TUTORATO 9 - SOLUZIONI

ESERCIZIO 1:

Ricordiamo che in $\mathbb{Z}_n$ si ha:

I è un ideale $\iff \exists q \in \mathbb{Z}$ t.c. $q \mid n$ e $I = q\mathbb{Z}_n$

$q\mathbb{Z}_n \subset w\mathbb{Z}_n \iff w \mid q$

Sia $n = p_1^{i_1} \cdots p_k^{i_k}$ una decomposizione in primi di n.

Allora $m\mathbb{Z}_n$ è massimale $\iff m = p_J$ per qualche J

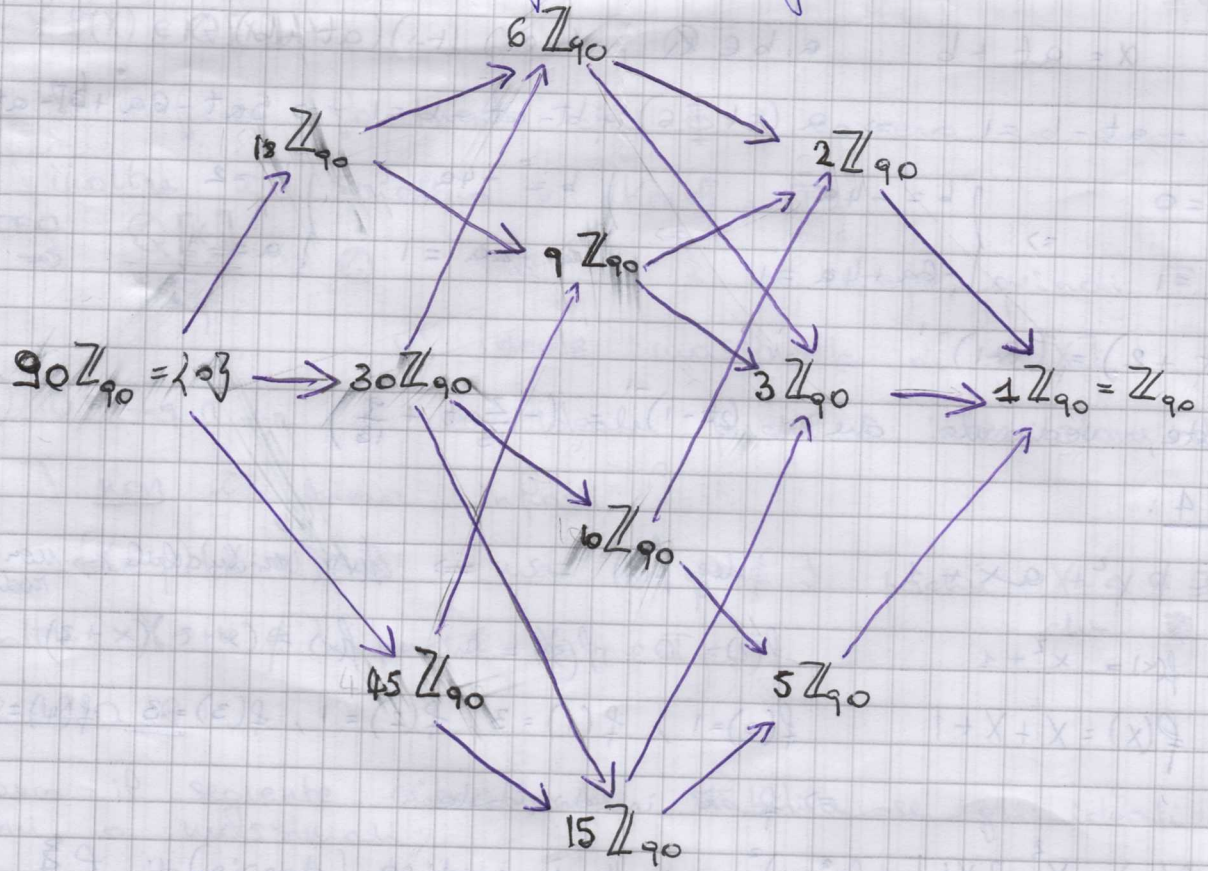
ed è minimale $\iff m = p_1^{i_1} \cdots p_J^{i_J - 1} \cdots p_k^{i_k}$ per qualche J.

Consideriamo $\mathbb{Z}_{101}$, 101 è primo, dunque $\mathbb{Z}_{101}$ non ha ideali non banali.

