# TERZO TEOREMA DI ISOMORFISMO

Note Title 11/14/2018

$A$ un anello, $I \subseteq J \subseteq A$ ideali. Allora:

(i) $J/I$ è un ideale di $A/I$

(ii) Si ha $\dfrac{A/I}{J/I} \simeq A/J$

Dim. (i) • $J/I$ è un sottogruppo additivo di $A/I$

• proprietà di assorbimento:

Sia $\overline{x} \in J/I$ e $\overline{a} \in A/I$.

Siano $x \in J$ la cui classe è $\overline{x}$

$a \in A$ ——— è $\overline{a}$

Allora $\overline{x} \cdot \overline{a} = \overline{a \cdot x}$, ma $a \cdot x \in J$ perché $J$ è ideale e $x \in J$, quindi $\overline{a \cdot x} \in J/I$

(ii) Ho $A \longrightarrow A/I \longrightarrow \dfrac{A/I}{J/I}$ omomorf. di anelli

$\rightsquigarrow \pi : A \longrightarrow \dfrac{A/I}{J/I}$

$\ker \pi = \{ a \in A \text{ t.c. } \overline{a} \text{ appartiene a } J/I \}$

$$= \{ a \in A \text{ t.c. } \exists i \in I \text{ t.c. } a+i \in J \}$$

$$= \{ a \in A \text{ t.c. } a \in J - i = J \} = J$$

1° teo isom. $\Longrightarrow$ $\dfrac{A}{\ker \pi} \simeq \dfrac{A/I}{J/I}$

$\ker \pi = J$

□

Esempio $\dfrac{\mathbb{Z}[x]}{(5, x^2+1)}$

$A = \mathbb{Z}[x]$

$J = (5, x^2+1)$

$I = (5)$

$$A/J \simeq \frac{A/I}{J/I} \simeq \frac{\mathbb{F}_5[y]}{(y^2+1)}$$

## Operazioni fra ideali

(i) $I, J$ ideali. Allora $IJ \subseteq I \cap J$

$IJ$ = ideale generato da $\{ij \mid i \in I, j \in J\}$

$$= \left\{ \sum_{k=1}^{r} i_k j_k \mid i_k \in I, j_k \in J \right\}$$

$i_k j_k \in I$ (perché è $i_k \cdot$ qualcosa)

$\in J$ ( —— qualcosa $\cdot j_k$)

$\Rightarrow \in I \cap J$

Oss In generale sono diversi: $A = \mathbb{Z}$, $I = J = (2)$

In $\mathbb{Z}$: prodotto di ideali = prod. di numeri

intersezione = m.c.m

(ii) Vale $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

Oss. In $\mathbb{Z}$, $\sqrt{(p_1^{e_1} \dots p_k^{e_k})} = (p_1 p_2 \dots p_k)$

$$\sqrt{I} = \left\{ a \in A \text{ t.c. } \exists\, n>0 \; a^n \in I \right\}$$

$\sqrt{IJ} \subseteq \sqrt{I \cap J}$ : ovvio $\left( B \subseteq C \Rightarrow \sqrt{B} \subseteq \sqrt{C} \right)$

$\sqrt{I \cap J} \subseteq \sqrt{IJ}$ : sia $a \in \sqrt{I \cap J}$, ovvero

esiste $n>0$ t.c. $a^n \in I \cap J$

$$a^{2n} = \underset{\substack{\cap \\ I \cap J \subseteq I}}{a^n} \cdot \underset{\substack{\cap \\ I \cap J \subseteq J}}{a^n} \in I \cdot J$$

$\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.

