

Tutorato di TE1

A.A. 2009-2010 - Docente: Prof. F. Pappalardi

Tutori: Annamaria Iezzi e Dario Spirito

TUTORATO 8

6 MAGGIO 2010

- Determinare un campo di spezzamento e il gruppo di Galois dei seguenti polinomi:
 - $(X^2 + X + 1)(X^3 + X^2 + 1) \in \mathbb{F}_2[X]$
 - $(X^3 + X + 1)(X^6 + X + 1) \in \mathbb{F}_3[X]$
 - $(X^4 + X + 1)(X^4 + X^3 + 1)(X^3 + X + 1)(X^2 + X + 1) \in \mathbb{F}_2[X]$
 - $(X^3 + X + 1)(X^3 + X^2 + 1)(X^9 + X^6 + 1)(X^{27} + 2X^9 + 1) \in \mathbb{F}_3[X]$
- Sia $f(X) = X^4 + X + 2 \in \mathbb{F}_3[X]$, e siano K un suo campo di spezzamento su \mathbb{F}_3 e $\alpha \in K$ una sua radice.
 - Dimostrare che f è irriducibile e separabile.
 - Dimostrare che esiste un unico automorfismo τ di $\mathbb{F}_3(\alpha)$ tale che $\tau(\alpha) = \alpha^3$.
 - Dimostrare che $K = \mathbb{F}_3(\alpha)$, e descrivere la corrispondenza di Galois per l'ampliamento $\mathbb{F}_3 \subseteq K$.
 - Determinare un elemento primitivo per ciascun campo intermedio tra \mathbb{F}_3 e K .
- Siano $f(X) = X^2 + 2X + 3$ e $g(X) = X^2 + 4$ polinomi in $\mathbb{F}_7[X]$. Determinare, in un loro campo di spezzamento, le radici dell'uno in funzione di quelle dell'altro.
- Sia α una radice del polinomio $f(X) = X^2 + 2 \in \mathbb{F}_5[X]$. Determinare un generatore del gruppo moltiplicativo del campo di spezzamento di f in funzione di α .
- Determinare tutti i polinomi irriducibili di terzo grado su \mathbb{F}_3 e quelli di quarto grado su \mathbb{F}_2 .
- Stabilire se esistono polinomi irriducibili su \mathbb{F}_3 di grado 2 o 3 che si spezzano linearmente sul campo con 27 elementi e in caso affermativo determinarne almeno uno.
- Sia $M_p := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{F}_p \right\}$.
 - Verificare che M_{11} è un campo ma M_5 no.
 - Dare una condizione necessaria e sufficiente perché M_p sia un campo.
 - In questo caso, dimostrare che l'applicazione

$$\psi : \mathbb{F}_p \longrightarrow M_p, \quad a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

è un'immersione, e che $[M_p, \mathbb{F}_p] = 2$

d) Nel caso $p = 7$, trovare l'inverso di $\begin{pmatrix} 1 & 2 \\ 5 & 1 \end{pmatrix}$.

e) Dimostrare che, se a e b sono a valori in un campo F di caratteristica 0, l'insieme M definito come prima è un campo se e solo se $i \notin F$. A cosa è isomorfo M in questo caso?