

Def. (Omorfismo di anelli):

$\varphi: R \rightarrow S$ (con R, S anelli) è un **OMORFISMO** se $\forall a, b \in R$:

$$1) \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$2) \varphi(ab) = \varphi(a)\varphi(b)$$

$$3) \varphi(1) = 1$$

N.B.

La richiesta $\varphi(1) = 1$ è IMPORTANTE !!! Infatti:

data P matrice di proiezione in $M_{n \times n}(\mathbb{C})$ sappiamo che $P^2 = P$, MA non è detto $P = Id$!!!

Se $\exists a^{-1}$, posso dire che $\varphi(a^{-1}) = \varphi(a)^{-1}$? Sì:

$$\varphi(a)\varphi(a^{-1}) = \varphi(1) = 1 = \varphi(a^{-1})\varphi(a)$$

$$\Leftrightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$$

In particolare, φ è un omorfismo di gruppi additivi. Il suo nucleo è:

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}$$

Ciò che valeva per gli omorfismi di gruppi continua a valere ancora:

$$\varphi \text{ iniettivo} \Leftrightarrow \ker \varphi = \{0\}$$

Esempi:

1) $\chi_R: \mathbb{Z} \rightarrow R$ è un omorfismo di anelli:
 $m \mapsto \hat{m} \cdot 1$

$$1) \chi_R(m+n) = \chi_R(m) + \chi_R(n)$$

$$2) \chi_R(mn) = \hat{m}\hat{n} \cdot 1 = (\hat{m} \cdot 1)(\hat{n} \cdot 1)$$

$$3) \chi_R(1) = \hat{1} \cdot 1 = 1$$

Se $\text{Ker } \chi_R = k\mathbb{Z}$ con $k \geq 0$, k si dice **CARATTERISTICA**
di R ed è t.c.:

- 1) $k=0 \Rightarrow \chi_R$ iniettivo
- 2) $k > 0 \Rightarrow \widehat{k}a = 0 \quad \forall a \in R$
 $(\widehat{k}a = (\widehat{k}\widehat{1})a = \widehat{0}_a = 0)$

$\Rightarrow k$ è il minimo intero positivo t.c. $\widehat{k}a = 0 \quad \forall a \in R$.

Un anello ha caratteristica 0 oppure p (con p primo),
supponiamo che la caratteristica sia $k > 0$, allora se
 $k = mn$ con $m, n > 1$:

$$0 = \chi_R(k) = \chi_R(mn) = \chi_R(m)\chi_R(n)$$

$$\Leftrightarrow \chi_R(m) = 0 \vee \chi_R(n) = 0 \quad (\text{da } m, n \notin k\mathbb{Z})$$

2) Se R sottanello di S , $R \xrightarrow{\varphi} S$ (inclusione) è un
omorfismo

Def. (Isomorfismo di anelli):

$\varphi: R \rightarrow S$ (con R, S anelli) è un **ISOMORFISMO** se è un
omorfismo biiettivo.

Proposizione (Proprietà (Universale) dell'anello dei polinomi):

Se $\varphi: R \rightarrow S$ è un omorfismo di anelli commutativi
ed $s \in S$ arbitrario, allora $\exists!$ omorfismo di anelli

$\varphi_s: R[x] \rightarrow S$ t.c. :

- 1) $\varphi_s(a) = \varphi(a) \quad \forall a \in R$
- 2) $\varphi_s(x) = s$ (dove x è una indeterminata)

Dim.:

1) !: supponiamo che $\exists \mathcal{C}_S$ e che rispetti le 2 proprietà. Se $f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$, allora :

$$\begin{aligned}\mathcal{C}_S(f(x)) &= \mathcal{C}_S(a_0) + \dots + \mathcal{C}_S(a_n) \mathcal{C}_S(x)^n \\ &= \mathcal{C}(a_0) + \mathcal{C}(a_1) s + \dots + \mathcal{C}(a_n) s^n\end{aligned}$$

2) \exists : definiamo $\mathcal{C}_S(a_0 + a_1 x + \dots + a_n x^n) = \mathcal{C}(a_0) + \dots + \mathcal{C}(a_n) s^n$ e mostriamo che è un automorfismo.

q.e.d.

