TUTORATO 8 • 01-12-2008 SOLUZIONI

ESERCIZIO 1:

$C = \frac{\mathbb{R}[X]}{I}$ con $I = (x^2+1)$

Trovare l'inverso di $X+I$

$C = \{ f(x) + I \mid f(x) \in \mathbb{R}[X] \} = \{ (aX+b) + I \mid a, b \in \mathbb{R} \}$

Sia $t = X + I$, si vede subito che $t^2 = -1$

Trovare l'inverso di $X+I$, è come trovare l'inverso di t.

L'inverso di t sarà un certo $\alpha \in C$ t.c. $\alpha t = 1$

e $\alpha = at + b$.

$\Rightarrow \alpha t = t(at+b) = at^2 + bt = -a + bt = 1 \iff a = -1$ e $b = 0$

$\Rightarrow t^{-1} = \alpha = -t$. Infatti $t(-t) = -t^2 = -(-1) = 1$.

ESERCIZIO 2:

La verifica che Φ è un omomorfismo la diamo solo per il punto (a), le altre sono analoghe.

(a) $\Phi : \mathbb{Z}[X] \to \mathbb{Z}$ t.c. $\Phi(f(X)) = f(0)$

Φ omomorfismo:

- $\Phi(0_{\mathbb{Z}[X]}) = \Phi(0) = 0$ ok
- $\Phi(f(X) \cdot g(X)) = (f(X)g(X))(0) = f(0)\,g(0)$ ok
- $\Phi(f(X) + g(X)) = (f(X) + g(X))(0) = f(0) + g(0)$
  $= \Phi(f(X)) + \Phi(g(X))$ ok $\Rightarrow \Phi$ è omomorfismo.

$\operatorname{Ker}\Phi = \{ f(x) \in \mathbb{Z}[X] \mid f(0) = 0 \} = \{ a_0 + a_1 X + \dots + a_k X^k \mid a_0 = 0 \} = (X)$

$\operatorname{Im}\Phi = \{ a \in \mathbb{Z} \mid f(0) = a \ \exists\, f(x) \in \mathbb{Z}[X] \} = \mathbb{Z}$

Per ogni $a \in \mathbb{Z}$ basta considerare $f(x) = a$, oppure $f(x) = X + a$ se si vuole un caso non banale.

Questo lo si poteva vedere anche applicando il TFO, infatti:

$$\frac{\mathbb{Z}[X]}{\operatorname{Ker}\Phi} \cong \operatorname{Im}\Phi$$

$$\frac{\mathbb{Z}[X]}{(X)} \cong \mathbb{Z}$$

(b) $\Phi : \mathbb{Z}[X] \to \mathbb{Z}_n$ t.c. $\Phi(f(X)) = \overline{f(0)}$

$\ker \Phi = \{ f(X) \in \mathbb{Z}[X] \mid f(0) \equiv 0 \pmod n \} = \{ a_0 + a_1 X + \dots + a_k X^k \mid a_0 \equiv 0 \pmod n \}$

$= (n, X)$

Per identificare $\operatorname{Im} \Phi$, applichiamo il TFO.

$$\frac{\mathbb{Z}[X]}{\ker \Phi} = \frac{\mathbb{Z}[X]}{(n,X)} \cong \mathbb{Z}_n \Rightarrow \operatorname{Im} \Phi = \mathbb{Z}_n$$

(c) $\Phi : \mathbb{Z}[X] \to \mathbb{Z}_n$ t.c. $\Phi\left(\sum_{i=0}^{k} a_i X^i\right) = \sum_{i=0}^{k} [a_i]_n$

$\ker \Phi = \{ a_0 + a_1 X + \dots + a_k X^k \in \mathbb{Z}[X] \mid \sum_{i=0}^{k} a_i \equiv 0 \pmod n \}$

$\operatorname{Im} \Phi = \{ [a]_n \mid \exists \sum_{i=0}^{k} a_i X^i \in \mathbb{Z}[X] \text{ t.c. } \sum a_i \equiv a \pmod n \} = \mathbb{Z}_n$

(d) $\Phi : \mathbb{Q}[X] \to \mathbb{C}$ t.c. $\Phi(f(X)) = f(i)$

$\ker \Phi = \{ f(X) \in \mathbb{Q}[X] \mid f(i) = 0 \} = \{ f(X) \in \mathbb{Q}[X] \mid f(X) = (X^2+1) q(X), \exists q(X) \in \mathbb{Q}[X] \} =$

