Combinatoria Algebrica
Appunti

Innamorato Italiano e Innamorata Giapponese

Contents

Chapter 1

Fondamenti di Algebra Astratta per Informatici

Vediamo le strutture algebriche principali e i morfismi utilizzati nel corso. Notiamo come sta roba non ce la sta a spiegare nessuno se non il sommo Gem, dato che appunto siamo informatici.

1.1 Gruppi

Definition 1.1.1: Gruppo

E' una coppia $(G, \cdot)$ dove:

- G e' un insieme non vuoto
- $\cdot$ e' un'operazione $G \times G \to G$ (chiusa su G)

Che soddsfa gli assiomi:

- Associativita'
- Esistenza dell'elemento *neutro* e
- Esistenza dell'*inverso* a^{-1} per ogni $a \in G$

Alcune delle proprieta' piu' importanti dei gruppi sono:

- **Unicita'** dell'elemento inverso e neutro
- **Inverso del prodotto**: $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- **Legge della cancellazione**: $a \cdot b = a \cdot c$ moltiplicando a sx per a^{-1} si ottiene $b = c$

Note:

Se vale anche la proprieta' *commutativa*, allora il gruppo si dice *abeliano*.

Example 1.1.1 (Gruppo di addizione sugli interi)

Un esempio classico e intuitivo è l'insieme dei numeri interi $\mathbb{Z}$ associato all'operazione di addizione $+$:

$$(\mathbb{Z}, +)$$

E' facile dimostrare che l'addizione sugli interi rispetta tutti gli assimi per essere un gruppo:

1. **Chiusura:** La somma di due numeri interi restituisce sempre un numero intero.

$$\forall a, b \in \mathbb{Z}, \quad (a + b) \in \mathbb{Z}$$

2. **Associatività:** L'ordine di raggruppamento delle addizioni non influisce sul risultato.

$$\forall a, b, c \in \mathbb{Z}, \quad (a + b) + c = a + (b + c)$$

3. **Esistenza dell'Elemento Neutro:** Esiste un elemento, lo 0, che addizionato a qualsiasi altro intero lo lascia inalterato.

$$\exists 0 \in \mathbb{Z} \text{ tale che } \forall a \in \mathbb{Z}, \quad a + 0 = 0 + a = a$$

4. **Esistenza dell'Elemento Inverso:** Per ogni intero a, esiste il suo inverso additivo (l'opposto) $-a$, tale che la loro somma dia l'elemento neutro.

$$\forall a \in \mathbb{Z}, \exists (-a) \in \mathbb{Z} \text{ tale che } a + (-a) = (-a) + a = 0$$

Inoltre, l'addizione gode anche della proprieta' commutativa, quindi possiamo dire che $(\mathbb{Z}, +)$ e' anche un gruppo *abeliano*.

Vediamo ora cosa sono i sottogruppi:

Definition 1.1.2: Sottogruppo

Dato un gruppo $(G, \cdot)$, si dice che B e' un suo sottogruppo se:

- $B \subset G$
- $(B, \cdot)$ e' un gruppo

Example 1.1.2 (Sottogruppo somma con interi pari)

Un esempio classico, partendo dal gruppo degli interi $(\mathbb{Z}, +)$, è l'insieme dei numeri interi pari, indicato con $2\mathbb{Z}$:

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

Invece di riverificare tutti gli assiomi, per dimostrare che $(2\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$, è sufficiente applicare il Criterio del Sottogruppo e verificare le seguenti tre condizioni:

1. **Non vuotezza (Elemento neutro):** L'elemento neutro del gruppo principale, lo 0, deve appartenere al sottoinsieme.

$$0 = 2 \cdot 0 \implies 0 \in 2\mathbb{Z}$$

   Questo ci assicura anche che l'insieme non sia vuoto.

2. **Chiusura rispetto all'operazione:** La somma di due numeri pari è ancora un numero pari. Siano $a, b \in 2\mathbb{Z}$; allora esistono due interi $m, n \in \mathbb{Z}$ tali che $a = 2m$ e $b = 2n$.

$$a + b = 2m + 2n = 2(m + n)$$

   Poiché $(m + n) \in \mathbb{Z}$, deduciamo che la somma $(a + b)$ appartiene ancora a $2\mathbb{Z}$.

3. **Chiusura rispetto all'inverso:** L'opposto di un numero pari è a sua volta pari. Sia $a = 2m \in 2\mathbb{Z}$. Il suo inverso additivo è:

$$-a = -(2m) = 2(-m)$$

   Poiché $-m \in \mathbb{Z}$, allora anche l'inverso additivo $-a$ appartiene a $2\mathbb{Z}$.

Conclusione: Poiché le condizioni sono soddisfatte, $(2\mathbb{Z}, +)$ è a tutti gli effetti un sottogruppo di $(\mathbb{Z}, +)$. In notazione algebrica, questo si indica spesso come $2\mathbb{Z} \leqslant \mathbb{Z}$.

Un importante teorema per i sottogruppi: TODO finisci

Theorem 1.1.1 Lagrange

Se G e' un gruppo finito e H un suo sottogruppo, allora la cardinalita' degli elementi di G divide esattamente

1.1.1 Centro di un Gruppo

Definition 1.1.3: Centro di un Gruppo

Sia G un gruppo. Il **centro** di G, tipicamente denotato con $Z(G)$, è l'insieme di tutti gli elementi di G che commutano con ogni elemento del gruppo stesso. In simboli:

$$Z(G) = \{z \in G \mid z \cdot g = g \cdot z, \forall g \in G\}$$

Note:

Proprietà fondamentali ed Esempi:

- **È un sottogruppo:** L'elemento neutro e commuta con tutto, quindi $e \in Z(G)$. Essendo chiuso rispetto al prodotto e all'inverso, costituisce un sottogruppo a tutti gli effetti ($Z(G) \leq G$).
- **È un sottogruppo normale:** Poiché ogni elemento $z \in Z(G)$ commuta con tutti i $g \in G$, la coniugazione lo lascia invariato: $gzg^{-1} = zgg^{-1} = z \in Z(G)$. Di conseguenza, $Z(G) \trianglelefteq G$.
- **Casi limite:** Se G è abeliano, il centro coincide con tutto il gruppo ($Z(G) = G$). Se invece $Z(G) = \{e\}$, si dice che il gruppo ha centro banale (es. il gruppo simmetrico S_n per $n \geq 3$).
- **Applicazione in Combinatoria Algebrica:** Il centro del gruppo generale lineare $GL(V)$ è costituito esattamente dalle matrici scalari non nulle ($Z = \{\lambda I \mid \lambda \in K^\times\}$). Questo fatto è il motore logico della dimostrazione del **Lemma di Schur**.

Example 1.1.3 (Centro del gruppo dei quaternioni)

Consideriamo il gruppo dei quaternioni Q_8, un noto gruppo non abeliano di ordine 8, i cui elementi sono:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

Le operazioni in questo gruppo seguono le regole di moltiplicazione $i^2 = j^2 = k^2 = -1$ e $ij = k$, $ji = -k$ (eccetera).
Vogliamo determinare il centro del gruppo, indicato con $Z(Q_8)$. Analizziamo gli elementi:

- Gli elementi 1 e -1 commutano con qualsiasi altro elemento all'interno di Q_8. Ad esempio, $1 \cdot i = i \cdot 1$ e $(-1) \cdot j = j \cdot (-1)$.
- Gli elementi $\pm i, \pm j, \pm k$ **non** commutano con tutti gli elementi del gruppo. Come si evince dalle regole di moltiplicazione, l'ordine dei fattori conta: $ij = k$, ma $ji = -k$, perciò $ij \neq ji$.

Di conseguenza, gli unici elementi che commutano con tutto Q_8 sono 1 e -1. Il centro del gruppo dei quaternioni è quindi il sottogruppo:

$$Z(Q_8) = \{1, -1\}$$

1.1.2 Sottogruppi Normali

Dobbiamo prima definire un'operazione che ci servira'

Definition 1.1.4: Operazione di Coniugio

Sia G un gruppo e siano $x, g \in G$. Si definisce **coniugio** di x tramite g l'operazione che associa ad x l'elemento:

$$x^g = gxg^{-1}$$

Due elementi $x, y \in G$ si dicono **coniugati** se esiste un elemento $g \in G$ tale che $y = gxg^{-1}$. Questa è una relazione di equivalenza che partiziona il gruppo in **classi di coniugio**.

