**Corso di Algebra - a.a. 2005-2006**

*Prova scritta del 23.2.2006 – soluzioni*

1. $K$ non è vuoto perchè contiene l'elemento neutro. Se $a, b \in K$ e $g \in G$, allora $gab^{-1}g^{-1} = gag^{-1}gb^{-1}g^{-1} = gag^{-1}(gbg^{-1})^{-1} \in H$ perchè $gag^{-1}$ e $gbg^{-1}$ appartengono ad $H$ e $H$ è un sottogruppo di $G$; ne segue che $ab^{-1} \in K$. Quindi $K$ è un sottogruppo di $G$. Se $a \in K$ e $\gamma \in G$, allora per ogni $g \in G$ si ha che $g(\gamma a\gamma^{-1})g^{-1} = (g\gamma)a(g\gamma)^{-1} \in H$. Quindi $\gamma a\gamma^{-1} \in K$, e $K$ è normale.

2. Sia $\sigma \in S_n$. Se scriviamo $\sigma$ come prodotto di cicli disgiunti di lunghezze $\ell_1, \ldots, \ell_h$, allora l'ordine di $\sigma$ è il minimo comune multiplo di $\ell_1, \ldots, \ell_h$. Questo significa che, se l'ordine di $\sigma$ è 12, uno degli $\ell_i$ deve essere divisibile per 3 e un altro (o lo stesso) per 4. Ne segue che $n \geq 7$. Viceversa, il prodotto in $S_7$ di un 3-ciclo e di un 4-ciclo disgiunti ha ordine 12.

3. 2 è invertibile modulo 35 perchè è primo con 35. Le potenze successive di 2 modulo 35 sono $2, 4, 8, 16, 32, 29, 23, 11, 22, 9, 18, 1$. Dunque la classe di 2 nel gruppo moltiplicativo di $\mathbb{Z}/35\mathbb{Z}$ ha ordine 12. Poiché $2^3 = 8$, se scriviamo $n = 3 + h$, $2^n \equiv 8 \mod 35$ se e solo se $2^h \equiv 1 \mod 35$. Per quanto si è osservato, questo accade se e solo se $h$ è divisibile per 12. Quindi gli $n$ cercati sono tutti e soli quelli della forma $3 + 12k$, dove $k$ è un intero non negativo.

4. (a) Se $b, b' \in \mathrm{Ann}(a)$ e $c \in A$, allora $(b - b')a = ba - b'a = 0$ e $(cb)a = c(ba) = 0$, quindi $b - b'$ e $cb$ appartengono a $\mathrm{Ann}(a)$, che è dunque un ideale.

   (b) È chiaro che $\mathrm{Ann}(a) \subset \mathrm{Ann}(a^n)$. Per dimostrare il viceversa, notiamo che, se $ba^n = 0$, allora $ba^{n-1} \in \mathrm{Ann}(a)$; poichè $\mathrm{Ann}(a)$ è primo, deve contenere uno dei fattori del prodotto $ba^{n-1}$. Però $a \notin \mathrm{Ann}(a)$, perchè per ipotesi $a^2 \neq 0$. Quindi $b \in \mathrm{Ann}(a)$, come si doveva dimostrare.

5. (a) In $\mathbb{C}[X]$ possiamo scrivere $P(X) = (X - \sqrt{5})(X + \sqrt{5})(X - i\sqrt{5})(X + i\sqrt{5})$. Quindi il campo di spezzamento di $P(X)$ è $L = \mathbb{Q}[\sqrt{5}, i\sqrt{5}] = \mathbb{Q}[\sqrt{5}, i]$. Ma $[L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt{5}]][\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2 \cdot 2 = 4$ perchè $i \notin \mathbb{Q}[\sqrt{5}]$.

   (b) Modulo 2, $P(X) = X^4 - 1 = (X - 1)^4$ perchè l'elevamento a quarta potenza è il quadrato dell'omomorfismo di Frobenius. Dunque il grado cercato è 1.

   (c) Modulo 3, $P(X) = (X^2 + 1)(X^2 - 1) = (X^2 + 1)(X - 1)(X + 1)$. Dato che $2^2 \equiv 1 \mod 3$, $X^2 + 1$ non ha radici in $K$. Dunque, se $\xi$ è una radice di $X^2 + 1$, il campo di spezzamento di $P(X) = (X - \xi)(X + \xi)(X - 1)(X + 1)$ è $K[\xi]$ e $[K[\xi] : K] = 2$.

   (d) Modulo 5, $P(X) = X^4$, e quindi il grado cercato è 1.