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

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

1. Quanti omomorfismi $S_3 \longrightarrow D_4$ ci sono?
2. Dimostrare che un gruppo G di cardinalità 36 non può essere semplice.
3. Sia $f : \mathbf{Z}_{51}^* \longrightarrow \mathbf{Z}_{51}^*$ l'omomorfismo dato da $f(x) = x^4$.
   (a) Dimostrare che $\mathrm{im}(f) \subset \ker(f)$;
   (b) calcolare la struttura del gruppo quoziente $\ker(f)/\mathrm{im}(f)$.
4. (a) Dimostrare che il polinomio $X^2 - 2$ è irriducibile in $\mathbf{F}_5[X]$.
   (b) Dimostrare che $\mathbf{F}_5(\sqrt{2})$ è un campo di spezzamente del polinomio $X^3 - 2$ su $\mathbf{F}_5$.
5. Quanti punti ha $\mathrm{Spec}(\mathbf{Z}_{144})$?
6. (a) Fattorizzare il polinomio $X^4 + 4$ in fattori irriducibili in $\mathbf{Q}[X]$.
   (b) Determinare il grado del campo di spezzamento di $X^4 + 4$ su $\mathbf{Q}$.

Soluzioni.

1. Poiché la cardinalità di D_4 non è divisibile per 3, ogni omomorfismo $f : S_3 \longrightarrow D_4$ ha la proprietà che $A_3 \subset \ker f$ e si fattorizza quindi via il gruppo quoziente S_3/A_3. Il numero di omomorfismi cercato è quindi uguale al numero di omomorfismi $S_3/A_3 \longrightarrow D_4$. Poichè S_3/A_3 ha ordine 2, questo numero è uguale al numero di elementi $x \in D_4$ con $x^2 = 1$. Ce ne sono sei.
2. Questo è l'esercizio 7 (c) del foglio 4.
3. (a) Va dimostrato che $f(f(x)) = x^{16} = 1$ per ogni $x \in \mathbf{Z}_{51}^*$. Si ha che $51 = 3 \cdot 17$. Per il Teorema di Lagrange si sa che $x^{16} \equiv 1 \pmod 3$ per ogni $x \in \mathbf{Z}$ non divisibile per 3 e si sa che $x^{16} \equiv 1 \pmod{17}$ per ogni $x \in \mathbf{Z}$ non divisibile per 17. Questo implica che $x^{16} = 1$ per ogni $x \in \mathbf{Z}_{51}^*$ come richiesto.
   Ogni $x \in \mathbf{Z}_3^*$ soddisfa $x^4 = 1$. Invece l'insieme $\{x \in \mathbf{Z}_{17}^* : x^4 = 1\}$ è un sottogruppo di ordine 4 di $\mathbf{Z}_{17}^*$. Per Il teorema cinese il sottogruppo $\{x \in \mathbf{Z}_{51}^* : x^4 = 1\}$ di $\mathbf{Z}_{51}^*$ ha quindi $2 \cdot 4 = 8$ elementi. Poichè $\#\mathrm{im}(f) \cdot \#\ker(f) = \#(\mathbf{Z}_{51}^*) = \varphi(51) = 32$, il nucleo di f ha $32/8 = 4$ elementi. Il gruppo quoziente $\ker(f)/\mathrm{im}(f)$ ne ha quindi $8/4 = 2$ ed è per forza ciclico.
4. Poiché 2 non è un quadrato in $\mathbf{F}_5$, il polinomio $X^2 - 2$ è irriducibile. Per la parte (b) osserviamo che $X^3 - 2 = (X+2)(X^2 - 2X - 1)$ dove $X^2 - 2X - 1$ è irriducibile in $\mathbf{F}_5[X]$. Questo implica che il campo di spezzamento di $X^3 - 2$ ha grado 2 su $\mathbf{F}_5$ ed è quindi isomorfo a $\mathbf{F}_5(\sqrt{2})$.
5. La domanda è: quanti ideali primi possiede l'anello $\mathbf{Z}_{144}$? Gli ideali primi di $\mathbf{Z}_{144}$ corrispondono biettivamente agli ideali primi di $\mathbf{Z}$ che contengono l'ideale (144). Si tratta dei divisiori primi di 144. Ce ne sono due: 2 e 3.
6. Si ha che $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$. Gli zeri sono $\pm 1 \pm i$ dove $i^2 = -1$. Il campo di spezzamento è quindi $\mathbf{Q}(i)$, il quale ha grado 2 su $\mathbf{Q}$.