Note:

Osservazioni e Proprietà:

- **Automorfismo Interno:** Per ogni $g \in G$, la mappa $\gamma_g : G \to G$ definita da $\gamma_g(x) = gxg^{-1}$ è un automorfismo del gruppo (chiamato automorfismo interno). Questo significa che il coniugio preserva tutte le proprietà algebriche dell'elemento (ad esempio, x e gxg^{-1} hanno sempre lo stesso ordine).
- **Nei Gruppi Abeliani:** Se G è commutativo, il coniugio è banale: $gxg^{-1} = xgg^{-1} = x$. In questo caso, ogni elemento forma una classe di coniugio a sé stante.
- **Invarianza dei Caratteri:** Questa è la proprietà più importante per il Modulo 2. I caratteri di una rappresentazione sono **funzioni di classe**, ovvero assumono lo stesso valore su tutti gli elementi di una stessa classe di coniugio: $\chi(x) = \chi(gxg^{-1})$.

Possiamo ora definire cosa sono i sottogruppi normali

Definition 1.1.5: Sottogruppo Normale

Sia G un gruppo e N un suo sottogruppo ($N \leq G$). Diciamo che N è un **sottogruppo normale** di G, e si denota con il simbolo $N \trianglelefteq G$, se è invariante rispetto all'operazione di coniugio per qualsiasi elemento del gruppo. In formule, deve valere:

$$gng^{-1} \in N \quad \forall n \in N, \forall g \in G$$

Note:

Condizioni Equivalenti Nella pratica algebrica, dire che $N \trianglelefteq G$ equivale a verificare una di queste due proprietà:

- **Invarianza globale per coniugio:** $gNg^{-1} = N$ per ogni $g \in G$.
- **Coincidenza dei laterali:** I laterali sinistri coincidono sempre con i laterali destri. Ovvero, $gN = Ng$ per ogni $g \in G$. (Attenzione: questo non significa che gli elementi commutino individualmente, cioè $gn = ng$, ma che gli *insiemi* risultanti siano identici).

Esempi e Proprietà Fondamentali

- **Gruppi Abeliani:** Se il gruppo G è commutativo (come i gruppi ciclici o il Gruppo di Klein V_4), allora *ogni* suo sottogruppo è banalmente normale, poiché $gng^{-1} = ngg^{-1} = n$.
- **Nucleo di un Omomorfismo:** Il nucleo di un qualsiasi omomorfismo $\phi : G \to H$ è sempre un sottogruppo normale di G ($\ker(\phi) \trianglelefteq G$).
- **Il Centro del Gruppo:** Il centro $Z(G)$, contenendo gli elementi che commutano con tutto, è sempre un sottogruppo normale di G.

Il Fine Ultimo: Il Gruppo Quoziente La normalità è la condizione necessaria e sufficiente per poter definire un'operazione coerente sull'insieme dei laterali $\{gN \mid g \in G\}$. Solo se $N \trianglelefteq G$, il prodotto $(aN) \cdot (bN) = (ab)N$ è ben definito. Questo ci permette di creare il **Gruppo Quoziente** G/N, una struttura fondamentale che "semplifica" il gruppo di partenza collassando tutto il sottogruppo N nell'elemento neutro.

1.1.3 Gruppi Simmetrici

Definition 1.1.6: Il Gruppo Simmetrico

Sia X un insieme. Il **Gruppo Simmetrico** di X, denotato con $Sym(X)$ o Perm(X), è l'insieme di tutte le funzioni biunivoche (permutazioni) $f : X \to X$. Sotto l'operazione di composizione di funzioni, $Sym(X)$ forma un gruppo.

Proposition 1.1.1 Isomorfismo fra gruppi simmetrici

Si puo' dimostrare che gruppi simmetrici di insiemi aventi la stessa cardinalita' n sono isomorfi, quindi si tende a considerare il gruppo simmetrico costituito dalle permutazioni degli interi $1, 2, \ldots, n$ denotato S_n.

Theorem 1.1.2 Classi di Coniugio del gruppo simmetrico

Dato un gruppo simmetrico S_n, due permutazioni $\sigma, \tau \in S_n$ appartengono alla stessa **classe di coniugio** se e solo se hanno la stessa **struttura ciclica**, ovvero se presentano lo stesso numero di cicli della stessa lunghezza nella loro scomposizione in cicli disgiunti.

Un **ciclo** (o permutazione ciclica) è un tipo speciale, e molto semplice, di permutazione.
Intuitivamente, un ciclo prende un sottoinsieme di elementi e li "fa ruotare" di una posizione, lasciando tutti gli altri elementi dell'insieme perfettamente immobili al loro posto.

Definition 1.1.7: Permutazione ciclica e Punto fisso

Sia X un insieme. Un ciclo di lunghezza k (chiamato anche *k-ciclo*) è una permutazione σ tale per cui esistono k elementi distinti $x_1, x_2, \ldots, x_k$ in X per i quali vale:

- $\sigma(x_1) = x_2$
- $\sigma(x_2) = x_3$
- $\ldots$
- $\sigma(x_{k-1}) = x_k$
- $\sigma(x_k) = x_1$

Per ogni altro elemento $y \in X$ che non fa parte di questo sottoinsieme, il ciclo non ha alcun effetto, ovvero $\sigma(y) = y$. In questo caso si dice che y è un punto fisso della permutazione.

Note:

Invece di scrivere la funzione o la matrice per esteso, in algebra si usa una notazione molto compatta. Il ciclo appena descritto si scrive semplicemente racchiudendo gli elementi interessati tra parentesi tonde, separati da spazi:

$$\sigma = (x_1\ x_2\ \ldots\ x_k)$$

Questa scrittura si legge tipicamente da sinistra a destra: ogni elemento viene mandato in quello alla sua destra, e l'ultimo elemento chiude il cerchio venendo rimandato al primo.

Example 1.1.4 (Cicli di S_5)

Consideriamo il gruppo simmetrico S_5, ovvero l'insieme delle permutazioni sull'insieme $X = \{1, 2, 3, 4, 5\}$.
Definiamo il ciclo $\pi = (1\ 3\ 5)$.
Ecco cosa fa esattamente questa permutazione quando viene applicata agli elementi di X:

- Manda 1 in 3: $\pi(1) = 3$
- Manda 3 in 5: $\pi(3) = 5$

- Manda 5 in 1: $\pi(5) = 1$

E gli elementi 2 e 4? Poiché non compaiono esplicitamente tra le parentesi del ciclo, la regola stabilisce che essi restino fissi:

- $\pi(2) = 2$
- $\pi(4) = 4$

Nota bene: Il ciclo (1 3 5) rappresenta esattamente la stessa funzione dei cicli (3 5 1) e (5 1 3). Poiché si tratta di un "girotondo", non importa da quale elemento si inizia a scrivere, purché si rispetti l'ordine sequenziale delle trasformazioni!

Note:

Proprietà e Relazione con le Partizioni:

- **Corrispondenza biunivoca:** Le classi di coniugio di S_n sono in corrispondenza biunivoca con le **partizioni** dell'intero n. Una partizione $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ tale che $\sum \lambda_i = n$ definisce univocamente una classe di coniugio.
- **Numero di Rappresentazioni:** In virtù della teoria generale, il numero di rappresentazioni irriducibili distinte di S_n su $\mathbb{C}$ è esattamente uguale al numero di partizioni $p(n)$.
- **Esempio S_3 ($n = 3$):** Le partizioni di 3 sono:
  - $(1, 1, 1) \rightarrow$ Identità (cicli di lunghezza 1).
  - $(2, 1) \rightarrow$ Trasposizioni $\{(12), (13), (23)\}$.
  - $(3) \rightarrow$ 3-cicli $\{(123), (132)\}$.
- **Rappresentazioni Notevoli:** Ogni S_n possiede sempre almeno due rappresentazioni di grado 1: la *banale* ($\chi(g) = 1$ per ogni g) e la *segnatura* ($\chi(g) = \text{sgn}(g)$).
- **Diagrammi di Young:** Le rappresentazioni irriducibili di S_n vengono classificate e costruite tramite i **Diagrammi di Young**, che sono la rappresentazione grafica delle partizioni di n.

1.1.4 Gruppi Lineari Generali

Definition 1.1.8: Il Gruppo Lineare Generale di uno Spazio Vettoriale

Sia V uno spazio vettoriale su un campo K. Il **Gruppo Lineare Generale** di V, denotato con $GL(V)$ o $\text{Aut}(V)$, è l'insieme di tutti gli **automorfismi lineari** dello spazio V (ovvero, tutte le applicazioni lineari biunivoche $f : V \rightarrow V$).
La struttura $(GL(V), \circ)$ forma un gruppo dove l'operazione interna è la **composizione di funzioni**:

- **Chiusura:** La composizione di due automorfismi lineari è ancora un automorfismo lineare.
- **Elemento neutro:** L'applicazione identica id_V (tale che $\text{id}_V(v) = v, \forall v \in V$).
- **Inverso:** L'applicazione lineare inversa f^{-1}, che esiste sempre ed è unica poiché f è una biiezione.

