

Proposizione:

Sia $\varphi: R \rightarrow S$ un omorfismo di anelli. Valgono le seguenti:

- 1) R_0 sottogruppo di $R \Rightarrow \varphi^*(R_0)$ sottogruppo di S
- 2) S_0 sottogruppo di $S \Rightarrow \varphi^*(S_0)$ sottogruppo di R .

N.B.

Non è in generale vero che se I è un ideale di R allora $\varphi^*(I)$ è un ideale di S :

(es. $\varphi: \mathbb{Z} \rightarrow \mathbb{Q}$ l'inclusione di \mathbb{Z} in \mathbb{Q} ↪)

Tuttavia ciò accade se φ è SURIETTIVA:

I ideale di R , $\varphi^*(I)$ è un ideale di S

(è sicuramente un sottogruppo additivo, inoltre

$$x \in \varphi^*(I), a \in S \Rightarrow x = \varphi(y) \text{ con } y \in I,$$

$a = \varphi(b)$ con $b \in R$ dato che φ suriettiva.

$$\Rightarrow xa = \varphi(y)\varphi(b) = \varphi(yb) \in \varphi^*(I) \text{ dato che}$$

$$yb \in I \Rightarrow \text{analogoamente } ax \in \varphi^*(I))$$

Proposizione:

Se J è ideale di S , allora $\varphi^{-1}(J) \supseteq \ker \varphi$ è un ideale di R .

Teorema (fondamentale dell'omorfismo):

Se $\varphi: R \rightarrow S$ è un omorfismo di anelli, $\exists!$

omorfismo di anelli $\hat{\varphi}: R/\ker \varphi \rightarrow S$ t.c. $\hat{\varphi} \circ \pi = \varphi$

Si ha:

$$\begin{array}{ccc}
 R & \xrightarrow{\varphi} & S \\
 \pi \downarrow & \nearrow \hat{\varphi} & \\
 R/\ker \varphi & &
 \end{array} \Rightarrow \boxed{\hat{\varphi} \circ \pi = \varphi}$$

Proposizione:

Supponiamo $\varphi: R \rightarrow S$ un omomorfismo di anelli unitivo. Dato I ideale di R , si ha che la mappa $I \rightarrow \varphi^{-1}(I)$ è una biiezione tra l'insieme degli ideali di R contenenti $\ker \varphi$ e l'insieme degli ideali di S .

Dim.:

$$1) I \text{ ideale di } R \Rightarrow I = \varphi^{-1}(\varphi(I)) \Leftrightarrow I \supseteq \ker \varphi$$

N.B.

$I \supseteq \varphi^{-1}(\varphi(I))$ è vero $\forall I$ sottinsieme di R .

Se I è ideale di R , allora $I \supseteq \varphi^{-1}(\varphi(I))$ se e solo se $I \supseteq \ker \varphi$:

$$\Rightarrow I \supseteq \ker \varphi$$

$$\Leftarrow a \in \varphi^{-1}(\varphi(I)) \Rightarrow \varphi(a) \in \varphi(I) \Rightarrow \varphi(a) = \varphi(x)$$

con $x \in I$. Quindi $a - x \in \ker \varphi$

$$\Rightarrow a = \underbrace{x}_{\in I} + \underbrace{(a-x)}_{\in \ker \varphi} \in I$$

$$2) J \text{ ideale di } S \Rightarrow J = \varphi^-(\varphi^-(J))$$

q.e.d.

Proposizione:

Siano S sottogruppo di R , I ideale di R . Allora:

- 1) $S+I$ è un sottogruppo di R
- 2) $S \cap I$ è un ideale di S
- 3) $S/(S \cap I) \cong (S+I)/I$

Dim.:

1) $a, b \in S, x, y \in I$:

$$\Rightarrow (a+x) + (b+y) = (a+b) + (x+y) \in S+I$$

$$\Rightarrow -(a+x) = (-a) + (-x) \in S+I$$

$$\Rightarrow 0 \in S, 0 \in I \Rightarrow 0 \in S+I$$

$$\Rightarrow 1 \in S, 0 \in I \Rightarrow 1 \in S+I$$

$$\Rightarrow (a+x)(b+y) = \underset{S}{\underset{\cap}{a}} b + \underset{I}{\underset{\cap}{a}} y + \underset{I}{\underset{\cap}{x}} b + xy \in S+I$$