Consideriamo $\mathbb{Z}_{90}$, $90 = 2 \cdot 3^2 \cdot 5$, i suoi ideali massimali sono $2\mathbb{Z}_{90}$, $3\mathbb{Z}_{90}$, e $5\mathbb{Z}_{90}$, mentre i suoi ideali minimali sono $45\mathbb{Z}_{90}$, $18\mathbb{Z}_{90}$ e $30\mathbb{Z}_{90}$.

I quozienti sono nell'ordine $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_{45}$, $\mathbb{Z}_{18}$ e $\mathbb{Z}_{30}$

Infine abbiamo il seguente diagramma delle inclusioni:



Dove le frecce indicano l'inclusione.

ESERCIZIO 2:

È immediato verificare che Φ sia un omomorfismo.

$\ker \Phi = \{ f(x) \in \mathbb{Z}[X] \mid f(i) = 0 \} = \{ f(x) \in \mathbb{Z}[X] \mid (x^2+1) \mid f(x) \} = (x^2+1)$

$\operatorname{Im} \Phi = \mathbb{Z}[i]$ per il TFO.

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

$$\frac{\mathbb{Z}[X]}{(x^2+1)} \cong \mathbb{Z}[i]$$

ESERCIZIO 3:

$$X^2 - 5X + 6 = (X-2)(X-3)$$

Quindi $\frac{\mathbb{Q}[X]}{I}$ non è un campo e non è un dominio.

$(X-3)+I$ è uno zero divisore di R, poiché

$$\big((X-3)+I\big)\big((X-2)+I\big) = I$$

Cerchiamo ora l'inverso di $(X-1)+I$:

Sia $t = X+I \Rightarrow (X-1)+I = t-1$ e $t^2 = 5t-6$

Cerchiamo $\alpha = at+b$ $a, b \in \mathbb{Q}$, t.c. $(t-1)(at+b) = 1$

$\Rightarrow at^2+bt-at-b = 1 \Rightarrow a(5t-6)+bt-at-b = 1 \Rightarrow 5at-6a+bt-at-b = 1$

$$\Rightarrow \begin{cases} 4a+b=0 \\ -6a-b=1 \end{cases} \Rightarrow \begin{cases} b=-4a \\ -6a+4a=1 \end{cases} \Rightarrow \begin{cases} b=-4a \\ -2a=1 \end{cases} \quad \begin{cases} b=2 \\ a=-\frac{1}{2} \end{cases}$$

$$\Rightarrow \left(-\tfrac{1}{2}t+2\right) = (t-1)^{-1}$$

Analogamente, vediamo che $(2t-1)^{-1} = \left(-\frac{2}{13}t + \frac{9}{13}\right)$

ESERCIZIO 4:

$\mathbb{Z}_5[x] \ni f(x) = x^2 + ax + 1$ $\quad \deg f(x) = 2 \Rightarrow f(x)$ irriducibile $\Leftrightarrow$ non ha radici in $\mathbb{Z}_5$

$a=0$ $\quad f(x) = x^2+1$ $\quad f(2) = 0$ $\quad f(3) = 0$ $\quad f(x) = (x+2)(x+3)$

$a=1$ $\quad f(x) = X^2+X+1$ $\quad f(0)=1,\ f(1)=3,\ f(2)=1,\ f(3)=3,\ f(4)=1$

$\Rightarrow f$ è irriducibile

$a=2$ $\quad f(x) = X^2+2X+1 = (x^2+1)^2 \Rightarrow 4$ è radice (doppia) di f

$a=3$ $\quad f(x) = x^2+3x+1 = (x-1)^2 = (x+4)^2 \Rightarrow 1$ è radice (doppia) di f

$a=4$ $\quad f(x) = x^2-x+1$ $\quad f(0)=1,\ f(1)=1,\ f(2)=3,\ f(3)=2,\ f(4)=3$

$\Rightarrow f$ irriducibile

Quindi per $a = 1, 4$ $A = \dfrac{\mathbb{Z}_5[X]}{(X^2+aX+1)}$ è un campo

Negli altri casi non è neanche un dominio.

Studiamo ora gli ideali nel caso $a = 0, 1$.

Per quanto detto, se $a=1$ A è un campo e quindi ha solo ideali banali.

$a=0$: $A = \dfrac{\mathbb{Z}_5[X]}{(X^2+1)} = \dfrac{\mathbb{Z}_5[X]}{((X+2)(X+3))} = I$

Per i teoremi di omomorfismo sugli anelli abbiamo che gli ideali di $\frac{B}{I}$ sono in corrispondenza biunivoca con gli ideali di B contenenti I.

In $\mathbb{Z}_5[X]$ gli ideali contenenti (X^2+1) sono $(X+2)$ e $(X+3)$

Quindi in A gli ideali sono $(X+2)+I$ e $(X+3)+I$.

