Logica per l'Informatica

Cenni di algebra universale

Claudio Sacerdoti Coen

<sacerdot@cs.unibo.it>

Universitá di Bologna

02/12/2020

Algebra universale

L'algebra universale studia le costruzioni/teoremi che funzionano su qualunque tipo di struttura algebrica

Vediamo in questi lucidi i primi esempi di teoremi di un corso di algebra universale

Alcune strutture algebriche interessanti

- $(\mathbb{A}, \circ)$ è un semigruppo sse $\circ$ è associativo (con $\circ \in \mathbb{A}^{\mathbb{A}\times\mathbb{A}}$)
- $(\mathbb{A}, \circ, e)$ è un monoide sse è un semigruppo e e è l'elemento neutro di $\circ$
- $(\mathbb{A}, \circ, e, \cdot^{-1})$ è un gruppo sse è un monoide e $\forall x \in \mathbb{A}. \qquad x \circ x^{-1} = e = x^{-1} \circ x$
- $(\mathbb{A}, +, 0, *)$ è un semianello sse $(\mathbb{A}, +, 0)$ è un monoide, $(\mathbb{A}, *)$ è un semigruppo e valgone le proprietà distributiva del $*$ rispetto al $+$, ovvero $\forall x, y. \qquad (x + y) * z = xz + yz = z * (x + y)$, e di assorbimento dello 0 rispetto al $*$, ovvero $\forall x. \qquad x * 0 = 0 = 0 * x$
- ...

In tutti questi casi l'insieme $\mathbb{A}$ si chiama sostegno della struttura.

Strutture algebriche abeliane

Una struttura algebrica con una sola operazione si dice commutativa o abeliana sse l'operazione gode della proprietà commutativa.

Un semianello $(\mathbb{A}, +, 0, *)$ dove $(\mathbb{A}, *)$ è un semigruppo abeliano si chiama semianello abeliano.

$(\mathbb{A}, +, 0, -, *)$ dove $(\mathbb{A}, +, 0, -)$ è un gruppo abeliano e $(\mathbb{A}, +, 0, *)$ un semianello si chiama anello.

Un anello è abeliano sse come semianello è abeliano.

Esempi

1. $(\mathbb{N}, +, 0, -, *)$ è un anello abeliano
2. $(\mathbb{N}, /)$ non è un semigruppo
3. $(\mathbb{N}, \mathit{min})$ è un semigruppo abeliano che non si può estendere a un monoide
4. $(\mathbb{N}, \mathit{max}, 0)$ è un monoide abeliano che non si può estendere a un gruppo
5. $(2^{\mathbb{A}}, \cup, \emptyset, \cap)$ è un semianello abeliano che non si può estendere a un anello
6. $(\mathbb{A}, \circ)$ dove $x \circ y = x$ è un semigruppo non abeliano che non si può estendere a un monoide
7. $(\mathbb{M}, \circ, \mathit{id}, \cdot^{-1})$ dove $\mathbb{M}$ è l'insieme delle mosse di un cubo di Rubrik, $m_1 \circ m_2$ esegue prima m_2 e poi m_1, id è la "mossa" che non fa nulla e m^{-1} è la contro-mossa di m è un gruppo non abeliano

Sottoinsiemi chiusi

Sottoinsieme chiuso

Sia $(A, \circ)$ un semigruppo e $B \subseteq A$. B si dice chiuso rispetto a $\circ$ sse $\forall x, y \in \mathbb{B}.x \circ y \in \mathbb{B}$.

Esempio: l'insieme $\mathbb{P}$ dei numeri pari è chiuso rispetto alla somma, quello dei numeri dispari no.

Sotto-struttura algebrica

Data una struttura algebrica di sostegno A e un $B \subseteq A$, B è una sotto-struttura algebrica della prima sse tutte le operazioni sono chiuse rispetto a B e tutti gli elementi elencati nella struttura appartengono a B.

