Teoria della Fattorizzazione

Lorenzo Saporito Relatore: Andrea Loi

Università degli Studi di Cagliari

29 Marzo 2023

Introduzione

- Teorema fondamentale dell'aritmetica
- Elementi irriducibili e elementi primi
- Fattorizzazioni non classiche (es. permutazioni)
- Teorema di esistenza e teorema inverso
- Esempi

Bibliografia

- An Abstract Factorization Theorem and Some Applications - S. Tringali;
- Factorization under Local Finiteness Conditions - L. Cossu, S. Tringali

Definizione

Sia H un insieme non vuoto e sia $\cdot : H \times H \to H$ un'operazione binaria su H tale che per ogni $x, y, z \in H$:

- $x(yz) = (xy)z$ (associatività)
- esiste $1 \in H$ tale che $x \cdot 1 = 1 \cdot x = x$ (elemento neutro)

Chiamiamo **monoide** la coppia $(H, \cdot)$

Definizione

Sia X un insieme non vuoto. Una relazione $R \subseteq X \times X$ è detta **preordine** se per ogni $x, y, z \in X$:

- xRx (riflessiva)
- xRy e $yRz \Rightarrow xRz$ (transitiva)

Useremo il simbolo $\preceq$ per indicare il preordine e scriveremo $x \prec y$ se risulta $x \preceq y$ e $y \not\preceq x$. Diremo che x, y sono $\preceq$-equivalenti se $x \preceq y \preceq x$.

Definizione

Sia H un monoide e $\preceq$ un preordine su H. La coppia $\mathcal{H} = (H, \preceq)$ è detta **premonoide.**

Definizione

Sia $\mathcal{H} = (H, \preceq)$ un premonoide. Un elemento $u \in \mathcal{H}$ è detto $\preceq$**-unità** se u è $\preceq$-equivalente a 1, cioè se $u \preceq 1 \preceq u$; altrimenti u si dirà $\preceq$**-non-unità**.
Indichiamo con $\mathcal{H}^*$ l'insieme delle $\preceq$-unità di $\mathcal{H}$.

Definizione

Sia $\mathcal{H} = (H, \preceq)$ un premonoide. Una $\preceq$-non-unità $a \in \mathcal{H}$ si dice:

- $\preceq$-**irriducibile** se $a \neq xy$ per ogni $x, y \in \mathcal{H} \setminus \mathcal{H}^*$ con $x, y \prec a$;
- $\preceq$-**atomo** se $a \neq xy$ per ogni $x, y \in \mathcal{H} \setminus \mathcal{H}^*$;
- $\preceq$-**quark** se non esiste $b \in \mathcal{H} \setminus \mathcal{H}^*$ tale che $b \prec a$.

Inoltre $\mathcal{H}$ si dirà $\preceq$-**fattorizzabile** se ogni $\preceq$-non-unità è prodotto (finito e non vuoto) di $\preceq$-irriducibili. Analogamente, $\mathcal{H}$ si dirà $\preceq$-**atomico**.

Osservazione

$\preceq$-atomo $\Rightarrow \preceq$-irriducibile
$\preceq$-quark $\Rightarrow \preceq$-irriducibile

Esempio 1

Consideriamo $(\mathbb{N}, \cdot)$ e definiamo $a \mid b \iff b \in a\mathbb{N}$.
$u \in \mathbb{N}$ è una $|$-unità $\iff u = 1$.
Sia quindi $a \neq 1$:

- a è $|$-irriducibile se e solo se è irriducibile nel senso classico, quindi se a è primo.
- a è $|$-atomo se e solo se a è primo
- a è $|$-quark se e solo se a è primo

Esempio 2

Sia $(A, +, \cdot)$ un dominio d'integrità e $H = A \setminus \{0\}$ con il preordine
$x \mid y \iff y \in xH$
$u \in \mathcal{H}$ è una $|$-unità $\iff u$ è un unità.
Sia ora $x \in \mathcal{H}$ una non-unità.

