Prof. Lidia Angeleri
Università degli Studi di Verona
a.a. 2009/2010

Esercizi per Algebra Computazionale
Foglio 1

1. Sia $\varphi : K \to F$ un omomorfismo di campi. Si verifichi che $\mathrm{Im}\varphi$ è un sottocampo di F.

2. Si dimostri:

   (a) Se un polinomio $f \in K[x]$ di grado 4 o 5 su un campo K è riducibile e non ha zeri, allora possiede un divisore monico irriducibile di secondo grado.

   (b) Gli unici polinomi monici irriducibili di secondo grado in $\mathbb{F}_3[x]$ sono $x^2 + 1, x^2 + x + 2$, e $x^2 + 2\,x + 2$.

   (c) $f = x^5 - x + 1$ è un polinomio irriducibile in $\mathbb{F}_3[x]$, ma riducibile in $\mathbb{F}_2[x]$.

   (d) Si scomponga f in polinomi irriducibili in $\mathbb{F}_2[x]$.

3. Si consideri il campo $F = \mathbb{F}_3[x]/(f)$ 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) Si calcolino i prodotti $(\overline{1} + \overline{x}) \cdot (\overline{2} + \overline{x})$ e $(\overline{1} + \overline{x})^2$.

   (c) Si determini l'elemento inverso di $(\overline{1} + \overline{2}\overline{x})$.

Prof. Lidia Angeleri
Università degli Studi di Verona
a.a. 2009/2010

Esercizi per Algebra Computazionale
Foglio 2

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

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

3. (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.