

# ANELLI - riassunto

$(A, +, \cdot)$  anello se  $(A, +)$  gruppo abeliano, NEUTRO: 0, INVERSO: opposto  
 $(A, \cdot)$  semigrupp  
 $(a+b) \cdot c = a \cdot c + b \cdot c$ ,  $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in A$

Regole di calcolo simili a quelle di  $(\mathbb{Z}, +, \cdot)$  ma attenzione:

- 1)  $\cdot$  può non essere commutativa (vedi prod. matrici in  $M_n(\mathbb{R})$ )
- 2)  $(A, \cdot)$  può non essere un monoide (vedi  $(2\mathbb{Z}, +, \cdot)$ )
- 3) possono esistere divisori di zero (vedi  $(\mathbb{Z}_6, +, \cdot)$ ) pag 182-183

- Se  $\cdot$  commutativa: anello commutativo
- Se  $(A, \cdot)$  monoide: anello con unità (elem. neutro risp.)
- Se  $(A, +, \cdot)$  commutativo, con unità e NON ha divisori di zero: dominio di integrità ( $\Rightarrow$  legge di ANNULLAMENTO del PRODOTTO) pag. 183 teor.

Gli anelli con unità hanno almeno 2 elementi:  $0_A, 1_A$

$(\mathbb{Z}_2, +, \cdot)$  ha solo quelli! pag 183 bis

$\rightarrow$  Se  $(A, +, \cdot)$  è anello comm. con  $1_A$  e  $\forall a \neq 0_A$  esiste  $a^{-1}$ : campo.

Oltre a  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  sono campi  $(\mathbb{Z}_p, +, \cdot)$  con  $p$  primo pag 184

Nei campi si ha la stessa aritmetica che in  $(\mathbb{Q}, +, \cdot)$

- \* un dominio di integrità finito è un campo. pag 185
- \* (Piccolo teor. di FERMAT):  $\forall a \in \mathbb{Z}, \forall p \in \mathbb{N}$  PRIMO, si ha  $a^p \equiv a \pmod{p}$  pag 186

## Sottostrutture di anelli

- sottoanello  $S$ :  $S$  sottogruppo risp.  $+$   
 $S$  sottosemigr. rispetto a  $\cdot$   
e se  $A$  ha unità questo deve appartenere a  $S$  pag 188
  - ideale  $I$ :  $I$  sottogruppo risp.  $\cdot$   
 $\forall a \in A, \forall i \in I$  si ha  $ai \in I$  e  $ia \in I$  pag 190
- Se  $S \neq A$  un sottoanello non è un ideale.

- Omomorfismi di anelli :  $f : (A, +, \cdot) \rightarrow (B, +, \cdot)$

deve essere omom. di gruppo pensato come  $f : (A, +) \rightarrow (B, +)$   
di semi-gr. " "  $f : (A, \cdot) \rightarrow (B, \cdot)$

pag 189

e se  $A \ni 1_A$  anche di monoidi  $f : (A, \cdot) \rightarrow (B, \cdot)$

- L'immagine  $f(S)$  di un sottoanello di  $A$  è un sottoanello di  $B$

- L'immagine  $f(I)$  di un ideale di  $A$  è un ideale di  $f(A)$  ma non è detto che sia un ideale di  $B$ .

- Il nucleo di  $f$ ,  $\ker f = \{ a \in A \mid f(a) = 0_B \}$  è ideale di  $A$  e similmente per  $f^{-1}(J)$ ,  $J$  ideale di  $B$ . pag 190

\* Se  $A \ni 1_A$ , l'unico ideale di  $A$  che contiene  $1_A$  è  $A$ . pag 191

\* Se  $A$  comm. con  $1_A$  i laterali additivi di ogni ideale  $I$  di  $A$  formano una partizione di  $A \Rightarrow$  rel. di equivalenza  $\Rightarrow$  quoziente:

$$\frac{A}{I} = \{ I+a, a \in A \}$$

È un anello comm. con unità  $I+1_A$  rispetto a

$$(I+a) \oplus (I+b) = I + (a+b)$$

$$(I+a) \odot (I+b) = I + ab$$

e  $f : A \rightarrow \frac{A}{I}$  pag 192

$$f(a) = I+a$$

è un omomorf. di anelli con unità, di nucleo  $I$ .