Note:

Distinzione tra $Sym(V)$ e $GL(V)$:

- **Natura delle trasformazioni:** Mentre $Sym(V)$ contiene *qualsiasi* funzione biettiva (anche quelle che "rimescolano" i vettori in modo selvaggio e non lineare), il gruppo $GL(V)$ è il sottogruppo di $Sym(V)$ costituito solo dalle trasformazioni che sono anche **lineari**.
- **Inclusione:** $GL(V) \leq Sym(V)$. In termini di Teoria delle Rappresentazioni, diciamo che una rappresentazione è un'azione di G su V tale che l'immagine dell'omomorfismo non sia semplicemente in $Sym(V)$,

ma sia contenuta interamente in $GL(V)$.

- **Esempio concettuale:** Se $V = \mathbb{R}^2$, una funzione che sposta il vettore $(1,1)$ in $(2,2)$ e il vettore $(2,2)$ in $(5,0)$ può appartenere a $Sym(V)$ (se è biettiva), ma non potrà mai appartenere a $GL(V)$ perché non rispetta la proporzionalità (linearità).
- **Il "filtro" della Rappresentazione:** Quando scriviamo $\rho : G \to GL(V)$, stiamo imponendo che ogni simmetria del gruppo G agisca sullo spazio V rispettando la sua struttura vettoriale (somma e prodotto per scalare), non solo come un semplice rimescolamento di punti.

Rappresentazione Matriciale $GL(n, K)$

Se lo spazio vettoriale V ha dimensione finita n, fissata una base di V, ogni isomorfismo lineare può essere rappresentato univocamente da una matrice quadrata di ordine n. Di conseguenza, $GL(V)$ è isomorfo al gruppo delle matrici invertibili a coefficienti nel campo K:

$$GL(n, K) = \{A \in M_n(K) \mid \det(A) \neq 0\}$$

In questa veste, l'operazione del gruppo diventa la **moltiplicazione riga per colonna** tra matrici e l'elemento neutro è la matrice identità I_n.

Proprietà Fondamentali

1. **Non Abelianità:** Se la dimensione $n \geq 2$, il gruppo $GL(V)$ è tipicamente **non commutativo** (poiché il prodotto di matrici non commuta in generale).
2. **Il Centro del Gruppo:** Il centro $Z(GL(V))$ (ovvero l'insieme degli elementi che commutano con ogni altro elemento del gruppo) è costituito esattamente dalle **matrici scalari** non nulle: $Z = \{\lambda I_n \mid \lambda \in K^\times\}$. Questo fatto è il motore logico del **Lemma di Schur**.
3. **Sottogruppo Speciale Lineare:** Il nucleo dell'omomorfismo determinante ($\det : GL(n, K) \to K^\times$) forma un importante sottogruppo normale di $GL(n, K)$, chiamato *Gruppo Speciale Lineare* $SL(n, K)$, composto da tutte e sole le matrici con determinante uguale a 1.

Il Ruolo Centrale nel Modulo 2

Questa definizione è il perno del corso di Combinatoria Algebrica. Definire una rappresentazione di un gruppo finito astratto G su uno spazio vettoriale V significa esattamente stabilire un omomorfismo:

$$\rho : G \to GL(V)$$

Stiamo, di fatto, "traducendo" la struttura moltiplicativa del gruppo astratto G in operazioni tra matrici invertibili, permettendoci così di sfruttare tutta la potenza dell'Algebra Lineare (autovalori, traccia, diagonalizzazione) per studiare le simmetrie del gruppo.

1.1.5 Gruppi Ciclici

Definition 1.1.9: Gruppo Ciclico

Un gruppo $(G, \cdot)$ si dice **ciclico** se esiste un elemento $g \in G$, detto **generatore**, tale che ogni elemento di G possa essere espresso come potenza intera di g:

$$G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$

Classificazione e Struttura

I gruppi ciclici sono classificati in base al loro ordine $|G|$:

- Se $|G| = \infty$, allora $G \cong (\mathbb{Z}, +)$.
- Se $|G| = n < \infty$, allora $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$, ovvero il gruppo delle classi di resto modulo n.

Proprietà Fondamentali

1. **Abelianità:** Ogni gruppo ciclico è abeliano. Infatti, $g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a$.
2. **Sottogruppi:** Ogni sottogruppo di un gruppo ciclico è a sua volta ciclico.
3. **Teorema dei Divisori:** Se G è un gruppo ciclico di ordine n, allora per ogni divisore d di n esiste un unico sottogruppo $H \leq G$ tale che $|H| = d$.
4. **Generatori:** Un elemento g^k di un gruppo ciclico d'ordine n è un generatore di G se e solo se $\gcd(k, n) = 1$. Il numero di tali generatori è dato dalla funzione $\varphi(n)$ di Eulero.

Example 1.1.5 (Gruppo Ciclico $\mathbb{Z}_6$)

Consideriamo il gruppo degli interi modulo 6 rispetto all'addizione, indicato con $\mathbb{Z}_6$. I suoi elementi sono le classi di resto modulo 6:

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

Verifica del Generatore

Verifichiamo se l'elemento $\overline{1}$ è un generatore di $\mathbb{Z}_6$. Calcoliamo i suoi multipli (poiché l'operazione è l'addizione, sommiamo l'elemento a se stesso):

- $1 \cdot \overline{1} = \overline{1}$
- $2 \cdot \overline{1} = \overline{1} + \overline{1} = \overline{2}$
- $3 \cdot \overline{1} = \overline{1} + \overline{1} + \overline{1} = \overline{3}$
- $4 \cdot \overline{1} = \overline{4}$
- $5 \cdot \overline{1} = \overline{5}$
- $6 \cdot \overline{1} = \overline{6} \equiv \overline{0} \pmod 6$

Poiché partendo da $\overline{1}$ siamo riusciti a ottenere l'intero insieme $\mathbb{Z}_6$, possiamo affermare che $\mathbb{Z}_6$ è un gruppo ciclico generato da $\overline{1}$. In notazione algebrica, scriviamo:

$$\mathbb{Z}_6 = \langle \overline{1} \rangle$$

Nota: In un gruppo ciclico possono esserci più generatori. Nel caso di $\mathbb{Z}_6$, anche $\overline{5}$ è un generatore ($\langle \overline{5} \rangle = \mathbb{Z}_6$), mentre elementi come $\overline{2}$ generano solo sottogruppi (nello specifico, il sottogruppo $\{\overline{0}, \overline{2}, \overline{4}\}$).

1.1.6 Azioni

Definition 1.1.10: Azione di un Gruppo

Sia G un gruppo e X un insieme non vuoto. Un' **azione** (a sinistra) di G su X è una funzione $\cdot : G \times X \to X$ che associa a ogni coppia (g, x) un elemento $g \cdot x \in X$, tale che siano soddisfatti i seguenti assiomi:

1. **Identità:** $e \cdot x = x$ per ogni $x \in X$ (dove e è l'elemento neutro di G).
2. **Compatibilità:** $(gh) \cdot x = g \cdot (h \cdot x)$ per ogni $g, h \in G$ e $x \in X$.

Note:

Concetti Chiave e Proprietà:

- **Omomorfismo di Permutazione:** Un'azione di G su X è equivalente a un omomorfismo di gruppi $\phi : G \to \mathrm{Sym}(X)$. In questo senso, ogni elemento del gruppo viene visto come una permutazione degli elementi di X.
- **Orbita:** L'orbita di un elemento $x \in X$ è l'insieme $G \cdot x = \{g \cdot x \mid g \in G\}$. Le orbite formano una

partizione dell'insieme X.

- **Stabilizzatore:** Lo stabilizzatore di $x \in X$ è il sottogruppo $G_x = \{g \in G \mid g \cdot x = x\}$. Contiene tutti gli elementi del gruppo che "lasciano fermo" x.
- **Teorema Orbita-Stabilizzatore:** Se G è finito, la cardinalità dell'orbita di x è data dal numero di laterali dello stabilizzatore: $|G \cdot x| = |G|/|G_x|$.
- **Dall'Azione alla Rappresentazione:** Se l'insieme X è uno spazio vettoriale V e l'azione è lineare (cioè $g \cdot (v + w) = g \cdot v + g \cdot w$ e $g \cdot (\lambda v) = \lambda(g \cdot v)$), allora l'azione è esattamente una **rappresentazione lineare** di G.

Example 1.1.6

Un esempio classico ed estremamente intuitivo è l'azione del gruppo diedrale D_4 (il gruppo delle simmetrie del quadrato) sull'insieme dei suoi vertici.