Esempio: $\mathbb{P}$ è un sottosemigruppo di $(\mathbb{N}, +)$, un sottosemigruppo di $(\mathbb{N}, *)$, un sottomonoide di $(\mathbb{N}, +, 0)$, un sottosemianello di $(\mathbb{N}, +, 0, *)$, ma non è un sottomonoide di $(\mathbb{N}, *, 1)$ perchè $1 \notin \mathbb{P}$.

Intersezione di sottostrutture algebriche

Teorema: data una struttura di cui B, C sono sottostrutture, allora $B \cap C$ lo è anch'essa.
Dimostrazione: tutti gli elementi elencati nella struttura stanno sia in B che in C, e quindi stanno nell'intersezione. Tutte le operazioni $\circ$ elencate nella struttura sono chiuse rispetto a B e C, ovvero $(\forall x, y \in \mathbb{B}.x \circ y \in \mathbb{B}) \wedge (\forall x, y \in \mathbb{C}.x \circ y \in \mathbb{C})$, da cui segue $(\forall x, y \in \mathbb{B} \cap \mathbb{C}.x \circ y \in \mathbb{B} \cap \mathbb{C})$. □

Esempio: $\mathbb{P}$ (i multipli di 2) e $3\mathbb{N}$ (i multipli di 3) sono sottomonoidi di $(\mathbb{N}, +, 0)$. Quindi lo è anche $\mathbb{P} \cap 3\mathbb{N}$, ovvero $6\mathbb{N}$ (i multipli di 6).

Unione di sottostrutture algebriche

L'unione di sottostrutture NON è (in generale) una sottostruttura.

Esempio: $2, 3 \in \mathbb{P} \cup 3\mathbb{N}$, ma $2 + 3 = 5 \notin \mathbb{P} \cup 3\mathbb{N}$.

Ancora sulle sottostrutture algebriche

Teorema: data una struttura algebrica $\mathcal{A}$ e una sua sottostruttura B, si ottiene una nuova struttura algebrica che ha come sostegno B, come elementi quelle di $\mathcal{A}$ e come operazioni quelle di $\mathcal{A}$ il cui dominio e codominio sono ristretti a B.
Dimostrazione: omessa, ma facile □

Esempio: $\mathbb{P}$ è un sottosemianello di $(\mathbb{N}, +, 0, *)$. Sia $+_{\mathbb{P}} := + \cap ((\mathbb{P} \times \mathbb{P}) \times \mathbb{P})$ e $*_{\mathbb{P}} := * \cap ((\mathbb{P} \times \mathbb{P}) \times \mathbb{P})$. Ovvero $x +_{\mathbb{P}} y = x + y$ per $x, y \in \mathbb{P}$, etc. Si ha $(\mathbb{P}, +_{\mathbb{P}}, 0, *_{\mathbb{P}})$ è un sottosemianello.

Pertanto, facendo un poco di confusione, si pensa alle sottostrutture come strutture il cui sostegno sia un sottoinsieme.

Prodotto cartesiano di strutture algebriche

Prodotto cartesiano di strutture algebrica

Date due strutture algebriche $\mathcal{A}$ di carrier $\mathbb{A}$ e $\mathcal{B}$ di carrier $\mathbb{B}$ dello stesso tipo (es. due monoidi, due gruppi, etc.), il loro prodotto cartesiano $\mathcal{A} \times \mathcal{B}$ è la struttura algebrica dello stesso tipo tale che

- il carrier è $\mathcal{A} \times \mathcal{B}$
- gli elementi $e_{\mathcal{A}\times\mathcal{B}}$ richiesti dal tipo di struttura sono coppie $\langle e_{\mathcal{A}}, e_{\mathcal{B}}\rangle$ di elementi corrispondenti nelle due strutture
- le operazioni $\circ_{\mathcal{A}\times\mathcal{B}}$ richiesti dal tipo di struttura agiscono applicando l'operazione corrispondente sugli elementi della coppia: $\langle x_1, y_1\rangle \circ_{\mathcal{A}\times\mathcal{B}} \langle x_2, y_2\rangle = \langle x_1 \circ_{\mathcal{A}} x_2, y_1 \circ_{\mathcal{B}} y_2\rangle$.