$= ((X^2+1))$

$\operatorname{Im} \Phi = \{ a_0 + a_1 i + \dots + a_n i^n \mid a_k \in \mathbb{Q} \} =$

$= \{ a + bi \mid a, b \in \mathbb{Q} \} = \mathbb{Q}[i]$

(e) $\Phi : \mathbb{Q}[X] \to \mathbb{R}$ t.c. $\Phi(f(X)) = f(\sqrt[3]{2})$

$\ker \Phi = \{ f(X) \in \mathbb{Q}[X] \mid f(\sqrt[3]{2}) = 0 \} = \{ f(X) \in \mathbb{Q}[X] \mid f(X) = (X^3-2) q(X) \ \exists q \} =$

$= ((X^3-2))$

$\operatorname{Im} \Phi = \mathbb{Q}[\sqrt[3]{2}]$ per il TFO.

ESERCIZIO 3:

Uno dei teoremi di omomorfismo sappiamo che esiste una biezione tra gli ideali di $\frac{A}{I}$ e gli ideali di A contenenti I.

Quindi gli ideali di $\mathbb{Z}_{60}$ sono in corrispondenza con gli ideali di $\mathbb{Z}$ contenenti $60\mathbb{Z}$, perché $\mathbb{Z}_{60} = \frac{\mathbb{Z}}{60\mathbb{Z}}$

$\Rightarrow$ gli ideali di $\mathbb{Z}_{60}$ sono della forma $K\mathbb{Z}_{60}$ t.c. $K \mid 60$

I massimali di $\mathbb{Z}_{60}$ saranno i $K\mathbb{Z}_{60}$ t.c. K è primo in $\mathbb{Z}$.

$$\frac{\mathbb{Z}_{60}}{5\mathbb{Z}_{60}} = \frac{\mathbb{Z}/60\mathbb{Z}}{5\frac{\mathbb{Z}}{60\mathbb{Z}}} \cong \frac{\mathbb{Z}_5}{5\mathbb{Z}}$$ per il doppio quoziente che è un campo

Analogamente si vede che $\frac{\mathbb{Z}_{60}}{15\mathbb{Z}_{60}} \cong \frac{\mathbb{Z}}{15\mathbb{Z}}$ che non è integro.

ESERCIZIO 4:

$\Phi : \mathbb{Z} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_7 \qquad \Phi(a) = ([a]_3, [a]_7)$

Φ omomorfismo:

$\Phi(0) = (\bar{0}, \bar{0})$

$\Phi(a \cdot b) = ([a \cdot b]_3, [a \cdot b]_7) = ([a]_3, [a]_4) \cdot ([b]_3, [b]_7) =$

$= \Phi(a) \cdot \Phi(b)$

$\Phi(a+b) = ([a+b]_3, [a+b]_7) = ([a]_3, [a]_7) + ([b]_3, [b]_7) =$

$= \Phi(a) + \Phi(b)$

Φ suriettivo

per il teorema cinese dei resti $\forall\, x, y \in \mathbb{Z}$

$\exists\, z \in \mathbb{Z} : \begin{cases} z \equiv x \bmod 3 \\ z \equiv y \bmod 7 \end{cases}$

$\Rightarrow \forall\, ([x]_3, [y]_7) \quad \exists\, z \in \mathbb{Z} : \Phi(z) = ([x]_3, [y]_7)$

$\ker \Phi = \left\{ a \in \mathbb{Z} : \begin{cases} a \equiv 0 \bmod 3 \\ a \equiv 0 \bmod 7 \end{cases} \right\} = \{ a \in \mathbb{Z} : a \equiv 0 \bmod 21 \} =$

$= 21\mathbb{Z}$

$\Rightarrow$ T.F.O. $\frac{\mathbb{Z}}{\ker \Phi} = \frac{\mathbb{Z}}{21\mathbb{Z}} \cong \mathbb{Z}_3 \times \mathbb{Z}_7$ per transitività $\Rightarrow \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$

