Prof. Lidia Angeleri
Università di Verona, 2010/11
Corso di Laurea in Matematica Applicata

Prova scritta per il Corso di Algebra

2 febbraio 2011

1. (a) Si enunci il Teorema di Kronecker. (*2 punti*)
   (b) Si dimostri il Teorema di Kronecker. (*3 punti*)
   (c) Si dia la definizione del campo di riducibilità completa F di un polinomio $f \in K[x]$ su un campo K. (*2 punti*)
   (d) Si discutano esistenza e unicità di F. (*3 punti*)

2. Sia F il campo di riducibilità completa del polinomio $f = x^3 - 9$ su $\mathbb{Q}$.
   (a) Si determini (a meno di isomorfismo) $G = \mathrm{Gal}(F/\mathbb{Q})$. (*4 punti*)
   (b) Si determini (a meno di isomorfismo) il gruppo di Galois $H = \mathrm{Gal}(F/\mathbb{Q}_3)$, dove $\mathbb{Q}_3$ è il campo di riducibilità completa del polinomio $g = x^3 - 1$ su $\mathbb{Q}$. È un sottogruppo normale di G? (*4 punti*)

3. Si decida se sono veri o falsi i seguenti enunciati.
   (a) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{7})$ è un'estensione di Galois.
   (b) Ogni estensione per radicali è un'estensione di Galois.
   (c) $x^3 + x^2 + 2x + 2$ è un polinomio irriducibile su $\mathbb{Z}/3\mathbb{Z}$.
   (d) Se f è un polinomio irriducibile e separabile di grado 5 su un campo K e L è il campo di riducibilità completa di f su K, allora $[L : K]$ divide 120.

   (*8 punti*)

4. Quanti sono i campi intermedi propri $GF(4) \subset L \subset GF(64)$? (*4 punti*)

Risposte

Esercizio 2

(a) Sappiamo che $\mathbb{Q} \subset F$ è un'estensione di Galois il cui gruppo di Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ è isomorfo a un sottogruppo di S_3. Calcoliamo l'ordine di G. Gli zeri di f sono $\sqrt[3]{9}, \alpha\sqrt[3]{9}, \alpha^2\sqrt[3]{9}$ dove α è una radice terza primitiva dell'unità. Dunque f è irriducibile su $\mathbb{Q}$ ed è pertanto polinomio minimo di $\sqrt[3]{9}$ su $\mathbb{Q}$. Segue che $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{9})$ è un'estensione di grado 3. Inoltre $\mathbb{Q}(\sqrt[3]{9}) \subset F$ è un'estensione propria e ha almeno grado 2. Dunque $6 \leq [F : \mathbb{Q}] \leq 3!$ e pertanto $[F : \mathbb{Q}] = |\mathrm{Gal}(F/\mathbb{Q})| = 6$. Concludiamo che $G \cong S_3$.

(b) Si ha $\mathbb{Q} \subset \mathbb{Q}_3 \subset F$, dove $\mathbb{Q} \subset \mathbb{Q}_3$ e $\mathbb{Q} \subset F$ sono estensioni di Galois. Per il Teorema Fondamentale della Teoria di Galois $H = \mathrm{Gal}(F/\mathbb{Q}_3)$ è un sottogruppo normale di G e $G/H \cong \mathrm{Gal}(\mathbb{Q}_3/\mathbb{Q})$. Sappiamo che $|\mathrm{Gal}(\mathbb{Q}_3/\mathbb{Q})| = [\mathbb{Q}_3 : \mathbb{Q}] = 2$ (infatti $\mathbb{Q}_3 = \mathbb{Q}(\alpha)$ e $x^2 + x + 1$ è polinomio minimo di α su $\mathbb{Q}$). Pertanto H ha ordine $\frac{6}{2} = 3$ ed è isomorfo a $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Esercizio 3

(a) FALSO, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt[4]{7})$ non è un'estensione di Galois perché non è normale: il polinomio minimo $x^4 - 7$ di $\sqrt[4]{7}$ su $\mathbb{Q}$ ha due zeri complessi coniugati non contenuti in $\mathbb{Q}(\sqrt[4]{7})$.

(b) FALSO, vedi (a).

(c) FALSO. $x^3 + x^2 + 2x + 2$ non è un polinomio irriducibile su $\mathbb{Z}/3\mathbb{Z}$ poiché ha lo zero 1.

(d) VERO: $K \subset L$ è un'estensione di Galois (campo di riducibilità completa di un polinomio separabile!) il cui gruppo di Galois $\mathrm{Gal}(f/K)$ è isomorfo a un sottogruppo di S_5. Per il Teorema di Lagrange $[L : K] = |\mathrm{Gal}(f/K)|$ divide $|S_5| = 5! = 120$.

Esercizio 4

Non esistono campi intermedi propri $GF(4) \subset L \subset GF(64)$, perché $GF(4) \subset GF(64)$ è un'estensione di grado 3 (si usi il Lemma del Grado).

