Prof. Lidia Angeleri
Università degli Studi di Verona
a.a. 2011/12

# Esercizi per Algebra Computazionale (Modulo I)

1. (a) Si verifichi che $f = x^5 - x + 1$ è un polinomio irriducibile in $\mathbb{F}_3[x]$, ma riducibile in $\mathbb{F}_2[x]$.
   (b) Si scomponga $f$ in polinomi irriducibili in $\mathbb{F}_2[x]$.

2. Si consideri il campo $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(f)$ per $f = x^2 + 1 \in \mathbb{F}_3[x]$.
   (a) Si elenchino gli elementi di $F$ e si determini la tavola dell'addizione in $F$.
   (b) Per $\alpha = \overline{x}$ si calcolino i prodotti $(1 + \alpha) \cdot (2 + \alpha)$ e $(1 + \alpha)^2$.
   (c) Si determini l'elemento inverso di $(1 + 2\alpha)$.

3. Si trovino tutti i sottocampi di $\mathbb{F}_{2^7}$, $\mathbb{F}_{2^{15}}$, $\mathbb{F}_{2^{18}}$.

4. Si determini (a meno di isomorfismo) il campo di riducibilitá completa dei polinomi
   (a) $x^4 + x^3 + 1$ su $K = \mathbb{Z}/2\mathbb{Z}$.
   (b) $x^3 + x^2 + x + 1$ su $K = \mathbb{Z}/3\mathbb{Z}$.
   (c) $x^4 + 2\,x^2 + 2\,x + 2$ su $K = \mathbb{Z}/3\mathbb{Z}$.

5. Sia $K = \mathbb{F}_2$.

   (a) Si verifichi che $f = x^4 + x + 1$ è irriducibile su $K$.

   (b) Si determinino tutti gli elementi di $K[x]/(f) \cong \mathbb{F}_{16}$.

   (c) Quali elementi sono primitivi?

   (d) Si determinino tutti i sottocampi di $\mathbb{F}_{16}$ e per ciascun sottocampo tutti i suoi elementi.

   (e) Si scomponga il polinomio $x^{16} - x$ in polinomi irriducibili su $K$.

   (f) Si scomponga il polinomio $x^{16} - x$ in polinomi irriducibili su $\mathbb{F}_4$.

   (g) Si scomponga il polinomio $x^{15} - 1$ in polinomi ciclotomici.

6. Si determini il numero di fattori nella scomposizione in fattori irriducibili di $x^{63}-1$ su $\mathbb{F}_2$ usando

   (a) i laterali 2-ciclotomici,

   (b) la scomposizione in polinomi ciclotomici.

7. (Per chi ha seguito il corso "Algebra" del CdS Matematica Applicata) Siano $p$ un numero primo, $n \in \mathbb{N}$, e $F$ un campo finito di $p^n$ elementi. Si ricordi che $\mathbb{F}_p \subset F$ è un'estensione di Galois il cui gruppo di Galois $G = \mathrm{Gal}(F/\mathbb{F}_p)$ è generato dall'automorfismo di Frobenius $\varphi : F \to F$, $x \mapsto x^p$, cioè $G =< \varphi >$.

   Sia $m$ un divisore di $n$. Consideriamo il sottogruppo $H =< \varphi^m >$ con il suo campo fisso $L = \mathrm{Fix}_F(H)$. Sappiamo per il Teorema Fondamentale della Teoria di Galois che il grado $[L : \mathbb{F}_p]$ è pari all'indice $[G : H]$ di $H$ in $G$. Si dimostri:

   (a) $H$ ha ordine $\frac{n}{m}$.

   (b) $L$ ha $p^m$ elementi.

   (c) $L$ è l'unico sottocampo di $F$ di $p^m$ elementi.