N.B.

Se $R \subseteq S$, si definisce \mathcal{C}_S mediante l'inclusione:

$$\mathcal{C}_S(a_0 + \dots + a_n x^n) = a_0 + \dots + a_n s^n$$

cioè permette di definire il concetto di radice di un polinomio:

s è radice di $a_0 + \dots + a_n x^n$ se $a_0 + \dots + a_n s^n = 0$

Se $f(x) = a_0 + \dots + a_n x^n$, scrivereemo $f(s) = a_0 + \dots + a_n s^n$

Teorema (di Ruffini):

Dati S anello commutativo, $R \subseteq S$ sottoanello, si ha che $s \in S$ è radice di $f(x) \in R[x]$ se e solo se $(x-s)$ divide $f(x)$ in $S[x]$

N.B.

1) Tale divisione si può sempre fare in qualsiasi anello dato che $x-s$ è unico !!!

2) $R[x] \subseteq S[x]$ dato che $R \subseteq S$.

Dim.:

\Leftrightarrow : $f(x) = (x-s)g(x) + c$ con $g(x), c \in S[x]$,
 c costante. Sappiamo che:

$$\mathcal{C}_S(f(x)) = \underbrace{\mathcal{C}_S(x-s)}_{=0} \mathcal{C}_S(g(x)) + c = c$$

$$\Rightarrow c = 0$$

q.e.d.

\Rightarrow l'immagine di \mathcal{C}_S si denota con $R[S]$ (caso in cui $\varphi: R \rightarrow S$ è l'inclusione)

Esercizio:

Dim. che l'immagine di un omomorfismo è sottounello del codominio.

$\Rightarrow R[S]$ è il minimo sottounello di S contenente R ed s :

$$R[S] = \{a_0 + \dots + a_n s^n \mid a_i \in R\}$$

Esempio:

Sappiamo che $\mathbb{Q} \subseteq \mathbb{R}$, ma $s = \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, e sia \mathcal{C} l'inclusione di \mathbb{Q} in \mathbb{R} . Calcoliamo:

$$\mathcal{C}_S(x^2 - 2) = s^2 - 2 = (\sqrt{2})^2 - 2 = 0$$

Inoltre:

$$\sqrt{2}^{2m} = 2^m \in \mathbb{Q}$$

$$\sqrt{2}^{2m+1} = 2^m \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$$

quindi $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. La scrittura di $v \in \mathbb{Q}[\sqrt{2}]$ come $v = a + b\sqrt{2}$ è unica! Infatti:

$$a + b\sqrt{2} = c + d\sqrt{2} \text{ con } b \neq d \Rightarrow \sqrt{2} = \frac{c-a}{b-d} \in \mathbb{Q} \not\models$$

$$\Rightarrow b=d, a=c.$$

Determiniamo il nucleo $\ker \varphi_s$:

$$\varphi(x) \in \ker \varphi_s \Leftrightarrow \varphi(x) = (x^2 - 2)g(x) + a + bx$$

con $g(x) \in \mathbb{Q}[x]$, $a, b \in \mathbb{Q}$ ($x^2 - 2$ è unico)

$$\Rightarrow 0 = \varphi_s(\varphi(x)) = \underbrace{\varphi_s(x^2 - 2)}_{=0} \varphi_s(g(x)) + a + bs$$

$$= a + bs$$

$\Rightarrow a = b = 0 \Rightarrow \varphi(x)$ è divisibile per $x^2 - 2$

Se invece di $\sqrt{2}$ prendiamo \sqrt{d} (con $d \in \mathbb{Z}^+$ non quadrato) si procede allo stesso modo. Sia ora $s = \sqrt[3]{2}$, si ha:

