Azzolini Riccardo 2018-10-26

Classi di resto e strutture algebriche

1 Classi di resto e insieme degli interi modulo m

Dato un intero $m \in \mathbb{N}^+$ maggiore di 1, la relazione binaria $m\mathbb{Z}$ su $\mathbb{Z}$ è una relazione di equivalenza, nella quale due elementi $x, y \in \mathbb{Z}$ sono in relazione, cioè $x(m\mathbb{Z})y$

- se $x - y$ è un multiplo di m
- equivalentemente, se x e y hanno lo stesso resto quando divisi per m

Questa relazione si dice **congruenza modulo m**. Essa ha m classi di equivalenza, che si indicano con $[x]_m$ e prendono il nome di **classi di resto**. L'insieme quoziente $\mathbb{Z}/m\mathbb{Z}$, cioè l'insieme di tutte le classi di resto modulo m, è chiamato **insieme degli interi modulo m** e si denota con $\mathbb{Z}_m$.

1.1 Esempio

$$m = 4$$

$$4(4\mathbb{Z})0 \quad 5(4\mathbb{Z})1 \quad 6(4\mathbb{Z})2$$
$$9(4\mathbb{Z})1 \text{ perché } 9 = 4 \cdot 2 + \mathbf{1} \text{ e } 1 = 4 \cdot 0 + \mathbf{1}$$

$$[0]_4 = \{0, 4, 8, 12, 16, ...\}$$
$$[1]_4 = \{1, 5, 9, 13, 17, ...\}$$
$$[2]_4 = \{2, 6, 10, 14, 18, ...\}$$
$$[3]_4 = \{3, 7, 11, 15, 19, ...\}$$
$$[4]_4 = [0]_4 \quad [5]_4 = [1]_4 \quad ...$$

$$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

1.2 Somma su $\mathbb{Z}_m$

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$$
$$[x]_m + [y]_m = [x + y]_m$$

Proprietà:

- commutativa
- associativa
- $[0]_m$ è l'elemento neutro
- ogni elemento $[x]_m$ è invertibile e il suo inverso è $[-x]_m$

1.2.1 Esempio

$$m = 4$$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

- L'inverso di $[0]_4$ (elemento neutro) è $[0]_4$.
- L'inverso di $[1]_4$ è $[3]_4$ (e viceversa).
- L'inverso di $[2]_4$ è $[2]_4$.

1.3 Prodotto su Z_m

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$$
$$[x]_m \cdot [y]_m = [x \cdot y]_m$$

Proprietà:

- commutativa
- associativa
- $[1]_m$ è l'elemento neutro

- $[x]_m$ è invertibile se e solo se $\text{MCD}(x, m) = 1$, quindi in particolare:
  - $[0]_m$ non è invertibile (indipendentemente da m) perché $\text{MCD}(0, m) = m > 1$
  - se m è primo, tutti gli elementi di $Z_m \setminus \{[0]_m\}$ sono invertibili

1.3.1 Esempi

$$m = 3$$

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

- $[0]_3$ non è invertibile.
- L'inverso di $[1]_3$ (elemento neutro) è $[1]_3$.
- L'inverso di $[2]_3$ è $[2]_3$.

$$m = 4$$

$\cdot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

- $[0]_4$ non è invertibile.
- L'inverso di $[1]_4$ (elemento neutro) è $[1]_4$.
- $[2]_4$ non è invertibile perché $\text{MCD}(2, 4) = 2 \neq 1$
- L'inverso di $[3]_4$ è $[3]_4$.

2 Semigruppi, monoidi e gruppi

Una struttura algebrica $(A, *)$ è

- un **semigruppo** se $*$ è associativa
- un **monoide** se è un semigruppo ed esiste l'elemento neutro
- un **gruppo** se è un monoide e ogni elemento di A è invertibile

Ciascuna di queste strutture può inoltre essere **commutativa** se l'operazione $*$ è commutativa.

2.1 Esempi su insiemi numerici

- $(\mathbb{N}, +)$ è un monoide e 0 è l'elemento neutro
- $(\mathbb{N}^+, +)$ è un semigruppo (dove $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$)
- $(\mathbb{Z}, +)$ è un gruppo commutativo detto *gruppo degli interi*:
  - 0 è l'elemento neutro
  - ogni $n \in \mathbb{Z}$ è invertibile e il suo inverso è $-n$: $n + (-n) = 0$
- $(\mathbb{Q}, \cdot)$ è un monoide commutativo, ma non un gruppo:
  - 1 è l'elemento neutro
  - ogni elemento $r \neq 0$ è invertibile ($r \cdot \frac{1}{r} = 1$), ma 0 non lo è
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo commutativo
- $(\mathbb{Z}_m, +)$ è un gruppo commutativo:
  - $[0]_m$ è l'elemento neutro
  - ogni $[x]_m \in \mathbb{Z}_m$ è invertibile: $[x]_m + [-x]_m = [0]_m$
- Se m è primo allora $(\mathbb{Z}_m \setminus \{[0]_m\}, \cdot)$ è un gruppo commutativo:
  - $[1]_m$ è l'elemento neutro
  - tutti gli elementi sono invertibili