$\frac{\mathbb{Z}}{21\mathbb{Z}} \cong \mathbb{Z}_{21}$

Es 5

(a) $\frac{\mathbb{Q}[x]}{I}$ non è integro

dim ①

$$\left((x+1)+I\right)\left((x-1)+I\right) = (x^2-1)+I = 0+I$$

$\Rightarrow$ esistono zerodivisori propri

dim ②

x^2-1 è riducibile $\Rightarrow$ (x^2-1) non è primo

$\Rightarrow$ $\frac{\mathbb{Q}[x]}{I}$ non è integro (non è un dominio)

(b) $f(x) = x^3+x+1$

$\deg f(x) = 3$, $f(x)$ riducibile $\overset{*}{\iff}$ ho radici in $\mathbb{Q}$

(perché $\deg f(x) \leq 3$!!!)

$f(x) \in \mathbb{Z}[x]$ α radice di $f(x)$ $\Rightarrow$ $\begin{matrix} a_0 \mid \alpha \\ a_n \mid \alpha \end{matrix}$ $\Rightarrow$ $1 \mid \alpha$ $\Rightarrow \alpha = \pm 1$

$f(1) = 3$
$f(-1) = -1$ $\Rightarrow$ $f(x)$ non ho radici $\overset{*}{\Rightarrow}$ $f(x)$ irriducibile

$\Rightarrow$ (x^3+x+1) è ideale primo

$\mathbb{Q}[x]$ è un PID $\Rightarrow$ (ideale primo $\Rightarrow$ massimale)

$\Rightarrow$ $\frac{\mathbb{Q}[x]}{I}$ campo

c)

$f(x) = 2x^2 + 2 \in \mathbb{Z}[x]$ è riducibile

$f(x) = 2(x^2+1)$ $\quad 2 \notin \mathcal{U}(\mathbb{Z}[x]) \Rightarrow 2x^2+2$ non è associato di x^2+1

$\Rightarrow f(x)$ è riducibile $\Rightarrow (2x^2+2)$ non è primo

$\Rightarrow \dfrac{\mathbb{Z}[x]}{I}$ non è integro

d)

$f(x) = x^3 + x + \bar{1} \in \mathbb{Z}_3[x]$ $\quad I = (f(x))$

$f(\bar{1}) = 0 \Rightarrow \bar{1}$ radice di $f(x)$

$f(x) = (x - \bar{1})(x^2 + \bar{2}x + \bar{2}) \Rightarrow f(x)$ non è irriducibile

$\dfrac{\mathbb{Z}_3[x]}{(f(x))}$ non è integro

Es 6

$$\phi \quad \mathbb{Z}[x] \to \mathbb{R}$$

$$f(x) \to f(\sqrt{2})$$

$$\ker \phi = \{ f(x) \in \mathbb{Z}[x] : f(\sqrt{2}) = 0 \}$$

$$\alpha = \sqrt{2}$$

$$\alpha^2 = 2 \quad \Rightarrow \quad \alpha^2 - 2 = 0$$

$f(x) = x^2 - 2$ (irriducibile per Eisenstein e si annulla in $\sqrt{2}$)

$\forall\, g(x) \in \mathbb{Z}[x]$ t.c. $g(\sqrt{2}) = 0 \Rightarrow$

$$g(x) = h(x)\,(x^2-2) = h(x) f(x) \quad \exists\, h(x) \in \mathbb{Z}[x]$$

$$\ker \phi = \{ f(x) h(x) \in \mathbb{Z}[x] : f(x) = x^2 - 2 \quad h(x) \in \mathbb{Z}[x] \} =$$

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

$$\operatorname{Im} \phi = \{ g \in \mathbb{R} : g = g(\sqrt{2}) \ \exists\, g(x) \in \mathbb{Z}[x] \} =$$

$$= \{ a + b\sqrt{2} \quad a, b \in \mathbb{Z} \} = \mathbb{Z}[\sqrt{2}]$$

dim

$$g(x) = \sum_{i=0}^{N} a_i x^i \quad \Rightarrow \quad \forall\, i = 2k \quad x^i = x^{2k} \Rightarrow \sqrt{2}^i = 2^k$$

$$i = 2k+1 \quad x^i = x^{2k+1} \Rightarrow \sqrt{2}^i = 2^k \sqrt{2}$$

$$\Rightarrow g(\sqrt{2}) = \sum_{i=0}^{N} a_i \sqrt{2}^i = a_0 + \sqrt{2} a_1 + 2 a_2 + 2\sqrt{2} a_3 + \dots$$

$$= a + b\sqrt{2}$$

per il T. F. O

$$\frac{\mathbb{Z}[x]}{(x^2-2)} \simeq \mathbb{Z}[\sqrt{2}]$$

$\mathbb{Z}[\sqrt{2}]$ integro $\Rightarrow$ (x^2-2) ideale primo $\Rightarrow$ x^2-2 irriducibile

