Corso di Algebra - a.a. 2011-2012

Prova scritta del 2.2.2012

1. Trovare tutte le soluzioni del sistema di congruenze
$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 4 \mod 7 \end{cases}$$
nell'intervallo $[300, 350]$.

2. Dimostrare che i gruppi $A_4 \times \mathbb{Z}/2\mathbb{Z}$ e $S_3 \times \mathbb{Z}/4\mathbb{Z}$ non sono isomorfi.

3. L'ideale $(11, X^2 - 2)$ è primo e/o massimale in $\mathbb{Z}[X]$?

4. Indichiamo con $\mathbb{F}_5$ il campo $\mathbb{Z}/(5)$. Per ognuno dei seguenti polinomi trovare il campo di spezzamento su $\mathbb{F}_5$ e il grado del medesimo su $\mathbb{F}_5$:
   (a) $P(X) = X^3 + X$
   (b) $Q(X) = X^3 - X^2 + 2X - 2$

Soluzioni

1. $1 = 3 \cdot 5 - 2 \cdot 7$, quindi una soluzione particolare del sistema è $x_0 = 3 \cdot 5 \cdot 4 - 2 \cdot 7 \cdot 3 = 18$. Le soluzioni del sistema sono tutti e soli gli interi congrui a x_0 modulo $5 \cdot 7 = 35$. L'unico tra questi interi che è compreso tra 300 e 350 è $350 - 35 + 18 = 333$.

2. $S_3 \times \mathbb{Z}/4\mathbb{Z}$ contiene elementi di ordine 4 perchè lo stesso è vero per $\mathbb{Z}/4\mathbb{Z}$. Invece l'ordine di un elemento $(a, b) \in A_4 \times \mathbb{Z}/2\mathbb{Z}$ è il minimo comune multiplo degli ordini di a e di b. Dato che gli elementi di A_4 diversi dall'identità hanno ordine 2 (i prodotti di trasposizioni disgiunte) o 3 (i 3-cicli), gli ordini possibili per gli elementi di $A_4 \times \mathbb{Z}/2\mathbb{Z}$ sono $1, 2, 3, 6$, e dunque $A_4 \times \mathbb{Z}/2\mathbb{Z}$ non contiene elementi di ordine 4.

3. Bisogna esaminare il quoziente $\mathbb{Z}[X]/(11, X^2 - 2)$, che per uno dei teoremi di isomorfismo può anche essere scritto come $(\mathbb{Z}[X]/(11))/((11, X^2 - 2)/(11))$. Ora $\mathbb{Z}[X]/(11)$ è isomorfo a $\mathbb{Z}/11\mathbb{Z}[X]$ e l'ideale $(11, X^2 - 2)/(11)$ si identifica all'ideale $(X^2 - 2)$ in $\mathbb{Z}/11\mathbb{Z}[X]$. Questo ideale è primo perchè il polinomio $X^2 - 2$ è irriducibile in $\mathbb{Z}/11\mathbb{Z}[X]$. Infatti se non fosse irriducibile avrebbe una radice in $\mathbb{Z}/11\mathbb{Z}$, ma si vede direttamente che non ne ha. Dato che $\mathbb{Z}/11\mathbb{Z}[X]$ è a ideali principali i suoi ideali primi non nulli sono anche massimali. Quindi $(X^2 - 2)$ è massimale. Ne segue che $\mathbb{Z}[X]/(11, X^2 - 2) \cong \mathbb{Z}/11\mathbb{Z}[X]/(X^2 - 2)$ è un campo, e quindi che $(11, X^2 - 2)$ è massimale, e in particolare primo.

4. (a) $P(X) = X(X^2 + 1) = X(X - 2)(X + 2)$ in $\mathbb{F}_5[X]$. Ne segue che $\mathbb{F}_5$ stesso è un campo di spezzamento per P. Il suo grado su $\mathbb{F}_5$ è ovviamente 1.
   (b) $Q(X) = (X - 1)(X^2 + 2)$. Il polinomio $X^2 + 2$ è irriducibile in $\mathbb{F}_5[X]$ perchè non ha radici in $\mathbb{F}_5$, come si vede per ispezione diretta. Sia ξ una radice di $X^2 + 2$ in una estensione di $\mathbb{F}_5$. L'altra radice di $X^2 + 2$ è $-\xi$ e un campo di spezzamento per Q è $\mathbb{F}_5[\xi, -\xi] = \mathbb{F}_5[\xi]$. Inoltre $X^2 + 2$ è il polinomio minimo di ξ su $\mathbb{F}_5$ e quindi $\left[\mathbb{F}_5[X] : \mathbb{F}_5\right] = \deg(X^2 + 2) = 2$.