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

Accompagnare le risposte con spiegazioni *chiare ed essenziali.* Ogni esercizio vale 6 punti.

1. Determinare il grado del campo di spezzamento del polinomio $X^8 - 1$ su $\mathbf{Q}$.

   Abbiamo che $X^8 - 1 = (X^4+1)(X^2+1)(X+1)(X-1)$. Per il criterio di Eisenstein (con $p = 2$ e sostituzione $X = Y+1$) il polinomio X^4+1 è irriducibile. Sia ζ una radice di X^4+1. Il campo $\mathbf{Q}(\zeta)$ è contenuto nel campo di spezzamento K di X^8-1. Poiché le altre radici di X^8-1 sono ζ^i con $2 \leq i \leq 8$, il polinomio X^8-1 si spezza completamente in $\mathbf{Q}(\zeta)$. Abbiamo quindi che $K = \mathbf{Q}(\zeta)$ e $[K : \mathbf{Q}] = 4$.

2. Sia G un gruppo finito e sia p un numero primo. Dimostrare che se H è un sottogruppo normale di G di cardinalità una potenza di p, allora H è contenuto in ogni p-sottogruppo di Sylow di G.

   Per un teorema di Sylow H è contenuto in un p-sottogruppo di Sylow P. Per vedere che H è contenuto in *ogni* p-sottogruppo di Sylow di G, osserviamo che, per un altro teorema di Sylow, ogni p-sottogruppo di Sylow Q è coniugato con P. In altre parole, esiste $x \in G$ tale che $xPx^{-1} = Q$. Poichè H è normale abbiamo che $xHx^{-1} = H$ e quindi $H = xHx^{-1} \subset xPx^{-1} = Q$ come richiesto.

3. Sia p un numero primo. Quanti polinomi monici e irriducibili di grado 4 ci sono in $\mathbf{Z}_p[X]$?

   Per ogni $n \geq 1$ si sa che $X^{p^n} - X = \prod_{\deg f | n} f$, dove f varia fra i polinomi monici irriducibili $f \in \mathbf{Z}_p[X]$ di grado un divisore di n. Dividendo la formula corrispondente a $n = 4$ per quella corrispondente a $n = 2$, troviamo che il prodotto dei polinomi monici irriducibili $f \in \mathbf{Z}_p[X]$ di grado *uguale* a 4, è uguale al polinomio $(X^{p^4} - X)/(X^{p^2} - X)$ di grado $p^4 - p^2$. Ci sono quindi esattamente $(p^4 - p^2)/4$ polinomi monici irriducibili $f \in \mathbf{Z}_p[X]$ di grado 4.

4. (a) Indicare un ideale massimale dell'anello $\mathbf{R}[X, Y]/(X^2 + Y^2 - 1)$ (cioè esibirne dei generatori).
   (b) Stessa domanda per l'anello $\mathbf{R}[X, Y]/(X^2 + Y^2 + 1)$.

   Prima osserviamo che gli ideali di $\mathbf{R}[X, Y]/(X^2 + Y^2 - 1)$ hanno sempre la forma $I/(X^2 + Y^2 - 1)$ dove I è un ideale di $\mathbf{R}[X, Y]$ che contiene $(X^2 + Y^2 - 1)$. L'ideale $I/(X^2 + Y^2 - 1)$ è massimale se e solo se I è un ideale massimale di $\mathbf{R}[X, Y]$. Mutatis mutandis, la stessa cosa vale per l'anello $\mathbf{R}[X, Y]/(X^2 + Y^2 - 1)$.

   Ci sono *tantissime* soluzioni. In (a) possiamo per esempio prendere $I = (X, Y - 1)$. Infatti $X^2 + Y^2 - 1 \in I$ e il quoziente $\mathbf{R}[X, Y]/I$ è isomorfo al campo $\mathbf{R}$. L'ideale I è quindi massimale. In (b) possiamo prendere $I = (X, Y^2 + 1)$. Questa volta il quoziente è isomorfo al campo $\mathbf{C}$.

5. Siano $a, b, c \in \mathbf{C}$ gli zeri del polinomio $X^3 + X^2 + 1$. Determinare
   $$\det \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}.$$

   Il determinante è uguale a $a^3 + b^3 + c^3 - 3abc$. Poiché per $x = a, b, c$ si ha che $x^3 = -x^2 - 1$, il determinante è uguale a $-(a^2 + b^2 + c^2) - 3 - 3abc$. Si ha che $a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + bc + ca)$. I coefficienti del polinomio $X^3 + X^2 + 1$ sono le funzioni simmetriche elementari valutate in a, b, c e quindi si ha che $a + b + c = -1$, $ab + bc + ca = 0$ e $abc = -1$. Concludiamo che il determinante è uguale a $-((-1)^2 - 2 \cdot 0) - 3 - 3(-1) = -1$.