

## ESERCIZIO 7

Sia  $(\mathbb{Z}[x], +)$  l'insieme dei polinomi a coefficienti interi con la struttura di gruppo definita dalla somma.

- 1) Sia  $I_1[x]$  il sottinsieme di  $\mathbb{Z}[x]$  dei polinomi con il termine noto pari. Stabilire se  $I_1[x]$  è un sottogruppo di  $(\mathbb{Z}[x], +)$ .
- 2) Siano  $F: \mathbb{Z}[x] \rightarrow \mathbb{Z}$  l'applicazione che associa ad ogni polinomio il coefficiente del termine di 4° grado e  $G: \mathbb{Z}[x] \rightarrow \mathbb{Z}$  quella che associa ad ogni polinomio il suo termine noto. Verificare se  $F$  e  $G$  sono **omomorfismi** di quelli di  $(\mathbb{Z}[x], +, \cdot)$  a  $(\mathbb{Z}, +, \cdot)$ .

$$\mathbb{I}_1[x] \subseteq \mathbb{Z}[x]$$

↑ sottogruppo?

①

- 1)  $\forall a(x), b(x) \in \mathbb{I}_1[x] \Rightarrow a(x) + b(x) \in \mathbb{I}_1[x]$
- 2)  $n$  di  $\mathbb{Z}[x]$  sta in  $\mathbb{I}_1[x]$
- 3)  $\forall a(x) \in \mathbb{I}_1[x] \Rightarrow -a(x) \in \mathbb{I}_1[x]$

$$\forall a(x) \in \mathbb{I}_1[x] \quad a_i \in \mathbb{Z}$$

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

$$a_0 = 2h$$

$$\begin{aligned} a(x) &= 2h + a_1 x + a_2 x^2 + \dots \\ b(x) &= 2k + b_1 x + b_2 x^2 + \dots \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{in } \mathbb{I}_1[x]$$

$$a(x) + b(x) = \underbrace{2h + 2k}_{2(h+k) \text{ e pari}} + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$$

$$2) n = \text{polin. nullo}$$

$$0 + 0x + 0x^2 + \dots + 0$$

$$\in \mathbb{I}_1[x] ? \quad \text{si perché } 2 \cdot 0 = 0 \text{ (pari)}$$

$$3) a(x) = 2h + a_1 x + \dots$$

$$-a(x) = -2h + a_1 x + \dots$$

$$2(-h) \text{ pari}$$

$\mathbb{I}_1[x]$  è  
sottogruppo d. $(\mathbb{Z}[x], +)$

②  $F: (\mathbb{Z}[x], +) \rightarrow (\mathbb{Z}, +)$

$$a(x) = a_0 + a_1 x + \dots + a_n x^n$$

$\downarrow F$

$a_1$

$$G: a(x) \mapsto a_0$$

$F, G$  sono **omomorfismi** di gruppi da  $(\mathbb{Z}[x], +)$

in  $(\mathbb{Z}, +)$ , cioè dicono retificatore che

$$F(a(x) + b(x)) = F(a(x)) + F(b(x))$$

$\downarrow$                                      $\downarrow$

in  $\mathbb{Z}[x]$                                     in  $\mathbb{Z}$

$$a(x) = a_0 + a_1 x + \dots + a_n x^n$$

$$b(x) = b_0 + b_1 x + \dots + b_n x^n$$

$$F(a(x) + b(x)) =$$

$$F(a_0 + b_0 + (a_1 + b_1)x + \dots) = a_1 + b_1 = ?$$

Si

$a_1$

$b_1$

## CLASSI DI RESTO $\mathbb{Z}_n$

$\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\}$  che sono le classi di equivalenza individuate dalla relazione in  $\mathbb{Z}$

$$a \equiv b \pmod{n} \Leftrightarrow a - b = kn$$

$\forall a, b \in \mathbb{Z}$  (relazione di equiv.)

