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 $G \times G \longrightarrow G$ (chiusa su G)

Che soddsfa gli assiomi:

- Associativita'
- Esistenza dell'elemento *neutro*
- Esistenza dell'*inverso* 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*.

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

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**.

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: $\chi(x) = \chi(gxg^{-1})$.
- **Legame con la Normalità:** Un sottogruppo N è normale ($N \trianglelefteq G$) se e solo se è un'unione di classi di coniugio, ovvero se è "chiuso" rispetto all'operazione di coniugio.

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 e Gruppi Lineari Generali

Definition 1.1.6: Il Gruppo Simmetrico $Sym(V)$

Sia V uno spazio vettoriale (considerato qui come un semplice insieme di punti). Il **Gruppo Simmetrico** di V, denotato con $Sym(V)$ o $\text{Perm}(V)$, è l'insieme di tutte le funzioni biunivoche (permutazioni) $f : V \to V$. Sotto l'operazione di composizione di funzioni, $Sym(V)$ forma un gruppo.

Definition 1.1.7: Il Gruppo Lineare Generale

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 $f : V \to V$).
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 in 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.

1.1.4 Gruppi Ciclici

Definition 1.1.8: 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:

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

Definition 1.1.9: Classi di Coniugio di Gruppi Simmetrici

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.

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:
  - $(1, 1, 1) \longrightarrow$ Identità (cicli di lunghezza 1).
  - $(2, 1) \longrightarrow$ Trasposizioni $\{(12), (13), (23)\}$.
  - $(3) \longrightarrow$ 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.

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.

1.1.5 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.

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.

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' $1 + \ldots + 1 = 0$). 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”).

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).

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, $\mathrm{char}(K)$, 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 $\{1, i\}$).

1.5 Omomorfismi, Isomorfismi e Automorfismi

1. Omomorfismo di Gruppi

Siano $(G, \cdot)$ e $(H, *)$ due gruppi. Una funzione $\phi : G \to H$ si dice **omomorfismo** se preserva l'operazione di gruppo, ovvero se:

$$\phi(x \cdot y) = \phi(x) * \phi(y) \quad \forall x, y \in G$$

Da questa definizione derivano due proprietà strutturali fondamentali:

- $\phi(e_G) = e_H$ (l'elemento neutro viene mappato nell'elemento neutro).
- $\phi(x^{-1}) = [\phi(x)]^{-1}$ (l'inverso viene mappato nell'inverso).

Strutture associate a un omomorfismo:

- **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:** $\mathrm{Im}(\phi) = \{\phi(x) \mid x \in G\}$. L'immagine rappresenta la porzione del codominio effettivamente raggiunta ed è sempre un sottogruppo di H ($\mathrm{Im}(\phi) \leq H$).

2. Isomorfismo

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

- **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.

3. Automorfismo

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

- 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 $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

L'Omomorfismo Determinante

Definizione

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.

La Proprietà di Omomorfismo

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!

Collegamento con la Teoria delle Rappresentazioni

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**.

Chapter 2

Fondamenti della Teoria delle Rappresentazioni

2.1 Struttura algebrica

Cosa vuol dire combinatoria algebrica?
Vuol dire studiare strutture algebriche (gruppi, anelli, campi, etc.) attraverso la combinatoria.

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.

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 $\rho : G \to GL(V)$ tale che $\rho(g)\rho(h) = \rho(gh)$ per ogni $g, h \in G$.

Note:

In altre parole è un'azione (omomorfismo è un $G \to$) di G su V con immagine $GL(V)$ tramite isomorfismi

Definition 2.1.3

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

Note:

Ovvero il nucleo di ρ contiene solo l'elemento neutro ($ker(\rho) = \{e\}$)

Definition 2.1.4

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 $\rho_{|U} : G \longrightarrow GL(U)$ è l'omomorfismo che mappa $g \longrightarrow \rho(g)_{|U}$

Example 2.1.2

$$G = \langle r | r^4 = i \rangle$$

Può essere rappresentato tramite rotazione di $V = R^2$. Ovvero $\rho(r) = \begin{pmatrix} \cos(\frac{\pi}{2}) & -\sin(\frac{\pi}{2}) \\ \sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2}) \end{pmatrix}$ ha sottorappresentazioni proprie?

Definition 2.1.5: R

Una rappresenrazione è riducibile se ammette una sottorappresentazione propria (ovvero $U \neq \{0\}$ e $U \neq V$)

Example 2.1.3
Sia G il gruppo simmetrico $G = S_3, V = K^3$ rappresentazione matriciale. $\sigma \in S_3, (x_1, x_2, x_3) \in K^3$

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

Ad esempio

$$\rho((123))(7, -4, 5/2) = (-4, 5/2, 7)$$

Example 2.1.4 (Esercizio)
Consideriamo i sottospazi $U = \{(t, t, t), t \in K\}$ e $W = \{(x_1, x_2, x_3), \in V | x_1 + x_2 + x_3 = 0\}$, mostrare che U e W sono sottorappresentazioni riducibili di ρ

Sol: $V = U \oplus W$

Definition 2.1.6

Una rappresentazione si dice indecomponibile se, ogni volta che $V = U \oplus W$ allora U e W sono sottorappresentazioni, abbiamo $U = V$ e $W = \{0\}$ o viceversa

Proposition 2.1.1
Chiaramente irriducibile $\implies$ indecomponibile

Note:
vale il viceversa? in generale n perché potrebbe esserci un completamentare

Example 2.1.5

$V = C^2$ $(Z, +)$

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

è un omomorfismo perché

$$\rho(n)\rho(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \rho(n+m)$$

Note:

$$e_i = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Lenma 2.1.1

Sia G un gruppo finito. E sia V una sottorappresentazione (su C) allora ogni sottorappresentazione $U \subseteq V$ ammette un complementare $W \subseteq V$ tale che $V = U \oplus W$ e W è una sottorappresentazione. Quindi indecomponibile $\implies$ irriducibile

Dimostrazione: Data una sottorappresentazione $U \subseteq V$ consideriamo $U^\perp = \{v \in V | \langle v, u \rangle = 0 \forall u \in U\}$, dove $\langle \cdot, \cdot \rangle$ è un prodotto scalare hermitiano su V (quello G inviariante), chiaramente $V = U \oplus U^\perp$ e $U^\perp$ è una sottorappresentazione perché $\forall v \in U^\perp, \forall g \in G, \forall u \in U$ abbiamo $\langle \rho(g)v, u \rangle = \langle v, \rho(g^{-1})u \rangle = 0$ perché $u \in U$ e $\rho(g^{-1})u \in U$

Definition 2.1.7

A anello con $1_A, (V, +)$ gruppo abeliano, è un A-modulo sinistro se $A \times V \to V$ tale che :

- $(a+b)v = av + bv$
- $a(v+w) = av + aw$
- $a(bv) = (ab)v$
- $1_A v = v$

Definition 2.1.8: $K[G]$

Combinazioni linerari formali di elementi di G con coefficienti in $K = \left\{\sum_{g\in G} a_g e_g | a_g \in K, supp(a_g) < \infty\right\}$ con prodotto a_g, e_g