Algebra 2 (Schoof) 2^o esonero 18 gennaio 2024, ore 11:00–13:00

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 $K \subset L$ un'estensione di campi di grado $[L : K]$ dispari. Sia $\alpha \in L$. Dimostrare che $K(\alpha) = K(\alpha^2)$.
2. Sia $\mathrm{Tr} : \mathbf{F}_{125} \to \mathbf{F}_5$ la mappa traccia. Quanti elementi x ci sono in $\mathbf{F}_{125}$ con $\mathrm{Tr}(x) = 2$?
3. (a) Dimostrare che $X^2 - 3$ e $X^2 - 2$ sono polinomi irriducibili in $\mathbf{F}_5[X]$.
   (b) Esibire un isomorfismo fra i campi $\mathbf{F}_5(\sqrt{2})$ e $\mathbf{F}_5(\sqrt{3})$.
4. Determinare il grado del campo di spezzamento del polinomio $X^5 - 2$ su $\mathbf{Q}$.
5. Sia $p > 2$ un primo.
   (a) Determinare la cardinalità del gruppo $\mathbf{F}_p^*/\mathbf{F}_p^{*2}$.
   (b) Dimostrare che almeno uno di -1, 2, -2 è un quadrato modulo p.
6. Siano n, m numeri naturali con $\mathrm{mcd}(n, m) = 1$. Supponiamo che il poligono regolare di n lati sia costruibile con riga e compasso. Stessa cosa per il poligono regolare di m lati. Dimostrare che anche il poligono regolare di nm lati è costruibile.

Soluzioni.

1. Questo è l'esercizio 6 del foglio 8.
2. La traccia è un omomorfismo suriettivo di gruppi additivi. Il nucleo consiste negli elementi di traccia zero ed ha $125/5 = 25$ elementi. L'insieme degli elementi di traccia 2 è una classe laterale e quindi anche lui ha 25 elementi.
3. Questo è l'esercizio 7 del foglio 11.
4. Il campo di spezzamento K contiene il sottocampo $\mathbf{Q}(\sqrt[5]{2})$ di grado 5 su $\mathbf{Q}$. Le altre radici di $X^5 - 2$ sono $\zeta\sqrt[5]{2}$, al variare di ζ fra le radici primitive dell'unità. Abbiamo quindi che $K = \mathbf{Q}(\sqrt[5]{2}, \zeta)$. Il polinomio minimo di ζ su $\mathbf{Q}$ è $X^4 + X^3 + X^2 + X + 1$. Ne segue che il grado $[K : \mathbf{Q}(\sqrt[5]{2})]$ non supera 4. Abbiamo quindi che $[K : \mathbf{Q}] \leq 20$. D'altra parte K contiene i sottocampi $\mathbf{Q}(\sqrt[5]{2})$ e $\mathbf{Q}(\zeta)$ rispettivamente di grado 5 e 4. Il grado $[K : \mathbf{Q}]$ è quindi divisibile per $4 \cdot 5 = 20$. Conclusione: $[K : \mathbf{Q}] = 20$.
5. Poiché $\mathbf{F}_p^*$ è ciclico, il gruppo $\mathbf{F}_p^*/\mathbf{F}_p^{*2}$ ha cardinalità 2 ed è quindi isomorfo a $\mathbf{Z}_2$. Se -1, 2, -2 non sono quadrati modulo p, allora loro immagini in $\mathbf{F}_p^*/\mathbf{F}_p^{*2}$ sono uguali all'elemento non neutro. Questo implica che anche loro prodotto non è un quadrato. Ma questo è assurdo, perché il prodotto è uguale a 4.
6. Per Bézout esistono $a, b \in \mathbf{Z}$ con $an + bm = 1$. Per ipotesi i numeri $\exp(\frac{2\pi i}{n})$ e $\exp(\frac{2\pi i}{m})$ appartengono al sottocampo F di $\mathbf{C}$ dei numeri costruibili. La relazione $\frac{a}{m} + \frac{b}{n} = \frac{1}{nm}$ implica che $\exp(\frac{2\pi i}{nm})$ è uguale a $\exp(\frac{2\pi i}{n})^b \exp(\frac{2\pi i}{n})^a$ e quindi appartiene ad F.