Fare la prova con  $A = \mathbb{R}[x]$ ,  $I = d(x) \cdot \mathbb{R}[x]$  e:

$d(x) = x^2+1$ ;  $d(x) = x^2-1$ ;  $d(x) = x^2$ .  
pag 192 pag 193 pag 193

- Polinomi a coefficienti in un campo: come di  $\mathbb{R}[x]$

pag 194 195

Sono un modo per costruire esempi finiti di ordine non primo. Ad es. se voglio un campo di ordine 4, cerco un polinomio di  $\mathbb{Z}_2[x]$  di

ordine 2 e irriducibile in  $\mathbb{Z}_2[x] - x^2+x+1 -$  e faccio il quoziente  $\mathbb{Z}_2[x]/(x^2+x+1) \cong \mathbb{Z}_4$  come  $\mathbb{Z}/4\mathbb{Z}$

$$\frac{\mathbb{Z}}{5\mathbb{Z}} = \{ 5\mathbb{Z} + 0, 5\mathbb{Z} + 1, 5\mathbb{Z} + 2, 5\mathbb{Z} + 3, 5\mathbb{Z} + 4 \}$$

" 0 nel quoziente"

parte da  $(\mathbb{Z}, +, \cdot) = (\mathbb{Z}, +, \cdot)$   
 $I = 5\mathbb{Z}$

↕

Rappresentanti: i resti nella div. per 5

$\mathbb{Z}_5$

$$5\mathbb{Z} + r = [r]_5$$

$$(5\mathbb{Z} + a) + (5\mathbb{Z} + b) = 5\mathbb{Z} + (a+b)$$

$$[a]_5 + [b]_5 = [a+b]_5$$

$$(5\mathbb{Z} + a) \cdot (5\mathbb{Z} + b) = 5\mathbb{Z} + ab$$

$$[a]_5 \cdot [b]_5 = [ab]_5$$

c'è isomorfismo tra  $\mathbb{Z}_5$  e  $\frac{\mathbb{Z}}{5\mathbb{Z}}$ .

mediante il passaggio al quoziente

Si possono creare campi con ordine  $p^n$

qualunque  $p \in \mathbb{N}$  primo.

Per prima cosa prendo tutti i polinomi a coefficienti in  $\mathbb{Z}_p$ :  $\mathbb{Z}_p[x]$ . Operazioni e proprietà come in  $\mathbb{R}[x]$ .  
Ad esempio:

$$\mathbb{Z}_3[x] = \left\{ \sum_{i=1}^n a_i x^i, a_i \in \mathbb{Z}_3, n \in \mathbb{N} \right\}$$

$[0]_3, [1]_3, [2]_3 = [-1]_3$  sono i soli elem. di  $\mathbb{Z}_3$ , quindi sono i "valori" che possono assumere gli  $a_i$ .  
Anche qui vale il teorema del quoziente e resto e tutta la teoria della divisibilità.

IRRIDUCIBILITÀ:

di grado

$p(x) \in \mathbb{Z}_3[x]$  è irrid. se non esistono

$a(x), b(x) \in \mathbb{Z}_3[x]$  t.c.  $p(x) = a(x)b(x)$  e  $\begin{cases} 0 < \text{grad } a(x) < \text{grad } p(x) \\ 0 < \text{grad } b(x) < \text{grad } p(x) \end{cases}$

Ad es. quali polinomi sono irriducibili in

R4

$\mathbb{Z}_2[x]$ ?

un po' di noi pol. irriduc.:

quelli di f. 1 :  $[0] + [1]x = x$

$$[1] + [1]x = 1 + x$$

di grado 2 :  $x^2 = x \cdot x$  NO irriduc.

$$x^2 + x = x(x+1) \quad \text{" "}$$

$$x^2 + 1 = (x+1)^2 \quad \text{NO irriduc.}$$

$$x^2 + x + 1 \quad \text{IRRIDUC. PERCHÉ}$$

se fosse riducibile avrei

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

$\Rightarrow -a$  è una radice di  $x^2 + x + 1$

cioè  $x^2 + x + 1$  è riducibile se (e solo se)

ha una radice in  $\mathbb{Z}_2$

Usa RUFFINI

$a=0$  ,  $a=1$  sono le radici ipotetiche

$$p(x) = x^2 + x + 1 \quad : \quad p(0) = 1 \neq 0 \Rightarrow 0 \text{ non è una radice}$$

$$p(1) = 1 + 1 + 1 = 1 \neq 0 \Rightarrow 1 \text{ non è una radice}$$

Considero l'ideale di  $\mathbb{Z}_2[x]$  :  $p(x)\mathbb{Z}_2[x] = I$

$$\left( \begin{array}{l} \forall a(x) \in \mathbb{Z}_2[x] \\ \forall b(x) \end{array} \right) : \quad p(x)a(x) - p(x)b(x) = p(x)(a(x) - b(x)) \in p(x)\mathbb{Z}_2[x]$$

è sgr di  $(\mathbb{Z}_2[x], +)$

$$b(x)(\underbrace{p(x)a(x)}_{\in I}) = p(x)(a(x)b(x)) \quad : \text{ è un ideale}$$