Definizione del Gruppo e dell'Insieme

- **L'insieme X:** Consideriamo i quattro vertici di un quadrato numerati in senso antiorario:

$$X = \{1, 2, 3, 4\}$$

- **Il gruppo G:** Consideriamo D_4, che contiene 8 elementi: 4 rotazioni (di $0°, 90°, 180°, 270°$) e 4 riflessioni (rispetto agli assi verticale, orizzontale e alle due diagonali).

Come agisce il gruppo sull'insieme

L'azione consiste nell'applicare la trasformazione geometrica al quadrato e osservare dove finisce ciascun vertice.
Prendiamo come esempio l'elemento $r \in D_4$, che rappresenta la **rotazione di $90°$ in senso antiorario**. La sua azione sui vertici sarà:

- $r \cdot 1 = 2$ (il vertice 1 si sposta nella posizione del vertice 2)
- $r \cdot 2 = 3$
- $r \cdot 3 = 4$
- $r \cdot 4 = 1$

Prendiamo invece l'elemento $s \in D_4$, che rappresenta la **riflessione rispetto all'asse verticale**. Supponendo che i vertici 1 e 4 siano a destra e 2 e 3 a sinistra, la sua azione sarà:

- $s \cdot 1 = 2$ e $s \cdot 2 = 1$ (i vertici in alto si scambiano)
- $s \cdot 3 = 4$ e $s \cdot 4 = 3$ (i vertici in basso si scambiano)

Verifica degli assiomi: Questa operazione soddisfa i due assiomi fondamentali delle azioni di gruppo. L'elemento neutro (la rotazione di $0°$) lascia ogni vertice al suo posto ($e \cdot x = x$), e combinare due simmetrie (ad esempio ruotare e poi riflettere) equivale ad applicare direttamente la simmetria risultante dalla loro composizione geometrica: $g \cdot (h \cdot x) = (gh) \cdot x$.

1.2 Campo

Definition 1.2.1: Campo

Un **campo** K e' una struttura algebrica dotata di due operazioni:

- *Somma*: t.c. $(K, +)$ e' un *gruppo abeliano* (con elem neutro 0)
- *Prodotto*: t.c. $(K \setminus \{0\}, \cdot)$ e' un *gruppo abeliano* (con elem neutro 1)
- Vale la proprieta' distributiva del prodotto rispetto alla somma

Come conseguenza diretta, si ha che l'elemento neutro della somma diventa **elemento assorbente** ($\forall a \in K. a \cdot 0 = 0$). Infatti, se un prodotto e' 0 allora e' sicuro che almeno uno degli operandi e' 0.

Example 1.2.1 (Campo $(\mathbb{Z}_5, +, \cdot)$)

Un ottimo esempio di campo finito è l'insieme delle classi di resto modulo 5, indicato con $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, equipaggiato con le consuete operazioni di addizione e moltiplicazione modulo 5.
Poiché 5 è un numero primo, la struttura $(\mathbb{Z}_5, +, \cdot)$ è un campo. La caratteristica chiave che lo distingue da altre strutture (come l'anello $\mathbb{Z}_6$) è che **ogni elemento diverso da zero possiede un inverso moltiplicativo**.

Verifica degli inversi moltiplicativi in $\mathbb{Z}_5$

Per ogni elemento $a \in \mathbb{Z}_5 \setminus \{\overline{0}\}$, esiste un elemento b tale che $a \cdot b = \overline{1}$:

- L'inverso di $\overline{1}$ è $\overline{1}$, poiché $\overline{1} \cdot \overline{1} = \overline{1}$.
- L'inverso di $\overline{2}$ è $\overline{3}$, poiché $\overline{2} \cdot \overline{3} = \overline{6} \equiv \overline{1} \pmod 5$.
- L'inverso di $\overline{3}$ è $\overline{2}$, essendo la moltiplicazione commutativa ($\overline{3} \cdot \overline{2} = \overline{1}$).
- L'inverso di $\overline{4}$ è $\overline{4}$, poiché $\overline{4} \cdot \overline{4} = \overline{16} \equiv \overline{1} \pmod 5$.

Campi infiniti: Gli esempi più classici e utilizzati di campi con infiniti elementi sono il campo dei numeri razionali $(\mathbb{Q}, +, \cdot)$, il campo dei numeri reali $(\mathbb{R}, +, \cdot)$ e il campo dei numeri complessi $(\mathbb{C}, +, \cdot)$.

1.2.1 Proprieta' Fondamentali

Caratteristica del Campo ($char(K)$): E' il piu' piccol intero positivo p tale che sommando l'elemento identita' 1 a se' stesso p volte si ottiene 0 (l'elemento neutro) (cioe' $1 + ... + 1 = 0$). Se non esiste un valore p (non si ritorna mai all'elemento neutro) allora $char(K) = 0$.
Chiusura Algebrica: Un campo K si dice algebricamentechiuso se ogni polinomio non costante a coefficienti in K ha almeno una raidce in K. Il campo $\mathbb{C}$ e' algebricamente chiuso, mentre $\mathbb{R}$ non lo e' (ad esempio, $x^2 + 1 = 0$).

1.3 Anelli

Definition 1.3.1: Anello

Un anello e' una terna $(R, +, \cdot)$, dove R e' un insieme dotato di due operazioni binarie interne (somma e prodotto), tale che:

- $(R, +)$ e' un *gruppo abeliano*
- $(R, \cdot)$ e' un *monoide*:
  - Associatività: $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in R$
  - Unità: $\exists 1 \in R \mid a \cdot 1 = 1 \cdot a = a, \forall a \in R$
- Proprieta' distributiva (sx e dx)

Come conseguenza diretta, si ha che l'elemento neutro della somma diventa **elemento assorbente** ($\forall a \in K. a \cdot 0 = 0$). Infatti, se un prodotto e' 0 allora e' sicuro che almeno uno degli operandi e' 0.

Note:

A differenza dei campi, in un anello generale non si richiede che il prodotto sia commutativo ($a \cdot b$ può essere diverso da $b \cdot a$), e non si richiede che ogni elemento non nullo abbia un inverso moltiplicativo (cioè non si può sempre "dividere").

Example 1.3.1 (Anello $(\mathbb{Z}_6, +, \cdot)$)

Un ottimo esempio per comprendere la differenza tra un anello e un campo è l'insieme delle classi di resto modulo 6:

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

I Divisori dello Zero in $\mathbb{Z}_6$

A differenza del campo $\mathbb{Z}_5$ analizzato in precedenza, in $\mathbb{Z}_6$ **non** tutti gli elementi non nulli possiedono un inverso moltiplicativo. Questo accade perché 6 è un numero composto, il che porta alla comparsa dei cosiddetti *divisori dello zero*.
Un divisore dello zero è un elemento non nullo che, moltiplicato per un altro elemento non nullo, restituisce zero. In $\mathbb{Z}_6$, se consideriamo gli elementi $\overline{2}$ e $\overline{3}$, osserviamo che:

$$\overline{2} \cdot \overline{3} = \overline{6} \equiv \overline{0} \pmod 6$$

Sia $\overline{2}$ che $\overline{3}$ sono diversi da $\overline{0}$, ma il loro prodotto è $\overline{0}$. A causa di questa proprietà, è matematicamente impossibile che $\overline{2}$ o $\overline{3}$ ammettano un inverso moltiplicativo (nessun numero moltiplicato per $\overline{2}$ potrà mai dare $\overline{1}$).
Conclusione: Poiché possiede divisori dello zero, la struttura $(\mathbb{Z}_6, +, \cdot)$ è un **anello commutativo**, ma non può essere un campo. Altri esempi classici di anelli includono l'anello dei polinomi o l'anello delle matrici quadrate $n \times n$ (che è un esempio di anello non commutativo).

1.3.1 Proprieta' fondamentali

Per manipolare gli anelli, definiamo alcune categorie di elementi e strutture interne fondamentali:

- **Divisori dello zero:** Un elemento $a \neq 0$ si dice divisore dello zero se esiste un elemento $b \neq 0$ tale che $a \cdot b = 0$. Si osservi che nei campi questa eventualità non si verifica mai per definizione.
- **Elementi Invertibili (Unità):** Gli elementi di R che possiedono un inverso moltiplicativo formano un gruppo rispetto all'operazione di prodotto, indicato con il simbolo $R^\times$ (o $U(R)$).
- **Ideali:** Un sottoinsieme $I \subseteq R$ è un **ideale sinistro** se è un sottogruppo additivo e "assorbe" il prodotto da sinistra: ovvero, per ogni $r \in R$ e ogni $x \in I$, si ha che $r \cdot x \in I$. Gli ideali rappresentano per gli anelli ciò

che i sottogruppi normali rappresentano per i gruppi, permettendo la costruzione degli **anelli quoziente** R/I.