2) ovvio ✓

3) considero $\varphi: S \rightarrow (S+I)/I$ con $\varphi(a) = [a+I]$

$$\Rightarrow \text{Ker } \varphi = \{a \in S \mid a+I = 0+I\} = S \cap I$$

$\Rightarrow \varphi$ è suriettivo:

$$a \in S, x \in I \Rightarrow (a+x) + I = (a+I) + (x+I)$$

$$= (a+I) + (0+I) = a+I = \varphi(a)$$

\Rightarrow per il teorema di omomorfismo $\exists! \hat{\varphi}$ t.c. $\varphi = \hat{\varphi} \circ \pi$
iettivo (sempre) e suriettivo (perché φ è
suriettivo)

$\Rightarrow \varphi$ è isomorfismo

q.e.d.

Esempio:

I ideale di $R \Rightarrow R \xrightarrow{\pi} R/I$ è un omorfismo suriettivo con nucleo I . Gli ideali di R/I sono della forma $S/I = \pi^{-1}(S)$ con S ideale di R t.c. $I \subseteq S$

Ideali principali:

Def. (Ideale Principale):

Se R è un anello commutativo e $a \in R$, l'insieme $aR = \{ab \mid b \in R\}$ è un ideale di R ed è detto IDEALE PRINCIPALE di R

Verifichiamo che aR è effettivamente un ideale:

$$1) 0 \in aR \quad (0 = a0)$$

$$2) x, y \in aR \Rightarrow x = ab, y = ac, \quad b, c \in R$$

$$\Rightarrow x + y = a(b+c) \in aR$$

$$3) x \in aR, b \in R \Rightarrow x = ac \Rightarrow xb = (ab)c \in aR$$

N.B.

$a \in aR$ dato che $a = a \cdot 1$.

$\Rightarrow aR$ è il più piccolo ideale di R che contiene a .

Proposizione:

Ogni ideale di \mathbb{Z} è un ideale principale in \mathbb{Z} .

Esistono ideali non principali? Sì:

Dati $R = \mathbb{Z}[x]$, $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) \in 2\mathbb{Z}\}$

(temune costante pari), si ha:

$$\varphi_0 : \mathbb{Z}[x] \rightarrow \mathbb{Z} \Rightarrow I = \varphi_0^{-1}(2\mathbb{Z})$$

$\Rightarrow I$ non è principale, se lo fosse esisterebbe

$g(x) \in \mathbb{Z}[x]$ t.c. $g(x)$ genera I . Quindi si avrebbe:

$$\begin{cases} 2 = g(x) h_1(x) \Rightarrow \deg g = \deg h_1 = 0 \\ x = g(x) h_2(x) \end{cases}$$

$$\Rightarrow g(x) = b \in 2\mathbb{Z} \Rightarrow x = b \cdot h_2(x) \Rightarrow \deg h_2 = -1$$

$$\Rightarrow x = b(vx + s) = bvx + bs \quad \leftarrow$$

Proposizione:

Un ideale I di un anello R coincide con R se e solo se contiene un elemento invertibile.

Dim.:

$$\Leftarrow : a \in I \text{ invertibile} \Rightarrow b \in R \Rightarrow b = a(a^{-1}b) \in I$$

$$\Rightarrow : \checkmark$$

q.e.d.

Esempio:

Gli ideali di un campo F sono $\{0\}, F$. (Infatti, se I ideale non è $\{0\}$, allora contiene un elemento invertibile e quindi, per la proposizione, $I = F$).

Proposizione:

Dati F campo, $S \neq \{0\}$ anello, se $\varphi : F \rightarrow S$ è un monomorfismo allora φ è iniettivo (ovvero $1 \notin \text{Ker } \varphi$)

Ideali massimali:

Def. (Ideale Massimale):

Un ideale $I \neq R$ di R è MASSIMALE se:

S ideale di R con $S \supseteq I \Rightarrow S = I \vee S = R$

(\nexists ideali S t.c. $I \subsetneq S \subsetneq R$)

Proposizione (Caratterizzazione degli ideali massimali):

Dati R anello commutativo, I ideale di R , si ha:

I massimale $\Leftrightarrow R/I$ è campo

Dim.:

$\Rightarrow a + I \in R/I$, $a + I \neq 0 + I \Rightarrow a \notin I$.

