Strutture algebriche

Andrea Canale

December 14, 2024

Contents

1 Strutture algebriche

Una struttura algebrica è un insieme sul quale sono definite delle operazioni binarie(noi ne tratteremo solo una).

Una struttura algebrica può essere di tre tipi:

- Semigruppo se l'operazione è associativa
- Monoide se l'operazione è associativa ed esiste un elemento neutro
- Gruppo se l'operazione è associativa, esiste elemento neutro ed esiste un inverso y tale che $x \cdot y = y \cdot x = e$

Se l'operazione commuta, la struttura si dice commutativa o abeliana(solo nel caso di gruppi).

L'operazione deve essere ben definita per tutti gli elementi della struttura algebrica(il dominio e il codominio devono coincidere con l'insieme nella struttura)

Un sottoinsieme $Y \subset X$ si dice stabile o chiuso rispetto a $*$ se $\forall a, b \in Y$, $a * b \in Y$

2 Strutture algebriche note

2.1 Strutture algebriche su numeri

- $(\mathbb{N}\backslash 0, +)$ È un semigruppo commutativo. La somma è associativa ma manca l'elemento neutro. La somma è commutativa
- $(\mathbb{N}, +)$ È un monoide commutativo. Infatti manca l'inverso
- $(\mathbb{Z}, +)$ È un gruppo abeliano. Esiste l'opposto.
- $(\mathbb{Z}_n, +)$ È un gruppo abeliano.
- $(\mathbb{Z}_n, \cdot)$ È un monoide commutativo. Non sempre esiste l'inverso

Strutture algebriche su insiemi Sia $Y \neq \emptyset, X = P(Y)$

La struttura $(X, \cup)$

- È associativa
- Ha elemento neutro $\emptyset$
- Non ha un inverso

La struttura $(X, \cap)$

- È associativa
- Ha elemento neutro Y
- Non ha un inverso

Sono entrambi dei monoidi commutativi

2.2 Monoide delle parole(o monoide libero su A)

A partire da un alfabeto(insieme non vuoto. $P = \{$stringhe finite su A$\}$
Definiamo su P l'operazione di concatenazione di parole: $x_1, ..., x_n * y_1, ..., y_n = x_1, ..., (x_n y)_1, ..., y_n$
$(P, *)$ È una struttura algebrica:

- È associativa
- Ha elemento neutro λ
- Non ha un inverso

Concludiamo che è un monoide non commutativo.

2.3 Gruppo delle permutazioni su X

Dato il gruppo delle funzioni biettive su $X : X = f \in f(x)|$f biettiva) È un gruppo non abeliano. È anche chiamato gruppo simmetrico su X. Notiamo che è l'insieme delle permutazione su X.

2.4 Gruppo delle matrici quadrate

Dato l'insieme $X = a \in M(n, K)|deta \neq 0)$, è detto gruppo lineare di ordine n a coefficienti in K. È un gruppo non commutativo se $n \geq 2$.

3 Notazione moltiplicativa e additiva

La notazione moltiplicativa si usa per gruppi del tipo $(G, *)$:

- $a * b = ab$
- $a^n = a \cdot a \cdot ... \cdot a$

- a^{-1} è l'inverso di a

La notazione additiva si usa per gruppi del tipo $(G, +)$:

- $a * b = a + b$
- $na = a + a + ... + a$
- $-a$ è l'inverso di a

4 Gruppi

4.1 Proprietà di un gruppo

Dato un gruppo G, valgono le seguenti proprietà:

- L'elemento neutro è unico
- L'inverso di un elemento è unico
- $(x * y)^{-1} = y^{-1} \cdot x^{-1}$
- Valgono le leggi di cancellazione destra e sinistra: $x * y = x * z$ si può semplificare $y = z$

Se G è finito, la sua cardinalità si dice ordine di G

4.2 Prodotto diretto tra gruppi

Dati due gruppi G_1 e G_2 possiamo costruire il prodotto scalare tra due gruppi e definirlo come prodotto diretto tra gruppi:

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

Dove $(a_1, b_1) \in G_1$ e $(a_2, b_2) \in G_2$

Il risultato di G_1 x G_2 sarà anch'esso un gruppo. Inoltre, il prodotto diretto tra gruppi abeliani è anch'esso abeliano.

Notiamo che $G^N = G$ x G x G ...

