**Corso di Algebra 1 – a.a. 2012-2013**

*Prova scritta del 20.9.2013*

1. Si consideri il seguente sistema di congruenze dipendente dal parametro $a$:

$$\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 1 \mod 3 \\ x \equiv a \mod 10 \end{cases}$$

   (a) Ponendo $a = 2$ si determinino tutte le soluzioni nell'intervallo $[302, 360]$.

   (b) Si discuta per quali valori di $a$ il sistema ammette soluzioni.

2. Sia $G$ gruppo e $H$ sottogruppo di indice 4.

   (a) Supponendo che $H$ sia normale in $G$ si verifichi che se $g \in G$ ha ordine dispari allora $g \in H$.

   (b) Nelle ipotesi del punto precedente si verifichi che se $K < G$ ha ordine dispari, allora $K < H$.

   (c) Si mostri con un esempio che le conclusioni sopra sono false se $H$ non è normale (suggerimento: cercare $H$ sottogruppo di $G = S_4$).

3. Sia $Q \in \mathbb{Z}[X]$ un polinomio non nullo e sia $a \in \mathbb{Z}$ il suo coefficiente direttivo. Se $p \in \mathbb{Z}$ è un primo indichiamo con $\overline{Q}$ la riduzione di $Q$ modulo $p$.

   (a) Supponiamo che $Q$ abbia grado strettamente positivo. Sia $p$ un primo che non divide $a$. Mostrare che $\overline{Q}$ non è nullo o invertibile in $\mathbb{Z}/(p)[X]$.

   (b) Mostrare che $(Q)$ non è un ideale massimale in $\mathbb{Z}[X]$.

4. Poniamo $K = \mathbb{Q}[i, \eta]$, dove $\eta$ è una radice sesta primitiva dell'unità.

   (a) Mostrare che $\sqrt{3} \in K$.

   (b) Calcolare il grado $[K : \mathbb{Q}]$.

*Soluzioni*

1. (a) Se $x_0$ è una soluzione particolare del sistema, le soluzioni sono tutti gli interi congrui a $x_0$ modulo $\mathrm{mcm}(5, 3, 10) = 30$. Dato che una soluzione particolare è ad esempio 22, le sole soluzioni nell'intervallo dato sono 322 e 352.

   (b) Dato che 5 e 3 sono primi fra loro la prima coppia di congruenze ammette una e una sola soluzione modulo $\mathrm{mcm}(5, 3) = 15$. Sia $s$ una soluzione, ad esempio $s = 7$. Le soluzioni della prima coppia di congruenze sono tutti e soli gli interi congrui a $s$ modulo 15. Uno di questi interi è soluzione anche dell'ultima congruenza se e solo se $a = s + 15h + 10k$, dove $h$ e $k$ sono interi. Ciò implica che $a$ è congruo a $s$ modulo 5, anzi è equivalente a quest'ultima condizione. Infatti, dato che 3 e 2 sono primi fra loro, possiamo trovare interi $a$ e $b$ tali che $1 = 3a + 2b$. Ma allora, se $a = s + 5\ell$, possiamo scrivere $a = s + 5 \cdot 3a\ell + 5 \cdot 2b\ell = s + 15a\ell + 10b\ell$. In conclusione il sistema ha soluzione se e solo se $a$ è congruo a $s$ modulo 5.

2. (a) Sia $\bar{g}$ la classe di $g$ in $G/H$ e sia $k$ l'ordine di $g$. Dato che $\bar{g}^k = 1$, l'ordine di $\bar{g}$ divide sia $\#(G/H) = 4$ che $k$ e quindi vale 1. In altre parole, $g \in H$.

   (b) Se $g \in K$ il suo ordine divide quello di $K$ e quindi è dispari. Segue allora dal punto (a) che $g \in H$.

   (c) Scegliamo come $H$ il sottogruppo di $G = S_4$ costituito da tutte le permutazioni di $\{1, 2, 3, 4\}$ che lasciano fisso 1. È chiaro che $H$ si identifica al gruppo delle permutazioni di $\{2, 3, 4\}$ e quindi a $S_3$. In particolare ha ordine 6 e quindi indice 4 in $G$. Però non contiene, ad esempio, il 3-ciclo $(1\,2\,3)$ che ha ordine 3.

3. (a) Sappiamo che $Q = aX^n +$ (termini di grado minore di $n$). Quindi $\overline{Q} = \overline{a}X^n +$ (termini di grado minore di $n$), dove $\overline{a}$ indica la classe di $a$ modulo $p$, che per ipotesi non è nulla. Ne segue che $\overline{Q}$ ha grado $n > 0$ e quindi che non è nullo o invertibile.

   (b) Supponiamo che $Q$ abbia grado nullo. Se $Q = \pm 1$ l'ideale $(Q)$ è $\mathbb{Z}[X]$ e quindi non è massimale. Se $Q = b$, dove $b$ è un intero diverso da $\pm 1$, allora $\mathbb{Z}[X]/(Q) = \mathbb{Z}/(b)[X]$ che non è un campo; quindi in questo caso $(Q)$ non è massimale. Supponiamo ora che $\deg(Q) > 0$. Sia $p$ un primo che non divide $a$. La sola costante appartenente a $(Q)$ è 0. Quindi l'ideale $I = (p, Q)$ contiene strettamente $(Q)$. D'altra parte $\mathbb{Z}[X]/I = (\mathbb{Z}/(p)[X])/(\overline{Q})$ e per il punto (a) questo anello non è nullo; in altre parole $I$ è un ideale proprio. Ne segue che $(Q)$ non è massimale in quanto strettamente contenuto in un ideale proprio.

4. (a) $\eta = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$, quindi $\sqrt{3} = \pm(2\eta - 1)/i \in K$.

   (b) $K = \mathbb{Q}[i, \sqrt{3}]$, quindi $\big[K : \mathbb{Q}\big] = \big[K : \mathbb{Q}[\sqrt{3}\big]\big[\mathbb{Q}[\sqrt{3} : \mathbb{Q}\big] = \big[K : \mathbb{Q}[\sqrt{3}\big] \cdot 2$. Dato che $\mathbb{Q}[\sqrt{3}] \subset \mathbb{R}$, $i \notin \mathbb{Q}[\sqrt{3}]$. Ne segue che $\big[K : \mathbb{Q}[\sqrt{3}]\big] = \big[\mathbb{Q}[\sqrt{3}, i] : \mathbb{Q}[\sqrt{3}]\big] = 2$ e dunque che $[K : \mathbb{Q}] = 4$.