COGNOME

NOME

Risolvere gli esercizi negli spazi predisposti. Accompagnare le risposte con spiegazioni chiare ed essenziali. Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 5 punti.

1. Determinare il polinomio minimo di $(1 + \sqrt{3})/\sqrt{2}$ su $\mathbf{Q}$.
2. Sia G un gruppo e sia $H \subset G$ un sottogruppo con $[G : H] = n$. Dimostrare che H contiene un sottogruppo N , normale in G , con la proprietà che $[G : N]$ divide $n!$.
3. (a) Esibire un anello A con $\#A^* = 3$.
(b) Sia A un anello con $\#A^*$ dispari. Dimostrare che $a + a = 0$ per ogni $a \in A$.
4. Siano $n \geq m \geq 1$ numeri naturali dispari. Sia σ un m -ciclo nel gruppo simmetrico S_n . Dimostrare che σ e σ^2 sono coniugati in S_n .
5. Sia p un primo e sia k un campo finito di p^2 elementi.
(a) Dimostrare che k contiene $\mathbf{Z}_p$.
(b) Dimostrare che per ogni $a \in \mathbf{Z}_p$ il polinomio $X^2 - a$ è riducibile nell'anello $k[X]$.
6. Sia A l'anello $\mathbf{Z}_3[X]/(X^4 - 1)$ e sia $\overline{X} \in A$ la classe laterale di X .
(a) Dimostrare che $\overline{X}$ è invertibile in A .
(b) Sia $J \subset A$ l'ideale generato da $\overline{X}^3 - 1$. Quanti elementi ha l'anello quoziente A/J ?

Soluzioni.

1. Questo è l'esercizio 1 del foglio 13.
2. Questo è l'esercizio 4 del foglio 1.
3. (a) Gli elementi invertibili del campo $\mathbf{F}_4$ sono tre. (b) Poiché $-1 \in A^*$ soddisfa $(-1)^2 = 1$, il fatto che la cardinalità del gruppo A^* è dispari, implica $-1 = 1$ in A . E quindi $a + a = 1 \cdot a + 1 \cdot a = (1 + 1)a = (1 + (-1))a = 0 \cdot a = 0$.
4. Per m dispari il quadrato di un m -ciclo σ è sempre un m -ciclo. Ecco perché σ e σ^2 sono coniugati.
5. (a) Poiché $\#k$ è una potenza di p , il sottocampo minimale di k può solo essere $\mathbf{Z}_p$. (b) Se $X^2 - a$ è riducibile in $\mathbf{Z}_p[X]$, lo è anche in $k[X]$. Se $X^2 - a$ è irriducibile in $\mathbf{Z}_p[X]$, allora il suo campo di spezzamento K è un'estensione di grado 2 di $\mathbf{Z}_p$ e ha quindi p^2 elementi. Poiché $\#k = \#K$, i campi k e K sono isomorfi. Il campo k contiene quindi gli zeri di $X^2 - a$.
6. (a) Si ha che $\overline{X}^4 = 1$ in A . (b) L'anello A/J è isomorfo a $\mathbf{F}_3[X]/(X^4 - 1, X^3 - 1)$. Poiché l'ideale $(X^4 - 1, X^3 - 1)$ è generato dal $\text{mcd}(X^4 - 1, X^3 - 1) = X - 1$, abbiamo che $A/J \cong \mathbf{Z}_3[X]/(X - 1) \cong \mathbf{Z}_3$.