5 Sottogruppi

Dato un gruppo $(G, *)$, un sottogruppo H di G è un sottoinsieme di G tale che $(H, *)$ è un gruppo. Viene indicato come: $H \leq G$

Un sottogruppo deve rispettare tre proprietà:

- H stabile rispetto a $*$

- H ha lo stesso elemento neutro di G
- H contiene l'inverso di ogni suo elemento e coincide con quello di G

Notiamo che un gruppo G ha sempre almeno due sottogruppi detti sottogruppi banali: G e $\{e\}$

Inoltre l'intersezione tra sottogruppi è un sottogruppo tale che $H_1, H_2 \leq G$, allora $H_1 \cap H_2 \leq G$

5.0.1 Sottogruppi di $\mathbb{Z}$

Tutti i sottogruppi di $\mathbb{Z}$ sono del tipo $N\mathbb{Z}$ per qualche $N \in \mathbb{N}$

Inoltre: $N\mathbb{Z} \cap M\mathbb{Z} = m\mathbb{Z}$ dove $m = mcm(N, M)$

5.1 Laterali

Dato un gruppo G e un suo sottogruppo $H \leq G$, definiamo le relazioni:

- $X \sim_1 Y$ Se $xy^{-1} \in H$
- $X \sim_2 Y$ Se $y^{-1}x \in H$

Queste due relazioni sono relazioni di equivalenza su G.

Sia G un gruppo e $H \leq G$. Dato un elemento $g \in G$ detto **rappresentante del laterale** si dice:

- Laterale sinistro di H il sottoinsieme: $gH = \{gh | h \in H\} \subset G$
- Laterale destro di H il sottoinsieme: $Hg = \{hg | h \in H\} \subset G$

Esempio:
$G = S_3 = \{(1), (1\ 2).(1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ $H = \{(1), (1\ 2)\}$
I laterali destri saranno della forma:
$H(1) = \{(1), (1\ 2)\} = H(1\ 2)$
$H(1\ 3) = \{(1)(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\} = H(1\ 3\ 2)$
E così via...
Per i laterali sinistri vale la stessa regola ma si inverte la moltiplicazione
$(1)H = \{(1), (1\ 2)\} = (1\ 2)H$
$(1\ 3)H = \{(1\ 3)(1), (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$
Se G è commutatitivo i laterali destri e sinistri coincidono.

Valgono queste proprietà per i laterali destri e sinistri:

- La funzione $\theta : H \to Hx$ che manda $h \to hx$(e il suo analogo sinistro) è biettiva
- Se G è finito, tutti i laterali destri e sinistri hanno la stessa cardinalità.

5.2 Teorema di Lagrange

Sia G un gruppo finito e $H \leq G$. L'ordine di H divide l'ordine di G.

Notiamo che il teorema di Lagrange non si inverte tranne per i gruppi abeliani.

6 Omomorfismi

Siano $(G_1, *_1)$ e $(G_2, *_2)$ gruppi, una funzione $f : G_1 \to G_2$ si dice omomorfismo se:

$$f(x *_1 y) = f(x) *_2 f(y)$$

6.1 Omomorfismi ben definiti

Un omomorfismo deve essere ben definito, ad esempio:

$f : \mathbb{Z}_8 \to \mathbb{Z}_{12}$

Se prendiamo $[1]_8 = [9]_8$, allora $f(1) = f(9)$

Quindi deve mantenere le proprietà del gruppo

In generale se $a = b$ allora $f(a) = f(b)$

6.2 Proprietà degli omomorfismi

Dato un omomorfismo $f : G_1 \to G_2$, valgono le seguenti proprietà:

- $f(eG_1) = eG_2$
- $f(x^{-1}) = f(x)^{-1}\ \forall x \in G_1$
- $f(x^n) = f(x)^n$
- Dato un sottogruppo H di G_1, allora $f(H) \leq G_2$ dove $f(H)$ è la funzione applicata su tutti gli elementi di H
- Dato un sottogruppo H di G_2, allora $f^{-1}(H) \leq G_1$

Se non valgono queste proprietà, la funzione non è omomorfismo.