Consideriamo $S = \{ab + c \mid b \in R, c \in I\}$. S è un ideale di R :

$$1) 0 = a0 + 0 \in S$$

$$2) (ab_1 + c_1) + (ab_2 + c_2) = a(b_1 + b_2) + c_1 + c_2 \in S$$

$$3) ab + c \in S, x \in R$$

$$\Rightarrow (ab + c)x = a(bx) + cx \in S$$

$$I \subseteq S: a0 + c \in S \quad \forall c \in I$$

$$a \in S \Rightarrow a1 + 0 \in S \Rightarrow S \neq I \Rightarrow S = R$$

$$\Rightarrow 1 \in S \Rightarrow 1 = ab + c, c \in I$$

$$\Rightarrow (a + I)(b + I) + (c + I) = (1 + I)$$

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

$\Leftarrow R/I$ campo \Rightarrow supponiamo S sia ideale di R ,

$I \not\subseteq S \Rightarrow \exists a \in S \setminus I \Rightarrow a + I \neq 0 + I$ in R/I
 $\Rightarrow \exists b \in R$ t.c. $(a+I)(b+I) = (1+I)$ ovvero:
 $ab + I = 1 + I \Leftrightarrow ab - 1 \in I$
 \Rightarrow dato che $I \not\subseteq S$, $ab - 1 \in S \Rightarrow 1 - ab \in S$
 $\Rightarrow 1 = (1 - ab) + ab \in S \Rightarrow S = R.$

q.e.d.

Proposizione:

Dati I, S ideali di R , si ha che $I+S = \{x+y \mid x \in I, y \in S\}$ e $I \cap S$ sono anch'essi ideali di R .

\Rightarrow la scrittura IS denota l'insieme di tutte le somme dei prodotti del tipo xy con $x \in I, y \in S$.
 Un generico elemento di IS è:

$$x_1y_1 + \dots + x_ny_n \text{ con } x_i \in I, y_i \in S$$

Proposizione:

Dati I, S ideali di R , si ha che se R è commutativo IS è un ideale di R .

N.B.

Si noti che $IS \subseteq I \cap S$:

$$\begin{aligned} x \in I, y \in S &\Rightarrow xy \in I \quad (x \in I) \wedge xy \in S \quad (y \in S) \\ &\Rightarrow xy \in I \cap S \end{aligned}$$

Esercizio:

R anello commutativo, I, S ideali di R . Dim. che se

$I + S = R$ allora $IS = I \cap S$.

Esempio (ideali massimali / principali ecc... di \mathbb{Z}):

Dato l'anello \mathbb{Z} , chi sono i suoi ideali massimali?

\Rightarrow gli ideali di \mathbb{Z} sono $m\mathbb{Z}$, quando si ha un m massimale?

$\Rightarrow m\mathbb{Z} \subseteq n\mathbb{Z}$ se e solo se $n|m$

Se $m = ab$ con $a, b > 1$ ($\Rightarrow a < m$):

$$m\mathbb{Z} \subsetneq a\mathbb{Z} \subsetneq \mathbb{Z}$$

$\Rightarrow m\mathbb{Z}$ non è massimale

$\Rightarrow 0\mathbb{Z}$ non è massimale: $0\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$

$\Rightarrow 1\mathbb{Z} = \mathbb{Z}$ non è massimale

Proposizione:

Se p è primo, allora $p\mathbb{Z}$ è massimale e $\mathbb{Z}/p\mathbb{Z}$ è un campo

Dim.:

$$p\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z} \text{ con } n|p \Rightarrow n=1 \vee n=p$$

$$\Rightarrow n\mathbb{Z} = \mathbb{Z} \vee n\mathbb{Z} = p\mathbb{Z}.$$

q.e.d.