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 $n \geq 2$ e sia $X = \{1, 2, \dots, n\}$. Il gruppo simmetrico S_n agisce sull'insieme $X \times X$ tramite $\sigma(x, y) = (\sigma(x), \sigma(y))$, per $\sigma \in S_n$ e $x, y \in X$. Quante orbite ci sono?
2. Esistono $\alpha, \beta \in \mathbf{C}$ trascendenti, tali che sia $\alpha + \beta$ che $\alpha\beta$ siano algebrici su $\mathbf{Q}$?
3. Dimostrare che il gruppo *additivo* dell'anello $\mathbf{Z}[X]$ è isomorfo al gruppo *moltiplicativo* dei numeri razionali positivi.
4. Sia f il polinomio $X^4 - X - 1$ in $\mathbf{Z}_3[X]$.
 - (a) Dimostrare che f è irriducibile nell'anello $\mathbf{Z}_3[X]$.
 - (b) Sia a uno zero di f in qualche campo di spezzamento di f . Determinare l'ordine moltiplicativo di a . (Cioè determinare il più piccolo esponente $m > 0$ tale che $a^m = 1$.)
6. Sia A l'insieme dei polinomi $\sum_{i=0}^n a_i X^i$ in $\mathbf{R}[X]$, con $a_1 = 0$.
 - (a) Dimostrare che A non è un ideale di $\mathbf{R}[X]$;
 - (b) Dimostrare che A è un sottoanello di $\mathbf{R}[X]$;
 - (c) Dimostrare che A non è un PID (dominio ad ideali principali).
6. Sia p un primo, sia R l'anello $\mathbf{F}_p[X, Y]$ e sia I l'ideale di R generato da X e Y . Determinare la cardinalità dell'anello quoziente R/I^n , al variare $n \geq 1$.

Soluzioni.

1. Questo è l'esercizio 2 del foglio 3.
2. Questo è l'esercizio 4 del foglio 8.
3. Sia $\{p_0, p_1, p_2, \dots\}$ l'insieme dei numeri primi. Per ogni $x \in \mathbf{Q}_{>0}^*$ esistono unici esponenti $e_i \in \mathbf{Z}$, quasi tutti nulli, tali che x è uguale a $\prod_{i \geq 0} p_i^{e_i}$. La mappa $\phi: \mathbf{Q}_{>0}^* \rightarrow \mathbf{Z}[X]$ data da $\phi(x) = \sum_{i \geq 0} e_i X^i$ è un isomorfismo di gruppi.
4. (a) Il polinomio f non ha zeri in $\mathbf{F}_9$. Ne segue che è irriducibile. (b) L'elemento a sta in un campo di 3^4 elementi. Per Lagrange l'ordine di a divide $3^4 - 1 = 80$. Il termine noto di f è uguale a $a^{1+3+3^2+3^3} = a^{40} = -1$. Ne segue che l'ordine non divide 40. Affermiamo che $a^{16} \neq 1$. Infatti $a^{16} = (a+1)^4 = a^4 + a^3 + a + 1 \neq 1$. Ne segue che l'ordine non divide 16. Concludiamo che l'ordine di a deve essere 80.
5. (a) Si ha che $1 \in A$ e quindi se A fosse un ideale, sarebbe $A = \mathbf{R}[X]$. Assurdo, perché si ha che $X \notin A$. (b) L'insieme A contiene 1 ed è chiuso per somme e prodotti. (c) L'insieme J dei polinomi $\sum_{i=0}^n a_i X^i$ in A con $a_0 = 0$ è un ideale. Sia g un generatore di J . Poiché $J \neq A$, il polinomio g non è invertibile e deve avere grado ≥ 2 . Si sa che g divide X^2 . Ne segue che $g = cX^2$ per qualche $c \in \mathbf{R}^*$. Similmente, g divide anche X^3 in A : si ha che $X^3 = h \cdot X^2$ per qualche $h \in A$. Poiché $\mathbf{R}[X]$ è un dominio, possiamo dividere l'equazione per X^2 . Vediamo che $h = c^{-1}X$. Contraddizione, perché h sta in A .
6. Ogni classe in R/I^n ha un rappresentante unico della forma $\sum_{0 \leq i+j < n} a_{ij} X^i Y^j$, con $a_{ij} \in \mathbf{F}_p$. Ci sono $1 + 2 + \dots + (n-1) + n = \frac{1}{2}n(n+1)$ copie (i, j) con $0 \leq i+j < n$. La cardinalità dell'anello R/I^n è quindi $p^{\frac{1}{2}n(n+1)}$.