1.4 Spazio Vettoriale

Definition 1.4.1: Spazio Vettoriale

Sia K un campo (i cui elementi sono detti *scalari*). Un insieme V (i cui elementi sono detti *vettori*) è un **spazio vettoriale su** K (o K-spazio vettoriale) se è dotato di due operazioni:

1. **Somma interna:** un'operazione $+ : V \times V \to V$ che rende $(V, +)$ un gruppo abeliano (commutativa, associativa, con elemento neutro 0_V e opposto per ogni vettore).
2. **Prodotto per uno scalare:** un'operazione esterna $\cdot : K \times V \to V$ tale che, per ogni scalare $\alpha, \beta \in K$ e per ogni vettore $u, v \in V$, valgano i seguenti quattro assiomi:
   - **Distributività rispetto alla somma vettoriale:** $\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$
   - **Distributività rispetto alla somma scalare:** $(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$
   - **Compatibilità del prodotto:** $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$
   - **Azione dell'identità scalare:** $1_K \cdot v = v$ (dove 1_K è l'elemento neutro moltiplicativo del campo K).

Example 1.4.1 (Piano Euclideo)

L'esempio più classico e geometricamente intuitivo è il piano euclideo, ovvero l'insieme delle coppie ordinate di numeri reali $\mathbb{R}^2$, considerato sul campo dei numeri reali $\mathbb{R}$.

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$$

Le due operazioni fondamentali in $\mathbb{R}^2$

Siano $\mathbf{u} = (x_1, y_1)$ e $\mathbf{v} = (x_2, y_2)$ due vettori in $\mathbb{R}^2$, e sia $c \in \mathbb{R}$ uno scalare. Le operazioni che rendono $\mathbb{R}^2$ uno spazio vettoriale sono definite componente per componente:

1. **Addizione vettoriale:** La somma di due vettori produce un nuovo vettore in $\mathbb{R}^2$.
$$\mathbf{u} + \mathbf{v} = (x_1 + x_2, y_1 + y_2)$$
2. **Moltiplicazione per uno scalare:** Il prodotto di un vettore per un numero reale "scala" (allunga, accorcia o inverte) il vettore, producendo un risultato che resta in $\mathbb{R}^2$.
$$c\mathbf{u} = c(x_1, y_1) = (cx_1, cy_1)$$

Nota sugli Assiomi: Queste due operazioni in $\mathbb{R}^2$ soddisfano rigorosamente tutti gli otto assiomi richiesti per gli spazi vettoriali (tra cui commutatività e associatività dell'addizione, esistenza del vettore nullo $\mathbf{0} = (0, 0)$, esistenza del vettore opposto, e le varie proprietà distributive). Altri esempi molto utilizzati in algebra lineare includono lo spazio dei polinomi di grado $\leq n$ o lo spazio delle matrici di dimensione $m \times n$.

1.4.1 L'Importanza del Campo K in Teoria delle Rappresentazioni

Nel contesto dello studio delle rappresentazioni $\rho : G \to GL(V)$, le proprietà algebriche del campo K determinano la validità dei teoremi fondamentali:

- **Chiusura Algebrica (Esistenza degli autovalori):** Se lavoriamo su $K = \mathbb{C}$ (che è un campo algebricamente chiuso), il Teorema Fondamentale dell'Algebra ci garantisce che ogni endomorfismo lineare abbia

sempre almeno un autovalore. Questa proprietà è il motore logico che fa funzionare il **Lemma di Schur** e ci permette di diagonalizzare l'azione del gruppo.

- **Caratteristica del Campo (Divisione per $|G|$):** Affinché sia valido il **Teorema di Maschke** (e le rappresentazioni siano completamente riducibili), è necessario che la caratteristica del campo, $\text{char}(K)$, non divida l'ordine del gruppo finito $|G|$. Solo sotto questa condizione l'elemento $|G| \cdot 1_K$ è invertibile in K, rendendo possibile l'operazione di "media sul gruppo" per costruire i proiettori equivarianti.
- **Dimensione Relativa:** La dimensione di uno spazio vettoriale dipende strettamente da K. Ad esempio, l'insieme dei numeri complessi $\mathbb{C}$ ha dimensione 1 se inteso come $\mathbb{C}$-spazio vettoriale, ma possiede dimensione 2 se lo strutturiamo come $\mathbb{R}$-spazio vettoriale (con base $\{1, i\}$).

1.4.2 Prodotto Hermitiano

Definition 1.4.2: Coniugato di un Numero Complesso

Sia $z = a + ib$ un numero complesso, con $a, b \in \mathbb{R}$. Si definisce **coniugato** di z, e si indica con $\overline{z}$ (o talvolta z^*), il numero complesso:

$$\overline{z} = a - ib$$

In termini geometrici, $\overline{z}$ è il simmetrico di z rispetto all'asse delle ascisse nel piano di Argand-Gauss.

Note:

Proprietà Fondamentali:

- **Prodotto con il coniugato:** Il prodotto di un numero per il suo coniugato è sempre un reale non negativo, pari al quadrato del modulo: $z \cdot \overline{z} = a^2 + b^2 = |z|^2$.
- **Linearità:** Il coniugato della somma è la somma dei coniugati: $\overline{z + w} = \overline{z} + \overline{w}$.
- **Moltiplicatività:** Il coniugato del prodotto è il prodotto dei coniugati: $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
- **Involuzione:** Coniugare due volte riporta al numero originale: $\overline{\overline{z}} = z$.
- **Caratterizzazione dei Reali:** Un numero è reale se e solo se coincide con il suo coniugato: $z = \overline{z} \iff z \in \mathbb{R}$.

Ruolo nei Caratteri: Nella teoria delle rappresentazioni, quando calcoliamo il prodotto scalare tra due caratteri χ_1 e χ_2, usiamo il coniugato:

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}$$

Questo garantisce che la "distanza" tra due rappresentazioni sia un valore sensato nel campo complesso.

Definition 1.4.3: Prodotto Hermitiano

Sia V uno spazio vettoriale su $\mathbb{C}$. Un **prodotto hermitiano** è una funzione $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ che associa a ogni coppia di vettori u, v uno scalare complesso, soddisfacendo le seguenti proprietà:

1. **Linearità nel primo argomento:** $\langle au + bw, v \rangle = a\langle u, v \rangle + b\langle w, v \rangle$.
2. **Simmetria Hermitiana (Antisimmetria):** $\langle u, v \rangle = \overline{\langle v, u \rangle}$ (dove la barra indica il coniugato complesso).
3. **Positività definita:** $\langle v, v \rangle \in \mathbb{R}$, $\langle v, v \rangle \geq 0$ e $\langle v, v \rangle = 0$ se e solo se $v = 0$.

Note:

Perché è diverso dal prodotto scalare reale?

- **Il problema del coniugato:** Se usassimo la formula reale $\sum x_i y_i$ con i numeri complessi, potremmo avere un vettore non nullo con "lunghezza" zero (es. $v = (1, i) \to 1^2 + i^2 = 1 - 1 = 0$). Il coniugato nella proprietà (2) serve a garantire che la norma $\|v\|^2 = \langle v, v \rangle$ sia sempre un numero reale positivo.
- **Semi-linearità:** Nota che a causa della simmetria hermitiana, se tiri fuori uno scalare dal *secondo* argomento, questo esce coniugato: $\langle u, \alpha v \rangle = \overline{\alpha} \langle u, v \rangle$.
- **Uso nel Modulo 2:** Lo usiamo per definire le **rappresentazioni unitarie**. Una matrice è unitaria se preserva questo prodotto. Grazie al "trucco della media", abbiamo dimostrato che ogni gruppo finito può essere rappresentato con matrici unitarie.

Example 1.4.2 (Esempio 1: Il Prodotto Hermitiano Standard in $\mathbb{C}^n$)

Siano $u = (z_1, z_2, \ldots, z_n)$ e $v = (w_1, w_2, \ldots, w_n)$ due vettori in $\mathbb{C}^n$. Il prodotto hermitiano standard è definito come:

$$\langle u, v \rangle = \sum_{i=1}^{n} z_i \overline{w_i} = z_1 \overline{w_1} + z_2 \overline{w_2} + \cdots + z_n \overline{w_n}$$

Se prendiamo ad esempio $u = (1, i)$ e $v = (i, 1 + i)$ in $\mathbb{C}^2$:

$$\langle u, v \rangle = 1 \cdot (\bar{i}) + i \cdot (\overline{1 + i}) = 1(-i) + i(1 - i) = -i + i - i^2 = -i + i + 1 = 1$$

Nota come, grazie al coniugato, il risultato finale è un numero che "tiene conto" della fase complessa.