- x è un $|$-atomo $\iff x$ è un irriducibile.
- x è un $|$-irriducibile $\iff x$ è un irriducibile.
  Infatti, se x non è irriducibile, $x = yz$, con y e z non-unità. Quindi $y \mid x$ e $z \mid x$. Se per assurdo $x \mid y$, $y = xu = (yz)u$
  $\Rightarrow zu = 1$
- x è un $|$-quark $\iff x$ è un irriducibile.
  Infatti, se x non è un $|$-quark, esiste y non-unità tale che $y \mid x$ e $x \nmid y$. Allora $x = yz$ e z è una non-unità.

Esempio 3

Sia $(S_n, \circ)$ con $n \geq 2$ e definiamo il preordine
$f \preceq g \iff |Fix(g)| \leq |Fix(f)|$, con $Fix(f) = \{x \mid f(x) = x\}$
f è una $\preceq$-unità $\iff f = id$.
Sia quindi $f \neq id$

- f è un $\preceq$-quark $\iff f$ è una trasposizione
- Le trasposizioni sono tutti e i soli $\preceq$-irriducibili. Infatti, se f non è una trasposizione, prendiamo $z \notin Fix(f)$ e $\tau = (z\ f(z))$. Allora, posto $\bar{f} = \tau \circ f$, abbiamo $f = \tau \circ \bar{f}$ e vale $\tau, \bar{f} \prec f$.
- Se τ è una trasposizione e $g \neq id$ non è una trasposizione, $\tau = (\tau \circ g) \circ g^{-1}$ mostra che τ non è un $\preceq$-atomo. Non ci sono $\preceq$-atomi

Definizione

Un preordine $\preceq$ su un insieme X è detto **artiniano** se per ogni successione non-crescente $(x_k)_{k\in\mathbb{N}}$ in X, ovvero se $x_{k+1} \preceq x_k$ per ogni k, esiste $k_0 \in \mathbb{N}$ tale che $x_k \preceq x_{k+1}$ per ogni $k \geq k_0$. Un premonoide $\mathcal{H} = (H, \preceq)$ è detto **artiniano**, se $\preceq$ è artiniano.

Definizione

Sia $\mathcal{H} = (H, \preceq)$ un premonoide e sia $x \in \mathcal{H}$. Chiamiamo $\preceq$-**altezza** di x, e la indichiamo con $ht(x)$, l'estremo superiore dell'insieme degli $n \in \mathbb{N}$ tali che esistono $x_1, \dots, x_n \in \mathcal{H} \setminus \mathcal{H}^*$ con $x_1 = x$ e $x_{i+1} \prec x_i$ per ogni $i = 1, \dots, n-1$. Per convenzione poniamo sup$\varnothing := 0$. Se risulta $ht(x) < \infty$ per ogni $x \in \mathcal{H}$, il premonoide $\mathcal{H}$ è detto **fortemente artiniano**.

Osservazione

$\mathcal{H}$ fortemente artiniano $\Rightarrow$ $\mathcal{H}$ artiniano.

Teorema (di esistenza della fattorizzazione)

Sia $\mathcal{H} = (H, \preceq)$ un premonoide artiniano. Allora $\mathcal{H}$ è $\preceq$-fattorizzabile. Se inoltre $\mathcal{H}$ è fortemente artiniano, ogni $\preceq$-non-unità è prodotto di $2^{ht(x)-1}$ o meno $\preceq$-irriducibili.