Prodotto cartesiano di strutture algebriche

Esempio: $(\mathbb{N}, +, 0)$ e $(\mathbb{Z}, *, 1)$ sono due monoidi abeliani.
Verifichiamo che lo sia anche
$(\mathbb{N}, +, 0) \times (\mathbb{Z}, *, 1) := (\mathbb{N} \times \mathbb{Z}, \circ, \langle 0, 1 \rangle)$ dove
$\langle n_1, z_1 \rangle \circ \langle n_2, z_2 \rangle = \langle n_1 + n_2, z_1 * z_2 \rangle$:

- Proprietà associativa:
$$\begin{aligned}
&(\langle n_1, z_1 \rangle \circ \langle n_2, z_2 \rangle) \circ \langle n_3, z_3 \rangle \\
&= \langle (n_1 + n_2) + n_3, (z_1 * z_2) * z_3 \rangle \\
&= \langle n_1 + (n_2 + n_3), z_1 * (z_2 * z_3) \rangle \\
&= \langle n_1, z_1 \rangle \circ (\langle n_2, z_2 \rangle \circ \langle n_3, z_3 \rangle)
\end{aligned}$$
- Elemento neutro:
$\langle n, z \rangle \circ \langle 0, 1 \rangle = \langle n + 0, z * 1 \rangle = \langle n, z \rangle$
- Proprietà commutativa:

...

Quindi, recapitolando, possiamo costruire nuove istanze di (sotto)strutture algebriche usando intersezioni e prodotti cartesiani.

Un altro meccanismo che ci permette di mettere in relazione strutture algebriche dello stesso tipo e di ottenere nuove (sotto)strutture algebriche sono i morfismi, ovvero le funzioni che rispettano tutte le operazioni delle strutture algebriche.

Morfismi di strutture algebriche

Date due strutture algebriche dello stesso tipo $\mathcal{A}$ di sostegno $\mathbb{A}$ e $\mathcal{B}$ di sostegno $\mathbb{B}$, un morfismo da $\mathcal{A}$ a $\mathcal{B}$ è una funzione $f \in B^A$ t.c.

1. per ogni elemento $e_{\mathcal{A}}$ elencato in $\mathcal{A}$, $f(e_{\mathcal{A}}) = e_{\mathcal{B}}$ (l'elemento corrispondente in $\mathcal{B}$)
2. per ogni operazione $op^n_{\mathcal{A}}$ elencata in $\mathcal{A}$, $\forall x_1, \ldots, x_n. f(op^n_{\mathcal{A}}(x_1, \ldots, x_n)) = op^n_{\mathcal{B}}(f(x_1), \ldots, f(x_n))$

Domini, codomini, immagini

Immagine di una funzione

Siano $\mathbb{A}, \mathbb{B}$ insiemi e $f \in \mathbb{B}^{\mathbb{A}}$.

- $\mathbb{A}$ è il dominio di f, indicata con $Dom(f)$
- $\mathbb{B}$ è il codominio di f, indicata con $Cod(f)$
- $\{y \in \mathbb{B} \mid \exists x \in \mathbb{A}.f(x) = y\}$ è l'immagine di f, indicata con $Imm(f)$

Restrizione di una funzione alla sua immagine

Teorema: per ogni $f \in \mathbb{B}^{\mathbb{A}}$ si ha f vista come elemento di $Imm(f)^{\mathbb{A}}$ è suriettiva.
Dimostrazione: omessa, ma banale □

Esempio: $|\cdot| \in \mathbb{Z}^{\mathbb{Z}}$, $Imm(|\cdot|) = \mathbb{N}$ e $|\cdot|$ è suriettiva su $\mathbb{N}$ ma non su $\mathbb{Z}$.