ESERCIZIO 5:

(a) I_q è MASSIMALE:

Consideriamo l'omomorfismo $\Phi: \mathbb{Q}[X] \to \mathbb{Q}$ t.c. $\Phi(f(x)) = f(q)$ $\forall f(X) \in \mathbb{Q}[X]$

Si verifica facilmente che Φ è davvero un omomorfismo, inoltre è suriettivo e $\ker \Phi = I_q$

$\xrightarrow{\text{TFO}}$ $\dfrac{\mathbb{Q}[X]}{I_q} \cong \mathbb{Q}$. Ma $\mathbb{Q}$ è un campo, quindi I_q è un ideale massimale di $\mathbb{Q}[X]$.

(b) $J = I_q \cap I_r$ è un ideale poiché è intersezione di ideali.

J non è primo, infatti:

$(X-q)(X-r) \in J$ ma $X-q \notin J$ poiché $X-q \notin I_r$ visto che $q-r \neq 0$

inoltre $X-r \notin J$ poiché $X-r \in I_q$.

ESERCIZIO 6:

Usiamo il seguente criterio per stabilire se gli ideali sono primi o massimali:

I è primo (risp. massimale) $\iff$ $\dfrac{A}{I}$ dominio (risp. campo)

(a) $\frac{\mathbb{Z}[X]}{(3,X)} \simeq \mathbb{Z}_3$, quindi $(3,X)$ è massimale

(b) $\frac{\mathbb{Z}[X]}{(X^2-3X+2)}$ non è un dominio, infatti $X^2-3X+2=(X-1)(X-2)$
Quindi nel quoziente $(X-1)+I$ è uno zero divisore non nullo. Quindi (X^2-3X+1) non è primo.

(c) $\frac{\mathbb{Z}[X]}{(X^2-3)} = \mathbb{Z}[\sqrt{3}]$, dunque (X^2-3) è primo, ma non massimale.
Infatti $\mathbb{Z}[\sqrt{3}]$ è un dominio, ma non un campo

(d) $\frac{\mathbb{Z}[X]}{(7,X^2-3)} \simeq \frac{\mathbb{Z}[\sqrt{3}]}{(7)}$ Ricordiamo che 7 è irriducibile in $\mathbb{Z}[\sqrt{3}]$, che è un dominio euclideo, quindi $\frac{\mathbb{Z}[\sqrt{3}]}{(7)}$ è un campo $\Rightarrow (7,X^2-3)$ è massimale.

ESERCIZIO 7:

(a) È una semplice verifica provare che i quadrati perfetti di $\mathbb{Z}_7$ sono: 0, 1, 2, 4.

(b) $\frac{\mathbb{Z}_7[X]}{(X^2+a)}$ è un campo $\iff (X^2+a)$ è massimale in $\mathbb{Z}_7[X]$
$\iff X^2+a$ è irriducibile.

X^2+a è irriducibile $\iff -a$ non è un quadrato perfetto in $\mathbb{Z}_7$

Ovvero per $-a = 3,5,6 \Rightarrow a = 4,2,1$

(c) Quindi $A = \mathbb{Z}_7[X]/(X^2+4)$ è un campo, per cui ogni elemento è invertibile. Il generico elemento di A sarà $(aX+b)+I$ $a,b \in \mathbb{Z}_7$
Quindi l'inverso di $at+b$ sarà $\alpha t+\beta$ t.c. $(at+b)(\alpha t+\beta)=1$
$\Rightarrow$ facendo i conti si vede che:

$$\alpha = 5a(a^2+2b^2)^{-1} \qquad \beta = 2b(a^2+2b^2)^{-1}$$

(d) Da (b) segue che $\mathbb{Z}_7[X]/(X^2+3)$ non è un campo, quindi essendo finito non può essere un dominio. Quindi ci sono degli zero divisori.

$at+b$ è uno zero divisore se $\exists\, \alpha t+\beta$ t.c.
$(at+b)(\alpha t+\beta)=0 \Rightarrow \begin{cases} 4a\alpha + b\beta = 0 \\ b\alpha + a\beta = 0 \end{cases}$ ha soluzioni non banali $\iff 4a^2-b=0 \iff b=$
$\Rightarrow$ I divisori dello zero sono del tipo

$at \pm 2a \Rightarrow t \pm 2,\ 2t \pm 4,\ 3t \pm 6,\ 4t \pm 1,\ 5t \pm 3,\ 6t \pm 5$

ESERCIZIO 8: Verrà riproposto nel prossimo tutorato, aspettiamo quindi a darne la soluzione.