$a \in \sqrt{I \cap J} \Rightarrow \exists n>0$ t.c. $a^n \in I \cap J$

$\Rightarrow$ $a^n \in I \Rightarrow a \in \sqrt{I}$

$a^n \in J \Rightarrow a \in \sqrt{J}$

$\sqrt{I \cap J} \supseteq \sqrt{I} \cap \sqrt{J}$

Sia $a \in \sqrt{I} \cap \sqrt{J}$. Allora $\exists\, m, n > 0$ t.c.

$$a^m \in I \quad e \quad a^n \in J$$

$$a^{m+n} \in I \cdot J \subseteq I \cap J \qquad \square$$

(iii) $A = \mathbb{F}_5[x]$, $I = (x^2+1)$ $J = (x^3-3)$

Chi è $I + J$?

$$I + J = (x^2+1,\ x^3-3)$$

$$= (x^2+1,\ x^3-3-x(x^2+1))$$

$$= (x^2+1,\ -3-x)$$

$$= (x^2+1,\ x+3) = (x^2+1-x(x+3),\ x+3)$$

$$= (1-3x,\ x+3)$$

$$= (x-2,\ x+3) = (x-2)$$

(iv) $I, J$ si dicono COPRIMI se $I + J = (1) = A$

[In $\mathbb{Z}$: $I = (m)$, $J = (n)$, $I + J = ((m,n))$]

$I, J$ coprimi $\Rightarrow$ $IJ = I \cap J$

Dim

$\exists\, i \in I$, $\exists\, j \in J$ t.c. $i + j = 1$

$IJ \subseteq I \cap J$ già vista

$a \in I \cap J$.

$$a = a \cdot 1 = a \cdot (i + j) = \underset{\in J}{a \cdot i} + \underset{\in I}{a \cdot j}$$

$$\in I \cdot J$$

(v) $I, J, K$ tre ideali. Supponiamo

$$I + J + K = A$$

Allora $I^n + J^n + K^n = A \quad \forall n$

Dim $1 = i + j + k \qquad i \in I,\ j \in J,\ k \in K$

$$1 = (i + j + k)^m = \sum_{a+b+c=m} \binom{m}{a,b,c} i^a j^b k^c$$

Se scelgo $m \geq 3n$, ogni addendo soddisfa

$\max\{a, b, c\} \geq n$

Se per esempio $a \geq n$, $i^a \in I^n \Rightarrow i^a j^b k^c \in I^n$

e similmente $b \geq n \Rightarrow i^a j^b k^c \in J^n$

$$c \geq n \Rightarrow i^a j^b k^c \in K^n$$

Quindi $1 =$ Somma di el. di $I^n +$
$J^n +$
$K^n \in I^n + J^n + K^n$

(b) se $I + J = J + K = K + I = (1)$, allora

$$IJ + JK + KI = (1)$$

Ipotesi: $\exists$ $i_1 + j_1 = 1$ $\quad i_1, i_2 \in I$
$j_2 + k_1 = 1$ $\quad j_1, j_2 \in J$
$k_2 + i_2 = 1$ $\quad k_1, k_2 \in K$

$$1 = (i_1 + j_1)(j_2 + k_1)(k_2 + i_2)$$

$$= i_1 j_2 k_2 + i_1 j_2 i_2 + \cdots + j_1 j_2 k_2$$

$i_1 j_2 k_2 \in IJ, JK, KI$ $\quad i_1 j_2 i_2 \in IJ$ $\quad j_1 j_2 k_2 \in J \cdot K$

$$\in IJ + JK + KI$$

(vi) $A = \mathbb{Q}[x, y]$ $\quad I = (x-1, y-1)$

$J = (1 - xy)$

- $I$ massimale
- $J \subsetneq I$

- $J$ è primo?

**Def** $I$ è MASSIMALE se $I \subsetneq J$ con $J$ ideale $\Rightarrow J = (1)$

$I$ è PRIMO se $x \cdot y \in I \Rightarrow x \in I \vee y \in I$

**Prop.** $I$ massimale $\iff A/I$ campo

$I$ primo $\iff A/I$ dominio d'integrità

**Soluzione** $$\frac{\mathbb{Q}[x,y]}{(x-1, y-1)} \simeq \frac{\mathbb{Q}[x,y]/(y-1)}{(x-1, y-1)/(y-1)}$$

Affermazione: $p(x,y) \equiv p(x,1) \mod (y-1)$

$a \equiv b \pmod m \iff m \mid a-b$

$\iff a-b \in (m)$

$a \equiv b \pmod I \iff a-b \in I$ ⌟

$y \equiv 1 \pmod{(y-1)}$

$y^k \equiv 1 \pmod{(y-1)}$

$$x^a y^b \equiv x^a \mod (y-1)$$

$$p(x,y) = \sum_{i,j} c_{ij} x^i y^j \equiv \underbrace{\sum_{i,j} c_{i,j} x^i}_{p(x,1)} \mod (y-1)$$

$$\frac{\mathbb{Q}[x,y]}{(x-1,y-1)} \simeq \frac{\mathbb{Q}[x,y]/(y-1)}{(x-1,y-1)/(y-1)} \simeq \frac{\mathbb{Q}[x]}{(x-1)} \simeq \mathbb{Q}$$

