Algebra 2 (Schoof) 2^o esonero 25 gennaio 2010, ore 11:00–13:00.

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

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

1. Determinare tutti i gruppi di ordine 175 a meno di isomorfismo.

   (*Questo esercizio è una variazione dell'Eserc.12.8.*) Sia G un gruppo di ordine $175 = 5^2 \cdot 7$. Per i teoremi di Sylow G ha un unico 7-sottogruppo di Sylow P, il quale è per forza normale. Similmente G ha un unico 5-sottogruppo di Sylow Q, il quale è normale. Poiché l'intersezione $P \cap Q$ è banale, i sottogruppi normali P e Q commutano e si ha che $G \cong P \times Q$. Il gruppo P ha ordine 7 ed è quindi isomorfo a $\mathbf{Z}_7$. Il gruppo Q ha ordine 5^2 ed è quindi commutativo (Eserc. 8.11). Si ha che $Q \cong \mathbf{Z}_{25}$ oppure $Q \cong \mathbf{Z}_5 \times \mathbf{Z}_5$.

   Per il teorema cinese del resto concludiamo che $G \cong \mathbf{Z}_{175}$ oppure $G \cong \mathbf{Z}_{35} \times \mathbf{Z}_5$.

2. Sia S_3 il gruppo simmetrico su 3 elementi e sia $\mathbf{Z}_6$ il gruppo additivo delle classi resto modulo 6. Quanti omomorfismi $f : S_3 \longrightarrow \mathbf{Z}_6$ ci sono? E quanti omomorfismi $f : \mathbf{Z}_6 \longrightarrow S_3$ ci sono?

   Poiché $\mathbf{Z}_6$ è abeliano, per ogni omomorfismo $S_3 \longrightarrow \mathbf{Z}_6$, il sottogruppo S_3' dei commutatori di S_3 è contenuto in $\ker f$. Si sa che $S_3' = A_3$. Ogni omomorfismo f si fattorizza quindi via un omomorfismo $S_3/A_3 \longrightarrow \mathbf{Z}_6$. Poiché S_3/A_3 è ciclico di ordine 2, ci sono *due* omomorfismi: quello banale e quello che manda il generatore nell'unico elemento di ordine 2 in $\mathbf{Z}_6$. In termini espliciti, per l'omomorfismo non banale $f : S_3 \longrightarrow \mathbf{Z}_6$ si ha: $f(\sigma) = \overline{0}$ per $\sigma \in S_3$ pari, mentre $f(\sigma) = \overline{3}$ per σ dispari.

   Per determinare gli omomorfismi $\mathbf{Z}_6 \longrightarrow S_3$ conviene prima osservare che ci sono esattamente sei omomorfismi $\mathbf{Z} \longrightarrow S_3$. Infatti, per ogni $\sigma \in S_3$ la mappa cha manda $k \in \mathbf{Z}$ alla permutazione σ^k è un omomorfismo. Per il Teorema di Lagrange si ha che $x^6 = 1$ per ogni $x \in S_3$. Questo implica che il sottogruppo $6\mathbf{Z}$ di $\mathbf{Z}$ è contenuto nel nucleo di ogni omomorfismo $\mathbf{Z} \longrightarrow S_3$. Questo dimostra che ci sono anche esattamente *sei* omomorfismi $\mathbf{Z}_6 \longrightarrow S_3$: per ogni $\sigma \in S_3$ la mappa cha manda $\overline{k} \in \mathbf{Z}_6$ nella permutazione σ^k è un omomorfismo ben definito.

3. Determinare il grado del campo di spezzamento del polinomio $(X^3 - 2)(X^2 - 2)$ su $\mathbf{Q}$.

   Sia ω una radice cubica primitiva dell'unità. Poichè le cinque radici di $(X^3 - 2)(X^2 - 2)$ sono $\pm\sqrt{2}$ e $\omega^i \sqrt[3]{2}$ (per $i = 0, 1, 2$), il campo di spezzamento di $(X^3 - 2)(X^2 - 2)$ è uguale a $F = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$. Per calcolare il grado $[F : \mathbf{Q}]$ osserviamo prima che i polinomi minimi di $\sqrt{2}$, $\sqrt[3]{2}$ e ω sono rispettivamente $X^2 - 2$, $X^3 - 2$ e $X^2 + X + 1$, di grado 2, 3 e 2. Si ha quindi che $[F : \mathbf{Q}] \le 2 \cdot 3 \cdot 2 = 12$.

   Per il criterio di Eisenstein il sottocampo $\mathbf{Q}(\sqrt[3]{2})$ di F ha grado 3 su $\mathbf{Q}$. Per la moltiplicatività del grado, $[F : \mathbf{Q}]$ è quindi divisibile per 3. Similmente il sottocampo $\mathbf{Q}(\sqrt{2}, \omega)$ di F ha grado 4 su $\mathbf{Q}$ e quindi $[F : \mathbf{Q}]$ è divisibile per 4. Concludiamo che $[F : \mathbf{Q}]$ è divisibile per 12 ed è quindi vale necessariamente $[F : \mathbf{Q}] = 12$ come richiesto.

   Per vedere che il campo $K = \mathbf{Q}(\sqrt{2}, \omega)$ ha grado 4 su $\mathbf{Q}$ osserviamo prima che $[K : \mathbf{Q}] \le 4$. Il sottocampo $\mathbf{Q}(\sqrt{2})$ ha grado 2 su $\mathbf{Q}$ e quindi $[K : \mathbf{Q}]$ è divisibile per 2. Poiché $\mathbf{Q}(\sqrt{2})$ è isomorfo ad un sottocampo di $\mathbf{R}$, la radice cubica primitiva dell'unità ω non può essere contenuta in K. Il grado di K su $\mathbf{Q}$ non può quindi essere 2 ma è 4.

4. Sia $\mathbf{F}_9$ un campo di 9 elementi. Determinare i gradi dei fattori irriducibili di $X^4 + 1 \in \mathbf{F}_9[X]$.

   Il campo $\mathbf{F}_9$ è il campo di spezzamento di $X^9 - X \in \mathbf{Z}_3[X]$. Poiché $X^4 + 1$ divide $X^9 - X = X(X^4 - 1)(X^4 + 1)$, il polinomio $X^4 + 1$ si fattorizza in fattori di grado 1 in $\mathbf{F}_9[X]$.