Immagini di morfismi

Teorema: sia f un morfismo da una struttura algebrica $\mathcal{A}$ a una struttura algebrica $\mathcal{B}$. $Imm(f)$ è una sottostruttura di $\mathcal{B}$.
Dimostrazione (cenni): Consideriamo come esempio il caso di un morfismo di monoidi dove $\mathcal{A} = (\mathbb{A}, \circ, a)$ e $\mathcal{B} = (\mathbb{B}, \bullet, b)$. Dobbiamo dimostrare $Imm(f)$ è una sottostruttura di $\mathcal{B}$, ovvero:

1. Dimostriamo $b \in Imm(f) = \{y \in \mathbb{B} \mid \exists x \in \mathbb{A}.f(x) = y\}$. Per l'assioma di separazione basta dimostrare $\exists x.f(x) = y$. Scelgo a: $f(a) = b$ poichè f è un morfismo.
2. Dimostriamo $\forall y_1, y_2 \in Imm(f) = \{y \in \mathbb{B} \mid \exists x \in \mathbb{A}.f(x) = y\}.y_1 \bullet y_2 \in Imm(f)$. Siano $y_1, y_2 \in Imm(f)$. Per l'assioma di separazione siano x_1 e x_2 t.c. $f(x_1) = y_1$ e $f(x_2) = y_2$. Poichè f è un morfismo si ha $f(x_1 \circ x_2) = f(x_1) \bullet f(x_2) = y_1 \bullet y_2$. Quindi $\exists x.f(x) = y_1 \bullet y_2$ e perciò $y_1 \bullet y_2 \in Imm(f)$. □

Immagini di morfismi

Esempio: $f(n) = 2^n$ è un morfismo da $(\mathbb{N}, +, 0)$ a $(\mathbb{N}, *, 1)$ t.c. $Imm(f)$ è l'insieme di tutte le potenze del 2. Pertanto l'insieme delle potenze del 2 è un sottomonoide di $(\mathbb{N}, *, 1)$.

Funzioni come osservazioni

Una funzione $f \in \mathbb{B}^{\mathbb{A}}$ può essere pensata come un modo per osservare sugli elementi di $\mathbb{A}$ delle proprietà $\mathbb{B}$.

Esempio: la funzione $|\cdot|$ (cardinalità) osserva per ogni insieme quanto sia la sua cardinalità.

Supponiamo che tali osservazioni siano le uniche che ci interessano in un determinato momento.

Pertanto vogliamo astrarre gli elementi di $\mathbb{A}$ mantenendo solamente le loro proprietà osservabili $\mathbb{B}$.

Abbiamo già introdotto in precedenza un meccanismo di astrazione: il quozientamento di $\mathbb{A}$ rispetto a una relazione di equivalenza $\equiv$. Possiamo riusare tale meccanismo? Sì!

Funzioni come osservazioni

Definizione: data una funzione $f \in \mathbb{B}^{\mathbb{A}}$, la relazione di equivalenza indotta da f, $\sim_f$, è definita come segue: $x_1 \sim_f x_2$ sse $f(x_1) = f(x_2)$.

Esempio: se f calcola l'età di una persona allora $\sim_f$ è la relazione "essere coetanei"

Definizione di proiezione $[\cdot]$**:** con un abuso di notazione chiamiamo $[\cdot] \in (\mathbb{A}_{/\sim_f})^{\mathbb{A}}$ la funzione che mappa ogni $x \in \mathbb{A}$ nella sua classe di equivalenza modulo $\sim_f$
$[x]_{\sim_f} := \{x' \in \mathbb{A} \mid x \sim_f x'\}$.

Esempio (cont): $[\cdot]$ associa a ogni insieme la classe di equivalenza di tutti gli insiemi con la sua stessa cardinalità.