Es 7 $\quad I = (f(x)) \quad J = (g(x)) \quad M = (x, 2)$

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

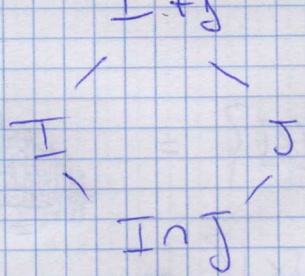
$g(x) = x+2$

a) $f(x)$ irriducibile (2 - Eisenstein)

$g(x)$ " (1° grado)

$\frac{\mathbb{Z}[x]}{J} \simeq \mathbb{Z}$ non è un campo $\Rightarrow$ J non è massimale

sappiamo che il reticolo (ordinato per inclusione)



è sempre verificato

se I fosse massimale $\Rightarrow$ $I + J = I$ cioè $J \subseteq I$

ma $g(x) \notin I$ $\Rightarrow$ $I + J \supsetneq I$ $\Rightarrow$ I non è massimale

per il T.F.O

$$\frac{\mathbb{Z}[x]}{(x^2-2)} \simeq \mathbb{Z}[\sqrt{2}]$$

$\mathbb{Z}[\sqrt{2}]$ integro $\Rightarrow$ (x^2-2) ideale primo $\Rightarrow$ x^2-2 irriducibile

Es 7 $\quad I = (f(x)) \quad J = (g(x)) \quad f(x) = x^2+2x+2$

$M = (x,2) \quad g(x) = x+2$

a) $f(x)$ irriducibile (2 - Eisenstein)

$g(x)$ " (1° grado)

$\frac{\mathbb{Z}[x]}{J} \simeq \mathbb{Z}$ non è un campo $\Rightarrow$ J non è massimale

sappiamo che il reticolo (ordinato per inclusione)

$I + J$

$I \qquad J$

$I \cap J$

è sempre verificato

se I fosse massimale $\Rightarrow I + J = I$ cioè $J \subseteq I$

ma $g(x) \notin I \Rightarrow I + J \supsetneq I \Rightarrow I$ non è massimale

α) $I \subseteq (x,2)$, $J \subseteq (x,2)$ $\Rightarrow$ $I+J \subseteq (x,2)$

$I+J \supseteq (x,2)$ infatti: $2 = f(x) - x\,g(x)$

$x = g(x) - 2 =$

$= g(x) - fx + x\,g(x) =$

$= (1+x)\,g(x) - fx$

β) $\Rightarrow x, 2 \in I+J \Rightarrow (x,2) \subseteq I+J$

α + β $\Rightarrow I+J = (x,2)$

c) $M = I+J$ è massimale $\dfrac{\mathbb{Z}[x]}{M} \simeq \mathbb{Z}_2$ campo

P.A.

sia N ideale massimale contenente $I \not\subseteq J \Rightarrow N \subseteq I+J$

$N \subseteq M$ (esiste un ideale contenente un ideale massimale) ⚡

d) $\dfrac{\mathbb{Z}[x]}{M} = \{ f(x) + M : f(x) \in \mathbb{Z}[x] \} =$

$\overset{*}{=} \{ f(0) + M : f(x) \in \mathbb{Z}[x] \} =$

$* \quad x \in M \Rightarrow x + M = 0 + M$

$f(x) = \sum_{i=0}^{N} a_i x^i = a_0 + x \sum_{i=1}^{N} a_i x^{i-1} \Rightarrow f(x) + M = (a_0 + M) + (x+M) \sum_{i=1}^{N} a_i x$

$= a_0 + M + (0+M) = a_0 + M$

$2 \in M \Rightarrow \forall f(0) \in \mathbb{Z} \quad f(0) + M = r(0) + M$ con $r(0) \equiv f(0) \bmod 2$

$= \{ r(0) + M : f(0) \in \mathbb{Z}[x] \} = \mathbb{Z}_2$