ARITMETICA 20 NOV 2017

Note Title 11/20/2017

Il teorema di omomorfismo permette di definire un omomorfismo

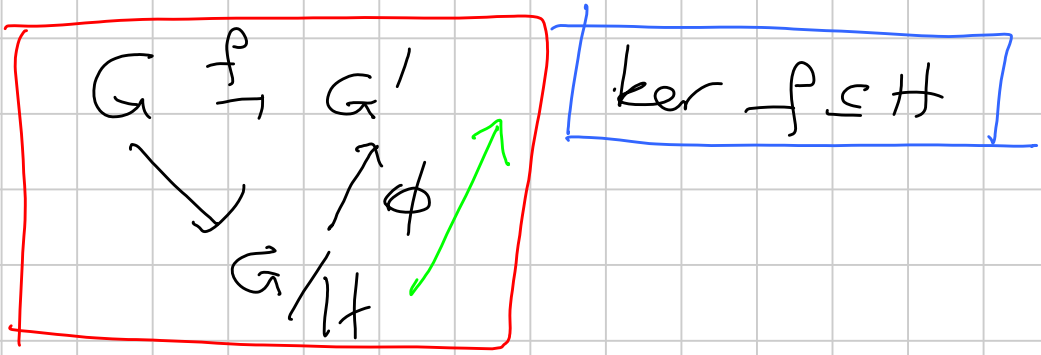
$$\varphi : G/H \to G' \qquad \varphi(xH) = \dots$$

a partire da un omomorfismo

$$f : G \to G'$$

tale che

$$\ker f \subseteq H$$



$\ker f \subseteq H$

e questo definisce un omomorfismo

$$\varphi : G/H \to G'.$$

ISOMORFISMO

Def. Un omomorfismo $f : G \to G'$ si dice un ISOMORFISMO se f è iniettivo e surgettivo.

$$f : \mathbb{R} \to \mathbb{R}_+ \qquad f(x) = e^x$$

$$f^{-1}(y) = \log y.$$

Teorema cinese del resto: $(m,n)=1$.

$$\mathbb{Z}/_{mn\mathbb{Z}} \overset{\text{isomorfo}}{\cong} \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

omomorfismo $f(x) = (\bar{x}_m, \bar{x}_n)$
(sono le proiezioni canoniche)

$$\ker f = \{ x \in \mathbb{Z} \mid x \equiv 0 \pmod m, x \equiv 0 \pmod n \}$$

$m \mid x$, $n \mid x$ $(m,n)=1 \Rightarrow mn \mid x$

$x \equiv 0 \pmod{mn}$

$$\ker f = mn\mathbb{Z}$$

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

π (da $\mathbb{Z}$ a $\mathbb{Z}/_{mn\mathbb{Z}}$), ϕ (da $\mathbb{Z}/_{mn\mathbb{Z}}$ a $\mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$)

ϕ è INIETTIVO.
Il n° di elementi di dominio e immagine è uguale (mn).
Quindi è anche surgettivo.

Consideriamo adesso i gruppi moltiplicativi
$(\mathbb{Z}/_{mn\mathbb{Z}})^*$ $(\mathbb{Z}/_{m\mathbb{Z}})^* \times (\mathbb{Z}/_{n\mathbb{Z}})^*$

(sempre sotto l'ipotesi $(m,n)=1$).

SONO ISOMORFI

Restringo l'isomorfismo

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

ai sottogruppi moltiplicativi $(*)$.

Ricordiamo che se $\bar{x} \in (\mathbb{Z}/mn\mathbb{Z})^*$

allora $\phi(\bar{x}) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

Quindi ho un omomorfismo

$$\phi^* : (\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

$$\left(\phi^*(\bar{a}\bar{b}) = \phi^*(\bar{a})\phi^*(\bar{b}) \right)$$

$$\left[\begin{array}{l} ab + mn\mathbb{Z} \to (ab + m\mathbb{Z},\ ab + n\mathbb{Z}) \\ a + mn\mathbb{Z} \to (a + m\mathbb{Z},\ a + n\mathbb{Z}) \\ b + mn\mathbb{Z} \to (b + m\mathbb{Z},\ b + n\mathbb{Z}) \end{array} \right]$$

E' UN ISOMORFISMO?

SÌ: la surgettività è il teorema cinese del resto: dati a, b $\exists\, x \equiv a \pmod m$ $x \equiv b \pmod n$ e inoltre, se $(a,m)=1$ $(b,n)=1$ allora $(x, mn)=1$,

INIETTIVITA': controlliamo il nucleo.

$\ker \phi^* = \{ x + mn\mathbb{Z} \mid \bar{x}_m = 1 , \bar{x}_n = 1 \}$

cioè $x \equiv 1 \pmod m$, $x \equiv 1 \pmod n$;
cioè $x \equiv 1 \pmod{mn}$.
Quindi $\ker \phi^* = \{\overline{1}\}$, ($\Rightarrow$ iniettivo).

