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

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

1. Siano $a, b, c \in \mathbf{Z}$ e siano $\alpha_1, \alpha_2, \alpha_3$ gli zeri complessi del polinomio $f = X^3+aX^2+bX+c \in \mathbf{Z}[X]$. Determinare la funzione simmetrica $(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)(\alpha_2+\alpha_3)$ in termini dei coefficienti di f.

2. Sia G un gruppo e sia $H \subset G$ un sottogruppo che contiene il sottogruppo $[G, G]$ dei commutatori. Dimostrare che H è un sottogruppo normale e che G/H è un gruppo abeliano.

3. (a) Quanti omomorfismi di gruppi $S_3 \longrightarrow \mathbf{Z}_9$ ci sono?
   (b) Quanti omomorfismi di gruppi $\mathbf{Z}_9 \longrightarrow S_3$ ci sono?

4. Quanti elementi invertibili contiene l'anello $\mathbf{Z}[X]/(X^2+1, X^2-4)$?

5. Sia $F = \{a + b\sqrt{5} : a, b \in \mathbf{Q}\}$.
   (a) Dimostrare che F è un sottoanello di $\mathbf{R}$.
   (b) Dimostrare che F è isomorfo all'anello $\mathbf{Q}[X]/(X^2-5)$.

6. Sia R un anello commutativo e sia $a \in R$ con $a \neq 0$.
   (a) Dimostrare che se a è un divisore di zero, allora non è invertibile.
   (b) Dimostrare che se R è finito, vale anche il viceversa.

Soluzioni.

1. Questo è l'esercizio 5 (a) del foglio 13.
2. Questo è l'esercizio 2 del foglio 14.
3. Ci sono tre omomorfismi $\mathbf{Z}_9 \longrightarrow S_3$, vale a dire quelli che mandano $\overline{1}$ in uno dei tre elementi di A_3. Invece, poiché $\mathbf{Z}_9$ è abeliano, ogni omomorfismo $S_3 \longrightarrow \mathbf{Z}_9$ si fattorizza via $S_3/[S_3, S_3]$. Dal fatto che l'ordine di $S_3/[S_3, S_3]$ è 2 ed è quindi coprimo con 9, segue che l'unico omomorfismo $S_3 \longrightarrow \mathbf{Z}_9$ è quello banale.
4. Dal fatto che $5 = (X^2+1) + (X^2-4)$ segue che l'ideale (X^2+1, X^2-4) è uguale a $(5, X^2-4)$. Abbiamo quindi un isomorfismo $R = \mathbf{Z}[X]/(X^2+1, X^2-4) \cong \mathbf{Z}_5[X]/(X^2-4)$. Per il Teorema cinese l'anello R è isomorfo a $\mathbf{Z}[X]/(X-2) \times \mathbf{Z}[X]/(X+2) \cong \mathbf{Z}_5 \times \mathbf{Z}_5$. Abbiamo quindi che $R^* = \mathbf{Z}_5^* \times \mathbf{Z}_5^*$. Dal fatto che $\mathbf{Z}_5$ è un campo segue che R ha $4 \cdot 4 = 16$ elementi invertibili.
5. L'insieme F contiene $0, 1$ ed è chiuso rispetto all'addizione e la moltiplicazione di $\mathbf{R}$. Infatti, si ha che $(a+b\sqrt{5}) + (c+d\sqrt{5}) = (a+c) + (b+d)\sqrt{5}$ e $(a+b\sqrt{5})(c+d\sqrt{5}) = (ac+5bd) + (ad+bc)\sqrt{5}$ per ogni $a, b, c, d \in \mathbf{Q}$. Per la parte (b) consideriamo l'omomorfismo $\phi : \mathbf{Q}[X] \longrightarrow \mathbf{R}$ dato da $\phi(g) = g(\sqrt{5})$. Verifichiamo che l'immagine di ϕ è F e il suo nucleo è (X^2-5). Il Teorema di isomorfismo implica quindi che F è isomorfo a $\mathbf{Q}[X]/(X^2-5)$.
   Dalla definizione di F segue che l'immagine di ϕ è F. È chiaro che $(X^2-5) \subset \ker(\phi)$. Per l'inclusione opposta, sia $g \in \ker(\phi)$. Facciamo una divisone con resto: esistono $q, r \in \mathbf{Q}[X]$ tali che $g = h(X^2-5)+r$ con r della forma $a+bX$ per qualche $a, b \in \mathbf{Q}$. Sostituzione di $\sqrt{5}$ ci da $0 = g(\sqrt{5}) = h(\sqrt{5}) \cdot 0 + r(\sqrt{5})$ e quindi $a + b\sqrt{5} = r(\sqrt{5}) = 0$. Dal fatto che $\sqrt{5} \notin \mathbf{Q}$ segue che $a = b = 0$ e quindi $r = 0$. Questo implica che X^2-5 divide g. Abbiamo quindi che $\ker(\phi) \subset (X^2-5)$ come richiesto.
6. (a) Se a è un divisore di zero, allora esiste $b \in R$ non zero con $ba = 0$. Supponiamo per assurdo che a sia anche invertibile. Allora esiste $c \in R$ con $ac = 1$. Questo implica che $0 = (ba)c = b(ac) = b \cdot 1 = b$. Contraddizione perché $b \neq 0$. Per (b) consideriamo l'applicazione $m : R \longrightarrow R$ data dalla moltiplicazione per a. Dalla proprietà distributiva di R segue che m è un omomorfismo di gruppi additivi. Se a *non* è un divisore di zero, allora il nucleo di m è $\{0\}$ e m è iniettivo. Il fatto che R è finito implica che m è quindi anche suriettivo. Esiste quindi un elemento $r \in R$ con $ar = m(r) = 1$. In altre parole, a è invertibile.