Laterali di I in  $\mathbb{Z}_2[x]$

$$I = (x^2+x+1) \mathbb{Z}_2[x] = p(x) \mathbb{Z}_2[x]$$

$$I + 0, I + 1, I + x, I + x + 1$$

Laterali che hanno rappresentante un polinomio di grado  $< \text{gr } p(x)$

Altri?

$$I + x^2 = \{ a(x) + x^2, a(x) \in I \} = \{ (x^2+x+1)q(x) + x^2 \mid q(x) \in \mathbb{Z}_2[x] \}$$

Se divido  $x^2$  per  $x^2+x+1$ ?

$$\begin{array}{r}
 x^2 \\
 -x^2 - x - 1 \\
 \hline
 -x - 1 \\
 \parallel \\
 x + 1
 \end{array}$$

$$\left. \begin{array}{l}
 x^2+x+1 \\
 1
 \end{array} \right\} (\mathbb{Z}_2[x])$$

$$(x^2+x+1)q(x) + x^2 = (x^2+x+1)q(x) + (x^2+x+1) \cdot 1 + (x+1) =$$

$$= \underbrace{(x^2+x+1)(q(x)+1)} + (x+1) \in I + (x+1)$$

In generale tutti i polinomi di  $\mathbb{Z}_2[x]$  appartengono a uno dei 4 laterali

$$\{ I + 0 = I, I + 1, I + x, I + x + 1 \}$$

Essi sono il quoziente  $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)\mathbb{Z}_2[x]}$

Se in  $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$  introduco  $+ e \cdot$  come  
indicato nei precedenti

ho un anello comm. con unità  $I+1$   
privo di div. di zero. Infatti

$$(I + a(x))(I + b(x)) = I + 0, \text{ cioè}$$

$$I + a(x)b(x) = I + 0$$

$$\Leftrightarrow a(x)b(x) - 0 \in I \Leftrightarrow a(x)b(x) \in I \Leftrightarrow$$

$$a(x)b(x) = (x^2+x+1) \cdot q(x)$$

irriducibile significa che se  $x^2+x+1$  divide  
 $a(x)b(x)$  allora divide uno dei due fattori

Ad es.  $a(x) = (x^2+x+1)d(x)$  oppure

$$\Rightarrow I + a(x) = I + (x^2+x+1)d(x) = I + 0$$

$\mathbb{Z}$  finito, privo di div. di zero  $\Rightarrow$  campo.

Cerchiamo la tabella moltiplicativa  
e additiva di  $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$

$$[0] = I \quad ; \quad I+1 = [1] \quad , \quad I+x = [x] \quad , \quad I+x+1 = [x+1]$$

$$I = (x^2 + x + 1) \text{ in } \mathbb{Z}_2[x]$$

$$(I+1)(I+1) = I + (x+1) = I \neq 0$$

$$(I+x)(I+x) = I + 2x = I \neq 0$$

+	[0]	[1]	[x]	[1+x]
[0]	[0]	[1]	[x]	[1+x]
[1]	[1]	[0]	[1+x]	[x]
[x]	[x]	[1+x]	[0]	[1]
[1+x]	[1+x]	[x]	[1]	[0]

$$[x]^2 = [1+x] \text{ pag. 5}$$

$$[x] \cdot [1+x] = [x+x^2] = [x+x+1] = [1]$$

·	[0]	[1]	[x]	[1+x]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[1+x]
[x]	[0]	[x]	[x+1]	[1]
[1+x]	[0]	[1+x]	[1]	[x]

$$\begin{aligned} [1+x]^2 &= [1+x^2] = \\ &= [1] + [x^2] = \\ &= [1] + [1+x] = \\ &= [0+x] \end{aligned}$$

Il gruppo moltiplicativo è generato da [x]:

$$[x], [x]^2 = [x+1], [x]^3 = [1]$$

Questa è la coppia di tabelle che danno le operazioni del campo di ord. 4

Queste cose si trovano ad es. a pag. 197



$$\begin{aligned}
 x^3 &= (x^3 + x^2 + 1) + x^2 + 1 \text{ in } \mathbb{Z}_2[x] \Rightarrow [x^3] = [x^2 + 1] \\
 x(1+x^2) &= x + x^3 = (x^3 + x^2 + 1) + x^2 + x + 1 \Rightarrow [x + x^3] = [x^2 + x + 1] \\
 x(x+x^2) &= x^2 + x^3 = (x^3 + x^2 + 1) + 1 \Rightarrow [x^2 + x^3] = [1] \\
 x(1+x+x^2) &= x + x^2 + x^3 = (x^3 + x^2 + 1) + 1 + x \Rightarrow [x + x^2 + x^3] = [1 + x] \\
 (1+x)^2 &= 1 + x^2 \\
 (1+x)x^2 &= x^2 + x^3 \Rightarrow [x^2 + x^3] = [1] \\
 (1+x)(1+x^2) &= 1 + x + x^2 + x^3 = (x^3 + x^2 + 1) + x \Rightarrow [(1+x)(1+x^2)] = [x] \\
 (1+x)(x+x^2) &= x(1+x^2) \Rightarrow [(1+x)(x+x^2)] = [x^2 + x + 1] \\
 (1+x)(1+x+x^2) &= 1 + x^2 + x^2 + x^3 = 1 + x^3 \Rightarrow [1 + x^3] = [x^2]
 \end{aligned}$$

