Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Prova scritta per il Corso di Algebra

14 gennaio 2009

1. Si dia la definizione di anello euclideo. (*3 punti*)

2. Si enunci il Teorema di Classificazione dei Campi Finiti. (*3 punti*)

3. Si decida se sono veri o falsi i seguenti enunciati.
   (a) Un'estensione $K \subset F$ di grado 7 non ha campi intermedi propri $K \subset L \subset F$.
   (b) Se $K \subset F$ è un'estensione di Galois di grado 4 e $K \subset L \subset F$ è un campo intermedio, allora $K \subset L$ è un'estensione di Galois.
   (c) Per ogni $n \geq 2$ il polinomio $x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ è irriducibile su $\mathbb{Z}$.

   (*6 punti*)

4. Siano K un campo, $f \in K[x]$ un polinomio irriducibile e separabile, e sia F il campo di riducibilità completa di f su K. Si dimostri: Se $\mathrm{Gal}(F/K)$ è un gruppo abeliano, allora per ogni zero $\alpha \in F$ di f si ha $F = K(\alpha)$. (*6 punti*)

5. Si dimostri che $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{3})$ non è un'estensione di Galois. (*6 punti*)

6. Siano $K = \mathbb{Z}/2\,\mathbb{Z}$ e $f = x^4 + x^3 + x^2 + x + 1 \in K[x]$. Si dimostri che $K[x]/(f)$ è isomorfo a $GF(16)$. (*6 punti*)

Risposte

3. (a) VERO. Altrimenti $[L : K]$ sarebbe un divisore non banale di 7 per il Lemma del Grado.

   (b) VERO. Infatti per il Teorema Fondamentale della Teoria di Galois sappiamo che $L \subset F$ è un'estensione di Galois, e inoltre $K \subset L$ è un'estensione di Galois se e solo se $H = \mathrm{Gal}(F/L)$ è un sottogruppo normale di $G = \mathrm{Gal}(F/K)$. Poiché G ha ordine $[F : K] = 4$, l'ordine di H dev'essere uguale a $1, 2$ oppure 4. Se $\mid H \mid \in \{1, 4\}$, allora $H = \{\mathrm{id}\}$ oppure $H = G$ è chiaramente un sottogruppo normale. Se $\mid H \mid= 2$, allora H è un sottogruppo di G di indice 2 ed è pertanto normale anche in questo caso.

   (c) FALSO ad esempio per $n = 4$, poiché $x^3 + x^2 + x + 1$ possiede lo zero -1 ed è quindi riducibile.

4. Poiché F è campo di riducibilità completa di un polinomio separabile su K, sappiamo che $K \subset F$ è un'estensione di Galois. Inoltre qualsiasi sottogruppo del gruppo abeliano $G = \mathrm{Gal}(F/K)$ è un sottogruppo normale, quindi applicando il Teorema Fondamentale della Teoria di Galois al campo intermedio $K \subset K(\alpha) \subset F$ vediamo che $K \subset K(\alpha)$ è un'estensione di Galois e pertanto normale. Ma allora il polinomio minimo h di α su K è prodotto di fattori lineari. Poiché f e h coincidono a meno di una costante, concludiamo che f è prodotto di fattori lineari su $K(\alpha)$ e dunque $F = K(\alpha)$.

5. Sia $F = \mathbb{Q}(\sqrt[4]{3})$. Il polinomio $f = x^4 - 3$ è irriducibile su $\mathbb{Q}$ per il Criterio di Eisenstein. Quindi f è il polinomio minimo di $\sqrt[4]{3}$ su $\mathbb{Q}$ e pertanto $[F : \mathbb{Q}] = 4$.

   Calcoliamo adesso il gruppo di Galois $G = \mathrm{Gal}(F/\mathbb{Q})$. Se $\sigma \in G$, allora $\sigma(\sqrt[4]{3})^4 = \sigma(3) = 3$ e $\sigma(\sqrt[4]{3}) \in F \subset \mathbb{R}$, quindi $\sigma(\sqrt[4]{3}) = \sqrt[4]{3}$ oppure $\sigma(\sqrt[4]{3}) = -\sqrt[4]{3}$. Poiché $1, \sqrt[4]{3}, (\sqrt[4]{3})^2, (\sqrt[4]{3})^3$ è una base di F su $\mathbb{Q}$, l'applicazione σ è univocamente determinata dai valori assunti su $\sqrt[4]{3}$. Concludiamo quindi che il gruppo di Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ ha ordine 2. Ma allora

   $$[F : \mathbb{Q}] \neq \mid \mathrm{Gal}(F/\mathbb{Q}) \mid$$

   e pertanto $\mathbb{Q} \subset F$ non è un'estensione di Galois.

6. Si verifica che f è irriducibile in quanto non ha zeri né divisori di grado due in $K[x]$. Dunque $F = K[x]/(f)$ è un campo. Inoltre $[F : K] = \deg f = 4$, quindi $F \cong K^4$ possiede $2^4 = 16$ elementi ed è pertanto isomorfo a $GF(16)$.