

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. Sia $n > 1$ un intero dispari e sia ϕ la funzione di Euler.
 - (a) Dimostrare che $\phi(n)$ è pari
 - (b) Dimostrare che $\phi(n)/2$ è dispari se e solo se n è potenza di un numero primo $p \equiv 3 \pmod{4}$.
2. Consideriamo gli ideali (X) , (X, Y) e (X, Y, Z) dell'anello $\mathbf{Z}[X, Y, Z]$. Quali fra loro sono ideali primi? Quali sono ideali massimali?
3. Sia p un numero primo. Sia G il gruppo degli automorfismi di un campo finito k di p^p elementi. Quante sono le orbite dell'azione di G su k ?
4. Determinare il grado del campo di spezzamento di $X^8 - 2$ su $\mathbf{Q}$.
5. Sia p un primo e sia P un p -sottogruppo di Sylow di un gruppo finito G . Dimostrare che ci sono esattamente $[G : N_G(P)]$ p -sottogruppi di Sylow in G . Qua $N_G(P)$ indica il normalizzante di P in G , cioè $N_G(P) = \{g \in G : gPg^{-1} = P\}$.
6. Dimostrare che esiste uno $\mathbf{Z}[i]$ -modulo di cardinalità 2, ma non ne esiste uno di cardinalità 3.

Soluzioni.

1. (a) L'elemento $-1 \in \mathbf{Z}_n^*$ ha ordine 2. Per Lagrange 2 divide $\#\mathbf{Z}_n^* = \phi(n)$. (b) Se $n = p^k$ per un primo $p \equiv 3 \pmod{4}$, allora $\phi(n)/2 = p^{k-1}(p-1)/2$ è dispari. Viceversa, se n è potenza di un primo $p \equiv 1 \pmod{4}$, allora $\phi(n)$ è divisibile per 4. Se n è divisibile per due primi p e q distinti, consideriamo l'omomorfismo canonico suriettivo $\mathbf{Z}_n^* \rightarrow \mathbf{Z}_{pq}^*$. Ne segue che $\phi(pq)$ divide $\phi(n)$. Poichè p e q sono dispari, sia $\phi(pq) = (p-1)(q-1)$ che $\phi(n)$ sono divisibili per 4.
2. L'anello $\mathbf{Z}[X, Y, Z]$ modulo (X) , (X, Y) e (X, Y, Z) è rispettivamente isomorfo a $\mathbf{Z}[Y, Z]$, $\mathbf{Z}[Z]$ e $\mathbf{Z}$. Sono tutti domini ma non campi. Gli ideali sono quindi primi, ma non massimali.
3. Poiché G ha ordine p , le orbite hanno 1 o p elementi. Le orbite di 1 elemento sono i punti fissi. Si tratta degli elementi del sottocampo $\mathbf{F}_p$ e ce ne sono p . Le altre orbite hanno p elementi. Ci sono $(\#k - \#\mathbf{F}_p)/p = (p^p - p)/p$ orbite. In totale ci sono quindi $p^{p-1} + p - 1$ orbite.
4. Il polinomio $X^8 - 2$ è di Eisenstein ed è quindi irriducibile. Sia a uno zero di $X^8 - 2$. Allora il grado $[\mathbf{Q}(a) : \mathbf{Q}]$ è uguale a 8. Nell'anello $\mathbf{Q}(a)[X]$ abbiamo che $X^8 - 2 = X^8 - a^8 = (X^4 - a^4)(X^4 + a^4)$. Gli zeri di $X^4 - a^4$ sono $\pm a$ e $\pm ia$ dove $i^2 = -1$. Ne segue che $i \in K$. Affermiamo che $K = \mathbf{Q}(a, i)$ e quindi $[K : \mathbf{Q}] = 8 \cdot 2 = 16$. Infatti, sia b uno zero di $X^4 + a^4$. Allora $b = az$ dove z soddisfa $z^4 + 1$. Ma il polinomio $X^4 + 1$ ha quattro zeri $(\pm 1 \pm i)/a^4$ distinti in $\mathbf{Q}(i, a)$.
5. Questo è l'esercizio 6 del foglio 2.
6. Questo è l'esercizio 4 del foglio 7.