono: infatti $[n+1] = [+1]$, perché $(n+1) - (+1) = n$, che è divisibile per n. In particolare $n+1$ e $+1$ sono congruenti ad $1 \pmod n$.

Proposizione 1 - congruenza compatibile con operazioni di $\mathbb{Z}$

La relazione di congruenza $\equiv_n$ è compatibile con le due operazioni definite in $\mathbb{Z}$. Ne segue che $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo unitario con $[0]$ elemento neutro additivo e $[1]$ elemento neutro moltiplicativo. Infatti, se a, b, c, d sono elementi di $\mathbb{Z}$:

$$a \equiv b \operatorname{mod}(n), c \equiv d \pmod n \implies \begin{cases} a + c \equiv b + d \pmod n \\ ac \equiv bd \pmod n \end{cases}$$

Dimostrazione:

$$\begin{aligned} (1)\ a \equiv b \pmod n &\iff a - b = hn \\ c \equiv d \pmod n &\iff c - d = kn \\ &\implies a + c - (b + d) = (h + k)n \\ &\implies a + c \equiv b + d \pmod n \qquad \triangle \end{aligned}$$

$$\begin{aligned} (2)\ ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d \\ akn + hnd = (ak + hd)n \implies ac \equiv bd \pmod n \qquad \square \end{aligned}$$

Da cui deduciamo che $\bar{a} + \bar{b} = \overline{a + b}$, $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$, $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n$.

Queste due operazioni sono **ben definite,** ovvero non dipendono dalla scelta dei rappresentanti delle classi di equivalenza (ad esempio $[5] + [4] = [2] + [1] = [3] = [0]$ (in modulo 3)).

Proposizione 2 - $\mathbb{Z}_n$ come dominio di integrità

In generale $\mathbb{Z}_n$ non è un *dominio di integrità,* infatti nei domini di integrità vale la legge di cancellazione. Prendiamo per esempio $(\mathbb{Z}_4, +, \cdot)$ dove $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ e verifichiamo che sia un dominio di integrità per la moltiplicazione:

$a \underset{4}{\cdot} b$	**0**	**1**	**2**	**3**

0	0	0	0	0
1	0	1	2	3
2	0	2	*0*	2
3	0	2	2	1

Ricordando la definizione di **dominio di integrità e divisore dello zero**, deduciamo che $\mathbb{Z}_4$ non è un *dominio di integrità*, perché in esso $\mathbf{2}$ è un divisore dello zero: infatti $(2 \cdot 2) \bmod 4 = 4 \bmod 4 = 0$.

Proposizione 3 - numeri primi e domini di integrità

Notiamo che $\mathbb{Z}_n$ è un dominio di integrità se e solo se n è un numero primo.

Dimostrazione:
Ipotizziamo per *assurdo* che $\mathbb{Z}_n$ sia un dominio di integrità e che n non sia primo, pertanto n *deve essere ottenuto da due numeri* $1 < a, b < n | a \cdot b = n$. Questo implica che $ab \equiv 0 \pmod n$, ma sia a che b non sono uguali a 0, ciò significa che questo *non è un dominio di integrità*, che è un **assurdo** che contraddice la nostra ipotesi.

Proposizione 4 - $\mathbb{Z}_n$ come campo e numeri primi

$\mathbb{Z}_n$ è un campo $\iff n$ è primo.
Dimostrazione:
$\implies$:
Dimostreremo che se n non è primo allora $\mathbb{Z}_n$ non è un campo.
Nella Proposizione 3 abbiamo visto come $\mathbb{Z}_n$ non sia un dominio di integrità se n non è primo. Quindi ci resta dimostrare che se un anello non è un dominio di integrità allora non è un campo. Ipotizziamo che a sia invertibile e che a sia un divisore dello zero. Ciò significa che $ax = 0$ per qualche $x \neq 0$. Allora $0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot x = x$ che è un assurdo. Pertanto, se a è un divisore dello zero allora non è invertibile, perciò un anello che contiene divisori dello zero non è un campo.
$\impliedby$:
Se un numero n è primo è coprimo con tutti i numeri da 1 a $n-1$, pertanto è possibile scrivere un'identità di Bézout del tipo $ax + ny = 1$ dove $a : \{1, 2, \dots, n-1\}$. Convertita in un'equazione congruenziale diventa $ax \equiv 1 \pmod n$. Notiamo come x quindi sia l'inverso di a, quindi a è invertibile.

Notiamo quindi che se n non è un numero primo, allora solo i numeri coprimi con esso saranno invertibili. Ma quanti sono gli elementi invertibili? Per scoprirlo, occorre utilizzare la funzione φ di Eulero.

TODO

- Collegare alla funzione φ di Eulero