6.3 Immagini e Nucleo

Dato un omomorfismo $f : G_1 \to G_2$:

L'insieme definito da $f(G_1)$ è detto immagini della funzione ed è denotato come $im(f)$

L'insieme definito come $\{x \in G_1 | f(x) = eG_2\}$ è detto nucleo ed è denotato come $ker(f)$

Un omomorfismo f è iniettivo, se e solo se, $ker(f) = \{eG_1\}$

6.4 Classificazione di omomorfismi

- **Monomorfismo** se è un omomorfismo iniettivo
- **Epimorfismo** se è suriettivo
- **Isomorfismo** se è biettivo
- **Endomorfismo** se $G_1 = G_2$(cioè f agisce sullo stesso gruppo)
- **Automorfismo** se è endomorfismo e monomorfismo

7 Isomorfismi

Due gruppi si dicono isomorfi se esiste un isomorfismo $f : G_1 \to G_2$. Viene indicato come $G_1 \simeq G_2$

Due gruppi isomorfi hanno le stesse proprietà, ad esempio: se G_1 è finito, lo sarà anche G_2 oppure se G_1 è abeliano lo è anche G_2, ecc...

8 Gruppi ciclici

Sia $(G_1, *)$ un gruppo, possiamo facilmente costruire sottogruppi di G_1 a partire da un elemento $g \in G_1$, definiamo un sottogruppo ciclico generato da x come:

$$<x> = \{g^n \in G_1 | n \in \mathbb{N}\}$$

Notiamo che questa notazione vale per gruppi scritti come notazione moltiplicativa, per gruppi in notazione additiva abbiamo:

$$<x> = \{ng \in G_1 | n \in \mathbb{N}\}$$

Se esiste un elemento x per il quale $<x> = G_1$, il gruppo G_1 si dice ciclico e x è il generatore di G_1

Notiamo inoltre che se G è un gruppo ciclico, allora G è abeliano. Da ciò ne ricaviamo che qualsiasi gruppo non abeliano sicuramente non è ciclico. Tuttavia non tutti i gruppi abeliani sono ciclici.

Osserviamo anche che il prodotto di gruppi ciclici non è necessariamente un gruppo ciclico.

8.1 Generatori di $\mathbb{Z}_N$

I generatori del gruppo Z_N coincidono con gli elementi invertibili $\mathbb{Z}_N^*$

8.2 Gruppi finiti di ordine primo

Se l'ordine di un gruppo $|G| = p$ è un numero primo e il gruppo è generato da x, per il teorema di Lagrange $|<x>| = d$ divide p, tuttavia ciò è possibile solo se $d = 1$ o $d = p$. Se noi imponiamo $x \neq e$ otteniamo che l'unica possibilità è $d = p$.

Quindi se G ha un ordine primo, allora è generato da qualsiasi $x \neq e$. Concludiamo che G è un gruppo ciclico generato da qualsiasi suo elemento $\neq e$

Per quello che abbiamo detto prima, tutti i gruppi di ordine primo sono abeliani.

8.3 Teorema di classificazione di gruppi ciclici

Se G è un gruppo ciclico, allora:

- Se G è infinito, allora G è isomorfo a $\mathbb{Z}$
- Se G è finito con ordine $|G| = n$, allora $G \simeq \mathbb{Z}_N$

8.4 Periodo di un gruppo ciclico

Dato un gruppo G ciclico e un elemento(anche non generatore) $x \in G$, definiamo il suo periodo come:

$$per(x) = |<x>|$$

Osserviamo che in generale, se $|<x>|$ ha periodo finito, allora il periodo è il minimo numero n tale per cui $x^n = e$.

Inoltre per il teorema di Lagrange, se $per(x)$ divide l'ordine di G

Ciò ci viene utile per risolvere potenze molto alte: poniamo $|G| = per(x) \cdot k$. Per risolvere x^n possiamo scrivere $x^{d \cdot k} = (x^d)^k$. Tuttavia $x^d = e$ quindi $x^n = e$.

Questo perchè: **Ogni elemento di un gruppo finito elevato all'ordine del gruppo dà l'elemento neutro**

Inoltre, l'unico elemento con periodo 1 è l'elemento neutro

Questo ha un applicazione particolare per il calcolo di potenze $\mathbb{Z}_N^*$.

Dato che in $\mathbb{Z}_N^*$, $|\mathbb{Z}_N^*| = \varphi(N)$, Otteniamo che $\overline{a}^{\varphi(N)} = \overline{1}$ se $(a, N) = 1$

8.5 Piccolo teorema di Fermat

Nel caso particolare in cui il modulo N sia un numero primo, si ha il piccolo teorema di Fermat:

$$p \nmid a \text{ allora } a^{p-1} \equiv 1 mod p$$

8.6 Criteri di ciclicità di prodotti ciclici

Dato due gruppi ciclici G_1 e G_2, $G_1\ x\ G_2$ è ciclico, se e solo se gli ordini di G_1 e G_2 sono coprimi. Notiamo che $|G_1\ x\ G_2| = |G_1| \cdot |G_2|$