Su  $\mathbb{Z}_n$  abbiamo  $+ \circ \cdot$  e una struttura di anello  $(\mathbb{Z}_n, +, \cdot)$

### ESERCIZIO 1

scrivere le tavole di composizione di  $+ \circ \cdot$  in  $\mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$

e determinare:

$$[2]^{-1}, -[2] \quad \text{in } \mathbb{Z}_3$$

lezio...ee



## ESERCIZIO 1 :

- L'insieme  $X = \{[0]_9, [1]_9, [2]_9\}$  è un sottogruppo di  $(\mathbb{Z}_9, +)$ ?
  - L'insieme  $H = \{[0]_6, [2]_6, [4]_6\}$  è un sottogruppo di  $(\mathbb{Z}_6, +)$ ?
- 

$X$  è sottogruppo di  $(\mathbb{Z}_9, +)$ ? No perché, es.,  
 $[1]_9 + [2]_9 = [3]_9 \notin X$

---

$H = \{[0]_6, [2]_6, [4]_6\}$  sottogruppo di  $(\mathbb{Z}_6, +)$ ?

+	[0]	[2]	[4]
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

→ tutti gli el. stanno in  $H$

$$[0] \in H, \quad -[2] = 4 \quad -[4] = 2 \quad \in H$$

## ESEMPIO 2

Sia  $[a]_n$  le classi di congruenza  
oltre a modulo n.

Calcolare

$$151 \div 3 = 1$$



$$[327]_3 + [151]_3 = [0]_3 + [1]_3 = [1]_3$$

$$[3]_{12} \times [15]_{12} =$$

$$327 = 3 \cdot 129 \Rightarrow [327]_3 = [0]_3$$

$$\Delta \cdot [15]_{12} = [3]_{12} \Rightarrow [3]_{12} \times [3]_{12} = [9]_{12}$$

$$\cdot [45]_{12} = [9]_{12}$$



$$45 \div 12 = 9$$

### ESEMPIO 3

Sia  $f : (\mathbb{Z}_3, +) \rightarrow (\mathbb{Z}_9, +)$

l'applicazione tale che

$$f([0]_3) = [0]_9$$

$$f([1]_3) = [1]_9$$

$$f([2]_3) = [4]_9$$

è un omomorfismo di gruppi?

$$\text{cioè } f([a]_3 + [b]_3) = f([a]_3) + f([b]_3)$$

$$\forall a, b = 0, 1, 2$$

$$f([1]_3 + [2]_3) = f([0]_3) = [0]_9 \quad \xrightarrow{\quad} \neq$$

$$f([1]_3) + f([2]_3) = [1]_9 + [4]_9 = [5]_9$$

NON

è un omomorfismo

④  $a, b$  non divisibile per 3

$$\begin{array}{c} \diagup \\ \exists \\ \end{array} \quad \begin{array}{c} \downarrow \text{coce} \\ [a]_3 \cdot [b]_3 \in \{[1]_3, [2]_3\} \end{array}$$

$$a \cdot b$$

$$[a \cdot b]_3 = [a]_3 \cdot [b]_3$$

$$[1]_3 \cdot [1]_3 = [1]_3$$

$$[2]_3 \cdot [2]_3 = [2]_3$$

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

$$\Rightarrow [a \cdot b]_3 \in \{[1]_3, [2]_3\}$$

⑤  $2^n \cdot 6 \cdot 9^n$  è divisibile per 7  $\forall n \in \mathbb{N}$

$$[2^n \cdot 6 \cdot 9^n]_7 = [0]_7$$

"

$$[2^n]_7 + [6 \cdot 9^n]_7$$

"

$$[2^n]_7 + [6]_7 \cdot [9]^n_7$$

"

$$= [7]_7 + [2]_7^n$$

$$[0]_7 + [2]_7^n$$

## ESERCIZIO 4

Dimostrare, utilizzando le clami di resto che se due numeri interi non sono divisibili per 3, il loro prodotto non è divisibile per 3

## ESERCIZIO 5

Dimostrare, utilizzando le clami di resto, che

$$2^m + 6 \cdot 9^n$$

è divisibile per 7,  $\forall n \in \mathbb{N}$

Anello dei polinomi  $(\mathbb{K}[n], +, \cdot)$

con  $\mathbb{K}$  campo.