Example 1.4.3 (Esempio 2: Prodotto di Frobenius su Matrici $M_n(\mathbb{C})$)

Lo spazio delle matrici quadrate $n \times n$ può essere visto come uno spazio vettoriale. Il prodotto hermitiano tra due matrici A e B è definito tramite la **traccia**:

$$\langle A, B \rangle = \mathrm{Tr}(AB^*) = \mathrm{Tr}(A\overline{B}^T)$$

Questo prodotto è fondamentale per dimostrare le relazioni di ortogonalità tra le entrate delle matrici delle rappresentazioni irriducibili.

Example 1.4.4 (Esempio 3: Prodotto tra Caratteri (Il più importante per te))

Sia G un gruppo finito e siano $\chi_1, \chi_2 : G \to \mathbb{C}$ i caratteri di due rappresentazioni. Lo spazio delle funzioni di classe possiede un prodotto hermitiano naturale definito "mediando" sul gruppo:

$$\langle \chi_1, \chi_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}$$

Perché è fondamentale?

- Se χ_1 è irriducibile, allora $\langle \chi_1, \chi_1 \rangle = 1$ (norma unitaria).
- Se χ_1 e χ_2 sono irriducibili e non isomorfe, allora $\langle \chi_1, \chi_2 \rangle = 0$ (ortogonalità).

1.5 Morfismi di Strutture Algebriche

In algebra astratta, un morfismo fra due strutture A, B e' una funzione che trasforma l'insieme di sostegno di A nell'insieme di sostegno di B (o in una sua parte) conservando determinate caratteristiche strutturali, in base alle quali si distinguono diversi morfismi.

1.5.1 Omomorfismi

E' un'applicazione fra strutture dello stesso tipo (Gruppi, Anelli, Campi, ecc...) che conserva le operazioni in esse definite

Definition 1.5.1: Omomorfismo

Siano A e B due strutture algebriche dello stesso tipo. Una funzione $\phi : A \to B$ si dice **omomorfismo** se:

$$\forall f \text{ delle strutture}, \forall x_1, ..., x_n . \phi(f_A(x_1, ..., x_n) = f_B(\phi(x_1), ..., \phi(x_n))$$

Dove f_A, f_B rappresentano la funzione f nelle strutture A e B rispettivamente.
Se la struttura ha elementi particolari (unita', zeri, ...), questi vanno considerati come funzioni costanti con zero parametri. Ad esempio, siano e_A, e_B gli elementi neutri delle singole strutture, allora:

$$\phi(e_A) = e_B$$

Omomorfismi di gruppi

Nei gruppi, gli omomorfismi sono "compatibili" con la struttura di gruppo. Ovvero, preserva sia gli elementi neutri che inversi:

$$\phi(a^{-1}) = [\phi(a)]^{-1}$$

Inoltre, valgono le seguenti proprieta':

- **Nucleo (Kernel):** $\ker(\phi) = \{x \in G \mid \phi(x) = e_H\}$. Il nucleo misura quanto l'omomorfismo "collassa" il gruppo di partenza ed è sempre un *sottogruppo normale* di G ($\ker(\phi) \trianglelefteq G$).
- **Immagine:** $\text{Im}(\phi) = \{\phi(x) \mid x \in G\}$. L'immagine rappresenta la porzione del codominio effettivamente raggiunta ed è sempre un sottogruppo di H ($\text{Im}(\phi) \leq H$).

Nel contesto del nostro corso, una **rappresentazione lineare** di un gruppo finito G su uno spazio vettoriale V (su un campo K) non è altro che un omomorfismo di gruppi:

$$\rho : G \to GL(V)$$

dove $GL(V)$ è il gruppo degli automorfismi lineari (matrici quadrate invertibili) dello spazio V. Se $\ker(\rho) = \{e_G\}$, la rappresentazione non "perde" informazioni sul gruppo e si dice **fedele**.

1.5.2 Isomorfismi

Definition 1.5.2: Isomorfismo

Un omomorfismo $\phi : A \to B$ si dice **isomorfismo** se la funzione ϕ è biunivoca (cioè iniettiva e suriettiva).

Isomorfismi di gruppi

Se A e B sono due gruppi, allora:

- **Criterio di iniettività:** Un omomorfismo ϕ è iniettivo se e solo se $\ker(\phi) = \{e_G\}$.
- Se esiste un isomorfismo tra G e H, i due gruppi si dicono isomorfi e si scrive $G \cong H$. Strutturalmente, sono indistinguibili dal punto di vista algebrico.

1.5.3 Automorfismi

Definition 1.5.3: Automorfismo

Un **automorfismo** è un isomorfismo di una struttura in sé stessa, ovvero una mappa biunivoca $\phi : A \to A$ che preserva le operazioni.

Automorfismi di gruppi

Nel caso in cui la struttura di A e' di gruppo:

- L'insieme di tutti gli automorfismi di un gruppo G, dotato dell'operazione di composizione di funzioni, forma un gruppo a sua volta, denotato con $\mathrm{Aut}(G)$.
- **Automorfismi interni:** Fissato un elemento $g \in G$, la mappa di coniugio $\gamma_g(x) = gxg^{-1}$ è sempre un automorfismo di G. L'insieme di questi automorfismi forma un sottogruppo denotato con $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

1.6 L'Omomorfismo Determinante

E' possibile definire la funzione del **determinante** come un omomorfismo di gruppi, vediamo come:

Definition 1.6.1: Determinante

Sia K un campo e $K^\times = K \setminus \{0\}$ il suo gruppo moltiplicativo (formato da tutti gli elementi non nulli di K con l'operazione di prodotto). L'applicazione **determinante** è una mappa:

$$\det : GL(n, K) \to K^\times$$

che associa a ogni matrice invertibile A il suo determinante $\det(A)$ (che è uno scalare in K). Poiché la matrice è invertibile, $\det(A) \neq 0$, quindi il codominio $K^\times$ è corretto.

Questa mappa è un omomorfismo di gruppi grazie al celebre **Teorema di Binet**, il quale garantisce che il determinante del prodotto di due matrici è uguale al prodotto dei loro determinanti:

$$\det(A \cdot B) = \det(A) \cdot \det(B) \quad \forall A, B \in GL(n, K)$$

In altre parole, la mappa det preserva (e trasporta) l'operazione di moltiplicazione dal "complicato" gruppo delle matrici al "semplice" gruppo degli scalari.

Nucleo (Kernel) e Immagine

Applicando le definizioni strutturali degli omomorfismi a questa mappa specifica, otteniamo due informazioni preziose:

- **Immagine:** La mappa è **suriettiva**. Per ogni scalare $\lambda \in K^\times$, esiste sempre almeno una matrice in $GL(n, K)$ che ha λ come determinante (basta prendere la matrice identità e sostituire il primo 1 in alto a sinistra con λ). Quindi, $\mathrm{Im}(\det) = K^\times$.
- **Nucleo:** Il nucleo è formato da tutte le matrici mappate nell'elemento neutro del codominio (che per la moltiplicazione in $K^\times$ è 1).

  $$\ker(\det) = \{A \in GL(n, K) \mid \det(A) = 1\}$$

  Questo insieme definisce il **Gruppo Speciale Lineare**, denotato con $SL(n, K)$. Poiché è il nucleo di un omomorfismo, $SL(n, K)$ è automaticamente un **sottogruppo normale** di $GL(n, K)$ ($SL(n, K) \trianglelefteq GL(n, K)$).

Conseguenza: Il Primo Teorema di Omomorfismo

Per il Primo Teorema di Omomorfismo, il quoziente del dominio rispetto al nucleo è isomorfo all'immagine. Questo ci dà una bellissima identità strutturale:

$$\frac{GL(n, K)}{SL(n, K)} \cong K^\times$$

Applicazione nel Modulo 2 (Caratteri e Rappresentazioni)

Se possediamo una rappresentazione di un gruppo G, ovvero un omomorfismo $\rho : G \to GL(n, \mathbb{C})$, possiamo comporla con l'omomorfismo determinante per creare una nuova mappa:

$$\det \circ \rho : G \to \mathbb{C}^{\times}$$

Poiché la composizione di due omomorfismi è ancora un omomorfismo, questa nuova mappa è a tutti gli effetti una **rappresentazione di grado 1** del gruppo G!

