

1. Determinare il polinomio minimo di $(1 + \sqrt{3})/\sqrt{2}$ su $\mathbf{Q}$.
2. Per quali numeri naturali n il polinomio $x^{n^4} + x^{n^3} + x^{n^2} + x^n + 1$ di $\mathbf{Q}[X]$ è divisibile per $x^4 + x^3 + x^2 + x + 1$?
3. Siano $a, b \in \mathbf{Z}$ con $\text{mcd}(a, b) = 1$. Dimostrare che l'anello $\mathbf{Z}[X, Y]/(aX + bY)$ è isomorfo all'anello dei polinomi $\mathbf{Z}[T]$.
4. Dimostrare che gli anelli $\mathbf{Z}[X]$ e $\mathbf{Z}[X, Y]/(XY - 1)$ non sono isomorfi.
5. Sia p un numero primo e sia $q = p^f$ per qualche $f \geq 1$. Sia d un divisore di $p - 1$. Dimostrare che $x \in \mathbf{F}_q^*$ è d -esima potenza in $\mathbf{F}_q^*$ se e solo se la sua norma è d -esima potenza in $\mathbf{F}_p^*$.
6. Sia R un anello commutativo con 1. Un elemento $e \in R$ si dice *idempotente* se $e^2 = e$.
 - (a) Determinare gli elementi idempotenti di $\mathbf{Z}_6$ e di $\mathbf{Z}_{100}$.
 - (b) Dimostrare: se $e \in R$ è idempotente anche $1 - e$ lo è.
 - (c) Sia $e \in R$ idempotente; dimostrare che la mappa naturale $R \longrightarrow R/(e) \times R/(1-e)$ è un isomorfismo di anelli.

7. (Funzione ϕ di Euler per $\mathbf{Z}_p[X]$). Sia p un primo. Per $f \in \mathbf{F}_p[X]$ definiamo

$$N(f) = \#\mathbf{F}_p[X]/(f) \quad \text{e} \quad \phi(f) = \#(\mathbf{F}_p[X]/(f))^*.$$

- (a) Siano $f, g \in \mathbf{F}_p[X]$. Dimostrare che $N(fg) = N(f)N(g)$. Se $\text{mcd}(f, g) = 1$ dimostrare che $\phi(fg) = \phi(f)\phi(g)$.
- (b) Sia $f \in \mathbf{F}_p[X]$ irriducibile. Dimostrare che $\phi(f) = N(f) - 1$. Dimostrare che $\phi(f^k) = (N(f) - 1)N(f)^{k-1}$, per ogni $k \geq 1$.
- (c) Sia $f \in \mathbf{F}_p[X]$. Dimostrare che

$$\phi(f) = N(f) \prod_{\substack{g|f \\ g \text{ irr}}} \left(1 - \frac{1}{N(g)}\right).$$

8. (a) Per ogni $n \leq 10$ diverso da 5, esibire un anello A con $\#A^* = n$.
 (b)* Dimostrare che non esiste un anello A con $\#A^* = 5$.
9. Sia $p > 2$ primo, sia $H \subset \mathbf{Z}_p^*$ il sottogruppo dei quadrati e sia H' la classe laterale dei non quadrati. Sia ζ una radice primitiva p -esima dell'unità e siano $\eta, \eta' \in \mathbf{Q}(\zeta)$ i *periodi di Gauss* dati da

$$\eta = \sum_{a \in H} \zeta^a, \quad \text{e} \quad \eta' = \sum_{a \in H'} \zeta^a.$$

- (a) Dimostrare che $\eta + \eta' = -1$.
- (b) Sia $\tau = \eta - \eta'$ la cosiddetta *somma di Gauss*. Dimostrare che $\tau = \sum_{a \in \mathbf{Z}_p^*} \chi(a) \zeta^a$ dove χ è l'unico omomorfismo $\mathbf{Z}_p^* \rightarrow \{\pm 1\}$ di nucleo H .
- (c) Calcolare il polinomio minimo di τ su $\mathbf{Q}$ per $p = 3$ e per $p = 5$.
- (d) Sia $\epsilon = (-1)^{\frac{p-1}{2}}$. Dimostrare che $\tau^2 = \epsilon p$ e che quindi $\eta = -\frac{1}{2} \pm \frac{1}{2} \sqrt{\epsilon p}$. (Sugg: si ha che $\tau^2 = \sum_{a,b} \zeta^{a+b} \chi(ab)$. Il cambiamento di variabile $b = ac$ ci dà che $\tau^2 = \sum_c \chi(c) \sum_a \zeta^{a(c+1)}$. Distinguere i casi $c = -1$ e $c \neq -1$).