MODO MIGLIORE DI DIMOSTRARE L'ISOMORFISMO

$$\frac{\mathbb{Q}[x]}{(x-1)} \simeq \mathbb{Q}$$

$$\Phi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}$$
$$p(x) \longmapsto p(1)$$

* $\Phi$ è suriettivo

* $\ker \Phi = \{$ polinomi che si annullano per $x=1 \}$

$\overset{\text{RUFFINI}}{=\!=}$ $(x-1)$

$\overset{1^\circ \text{ teo isom.}}{\Longrightarrow}$ $\dfrac{\mathbb{Q}[x]}{(x-1)} \simeq \mathbb{Q}$

Conseguenza: $(x-1, y-1)$ è massimale in $A$

- $(1-xy) \subseteq (1-x, 1-y) = I$

$$1 - xy \equiv 1 - x\big(y - (y-1)\big) \mod I$$

$$\equiv 1 - x \mod I$$

$$\equiv (1-x) - (1-x) \equiv 0 \mod I$$

- $J$ è primo?

$\frac{\mathbb{Q}[x,y]}{J}$ è un dominio

$\mathbb{Q}[x,y]$ è a fattorizzazione unica

Basta verificare che $1-xy$ è irriducibile,

cosa che è perché è di grado 1:

$$1 - xy = p(x,y) \cdot q(x,y)$$

$$1 = \underbrace{\deg_y p}_{=0} + \underbrace{\deg_y q}_{=1}$$

$$1 = \underbrace{\deg_x p}_{\substack{0 \\ 1}} + \underbrace{\deg_x q}_{\substack{1 \\ 0}}$$

$$\frac{\mathbb{Q}[x,y]}{(1-xy)} \simeq \underbrace{\left\{ \frac{p(x)}{x^k} \;\middle|\; \begin{matrix} p(x) \in \mathbb{Q}[x] \\ k \in \mathbb{N} \end{matrix} \right\}}_{A}$$

- $A$ è un anello
- $A$ è un dominio $\quad \dfrac{p(x)}{x^k}\,\dfrac{q(x)}{x^h} = \dfrac{p(x)q(x)}{x^{k+h}}$

è zero $\iff p(x)\,q(x) = 0$

$\iff p(x) = 0$ oppure $q(x) = 0$

- $\dfrac{\mathbb{Q}[x,y]}{(1-xy)} \simeq A$

$\psi\colon \mathbb{Q}[x,y] \longrightarrow A$ omomorfismo di anelli

$p(x,y) \longmapsto p\left(x, \frac{1}{x}\right)$

$\ker \psi \supseteq (1-xy)$: se valuto $1-xy$ in $y = 1/x$ trovo

$1 - x \cdot \frac{1}{x} = 0$

$$p(x,y) = \sum c_{ij}\, x^i y^j$$

$$\psi(p(x,y)) = \sum_{i,j} c_{ij}\, x^{i-j} = 0$$

$$\psi(p) = 0 \iff \sum_{i-j=k} c_{ij} = 0$$

(provare a finire da qui)

$$p(x,y) = \sum_{i,j} c_{ij}\, x^i y^j$$

$$y \equiv x^{-1} \mod (1-xy)$$

$$x^N p(x,y) \equiv \left(\text{polinomio in } x,\ x^{-1}\right) x^N \mod (1-xy)$$

($N$ scelto per annullare i denominatori)