Oss. Se $p \neq q$ sono primi dispari tali che $p \mid m$ $q \mid n$, allora $(m,n) = 1$

$\left(\mathbb{Z}/_{mn\mathbb{Z}}\right)^*$ NON È CICLICO.

Dim. $\left(\mathbb{Z}/_{mn\mathbb{Z}}\right)^* \cong \left(\mathbb{Z}/_{m\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*$

$\left(\mathbb{Z}/_{m\mathbb{Z}}\right)^* = G_1$, $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^* = G_2$

$p-1 \mid \text{ord}(G_1)$ pari

$q-1 \mid \text{ord}(G_2)$ pari

Gli ordini dei due gruppi NON SONO PRIMI fra loro. $\rightarrow$ Il prodotto diretto non può essere ciclico.

ANCORA SUI GRUPPI CICLICI

Corrispondenza fra sottogruppi tramite un omomorfismo.

$f : G \to G'$

$H < G \Rightarrow f(H) < G'$ $\qquad$ $H' < G' \Rightarrow f^{-1}(H') < G$

È una corrispondenza biunivoca? NO.

Se $K = \ker f \neq \{e\}$

$f(\{e\}) = \{e'\}$ $\quad f(K) = \{e'\}$.

$(H \subseteq K \Rightarrow f(H) = \{e'\})$.

Teo. Sia $f: G \to G'$ un omomorfismo surgettivo con $\ker f = K$.

Allora esiste una corrispondenza BIUNIVOCA fra

- i sottogruppi H di G tali che $H \supseteq K$ e
- i sottogruppi H' di G'.

La corrispondenza è data da

$f(H) = H'$ e $f^{-1}(H') = H$.

Dim. Se $H < G$, allora $H' < G'$. (OK)

Se $H' < G'$, allora $H = f^{-1}(H') < G$ (OK)

che contiene K.

Infatti $H' \ni e'$ $\quad f^{-1}(H') \supseteq f^{-1}(\{e'\}) = K$,

Ora dobbiamo vedere che queste due funzioni sono una l'inversa dell'altra, cioè

① $H < G \Rightarrow f^{-1}(f(H)) = H$

② $H' < G' \Rightarrow f(f^{-1}(H')) = H'$.

① È ovvio che $f^{-1}(f(H)) \supseteq H$

(in realtà questo vale per qualsiasi funzione $f: G \to G'$)

Dim. Sia $x \in H$. Allora $f(x) \in f(H)$, cioè $x \in f^{-1}(f(H))$.

D'altra parte, è vero anche che $f^{-1}(f(H)) \subseteq H$

Dim. Sia $x \in f^{-1}(f(H))$ cioè $f(x) \in f(H)$, e quindi esiste $h \in H$ tale che $f(x) = f(h)$

OMOMORFISMI: $f(x) = f(h) \Leftrightarrow xK = hK$ ($K = \ker f$)

$x \in HK = H$

(2) Anche qui c'è una parte ovvia:

$f(f^{-1}(H')) \subseteq H'$

Dim. Sia $x \in f(f^{-1}(H'))$

cioè $x = f(y)$ con $y \in f^{-1}(H')$

cioè $f(y) \in H' \Rightarrow x \in H'$.

Vediamo ora che $H' \subseteq f(f^{-1}(H'))$.

Sia $y' \in H'$ Allora esiste $x \in G$ tale che

$f(x) = y' \in H'$

$x \in f^{-1}(\{y'\}) \subseteq f^{-1}(H')$.

$y' \in f(f^{-1}(H'))$.

Consideriamo $m \geq 1$ e $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ la proiezione canonica.

Corr. biunivoca fra:

- sottogruppi di $\mathbb{Z}$ contenenti $\ker \pi = m\mathbb{Z}$
- sottogruppi di $\mathbb{Z}/m\mathbb{Z}$

$d\mathbb{Z} \geq m\mathbb{Z} \Leftrightarrow d\mathbb{Z} \ni m$

$\langle d \rangle \geq \langle m \rangle$

$\Rightarrow$ $n = dk$ per qualche $k \in \mathbb{Z}$.
$\Leftarrow$ $d \mid n$.

CONCLUSIONE: $\forall\, d \mid m$ esiste uno e un solo sottogruppo di $\mathbb{Z}/m\mathbb{Z}$ (l'immagine di $d\mathbb{Z} = d\mathbb{Z}/(m\mathbb{Z})$.
Questo sottogruppo è CICLICO $(= \langle \bar{d} \rangle)$
(e anche (esercizio) il quoziente è un gruppo ciclico).