$$\begin{array}{r}
 x^4 \\
 x^4 + x^3 + x \\
 \hline
 x^3 + x \\
 x^3 + x^2 + 1 \\
 \hline
 x^2 + x + 1
 \end{array}
 \left. \vphantom{\begin{array}{r} x^4 \\ x^4 + x^3 + x \\ \hline x^3 + x \\ x^3 + x^2 + 1 \\ \hline x^2 + x + 1 \end{array}} \right\} \frac{x^3 + x^2 + 1}{x + 1} \Rightarrow$$

$$\begin{aligned}
 x^2(1+x^2) &= x^2 + x^4 \\
 x^2(x+x^2) &= x^3 + x^4 \\
 x^2(1+x+x^2) &= x^2 + x^3 + x^4 \\
 (1+x^2)^2 &= 1 + x^4 \\
 (1+x^2)(x+x^2) &= x + x^2 + x^2(x+x^2) \\
 (1+x^2)(1+x+x^2) &= (1+x^2)^2 + x(1+x^2) \\
 (x+x^2)(x+x^2) &= x^2(1+x)^2 = x^2 + x^4 \\
 (x+x^2)(1+x+x^2) &= x + x^2 + (x+x^2)^2 \\
 (1+x+x^2)^2 &= 1 + x^2 + x^4
 \end{aligned}$$

$$\begin{aligned}
 [x^2][x^2] &= [x^2 + x + 1] \\
 \Rightarrow [x^2(1+x^2)] &= [x + 1] \\
 \Rightarrow [x^2(x+x^2)] &= [x^2 + 1 + x^2 + x + 1] = [x] \\
 \Rightarrow [x^2(1+x+x^2)] &= [x + x^2] \\
 \Rightarrow [(1+x^2)^2] &= [x^2 + x] \\
 \Rightarrow [(1+x^2)(x+x^2)] &= [x + x^2 + x] = [x^2] \\
 \Rightarrow [(1+x^2)(1+x+x^2)] &= [x^2 + x + x^2 + x + 1] = [1] \\
 \Rightarrow [(x+x^2)(x+x^2)] &= [x + 1] \\
 \Rightarrow [(x+x^2)(1+x+x^2)] &= [x + x^2 + x + 1] = [x^2 + 1] \\
 \Rightarrow [(1+x+x^2)^2] &= [1 + x^2 + x^2 + x + 1] = [x]
 \end{aligned}$$

TABELLA MOLTIPL. (Salto le [ ])

0	1	x	1+x	x <sup>2</sup>	1+x <sup>2</sup>	x+x <sup>2</sup>	1+x+x <sup>2</sup>
0	0	0	0	0	0	0	0
1	0	1	x	1+x <sup>2</sup>	1+x <sup>2</sup>	x+x <sup>2</sup>	1+x+x <sup>2</sup>
x	0	x	x <sup>2</sup>	x+x <sup>2</sup>	1+x <sup>2</sup>	1	1+x
1+x	0	1+x	x+x <sup>2</sup>	1+x <sup>2</sup>	1	x	1+x+x <sup>2</sup>
x <sup>2</sup>	0	x <sup>2</sup>	1+x <sup>2</sup>	1	1+x+x <sup>2</sup>	x	x+x <sup>2</sup>
1+x <sup>2</sup>	0	1+x <sup>2</sup>	1+x+x <sup>2</sup>	x	1+x	x+x <sup>2</sup>	x <sup>2</sup>
x+x <sup>2</sup>	0	x+x <sup>2</sup>	1	1+x+x <sup>2</sup>	x	x <sup>2</sup>	1
1+x+x <sup>2</sup>	0	1+x+x <sup>2</sup>	1+x	x <sup>2</sup>	x+x <sup>2</sup>	1	1+x <sup>2</sup>

Nota:  $[x], [x^2], [x^3] = [1+x^2], [x^4] = [1+x+x^2], [x^5] = [1+x], [x^6] = [x+x^2], [x^7] = [1]$ : cioè ogni elem.  $\neq [0]$  nel quoziente è una potenza di  $[x]$   
 $\Rightarrow$  questi elem. formano un gruppo ciclico di ordine 7.