Funzioni come osservazioni

Teorema: $[\cdot] \in (\mathbb{A}_{/\sim_f})^{\mathbb{A}}$ è suriettiva.
Dimostrazione: devo dimostrare che per ogni $y \in \mathbb{A}_{/\sim_f}$ esiste un $x \in \mathbb{A}$ t.c. $[x] = y$. Per il teorema sull'insieme quoziente, $y = [a]_{\sim_f}$ per un qualche $a \in \mathbb{A}$. Scelgo a per x e ho $[a] = [a]_{\sim_f}$ per definizione di $[\cdot]$. □

Intermezzo: composizione di funzioni

Definizione: date $f \in \mathbb{B}^{\mathbb{A}}$ e $g \in \mathbb{C}^{\mathbb{B}}$, la funzione composta $g \circ f \in \mathbb{C}^{\mathbb{A}}$ è definita come segue: $(g \circ f)(x) := g(f(x))$.

Teorema: per ogni f, g, g', se f è suriettiva e $g \circ f = g' \circ f$ allora $g = g'$.
Dimostrazione: siano f, g, g' t.c. f è suriettiva (H) e $g \circ f = g' \circ f$. Quindi, per l'assioma di estensionalità, $\forall x.(g \circ f)(x) = g(f(x)) = g'(f(x) = (g' \circ f)(x)$ (K). Devo dimostrare $g = g'$. Per l'assioma di estensionalità è sufficiente dimostrare $\forall y.g(y) = g'(y)$. Fisso y. Da H si ha che c'è un x t.c. $f(x) = y$. Quindi devo dimostrare $g(f(x) = g'(f(x))$, il che segue da K. □

Intermezzo: composizione di funzioni

Teorema: per ogni f, g, se $g \circ f$ è suriettiva allora anche g lo è.
Dimostrazione: siano f, g t.c. $g \circ f$ è suriettiva, ovvero $\forall z.\exists x.g(f(x) = z$ (H). Dobbiamo dimostra g suriettiva, ovvero $\forall z.\exists y.g(y) = z$. Fisso z. Da H sia x t.c. $g(f(x)) = z$ (K). Scelgo $f(x)$ per y e dimostro $g(f(x)) = z$, che segue da K. □

Funzioni come osservazioni

Teorema: per ogni $f \in \mathbb{B}^{\mathbb{A}}$ esiste un'unica $g \in \mathbb{B}^{\mathbb{A}/\sim_f}$ t.c. $g \circ [\cdot] = f$.
Dimostrazione:

- Esistenza: scelgo come g la relazione $\{\langle [a]_{\sim_f}, f(a)\rangle \mid a \in \mathbb{A}\}$ (abbreviabile con abuso di notazione come $g([a]_{\sim_f}) = f(a)$). Dimostro che la relazione è una funzione, ovvero che a ogni classe di equivalenza resta associato un solo valore. È sufficiente dimostrare che per ogni a, b se $[a]_{\sim_f} = [b]_{\sim_f}$ allora $g([a]_{\sim_f}) = g([b]_{\sim_f})$. Infatti siano a, b t.c. $[a]_{\sim_f} = [b]_{\sim_f}$. Quindi, per quanto dimostrato a inizio corso, si ha $a \sim_f b$, ovvero $f(a) = f(b)$. Quindi $g([a]_{\sim_f}) = f(a) = f(b) = g([b]_{\sim_f})$.

  Infine devo dimostrare che $g \circ [\cdot] = f$, ovvero, per l'assioma di estensionalità, che per ogni x si ha $(g \circ [\cdot])(x) = f(x)$. Il che è ovvio poichè $(g \circ [\cdot])(x) = g([x]) = g([x]_{\sim_f}) = f(x)$.

