COGNOME .... *NOME* ....

Accompagnare le risposte con spiegazioni *chiare ed essenziali.* Ogni esercizio vale 7.5 punti.

1. Dire se i seguenti ideali degli anelli $\mathbf{Z}[X]$, $\mathbf{Q}[X]$ e $\mathbf{Z}_5[X]$ sono primi o meno:

$$(X^3 - 15X + 45), \qquad (X^3 - 15X + 45, 2), \qquad (X^3 - 15X + 45, X - 1).$$

(Sono richieste quindi $3 \times 3 = 9$ risposte ....)

Sia $I_1 = (X^3 - 15X + 45)$. Il polinomio $X^3 - 15X + 45$ è di Eisenstein rispetto al primo 5 ed è irriducibile in $\mathbf{Z}[X]$. Per il Lemma di Gauss lo è anche in $\mathbf{Q}[X]$. Poiché $\mathbf{Z}[X]$ e $\mathbf{Q}[X]$ sono UFD, l'ideale I_1 è quindi primo in questi anelli. In $\mathbf{Z}_5[X]$ invece, l'anello quoziente $\mathbf{Z}_5[X]/(X^3)$ non è un dominio e quindi I_1 non è primo.

Sia $I_2 = (X^3 - 15X + 45, 2)$. L'elemento 2 è invertibile in $\mathbf{Q}[X]$ e $\mathbf{Z}_5[X]$. Poiché I_1 contiene 2, l'ideale I_1 è uguale all'anello stesso e quindi non è primo in $\mathbf{Q}[X]$ e $\mathbf{Z}_5[X]$. Invece $\mathbf{Z}[X]/I_2 \cong \mathbf{Z}_2[X]/(X^3+X+1)$ è un dominio perchè X^3+X+1 è irriducibile e quindi primo nel PID $\mathbf{Z}_2[X]$. L'ideale I_2 è quindi primo in $\mathbf{Z}[X]$.

Infine, sia $I_3 = (X^3 - 15X + 45, X - 1)$. Per ogni anello commutativo R abbiamo che $R[X]/(X-1) \cong R$ tramite l'isomorfismo che manda $f \in R[X]$ in $f(1)$. Si ha quindi che $R[X]/(X^3 - 15X + 45, X - 1) \cong R/(1^3 - 15 \cdot 1 + 45) = R/(31)$. Poiché 31 è invertibile quando $R = \mathbf{Q}$ o $\mathbf{Z}_5$, si tratta dell'anello zero. L'ideale I_3 non è primo in questi casi. Invece per $R = \mathbf{Z}$, l'anello $R/(31)$ è un campo e quindi l'ideale I_3 è primo in questo caso.

2. Siano A, B, C, D, A', B', C' e D' gruppi abeliani. Nel seguente diagramma commutativo le due righe sono esatte

$$\begin{array}{ccccccc} A & \xrightarrow{\phi} & B & \xrightarrow{\psi} & C & \xrightarrow{\chi} & D \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle k} \\ A' & \xrightarrow{\phi'} & B' & \xrightarrow{\psi'} & C' & \xrightarrow{\chi'} & D'. \end{array}$$

Dimostrare che se f è suriettiva e g e k sono iniettive, allora h è iniettiva.

Sia $c \in C$ con $h(c) = 0$. Sia $d = \chi(c)$. Allora per la commutatività del diagramma si ha che $k(d) = 0$. Poiché k è iniettiva, questo implica che $d = 0$. Esiste quindi per esattezza $b \in B$ con $\psi(b) = c$. Per la commutatività l'elemento $b' = g(b)$ soddisfa $\psi'(b') = 0$. Esiste quindi per l'esattezza $a' \in A'$ con $\phi(a') = b'$. Per la suriettività di f esiste $a \in A$ con $f(a) = a'$. Sia $\tilde{b} = \phi(a)$. Per la commutatività si ha che $g(\tilde{b}) = b'$. Poichè $b' = g(b)$ si ha che $g(b) = g(\tilde{b})$. Per l'iniettività di g si ha quindi $\tilde{b} = b$ e poi $c = \psi(b) = \psi(\tilde{b}) = \psi\phi(a) = 0$, dimostrando l'iniettività di h.

3. Determinare l'ordine del gruppo moltiplicativo dell'anello $\mathbf{Z}[X]/(2, X^4 + X^2 + X + 1)$.

L'anello $R = \mathbf{Z}[X]/(2, X^4 + X^2 + X + 1)$ è isomorfo a $\mathbf{Z}_2[X]/(X^4 + X^2 + X + 1)$. Si ha che $X^4 + X^2 + X + 1 = (X+1)(X^3 + X^2 + 1)$ in $\mathbf{Z}_2[X]$. Il polinomi $X + 1$ e $X^3 + X^2 + 1$ sono irriducibili in $\mathbf{Z}_2[X]$. Siccome $\mathbf{Z}_2[X]$ è un PID, generano ideali massimali. Per il Teorema Cinese del resto abbiamo che

$$R \;\cong\; \mathbf{Z}_2[X]/(X+1) \times \mathbf{Z}_2[X]/(X^3 + X^2 + 1).$$

Il primo fattore è isomorfo al campo $\mathbf{Z}_2$ e il secondo ad un campo k di $2^3 = 8$ elementi. Abbiamo quindi che $R^* \cong \mathbf{Z}_2^* \times k^* \cong k^*$. Il gruppo R^* ha quindi $8 - 1 = 7$ elementi.

4. Sia M il $\mathbf{Q}[X]$-modulo $\mathbf{Q}[X]/(X^3)$. Determinare i $\mathbf{Q}[X]$-sottomoduli di M.

Il modulo $M = \mathbf{Q}[X]/(X^3)$ ha anche la struttura di anello. Gli $\mathbf{Q}[X]$-sottomoduli di M sono esattamente gli ideali di $\mathbf{Q}[X]/(X^3)$. Gli ideali di $\mathbf{Q}[X]/(X^3)$ sono le immagini degli ideali di $\mathbf{Q}[X]$ che contengono X^3. Siccome $\mathbf{Q}[X]$ è un PID, si tratta degli ideali generati dai divisori $1, X, X^2$ e X^3 di X^3. I sottomoduli sono quindi M, $(X)/(X^3)$, $(X^2)/(X^3)$ e $\{0\}$. Fine.

Osserviamo che il modulo M è uno spazio vettoriale su $\mathbf{Q}$ di dimensione 3. Una base è data da $\{1, X, X^2\}$. In questi termini si ha che $(X)/(X^3) = \mathrm{Span}\{X, X^2\}$ e $(X^2)/(X^3) = \mathrm{Span}\{X^2\}$.