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

Infatti:

$$a + b\sqrt[3]{2} = 0 \Rightarrow (a + b\sqrt[3]{2})(a - b\sqrt[3]{2}) = 0$$

$$\Rightarrow a^2 = 2b^2 \Rightarrow \text{se } b \neq 0 \quad \left(\frac{a}{b}\right)^2 = 2 \not\models$$

Congruenze:

Def. (Congruenza):

Una CONGRUENZA su un anello R è una relazione di equivalenza \sim t.c.:

$$a \sim b \wedge c \sim d \Rightarrow a+c \sim b+d \wedge ac \sim bd$$

$$\forall a, b, c, d \in R$$

Esempio:

1) Definiamo $\sim_{\mathbb{Z}}$ su \mathbb{R} t.c.:

$$a \sim_{\mathbb{Z}} b \Leftrightarrow a - b \in \mathbb{Z}$$

$\Rightarrow \sim_{\mathbb{Z}}$ è relazione di equivalenza, MA NON È congruenza:

$$c \sim_{\mathbb{Z}} d \not\Rightarrow ac \sim_{\mathbb{Z}} bd$$

2) Definiamo $\sim_{m\mathbb{Z}}$ su \mathbb{Z} t.c.:

$$a \sim_{m\mathbb{Z}} b \Leftrightarrow a - b \in m\mathbb{Z}$$

$\Rightarrow \sim_{m\mathbb{Z}}$ è relazione di equivalenza ed è congruenza:

$$a \sim_{m\mathbb{Z}} b \wedge c \sim_{m\mathbb{Z}} d \Rightarrow a - b, c - d \in m\mathbb{Z}$$

$$\Rightarrow a - b = mx, c - d = my$$

$$\begin{aligned} \Rightarrow (a+c) - (b+d) &= (a - b) + (c - d) = mx + my \\ &\stackrel{|}{=} m(x+y) \in m\mathbb{Z} \end{aligned}$$

$$\Rightarrow a+c \sim_{m\mathbb{Z}} b+d$$

$$\begin{aligned} \Rightarrow ac - bd &= ac - bc + bc - bd = (a-b)c + b(c-d) \\ &\stackrel{|}{=} mxc + myb \\ &\stackrel{|}{=} m(xc + yb) \in m\mathbb{Z} \end{aligned}$$

$$\Rightarrow ac \sim_{m\mathbb{Z}} bd$$

Si ha che, data \sim congruenza su un anello R , su R/\sim si possono definire le seguenti operazioni:

$$1) [a] + [b] = [a+b]$$

$$\forall a, b \in R$$

$$2) [a] \cdot [b] = [ab]$$

Tali operazioni NON DIPENDONO dai rappresentanti delle classi di equivalenza, infatti:

mostriamo che $[a+b] = [c+d]$, $[ab] = [cd]$

$\forall a, b, c, d \in R$ t.c. $a \sim c$, $b \sim d$.

\Rightarrow deve essere $a+b \sim c+d$, $ab \sim cd$ MA ciò è
ESATTAMENTE la definizione di congruenza.

$\Rightarrow a \sim c$, $b \sim d \Rightarrow a+b \sim c+d$, $ab \sim cd$
 \sim è congruenza

Quindi R/\sim è un anello rispetto a tali operazioni,
con elemento neutro rispetto a $+ [0]$ rispetto a $\circ [1]$.
Vale inoltre che $\pi: R \rightarrow R/\sim$ con $\pi(a) = [a]$ è
un omomorfismo con nucleo $\text{Ker } \pi = [0]$. Inoltre
 $[0]$ è sottogruppo di $(R, +)$:

1) $0 \in [0]$

2) $a \in [0] \Rightarrow a \sim 0 \Rightarrow -a \sim -a$

$$\Rightarrow a - a \sim 0 - a \Rightarrow 0 \sim -a \Rightarrow -a \sim 0$$

$$\Rightarrow -a \in [0]$$

3) $a, b \in [0] \Rightarrow a \sim 0 \wedge b \sim 0 \Rightarrow a+b \sim 0+0$

$$\Rightarrow a+b \sim 0 \Rightarrow a+b \in [0] \quad (\sim \text{ è congruenza})$$