- Unicità: dimostro che per ogni g' t.c. $g' \circ [\cdot] = f$ si ha $g' = g$. Sia g' t.c. $g' \circ [\cdot] = f = g \circ [\cdot]$. Allora $g' = g$ in quanto abbiamo dimostrato che $[\cdot]$ è suriettiva. □

Funzioni come osservazioni

Primo teorema di omomorfismo per insiemi: Per ogni $f \in \mathbb{B}^{\mathbb{A}}$ si ha

1. $[\cdot] \in (\mathbb{A}_{/\sim_f})^{\mathbb{A}}$ è suriettiva.
2. $\exists! g \in \mathbb{B}^{\mathbb{A}/\sim_f}. g \circ [\cdot] = f$
3. la funzione del punto precedente è iniettiva
4. $\mathbb{A}_{/\sim_f}$ è in biezione con $Imm(f)$

Dimostrazione: I punti 1 e 2 sono stati appena dimostrati. Per 3 dimostriamo che $\forall y_1, y_2 \in \mathbb{A}_{/\sim_f}. g(y_1) = g(y_2) \Rightarrow y_1 = y_2$. Siano y_1 e y_2 t.c. $g(y_1) = g(y_2)$ (H). Per il teorema dell'insieme quoziente esistono $a_1, a_2 \in \mathbb{A}$ t.c. $y_1 = [a_1]_{\sim_f} = [a_1]$ e $y_2 = [a_2]_{\sim_f} = [a_2]$. Quindi, per H, $g([a_1]) = f(a_1) = f(a_2) = g([a_2])$ e perciò $a_1 \sim_f a_2$. Quindi, per il teorema dimostrato a inizio corso, $y_1 = [a_1]_{\sim_f} = [a_2]_{\sim_f} = y_2$. Infine per dimostrare 4 esibisco la biezione g del punto 3. Infatti g è iniettiva (per il punto 3) e g è suriettiva in quanto $g \circ [\cdot] = f$ e f è suriettiva su $Imm(f)$.

Primo teorema di omomorfismo per insiemi

Cosa ci dice l'enunciato del teorema?

Ricapitoliamo: leggiamo una funzione $f \in \mathbb{B}^{\mathbb{A}}$ come un'osservazione che possiamo compiere sugli elementi di $\mathbb{A}$. Vogliamo astrarre gli elementi di $\mathbb{A}$ tenendo valide solamente tali osservazioni e scordandoci il resto.

Diciamo che due elementi di $\mathbb{A}$ sono equivalenti ($\sim_f$) sse l'osservazione f restituisce lo stesso valore su entrambi.

Otteniamo $\mathbb{A}_{/\sim_f}$, l'insieme degli elementi di $\mathbb{A}$ una volta astratti. Il primo teorema di omomorfismo ci dice che ho esattamente uno di questi elementi astratti per ogni possibile risultato (in $\mathbb{B}$) che è osservabile tramite la f, e viceversa.

Ovviamente $Imm(f)$ è una rappresentazione più concisa/efficiente di $\mathbb{A}_{/\sim_f}$ (che è data da insiemi di insiemi di elementi di $\mathbb{A}$).

Primo teorema di omomorfismo per insiemi

Esempio: considero $|\cdot| \in \mathbb{Z}^{\mathbb{Z}}$ che a ogni numero intero z associa la sua magnitudo $|z|$ (ovvero la sua distanza dallo 0, dimenticando la direzione).

Si ha $\mathit{Imm}(|\cdot|) = \mathbb{N} = \{0, 1, \ldots\}$ mentre
$\mathbb{Z}_{/\sim_{|\cdot|}} = \{[0]_{\sim_{|\cdot|}}, [1]_{\sim_{|\cdot|}}, \ldots\} = \{\{0\}, \{-1, 1\}, \{-2, 2\}, \ldots\}$.

I due insiemi sono in biezione come testimoniato dalla funzione biettiva $h(n) = \{-n, n\}$ che associa a ogni magnitudo l'insieme degli interi che hanno quella magnitudo, e viceversa.