### ALGORITMO DELLA DIVISIONE

Siano  $a(n), b(n) \in \mathbb{K}[n]$  con  $b(n) \neq 0$   
 $\Rightarrow \exists! q(n), r(n) \in \mathbb{K}[n]$  tali che:

1.  $a(n) = b(n)q(n) + r(n)$
2.  $0 \leq \deg r(n) < \deg b(n)$

### ESERCIZIO 1

Determinare quoziente e resto della divisione di  $a(n)$  per  $b(n)$  nei seguenti casi:

$$\begin{aligned} 1. \quad a(n) &= n^4 - 2n^3 + n^2 + n - 1 \\ b(n) &= 3n^3 - 5 \end{aligned} \quad \left. \begin{array}{l} \text{in} \\ \text{in } \mathbb{R}[n] \end{array} \right.$$

$$\begin{aligned} 2. \quad a(n) &= n^4 + 2n^3 - n^2 + 4n - 6 \\ b(n) &= n^2 + 2 \end{aligned} \quad \left. \begin{array}{l} \text{in} \\ \text{in } \mathbb{R}[n] \end{array} \right.$$

$$3. \quad \begin{aligned} a(n) &= n^3 + n^2 + 3n + 1 \\ b(n) &= n^2 - 2 \end{aligned} \quad \left. \begin{array}{l} \text{tu} \\ \mathbb{Z}_5[n] \end{array} \right\}$$

$$4. \quad \begin{aligned} a(n) &= n^4 + 3n + 2 \\ b(n) &= 4n^2 + 1 \end{aligned} \quad \left. \begin{array}{l} \text{tu} \\ \mathbb{Z}_7[n] \end{array} \right\}$$

$$1) \quad a(x) = x^4 - 2x^3 + x^2 + x - 1$$

$$b(x) = 3x^3 - 5$$

$$\begin{array}{r|l} \begin{array}{r} x^4 - 2x^3 + x^2 + x - 1 \\ -x^4 \qquad \qquad \qquad + \frac{5}{3}x \\ \hline 0 \quad -2x^3 + x^2 + \frac{8}{3}x - 1 \\ \qquad + 2x^3 \qquad \qquad \qquad - \frac{10}{3} \\ \hline 0 \quad +x^2 + \frac{8}{3}x - \frac{13}{3} \end{array} & \begin{array}{l} 3x^3 - 5 \\ \hline \frac{1}{3}x - \frac{2}{3} \end{array} \end{array}$$

$\underbrace{\qquad\qquad\qquad}_{\deg < 3}$

$$\Rightarrow q(x) = \frac{1}{3}x - \frac{2}{3}$$

$$r(x) = x^2 + \frac{8}{3}x - \frac{13}{3}$$

$$\underline{\text{Proof:}} \quad b(x) \cdot q(x) + r(x)$$

$$2) \quad a(x) = x^4 + 2x^3 - x^2 + 4x - 6$$

$$b(x) = x^2 + 2$$

... .