Chapter 2

Fondamenti della Teoria delle Rappresentazioni

Questo corso si colloca all'intersezione tra **Algebra** (gruppi, anelli, campi, spazi vettoriali) e **Combinatoria** (conteggio). Lo scopo è rendere gli oggetti algebrici *astratti* più *concreti*, studiandoli attraverso le loro azioni lineari su spazi vettoriali.
L'idea di fondo è semplice: invece di studiare un gruppo astratto G direttamente, lo "rappresentiamo" tramite matrici invertibili, che sono oggetti molto più maneggevoli.

2.1 Rappresentazioni e Sottorappresentazioni

Una **struttura algebrica astratta** — ad esempio un gruppo — è definita da un insieme e da operazioni che soddisfano degli assiomi.

Definition 2.1.1: Struttura algebrica

Si definisce struttura algebrica una coppia $(G, *)$ dove G è un insieme e $*$ è una operazione binaria su G

Example 2.1.1 (Strutture algebriche)

- **Gruppo**: $(G, *)$ con $*$ binaria e associativa, G con elemento neutro e ogni elemento ha un inverso
- **Anello**: $(G, +, \cdot)$ con $+$ e $\cdot$ binarie e associative, G con elemento neutro per $+$ e ogni elemento ha un inverso per $+$
- **Campo**: $(G, +, \cdot)$ con $+$ e $\cdot$ binarie e associative, G con elemento neutro per $+$ e ogni elemento ha un inverso per $+$

Per "astratta", dal latino, "tirata fuori", si intende estrapolata dal suo contesto originale. La combinatoria quindi, vuole studiare le struttura algebriche e darne una rappresentazione più concreta.
Questa struttura, infatti, può sembrare "sospesa nel vuoto", decontestualizzata. L'idea delle rappresentazioni è di portarla **dentro** uno spazio concreto, dove possiamo agire con strumenti dell'algebra lineare.
Ad esempio, un gruppo può agire su uno spazio vettoriale tramite trasformazioni lineari. Questo lo "rappresenta" come un gruppo di matrici.

Definition 2.1.2: Rappresentazione di un gruppo

Sia G un gruppo, K un campo e V uno spazio vettoriale su K. si definisce una rappresentazione di G su V è un omomorfismo

$$\rho : G \to GL(V)$$

Note:

La rappresentazione e' un omomorfismo, quindi:

$$\forall g, h \in G.\ \rho(g)\rho(h) = \rho(gh)$$

Ricordiamo che $\mathrm{GL}(V)$ è il gruppo degli isomorfismi lineari di V in sé (automorfismi lineari, o equivalentemente matrici invertibili se $V = K^n$).

Note:

In altre parole, ρ è un'azione di G su V che non è solo per biiezioni (come in $\mathrm{Sym}(V)$), ma per **trasformazioni lineari invertibili**.

Definition 2.1.3: Rappresentazione fedele

Diciamo che la rappresentazione è fedele se ρ è iniettiva, ovvero se $\rho(g) = \rho(h) \implies g = h$.

Note:

Ovvero il nucleo di ρ contiene solo l'elemento neutro ($ker(\rho) = \{e\}$) e G si immerge come sottogruppo di $\mathrm{GL}(V)$.

Example 2.1.2 (Gruppo di Klein)

Consideriamo il gruppo di Klein $G = \{a, b, c, d\}$ con tavola di Cayley:

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

L'elemento neutro è c (la riga c è l'identità). Si tratta di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ogni elemento ha ordine 2.
Una rappresentazione su $V = \mathbb{R}^2$ è data da:

$$\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(a) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho(d) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Si può verificare che è un omomorfismo (ad es. $\rho(a)\rho(b) = \rho(d)$, che corrisponde a $a * b = d$ nella tavola).
Rispetto alla decomposizione $V = \langle e_1 \rangle \oplus \langle e_2 \rangle$, le due rette coordinate sono **stabili** sotto l'azione di G: $\rho(g) \cdot e_i$ è sempre nella direzione di e_i. Al contrario, la decomposizione $V = \langle (1,1) \rangle \oplus \langle (1,-1) \rangle$ **non è stabile**, perché le basi non vengono mandate in sé stesse dagli elementi del gruppo.

Definition 2.1.4: Sottorappresentazione

Sia (V, ρ) una rappresentazione di G su V, diciamo che un sottospazio vettoriale $U \subseteq V$ è una sottorappresentazione di ρ se $\rho(g)U \subseteq U$ per ogni $g \in G$.

Note:

In altre parole $(U, \rho_{|U})$ è una rappresentazione di G su U, dove $\rho_{|U} : G \to GL(U)$ è l'omomorfismo che mappa $g \to \rho(g)_{|U}$

2.1.1 Rappresentazioni Riducibili e Decomponibili

Definition 2.1.5: Rappresentazione Irriducibile

Una rappresentazione (ρ, V) di un gruppo G si dice **irriducibile** se gli unici sottospazi di V che siano G-invarianti (sottorappresentazioni) sono i sottospazi banali $\{0\}$ e V stesso. In caso contrario, ovvero se esiste un sottospazio proprio $0 < U < V$ che e' una sottorappresentazione di ρ, la rappresentazione si dice **riducibile**.

Example 2.1.3 (Rappresentazione di C_4 e Dipendenza dal Campo K)

Si consideri il gruppo ciclico di ordine 4, $G = C_4 = \langle z \mid z^4 = 1 \rangle$, e la sua rappresentazione naturale su $V = \mathbb{R}^2$ definita mandando il generatore z nella matrice di rotazione di $\pi/2$:

$$\rho(z) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

L'obiettivo è analizzare la riducibilità di ρ al variare del campo degli scalari K.

1. Analisi sul campo reale ($K = \mathbb{R}$): Per determinare se esistono sottorappresentazioni proprie, cerchiamo sottospazi stabili di dimensione 1, il che equivale a cercare gli autovalori reali di $\rho(z)$. Il polinomio caratteristico è:

$$p(\lambda) = \det(\rho(z) - \lambda I) = \det \begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1$$

Le radici di $p(\lambda)$ sono $\pm i$, le quali **non appartengono** a $\mathbb{R}$. Non esistendo autovalori reali, non esistono rette in $\mathbb{R}^2$ stabili sotto l'azione della rotazione.

Conclusione: ρ è **irriducibile** su $\mathbb{R}$.

2. Analisi sul campo complesso ($K = \mathbb{C}$): Se estendiamo lo spazio vettoriale a $V_{\mathbb{C}} = \mathbb{C}^2$, gli autovalori $\lambda_1 = i$ e $\lambda_2 = -i$ sono ora ammissibili. Ad essi corrispondono i rispettivi autospazi (sottospazi di dimensione 1):

$$V_i = \operatorname{span}_{\mathbb{C}} \left\{ \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}, \quad V_{-i} = \operatorname{span}_{\mathbb{C}} \left\{ \begin{pmatrix} 1 \\ i \end{pmatrix} \right\}$$

Questi sottospazi sono G-invarianti, poiché l'azione di z (e delle sue potenze) si limita a moltiplicare i vettori per uno scalare ($\pm i$). Lo spazio si decompone nella somma diretta:

$$V_{\mathbb{C}} = V_i \oplus V_{-i}$$

Conclusione: ρ è **riducibile** su $\mathbb{C}$.

Note:

Osservazioni sulla Riducibilità:

- Una rappresentazione di dimensione 1 è sempre irriducibile per motivi dimensionali (non esistono sottospazi propri non nulli).
- Il concetto di irriducibilità dipende dal campo K (come visto nell'esempio delle rotazioni su $\mathbb{R}$ vs $\mathbb{C}$).
- Scomporre una rappresentazione riducibile in somma diretta di irriducibili è l'obiettivo principale del corso (completabilità garantita dal Teorema di Maschke).

Example 2.1.4 (Rappresentazione Naturale di S_3)

Sia $G = S_3$ agente su $V = \mathbb{R}^3$ tramite permutazione delle coordinate:

$$\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

Questa rappresentazione è **riducibile** in quanto ammette i seguenti sottospazi G-invarianti propri:

1. $U = \{(t,t,t) \mid t \in \mathbb{R}\}$, sottospazio di dimensione 1 (retta diagonale). Poiché ogni permutazione scambia coordinate identiche, U è puntualmente fisso.
2. $W = \{(x_1,x_2,x_3) \in \mathbb{R}^3 \mid x_1+x_2+x_3 = 0\}$, sottospazio di dimensione 2 (piano iperortogonale a U). Poiché la somma è commutativa, permutare gli addendi non cambia il risultato zero.

Si verifica facilmente che $U \cap W = \{0\}$, pertanto lo spazio si decompone nella somma diretta:

$$V = U \oplus W$$

Dove U è la rappresentazione banale e W è la **rappresentazione standard** di S_3. Entrambe sono irriducibili.