Come in informatica, anche in algebra è importante non solo l'astrazione, ma anche la possibilità di passare all'occorrenza da una "struttura dati" a un'altra isomorfa per sfruttare la libreria.

Morfismi come osservazioni

Cosa succede se invece di partire da una funzione partiamo da un morfismo?

Punto di vista: un morfismo da una struttura $\mathcal{A}$ di sostegno $\mathbb{A}$ a una struttura $\mathcal{B}$ di sostegno $\mathbb{B}$ (che sono già ambedue astrazioni!) effettua delle osservazioni sugli elementi di $\mathcal{A}$, ma preservando la struttura che già sappiamo interessarci.

Come nel caso delle funzioni, ci aspettiamo quindi di poter ulteriormente astrarre $\mathcal{A}$ tenendo solamente in conto le osservazioni date dal morfismo e la struttura pre-esistente.

Morfismi come osservazioni

Primo teorema di omomorfismo per strutture algebriche:
Per ogni f morfismo da $\mathcal{A}$ (di supporto $\mathbb{A}$) a $\mathcal{B}$ (di supporto $\mathbb{B}$) si ha

1. $\mathbb{A}_{/\sim_f}$ è il sostegno di una struttura algebrica dello stesso tipo
2. $[\cdot] \in (\mathbb{A}_{/\sim_f})^{\mathbb{A}}$ è un morfismo suriettivo.
3. $\exists! g \in \mathbb{B}^{\mathbb{A}_{/\sim_f}}. g \circ [\cdot] = f$ e g è un morfismo
4. il morfismo del punto precedente è iniettivo
5. $\mathbb{A}_{/\sim_f}$ è isomorfo a $Imm(f)$

Dimostrazione: (dopo l'esempio)

Primo teorema di omomorfismo per strutture algebriche

Esempio: $(\mathbb{Z}, *, 1)$ è un monoide. La funzione $|\cdot| \in \mathbb{Z}^{\mathbb{Z}}$ che a ogni numero intero z associa la sua magnitudo $|z|$ (ovvero la sua distanza dallo 0, dimenticando la direzione) è un morfismo. Infatti:

1. $|1| = 1$
2. $\forall x, y. |x * y| = |x| * |y|$

Si ha $Imm(|\cdot|) = \mathbb{N} = \{0, 1, \ldots\}$ è un sottomonoide di $(\mathbb{Z}, *, 1)$ mentre $\mathbb{Z}_{/\sim_{|\cdot|}} = \{[0]_{\sim_{|\cdot|}}, [1]_{\sim_{|\cdot|}}, \ldots\} = \{\{0\}, \{-1, 1\}, \{-2, 2\}, \ldots\}$ ha la struttura di monoide $(\mathbb{Z}_{/\sim_{|\cdot|}}, \circ, [1]_{\sim_{|\cdot|}})$ ove $[x]_{\sim_{|\cdot|}} \circ [y]_{\sim_{|\cdot|}} = [x * y]_{|\cdot|}$ (ovvero $\{-n, n\} \circ \{-m, m\} = \{-n * m, n * m\}$).

I due monoidi sono isomorfi come testimoniato dall'isomorfismo $h(n) = \{-n, n\}$ che associa a ogni magnitudo l'insieme degli interi che hanno quella magnitudo, e viceversa, rispettando il prodotto e il suo elemento neutro.