$$r(x) = 0$$

$$q(x) = x^2 + 2x - 3$$

$$3) \quad a(x) = x^3 + x^2 + 3x + 1 \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{ in } \mathbb{Z}_5[x]$$

$$b(x) = x^2 - 2$$

$$q(x) = (x+1)$$

$$r(x) = 3$$

*x e sono in  $\mathbb{Z}_5$*

$$\begin{array}{r} x^3 + x^2 + 3x + 1 \\ -x^3 \quad \quad \quad -2x \\ \hline 0 + x^2 + 5x + 1 \\ \quad \quad \quad -2x \quad \quad \quad -2 \\ \hline 0 \quad \quad \quad -2 \\ \end{array}$$

$$4) \quad a(x) = x^6 + 3x + 4 \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{ in } \mathbb{Z}_7[x]$$

$$b(x) = 4x^2 + 1$$

$$\begin{array}{r} x^4 \quad \quad \quad 3x + 4 \\ -x^4 \quad -2x^2 \\ \hline 0 \quad -2x^2 + 3x + 4 \\ \quad \quad \quad + 16x^2 \quad \quad \quad + 4 \\ \hline \quad \quad \quad 14x^2 + 3x + 6 \\ \quad \quad \quad 0 \quad \quad \quad \quad \quad r(x) \\ \end{array}$$

$\frac{1}{4}x^2 - 2 \cdot 4^1 = 2 \cdot 2$   
 $[4]_7 = [2]_7$   
 perche'  $[4][2] = [8] = [1]$

## MCD tra polinomi:

$a(n), b(n) \in \mathbb{K}[n]$  non nulli

$\text{MCD}(a(n), b(n))$  è ogni polinomio

$d(n) \in \mathbb{K}[n]$  tale che

1.  $d(n) | a(n)$  e  $d(n) | b(n)$

2. Se  $\exists c(n) \in \mathbb{K}(n)$  tale che

$$c(n) | a(n) \text{ e } c(n) | b(n) \Rightarrow c(n) | d(n)$$

di grado  
massimo

Si calcola con l'algoritmo delle divisioni successive:

Sia  $\deg(a(n)) \geq \deg(b(n))$ .

Dividiamo  $a(n)$  per  $b(n)$ :

$$a(n) = b(n) q_1(n) + r_1(n)$$

con  $\deg r_1(n) < \deg b(n)$

— se  $r_1(n) = 0 \Rightarrow b(n) | a(n)$

— se  $r_1(n) \neq 0$  dividiamo

$b(n)$  per  $r_1(n)$  e ottieniamo

$$b(n) = r_1(n) \cdot q_2(n) + r_2(n)$$

- se  $r_2(n) = 0 \Rightarrow \text{MCD} \mid r_1(n)$
  - se  $r_2(n) \neq 0$  dividiamo  $r_1(n)$   
per  $r_2(n)$
- $$r_1(n) = r_2(n) q_3(n) + r_3(n)$$
- .....

Se  $r_k(n)$  è il primo resto NULLO  
 $\Rightarrow \text{MCD} = r_{k-1}(n)$  (ultimo resto)  
 NON NULLO

### ESERCIZIO 2

Calcolare il MCD ( $a(n), b(n)$ ) con

$$\begin{aligned} 1. \quad a(n) &= n^3 - 2n + 1 \\ b(n) &= n^2 - 1 \end{aligned} \quad \left. \right\} \text{in } \mathbb{R}[n]$$

$$\begin{aligned} 2. \quad a(n) &= n^4 + 3n^3 - 12n - 36 \\ b(n) &= n^2 - 9 \end{aligned} \quad \left. \right\} \text{in } \mathbb{R}[n]$$

$$\begin{aligned} 3. \quad a(n) &= n^3 + n^2 + n + 1 \\ b(n) &= 3n^2 + 2n + 2 \end{aligned} \quad \left. \right\} \text{in } \mathbb{Z}_5[n]$$