Dimostrazione

Sia X l'insieme delle $\preceq$-non-unità di $\mathcal{H}$ che non sono prodotto di $\preceq$-irriducibili e supponiamo per assurdo $X \neq \varnothing$.
Mostriamo che esiste $x \in X$ $\preceq$-minimale, ovvero se $y \preceq x$ si ha $x \preceq y$.
Sia $x_0 \in X$ e definiamo ricorsivamente una successione in X. Se per qualche $k \in \mathbb{N}$, x_k non è $\preceq$-minimale, prendiamo $y \in X$ tale che $y \prec x_k$ e poniamo $x_{k+1} = y$; altrimenti $x_{k+1} = x_k$.
Per ipotesi esiste $k_0 \in \mathbb{N}$ tale che $x_k \preceq x_{k+1}$ per ogni $k \geq k_0$, cioè sono $\preceq$-equivalenti e x_{k_0} è quindi un elemento $\preceq$-minimale.

Dimostrazione

Sia $x \in X$ un elemento $\preceq$-minimale, in particolare x non è $\preceq$-irriducibile. Allora esistono $y, z \in \mathcal{H} \setminus \mathcal{H}^*$ tali che $x = yz$, con $y, z \prec x$.
Poiché x è $\preceq$-minimale, deve essere $y, z \notin X$. Allora y e z sono prodotto di $\preceq$-irriducibili e quindi anche x. $\square$

Corollario

Sia $\mathcal{H} = (H, \preceq)$ un premonoide fortemente artiniano e supponiamo che, se $x \in \mathcal{H} \setminus \mathcal{H}^*$ non è un $\preceq$-quark, esistono $y, z \in \mathcal{H} \setminus \mathcal{H}^*$ con $y, z \preceq x$ tali che $x = yz$ e $ht(y) + ht(z) \leq ht(x)$. Allora:

(i) ogni $\preceq$-irriducibile è un $\preceq$-quark;

(ii) ogni $\preceq$-non-unità x è prodotto di al più $ht(x)$ $\preceq$-quark.

Teorema (inverso)

Sia H un monoide e siano $A, S \subseteq H$ tali che $1 \notin A \cup S$. Allora le seguenti sono equivalenti:

(i) ogni elemento di S fattorizza nel prodotto (finito e non vuoto) di elementi di A;

(ii) esiste un preordine $\preceq$ fortemente artiniano su H tale che ogni elemento S è una $\preceq$-non-unità e un elemento $x \in H$ è un $\preceq$-irriducibile se e solo se è un $\preceq$-quark se e solo se $x \in A$;

(iii) esiste un preordine $\preceq$ artiniano su H tale che ogni elemento S è una $\preceq$-non-unità e ogni $\preceq$-irriducibile è un elemento di A;

Esempio (Teorema fondamentale dell'aritmetica)

Il premonoide $(\mathbb{N}, |)$ è banalmente artiniano per il principio del buon ordinamento. Dal teorema di esistenza abbiamo che:
Ogni numero naturale $n \neq 1$ è prodotto di $|$-irriducibili, cioè di numeri primi.
Osserviamo inoltre che nonostante $\mathbb{N}$ sia anche fortemente artiniano, questo non ci dà nuove informazioni sulla lunghezza della fattorizzazione.

Esempio (Domini noetheriani)

Sia $(A, +, \cdot)$ un dominio d'integrità e $H = A \setminus \{0\}$ con il preordine $x \mid y \iff y \in xH \iff yH \subseteq xH$
Se ora A è un dominio noetheriano il preordine $|$ è artiniano. Dal teorema di esistenza segue quindi:
Ogni dominio noetheriano è fattorizzabile.

Esempio (Permutazioni)

Il premonoide $(S_n, \preceq)$ è fortemente artiniano, infatti $ht(f) = n - 1 - |Fix(f)|$ per ogni $f \neq id$.
Data $f \neq id$ non trasposizione, abbiamo visto che $f = \tau \circ \bar{f}$, con $\tau, \bar{f} \prec f$.
Inoltre $ht(\tau) + ht(\bar{f}) = 1 + ht(\bar{f}) \leq ht(f)$.
Allora, per il corollario, una permutazione $f \neq id$ è prodotto di al più $n - 1 - |Fix(f)|$ trasposizioni.

Grazie per l'attenzione