└ $\psi$ è l'identità su un polinomio nella sola $x$ $\Longrightarrow$ $\psi(p) = 0$

se e solo se $p \in (1-xy)$

## Interpolazione

$a_1 < a_2 < \dots < a_n$ razionali

$b_1, b_2, \dots, b_n$

$\exists!\ p(x) \in \mathbb{Q}[x]$ t.c. $\deg p \le n-1$

$p(a_i) = b_i \quad \forall i$

$I_i = (x - a_i)$ ideali di $\mathbb{Q}[x]$

$i \neq j \Longrightarrow I_i + I_j = (1)$

$\psi$

$(x-a_i) - (x-a_j) = a_j - a_i \in \mathbb{Q}^\times$

$$\frac{\mathbb{Q}[x]}{((x-a_1)(x-a_2)\dots(x-a_n))} \overset{\text{TCR}}{\simeq} \frac{\mathbb{Q}[x]}{I_1} \times \dots \times \frac{\mathbb{Q}[x]}{I_n}$$

$$\simeq \mathbb{Q} \times \dots \times \mathbb{Q}$$

$$\mathbb{Q}[x] \longrightarrow \mathbb{Q} \times \dots \times \mathbb{Q}$$

$$p(x) \longmapsto (p(a_1), p(a_2), \dots, p(a_n))$$

$$\frac{\mathbb{Q}[x]}{((x-a_1)\dots(x-a_n))} \simeq \mathbb{Q} \times \dots \times \mathbb{Q}$$

$$\overline{p(x)} \longmapsto (p(a_1), \dots, p(a_n))$$

$$\overline{r(x)} \longmapsto (b_1, b_2, \dots, b_n)$$

siccome è un isom., $(b_1, \dots, b_n)$ proviene da un certo $\overline{r(x)}$

Sia $r(x)$ nella classe di $\overline{r(x)}$

Divido $r(x)$ per $(x-a_1)\dots(x-a_n)$ con resto:

$$r(x) = q(x)(x-a_1)\dots(x-a_n) + s(x)$$

con $\deg s(x) < \deg((x-a_1)\dots(x-a_n)) = n$

ed inoltre $r(a_i) = s(a_i)$

Unicità: se ne ho due, $s$ ed $s'$, allora

$(x-a_1) \dots (x-a_n) \mid s - s'$,

questo implica $s = s'$ per questioni di grado.

## Massimali in $\mathbb{Z}[x]$: introduzione

$I = (5)$ $\qquad \mathbb{Z}[x]/(5) \simeq \mathbb{F}_5[x]$

$I$ è primo, ma non massimale!

$J = (5, x-5) = (5, x)$

$$\frac{\mathbb{Z}[x]}{J} \simeq \frac{\mathbb{Z}[x]/(5)}{(5,x)/(5)} \simeq \frac{\mathbb{F}_5[x]}{(x)} \simeq \mathbb{F}_5$$

Sia $p(x)$ un pol. irrid. mod 5. Allora

$$\frac{\mathbb{Z}[x]}{(5, p(x))} \simeq \frac{\mathbb{F}_5[x]}{(\overline{p(x)})} \simeq \text{campo}$$

$$\frac{\mathbb{Z}[x]}{(5, x^2+1)} \simeq \frac{\mathbb{F}_5[y]}{(y^2+1)} \simeq \frac{\mathbb{F}_5[y]}{(y^2-4)}$$

$$\simeq \frac{\mathbb{F}_5[y]}{((y-2)(y+2))} \overset{\text{TCR}}{\simeq} \frac{\mathbb{F}_5[x]}{(x-2)} \times \frac{\mathbb{F}_5[x]}{(x+2)}$$

$$\simeq \mathbb{F}_5 \times \mathbb{F}_5$$

Gli ideali massimali in $\mathbb{Z}[x]$ sono tutti e soli quelli della forma

$$(p, \; q(x))$$

dove $p$ = primo e $q(x)$ irriduc. mod $p$

IDEA CHIAVE $I$ max $\Rightarrow$ $I \cap \mathbb{Z}$ primo di $\mathbb{Z}$

$I \cap \mathbb{Z} = (0)$ oppure $I \cap \mathbb{Z} = (p)$

↓ ↓

$I$ non massimale in $I$ c'è anche un polinomio