Definition 2.1.6: Rappresentazione Indecomponibile

Una rappresentazione (ρ, V) si dice **indecomponibile** se non può essere scritta come somma diretta di due sottorappresentazioni proprie non banali. Ovvero, se $V = U \oplus W$ con U, W sottorappresentazioni, allora necessariamente $U = 0$ oppure $W = 0$.

Note:

Irriducibile vs Indecomponibile:

- Ogni rappresentazione **irriducibile** è banalmente **indecomponibile** (se non ha sottospazi stabili, a maggior ragione non può essere somma diretta di sottospazi stabili).
- Il viceversa non è sempre vero: esistono rappresentazioni che possiedono sottospazi stabili (sono riducibili) ma che non ammettono un complemento stabile (sono indecomponibili).
- **Nel Modulo 2:** Grazie al Teorema di Maschke, lavorando su un campo di caratteristica 0 (come $\mathbb{C}$) e con gruppi finiti, ogni sottorappresentazione ammette un complemento stabile. Di conseguenza, in questo contesto i concetti di irriducibile e indecomponibile **coincidono**.

Example 2.1.5 (Blocco di Jordan)

Sia $G = (\mathbb{Z}, +)$, $V = \mathbb{C}^2$, e definiamo

$$\rho : \mathbb{Z} \longrightarrow \mathrm{GL}(\mathbb{C}^2), \qquad n \longmapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Questo è un omomorfismo perché $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$.

Il sottospazio $U = \langle e_1 \rangle = \langle (1,0) \rangle$ è una sottorappresentazione propria (poiché $\rho(n)e_1 = e_1 \in U$ per ogni n), quindi V *non è irriducibile.*

Tuttavia, notiamo che per ogni (x,y) con $y \neq 0$:

$$\rho(n)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+ny \\ y \end{pmatrix}$$

che è linearmente indipendente da (x,y) per n generico. Quindi **non esiste** alcun $W \subseteq V$ con $V = U \oplus W$ stabile, e la rappresentazione è **indecomponibile**.

Questo è il tipico blocco di Jordan di dimensione 2. La situazione si verifica perché $G = \mathbb{Z}$ è un gruppo infinito. Vedremo che per gruppi **finiti** con $\mathrm{char}(K) = 0$ la situazione è radicalmente diversa.

2.1.2 Teorema di Maschke

Per procedere serve costruire un prodotto scalare G-invariante:
Costruzione: Sia (ρ, V) una rappresentazione di un gruppo finito G su uno spazio vettoriale complesso V ($K = \mathbb{C}$). Dato un prodotto hermitiano arbitrario $(\cdot,\cdot)$ su V, definiamo:

$$\langle v, u\rangle_G := \frac{1}{|G|}\sum_{g\in G}(\rho(g)v, \rho(g)u)$$

per ogni $v, u \in V$.
Si tratta della media sui trasformati di (v, u) lungo tutto il gruppo. Il fatto che G sia finito e $\mathrm{char}(K) = 0$ (quindi $|G| \neq 0$ in K) garantisce che la divisione abbia senso.

Proposition 2.1.1 Esistenza di un Prodotto Hermitiano G-invariante

Sia (ρ, V) una rappresentazione di un gruppo finito G su uno spazio vettoriale complesso V. Esiste sempre su V un prodotto hermitiano $\langle\cdot,\cdot\rangle_G$ che sia G-invariante, ovvero tale che:

$$\langle\rho(g)v, \rho(g)u\rangle_G = \langle v, u\rangle_G \quad \forall g \in G, \forall v, u \in V$$

Dimostrazione: Sia $H(v, u)$ un prodotto hermitiano arbitrario su V (la cui esistenza è garantita dalla struttura di spazio vettoriale complesso). Consideriamo il prodotto scalare definito prima:

$$\langle v, u\rangle_G := \frac{1}{|G|}\sum_{x\in G}(\rho(x)v, \rho(x)u)$$

Per verificare l'invarianza, applichiamo un elemento generico $h \in G$:

$$\langle\rho(h)v, \rho(h)u\rangle_G = \frac{1}{|G|}\sum_{x\in G}(\rho(x)\rho(h)v, \rho(x)\rho(h)u)$$

Poiché ρ è un omomorfismo, $\rho(x)\rho(h) = \rho(xh)$. Sostituendo:

$$\langle\rho(h)v, \rho(h)u\rangle_G = \frac{1}{|G|}\sum_{x\in G}(\rho(xh)v, \rho(xh)u)$$

Al variare di x in G, l'elemento xh percorre tutti gli elementi del gruppo esattamente una volta (la traslazione a destra è una permutazione di G). Possiamo quindi effettuare il cambio di variabile $k = xh$, ottenendo:

$$\langle\rho(h)v, \rho(h)u\rangle_G = \frac{1}{|G|}\sum_{k\in G}(\rho(k)v, \rho(k)u) = \langle v, u\rangle_G$$

Questo dimostra che il prodotto è G-invariante. Le proprietà di linearità, simmetria hermitiana e positività di $\langle\cdot,\cdot\rangle_G$ discendono direttamente dalle proprietà del prodotto hermitiano costruito prima.

Theorem 2.1.1 Teorema di Maschke (Versione Sintetica)

Sia G un gruppo finito e (ρ, V) una rappresentazione di G su un campo K (con $\mathrm{char}(K) \nmid |G|$). Allora ogni sottorappresentazione $U \subseteq V$ ammette un complemento G-invariante W, tale che

$$V = U \oplus W$$

Corollary 2.1.1

Per G finito e $\mathrm{char}(K) = 0$: indecomponibile $\iff$ irriducibile.

Dimostrazione: Data una sottorappresentazione $U \subseteq V$, prendiamo il complemento ortogonale rispetto al prodotto G-invariante costruito prima:

$$U^\perp = \{v \in V \mid \langle v, u\rangle = 0 \ \forall\, u \in U\}.$$

Allora $V = U \oplus U^\perp$ come spazi vettoriali (proprietà standard dei prodotti hermitiani). È sufficiente mostrare che $U^\perp$ è G-stabile. Siano $v \in U^\perp$ e $u \in U$:

$$\langle \rho(g)v,\, u\rangle = \langle \rho(g)^{-1}\rho(g)v,\, \rho(g)^{-1}u\rangle = \langle v,\, \rho(g)^{-1}u\rangle = 0$$

dove l'ultimo passaggio usa che $\rho(g)^{-1}u \in U$ (perché U è G-stabile) e $v \in U^\perp$.

2.2 Algebra di Gruppo

Vogliamo ora riformulare tutta la teoria in un linguaggio più algebrico: guardare gli elementi di G come "scalari che agiscono su V".

Definition 2.2.1: A-modulo sinistro

Sia A un anello con unità 1_A e $(V, +)$ un gruppo abeliano. V è un A-modulo sinistro se esiste un'operazione $A \times V \to V$ tale che:

- $a(v + u) = av + au$
- $(a + b)v = av + bv$
- $(ab)v = a(bv)$
- $1_A \cdot v = v$

Questa è esattamente la definizione di spazio vettoriale, ma con A anello al posto di campo.

Definition 2.2.2: Algebra di gruppo

L'**algebra di gruppo** $K[G]$ è l'insieme delle combinazioni lineari formali degli elementi di G a coefficienti in K:

$$K[G] = \left\{ \sum_{g \in G} a_g \cdot g \;\middle|\; a_g \in K \right\}.$$

Gli elementi di G formano una K-base di $K[G]$. Il prodotto in $K[G]$ è definito estendendo per bilinearità il prodotto in G:

$$(a_{g_1} \cdot g_1)(a_{g_2} \cdot g_2) := (a_{g_1} \cdot a_{g_2}) \cdot (g_1 g_2)$$

dove il primo prodotto è in K e il secondo è in G. Questo rende $K[G]$ un **anello** (non commutativo in generale).

Proposition 2.2.1 $K[G]$-modulo sinistro come rappresentazione di G

Le seguenti condizioni sono equivalenti:

1. V è una rappresentazione di G (cioè esiste $\rho : G \to \mathrm{GL}(V)$).
2. V è un $K[G]$-modulo sinistro.

Dimostrazione: (2) $\Rightarrow$ (1): l'inclusione $G \hookrightarrow K[G]$ (ogni g è un elemento di base) restringe l'azione di $K[G]$ su V a un'azione di G per isomorfismi lineari, cioè fornisce $\rho : G \to \mathrm{GL}(V)$.
(1) $\Rightarrow$ (2): si estende l'azione per K-linearità:

$$\left(\sum_{g\in G} a_g \cdot g\right) \cdot v := \sum_{g\in G} a_g \cdot \rho(g)(v)$$

e si verifica che questo soddisfa gli assiomi di modulo.