Allora, se $I = [0]$, \sim è esattamente \sim_I del Teorema
di Lagrange:

1) $a \sim b \Leftrightarrow a \sim b \wedge -b \sim -b$

$$\Rightarrow a - b \sim b - b \Rightarrow a - b \sim 0 \Rightarrow a - b \in I$$

2) $a - b \in I \Rightarrow a - b \sim 0 \wedge b \sim b$

$$\Rightarrow a - b + b \sim 0 + b \Rightarrow a \sim b$$

Le classi di equivalenza sono invece le classi

laterali $a + I$ e quindi si ha:

$$1) (a + I) + (b + I) = (a + b) + I$$

$$2) (a + I)(b + I) = ab + I$$

Quindi di R/\sim scriveremo R/I , dove $I = [0]$ è il NUCLEO della congruenza \sim . Si ha:

$$a \cdot 0 = 0_a = 0 \quad \forall a \in R$$

$$\Rightarrow x \in [0] = \{1, a \in R\}$$

$$\Rightarrow [a][x] = [ax]$$

$$= [a] \cdot [0] = [a \cdot 0] = [0] = I$$

$$\Rightarrow ax \in I \text{ e analogamente } xa \in I$$

Def. (Ideale):

Un sottinsieme I di un anello R è un IDEALE se:

$$1) 0 \in I$$

$$2) x+y \in I \quad \forall x, y \in I$$

$$3) ax \in I \wedge xa \in I \quad \forall x \in I \quad \forall a \in R$$

In particolare, I è sottogruppo di $(R, +)$:

$$x \in I \Rightarrow -1 \cdot x \in I \text{ per (3)} \Rightarrow -x \in I$$

Proposizione:

1) Il nucleo di una congruenza è un ideale.

2) Se $I \subseteq R$ è un ideale, la relazione \sim_I t.c.

$$a \sim_I b \Leftrightarrow a-b \in I \quad \forall a, b \in R$$

è una congruenza.

Dim.:

1) già visto ✓

2) Supponiamo $a \sim_I b, c \sim_I d$. Allora:

$$\begin{aligned} a-b &= x \in I, c-d = y \in I \Rightarrow (a+c)-(b+d) \\ &= (a-b)+(c-d) = x+y \in I \end{aligned}$$

Moltre:

$$\begin{aligned} ac-bd &= ac+bc-bc-bd = (a-b)c+b(c-d) \\ &= xc+by \in I \end{aligned}$$

q.e.d.

Esempi:

1) Il nucleo di un omomorfismo di anelli è un ideale:

$$\begin{aligned} \varphi: R &\rightarrow S \text{ omomorfismo} \Rightarrow x \in \text{Ker } \varphi, a \in R \\ \Rightarrow \varphi(ax) &= \varphi(a)\varphi(x) = \varphi(a)0 = 0 \\ \Rightarrow \varphi(xa) &= \varphi(x)\varphi(a) = 0\varphi(a) = 0 \end{aligned}$$

2) Dato I ideale e \sim_I congruenza, si ha che $R/\sim_I = R/I$ è un anello e $\pi: R \rightarrow R/I$ con $\pi(a) = a+I$ è un omomorfismo di nucleo I

3) L'unico sottanello di R che è anche un ideale è R stesso:

in un sottanello c'è 1, e quindi anche $1a=a$ (per le proprietà degli ideali)

4) $\{0\}$ è un ideale

5) Gli ideali di \mathbb{Z} sono i sottinsiemi di $m\mathbb{Z}$, con $m \geq 0$.

Infatti:

$$x, y \in m\mathbb{Z} \Rightarrow x = my \Rightarrow ax = a my = may \in m\mathbb{Z}$$

Proposizione:

$\mathbb{Z}/m\mathbb{Z}$ ha caratteristica m

Dim.:

L'unico monomorfismo $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ è $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$

E.c. $\pi(a) = a + m\mathbb{Z}$ e ha nucleo $\ker \pi = m\mathbb{Z}$

q.e.d.