Prof. Lidia Angeleri
Università di Verona, 2010/11
Corso di Laurea in Matematica Applicata

Prova scritta per il Corso di Algebra

16 febbraio 2011

1. Sia F un campo.
   (a) Dato un sottocampo $K \subset F$, si definisca il gruppo di Galois $\mathrm{Gal}(F/K)$. (*2 punti*)
   (b) Dato un sottogruppo $G \leq \mathrm{Aut}F$, si definisca il campo fisso $\mathrm{Fix}_F(G)$. (*2 punti*)
   (c) Quando un'estensione $K \subset F$ è detta estensione di Galois ? (si diano almeno due enunciati equivalenti) (*4 punti*)

2. Si consideri $\alpha = 1 + \sqrt{5} \in \mathbb{R}$ e sia $F = \mathbb{Q}(\alpha, i)$.
   (a) Si determini il polinomio minimo dell'elemento α su $\mathbb{Q}$. (*2 punti*)
   (b) Si verifichi che $[F : \mathbb{Q}] = 4$ e si dimostri che $\{1, \alpha, i, i\alpha\}$ è una $\mathbb{Q}$-base di F. (*3 punti*)
   (c) Si dimostri che $\mathbb{Q} \subset F$ è un'estensione di Galois il cui gruppo di Galois $\mathrm{Gal}(F/\mathbb{Q})$ è isomorfo al gruppo di Klein. (*3 punti*)

3. Si decida se sono veri o falsi i seguenti enunciati.
   (a) Il polinomio $x^{15} + x^{10} + x^5 + 1$ è irriducibile su $\mathbb{Z}$.
   (b) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[6]{5})$ è un'estensione di Galois.
   (c) $\mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/2\mathbb{Z}[x]/(x^4 + x^3 + 1)$ è un'estensione di campi di grado 4.

   (*6 punti*)

4. Si dimostri che le seguenti estensioni di campi sono sempre estensioni di Galois:
   (a) $\mathbb{R} \subset \mathbb{R}(\alpha)$, dove $\alpha \in \mathbb{C}$ è un numero complesso arbitrario; (*4 punti*)
   (b) $\mathbb{Q} \subset L$, dove L è un campo intermedio di $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{5})$. (*4 punti*)

Risposte

Esercizio 2

(a) Si verifica che $\alpha^2 = 4 + 2\alpha$, dunque $f = x^2 - 2x - 4$ è il polinomio minimo di α su $\mathbb{Q}$ (infatti gli zeri di f sono $\alpha, 2 - \alpha$, e f è quindi irriducibile poiché non ha zeri in $\mathbb{Q}$).

(b) $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ è un'estensione di grado 2 con $\mathbb{Q}$-base $1, \alpha$,

$\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha)(i) = F$ è un'estensione di grado 2 con $\mathbb{Q}(\alpha)$-base $1, i$.

Dunque $[F : \mathbb{Q}] = 4$ e ogni elemento di F è combinazione lineare di $1, i$ con coefficienti di forma $a + b\alpha$ dove $a, b \in \mathbb{Q}$. Deduciamo che $\{1, \alpha, i, i\alpha\}$ è un insieme di generatori di F su $\mathbb{Q}$, e per ragioni di dimensione dev'essere una base.

(c) Da (b) segue che un elemento $\varphi \in \mathrm{Gal}(F/\mathbb{Q})$ è determinato dalle immagini $\varphi(i), \varphi(\alpha)$. Sappiamo che $\varphi(i)$ dev'essere uno dei due zeri $i, -i$ di $x^2 + 1$ e $\varphi(\alpha)$ dev'essere uno dei due zeri $\alpha, 2-\alpha$ di f. Quindi abbiamo esattamente 4 possibilità di assegnare valori a $\varphi(i)$ e $\varphi(\alpha)$ e pertanto 4 elementi in $\mathrm{Gal}(F/\mathbb{Q})$:

$$\varphi_1 = id,$$

$$\varphi_2 : i \mapsto -i, \alpha \to \alpha,$$

$$\varphi_3 : i \mapsto i, \alpha \to 2 - \alpha,$$

$$\varphi_4 : i \mapsto -i, \alpha \to 2 - \alpha.$$

Segue che $\mid \mathrm{Gal}(F/\mathbb{Q}) \mid = [F : \mathbb{Q}]$, quindi $\mathbb{Q} \subset F$ è un'estensione di Galois. Inoltre si vede facilmente che ${\varphi_i}^2 = id$ per ogni $i = 1, 2, 3, 4$. Quindi $\mathrm{Gal}(F/\mathbb{Q})$ è isomorfo al gruppo di Klein.

Esercizio 3

(a) FALSO, ha lo zero -1.

(b) FALSO, non è normale (poiché il polinomio minimo $x^6 - 5$ di $\sqrt[6]{5}$ su $\mathbb{Q}$ ha zeri in $\mathbb{C} \setminus \mathbb{R}$).

(c) VERO: x^4+x^3+1 non ha zeri,né divisori irriducibili di grado 2 in $\mathbb{Z}/2\mathbb{Z}[x]$, quindi è un polinomio irriducibile e $\mathbb{Z}/2\mathbb{Z}[x]/(x^4 + x^3 + 1)$ è un campo di dimensione 4 su $\mathbb{Z}/2\mathbb{Z}$.

Esercizio 4

(a) Si ha $\mathbb{R} \subset \mathbb{R}(\alpha) \subset \mathbb{C}$, dove $\mathbb{R} \subset \mathbb{C}$ è un'estensione di Galois di grado 2 (campo di riducibilità completa di $X^2 + 1$ su $\mathbb{R}$). Per il Lemma del Grado $\mathbb{R} = \mathbb{R}(\alpha)$ oppure $\mathbb{R}(\alpha) = \mathbb{C}$ e in entrambi i casi $\mathbb{R} \subset \mathbb{R}(\alpha)$ è un'estensione di Galois.

(b) Si ha $\mathbb{Q} \subset L \subset F = \mathbb{Q}(i, \sqrt{5})$ dove $\mathbb{Q} \subset F$ è un'estensione di Galois di grado 4 (vedi Esercizio 2). Per il Lemma del Grado $\mathbb{Q} = L$ oppure $L = F$ oppure $\mathbb{Q} \subset L$ è un'estensione di grado due. Nei primi due casi $\mathbb{Q} \subset L$ è chiaramente un'estensione di Galois. Ma anche nel terzo caso abbiamo un'estensione finita, normale (grado due!) e separabile (caratteristica zero!) e pertanto un'estensione di Galois.