Algebra 1 (Schoof) 1^o appello 4 febbraio 2013, ore 14:00–16:00.

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

Accompagnare le risposte con spiegazioni *chiare ed essenziali.* Ogni esercizio vale 5 punti.

1. Sia $H \subset \mathbf{Z}_{35}^*$ il sottogruppo dato da $H = \{\overline{a} \in \mathbf{Z}_{35}^* : a \equiv 1 \pmod 5\}$. Calcolare l'ordine dell'elemento $\overline{19}H$ nell gruppo quoziente $\mathbf{Z}_{35}^*/H$.
2. Sia G un gruppo con la proprietà che $G/Z(G)$ è ciclico. Dimostrare che G è abeliano.
3. Siano $\alpha_1, \alpha_2, \ldots, \alpha_7 \in \mathbf{C}$ tali che $X^7 + X + 2 = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_7)$. Determinare $\alpha_1^7 + \alpha_2^7 + \cdots + \alpha_7^7$.
4. Sia Q_4 il gruppo dei quaternioni e sia S_3 il gruppo simmetrico su 3 simboli. Quanti omomorfismi $Q_4 \longrightarrow S_3$ ci sono?
5. Per ogni $a \in \mathbf{R}$ determinare il numero di ideali dell'anello $\mathbf{R}[X]/(X^2 - a)$.
6. Sia $R = \{f \in \mathbf{C}[X] : f(0) \in \mathbf{Z}\}$.
   (a) Dimostrare che R è un sottoanello di $\mathbf{C}[X]$.
   (b) Sia $I \subset R$ l'ideale generato dall'elemento $2 \in R$. Determinare $\#(R/I)$. Giustificare la risposta.

Soluzioni.

1. Dal fatto che $19 \not\equiv 1 \pmod 5$ mentre $19^2 \equiv 1 \pmod 5$ segue che $\overline{19}H$ ha ordine 2.
2. Questo è l'esercizio 3 (c) del foglio 13.
3. Questo è l'esercizio 9 del foglio 15.
4. Sia $f : Q_4 \longrightarrow S_3$ un'omomorfismo non banale. Allora l'immagine di f ha cardinalità 2 ed è quindi abeliano. Questo significa che f si fattorizza via $\overline{f} : Q_4/[Q_4, Q_4] \longrightarrow S_3$. Dal fatto che $[Q_4, Q_4] = \{\pm 1\}$ segue che $Q_4/[Q_4, Q_4]$ è isomorfo al gruppo di Klein $V_4 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Il numero di omomorfismi non banali da $\mathbf{Z}_2 \longrightarrow S_3$ è uguale al numero di elementi di ordine 2 in S_3, vale a dire a 3. Ci sono quindi $3^2 + 1 = 10$ omomorfismi $Q_4 \longrightarrow S_3$.
5. Gli ideali di $\mathbf{R}[X]/(X^2 - a)$ corrispononо biettivamente agli ideali di $\mathbf{R}[X]$ che contengono $X^2 - a$. L'anello $\mathbf{R}[X]$ è un dominio ad ideali principali e ogni suo ideale non nullo è generato da un unico polinomio monico. Gli ideali di $\mathbf{R}[X]$ che contengono $X^2 - a$ corrispondono quindi biettivamente ai divisori monici di $X^2 - a$ in $\mathbf{R}[X]$. Ce ne sono due se $a < 0$, tre se $a = 0$ e quattro quando $a > 0$.
6. Se $f, g \in \mathbf{C}[X]$ hanno termine noto $f(0)$ in $\mathbf{Z}$, il loro prodotto e la loro somma hanno la stessa proprietà. Ne segue che R è un sottoanello di $\mathbf{C}[X]$. L'applicazione $\phi : R \longrightarrow \mathbf{Z}_2$ data da $\phi(f) = f(0) \pmod 2$ è un omomorfismo suriettivo di anelli. Affermiamo che il nucleo I di ϕ è l'ideale di R generato da 2. Quindi il primo teorema di isomorfismo implica che R/I è isomorfo a $\mathbf{Z}_2$. Ne segue che $\#(R/I) = 2$.

   Verifichiamo che il nucleo I di ϕ è generato da 2. Infatti, si ha che $2 \in I$. Viceversa, se $f \in R$ è contenuto nel nucleo di ϕ, allora il suo termine noto è pari. Questo implica che $\frac{1}{2}f$ è un polinomio in $\mathbf{C}[X]$ con termine noto in $\mathbf{Z}$. In altre parole, $\frac{1}{2}f$ appartiene ad R e quindi $f = \frac{1}{2}f \cdot 2$ è un multiplo di 2.