1) MCD( $a(x), b(x)$ )

$$\left. \begin{array}{l} a(x) = x^3 - 2x + 1 \\ b(x) = x^2 - 1 \end{array} \right\} \text{in } \mathbb{R}[x]$$

$$\begin{array}{r|l} x^3 - 2x + 1 & x^2 - 1 \\ -x^3 + x & x \\ \hline 0 & \underbrace{-x + 1}_{r_1(x)} \end{array}$$

$$a(x) = b(x) \cdot x + (-x+1)$$

dividiamo  $b(x)$  per  $(-x+1)$   
 $\uparrow$   
 $\uparrow$   
 $(x-1)(x+1)$  divisibile  
per  $-(x-1)$

$$\rightarrow r_2(x) = 0$$

$$\Rightarrow \text{MCD} = r_1(x) = -x+1$$

$$\begin{aligned} \text{e MCD monico e } x-1 \\ = -(-x+1) \end{aligned}$$

$$2) \text{ MCD}(a(x), b(x)) = 15(x+3)$$

$$3) \quad a(x) = x^3 + x^2 + x + 1 \\ b(x) = 3x^2 + 2x + 2 \quad \left. \right\} \mathbb{Z}_3[x]$$

$$\begin{array}{r|l} x^3 + x^2 + x + 1 & 3x^2 + 2x + 2 \\ -x^3 - 4x^2 - 4x & \\ \hline 0 - 3x^2 - 3x + 1 & 3^{-1}x - 1 \\ 3x^2 + 2x + 2 & " \\ \hline 0 - x + 3 & 2 \\ & \underbrace{q_1(x)}_{x_1(x)} \end{array}$$

division  $b(x)$  por  $R_1(x)$

$$\begin{array}{r|l} 3x^2 + 2x + 2 & -x + 3 \\ -3x^2 + 9x & -3x - 1 \\ \hline 0 + x + 2 & \\ -x + 3 & \\ \hline 0 & 0 \end{array}$$

$$R_2(x) = 0$$

$$\text{MCD} = 4x + 3 \quad \text{MCD monico} = 4(4x + 3) \\ = 2x + 2$$

Teorema di RUFFINI e scomposizione  
di polinomi in  $\mathbb{K}[x]$

$f(x) \in \mathbb{K}[x]$ ,  $\alpha \in \mathbb{K}$ .

$\alpha$  è radice di  $f(x) \Leftrightarrow f(x)$  è  
divisibile per  $x - \alpha$ .

Conseguenze:

1.  $\deg f(x) = 1$        $f(x)$  è IRREDUCIBILE  
e ha una radice

2.  $\deg f(x) \geq 2$

se  $f(x)$  ha almeno una radice

$\Rightarrow f(x)$  è riducibile

Now è vero il viceversa

$(x^2 + 1)(x^2 + 2)$  riducibile in  $\mathbb{R}[x]$   
ma non ha radici

### ESERCIZIO 3 :

Si determini la scomposizione in fattori irriducibili dei polinomi:

$$1) a(n) = n^4 + 2n^3 - n^2 + 4n - 6 \quad \text{in } \mathbb{R}[n]$$

(ricordare ex 1.2)

$$2) a(n) = 2n^3 - 7n^2 + 4n + 4 \quad \text{in } \mathbb{R}[n]$$

dopo aver verificato che 2 è radice

$$3) a(n) = n^3 + 4n + 1 \quad \left. \begin{array}{l} \\ b(n) = n^3 + 3n + 2 \end{array} \right\} \quad \text{in } \mathbb{Z}_5[n]$$

$$4) a(n) = n^4 - 10n^2 + 24 \quad \text{in } \mathbb{Q}[n]$$

$$5) a(n) = n^4 - n^2 - 42$$

in  $\mathbb{R}[n], \mathbb{Q}[n], \mathbb{Z}_3[n], \mathbb{Z}_5[n]$

## ESERCIZIO 4

Nell'anello dei polinomi  $\mathbb{Z}_7[n]$  siamo

$$p(n) = n^4 + 1$$

$$q(n) = n^2 + 3n - k$$

1. stabilire se  $p(n)$  ha radici in  $\mathbb{Z}_7[n]$
2. determinare  $k \in \mathbb{Z}_7$  per cui  
 $p(n)$  è divisibile per  $q(n)$