Morfismi come osservazioni

Primo teorema di omomorfismo per strutture algebriche: Per ogni f morfismo da $\mathcal{A}$ (di supporto $\mathbb{A}$) a $\mathcal{B}$ (di supporto $\mathbb{B}$) si ha

1. $\mathbb{A}_{/\sim_f}$ è il sostegno di una struttura algebrica dello stesso tipo
2. $[\cdot] \in (\mathbb{A}_{/\sim_f})^{\mathbb{A}}$ è un morfismo suriettivo.
3. $\exists! g \in \mathbb{B}^{\mathbb{A}_{/\sim_f}}. g \circ [\cdot] = f$ e g è un morfismo
4. il morfismo del punto precedente è iniettivo
5. $\mathbb{A}_{/\sim_f}$ è isomorfo a $Imm(f)$

Dimostrazione (cenni): segue quella del primo teorema di omomorfismo per insiemi. Vediamo solamente le parti nuove e lo facciamo solo nel caso particolare in cui $\mathcal{A} = (\mathbb{A}, \circ, a)$ e $\mathcal{B} = (\mathbb{B}, \bullet, b)$ siano monoidi.

Morfismi come osservazioni

Dimostrazione di 1: $\mathbb{A}_{/\sim_f}$ è il sostegno di un monoide. Scegliamo come monoide $(\mathbb{A}_{/\sim_f}, \oplus, [a]_{\sim_f})$ dove $\oplus$ è la relazione $[x]_{\sim_f} \oplus [y]_{\sim_f} = [x \circ y]_{\sim_f}$. Dobbiamo dimostrare:

- $\oplus$ è una funzione. Infatti per ogni x, x', y, y', se $[x]_{\sim_f} = [x']_{\sim_f}$ e $[y]_{\sim_f} = [y']_{\sim_f}$ per il teorema visto a inizio corso si ha $x \sim_f x'$ e $y \sim_f y'$, ovvero $f(x) = f(x')$ e $f(y) = f(y')$. Pertanto $f(x \circ y) = f(x) \bullet f(y) = f(x') \bullet f(y') = f(x' \circ y')$ e perciò $x \circ y \sim_f x' \circ y'$ e quindi $[x \circ y]_{\sim_f} = [x' \circ y']_{\sim_f}$. Pertanto $\oplus$ associa a ogni input un solo output.
- per ogni x, y, z, $([x]_{\sim_f} \oplus [y]_{\sim_f}) \oplus [z]_{\sim_f} = [(x \circ y) \circ z]_{\sim_f} = [x \circ (y \circ z)]_{\sim_f} = [x]_{\sim_f} \oplus ([y]_{\sim_f} \oplus [z]_{\sim_f})$
- per ogni x, $[x]_{\sim_f} \oplus [a]_{\sim_f} = [x \circ a]_{\sim_f} = [x]_{\sim_f}$ e $[a]_{\sim_f} \oplus [x]_{\sim_f} = [a \circ x]_{\sim_f} = [x]_{\sim_f}$

Morfismi come osservazioni

Dimostrazione di 2: $[\cdot] \in (\mathbb{A}_{/\sim_f})^{\mathbb{A}}$ è un morfismo.

- $[a] = [a]_{\sim_f}$
- per ogni x, y, $[x \circ y] = [x \circ y]_{\sim_f} = [x]_{\sim_f} \oplus [y]_{\sim_f}$

Dimostrazione di 3: g è un morfismo.

- $g([a]_{\sim_f}) = f(a) = b$
- per ogni x, y, $g([x]_{\sim_f} \oplus [y]_{\sim_f}) = g([x \circ y]_{\sim_f}) = f(x \circ y) = f(x) \bullet f(y) = g([x]_{\sim_f}) \bullet g([y]_{\sim_f})$ □

Conclusioni

Algebra universale:

1. Vi sono numerose strutture algebriche interessanti
2. Ci sono definizioni/costruzioni/teoremi che funzionano su ogni tipo di strutture algebriche
   - le operazioni chiuse generano sottostrutture
   - intersezione di sottostrutture sono ancora sottostrutture
   - prodotti cartesiani di strutture sono ancora strutture
   - immagini di morfismi sono sottostrutture
   - dato un morfismo pensato come osservazioni, otteniamo un'astrazione in due modi diversi ma isomorfi: come immagine del morfismo o come quoziente del dominio
   - ...