2.2 Esempio: concatenazione di parole

Dato l'insieme delle parole A^+ su un alfabeto A, è possibile definire l'operazione di **concatenazione**, che corrisponde a scrivere due parole una dopo l'altra:

$$\circ : (u, v) \in A^+ \times A^+ \mapsto uv \in A^+$$

Esempio:

$$u = ab \quad v = bca$$
$$u \circ v = abbca$$
$$v \circ u = bcaab$$

La struttura $(A^+, \circ)$ è un semigruppo:

- $\circ$ è associativa (ma non commutativa)
- non esiste un elemento neutro
- nessun elemento è invertibile

È possibile aggiungere all'insieme delle parole la **parola vuota** ε:

$$\#\varepsilon = 0$$
$$u \circ \varepsilon = u = \varepsilon \circ u$$

L'insieme delle parole che comprende anche quella vuota si denota con A^*:

$$A^* = A^+ \cup \{\varepsilon\}$$

La struttura $(A^*, \circ)$ è un monoide chiamato *monoide delle parole*:

- ε è l'elemento neutro
- solo ε è invertibile, quindi non è un gruppo

2.3 Esempio: composizione di funzioni

Con B^A si denota l'insieme delle funzioni da A a B.

In particolare, su A^A si definisce l'operazione di composizione di funzioni:

$$\circ : A^A \times A^A \to A^A$$
$$f : A \to A \qquad g : A \to A \qquad f, g \in A^A$$
$$(f \circ g)(a) = f(g(a)) \qquad f \circ g : A \to A$$
$$(g \circ f)(a) = g(f(a)) \qquad g \circ f : A \to A$$

Quest'operazione ha le seguenti proprietà:

- è associativa, ma non commutativa
- l'elemento neutro è la *funzione identità* (o *identica*) id_A
- $f \in A^A$ è invertibile se e solo se è biettiva (e in tal caso, il suo inverso è f^{-1})

la struttura $(a^a, \circ)$ è quindi un monoide, ma non un gruppo.

Se $\pi(A)$ è l'insieme delle funzioni biettive (o permutazioni) di A in A, $(\pi(A), \circ)$ è un gruppo detto *gruppo delle permutazioni* di A.

3 Anelli e campi

Un **anello** è una struttura algebrica $(S, *, \odot)$ con due operazioni tali che:

- $(S, *)$ è un *gruppo commutativo*
- $(S, \odot)$ è un *monoide*
- vale la proprietà *distributiva* di $\odot$ su $*$:

$$x \odot (y * z) = (x \odot y) * (x \odot z)$$
$$(y * z) \odot x = (y \odot x) * (z \odot x)$$

Un **campo** è un anello dove $(S \setminus \{0\}, \odot)$ è un *gruppo commutativo* (con 0 si indica l'elemento neutro di $*$).

3.1 Esempi

- $(\mathbb{Z}, +, \cdot)$ è un anello detto *anello degli interi*:
  - $(\mathbb{Z}, +)$ è un gruppo commutativo, con elemento neutro 0
  - $(\mathbb{Z}, \cdot)$ è un monoide (commutativo), con elemento neutro 1
  - $x \cdot (y + z) = x \cdot y + x \cdot z$
  - non è un campo perché $(\mathbb{Z} \setminus \{0\}, \cdot)$ non è un gruppo (solo 1 è invertibile)
- $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono campi
  - $(\mathbb{Q} \setminus \{0\}, \cdot)$ e $(\mathbb{R} \setminus \{0\}, \cdot)$ sono gruppi commutativi
- $(\mathbb{C}, +, \cdot)$ è il campo dei complessi
- $(\mathbb{Z}_m, +, \cdot)$ è un anello:
  - $(\mathbb{Z}_m, +)$ è un gruppo commutativo
  - $(\mathbb{Z}_m, \cdot)$ è un monoide, con elemento neutro $[1]_m$
  - se $m = p$, dove p è un numero primo, allora $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ è un gruppo commutativo, quindi $(\mathbb{Z}_p, +, \cdot)$ è un campo

4 Sottoinsieme stabile

Se $(A, *)$ è una struttura algebrica, un sottoinsieme $B \subseteq A$ si dice **stabile** rispetto a $*$ se per ogni $b_1, b_2 \in B$ si ha $b_1 * b_2 \in B$.

4.1 Esempi

Data la struttura $(\mathbb{N}, +)$:

- il sottoinsieme dei numeri pari $2\mathbb{N} \subseteq \mathbb{N}$ è stabile perché se n e m sono pari, allora anche $n + m$ è pari

$$n, m \in 2\mathbb{N} \implies n + m \in 2\mathbb{N}$$

- il sottoinsieme dei numeri dispari $D = \mathbb{N} \setminus 2\mathbb{N}$ non è stabile perché la somma di due numeri dispari è pari

$$n, m \in D \implies n + m \in 2\mathbb{N}$$

Data la struttura $(\mathbb{Z}_4, +)$, il sottoinsieme

$$H = \{[1]_4, [2]_4\}$$

non è stabile perché

$$[1]_4 + [2]_4 = [3]_4 \notin H$$