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

Esercizi / Domande per il Corso di Algebra

1. Siano R un dominio, $f \in R[x]$. Si dia la definizione di polinomio primitivo. Si dia un esempio di un polinomio non primitivo su un dominio R. (*3 punti*)

2. Si enunci il Lemma di Dedekind. (*3 punti*)

3. Si decida se sono veri o falsi i seguenti enunciati.

   (a) Se f è il polinomio minimo di un elemento a su un campo K e g è il polinomio minimo di un elemento b su K, allora fg è il polinomio minimo di ab su K.

   (b) Se p è un numero primo, allora il campo $\mathbb{Q}[x]/(x^2 - p)$ ha caratteristica p.

   (c) L'insieme di tutti i sottocampi di un campo finito è totalmente ordinato rispetto all'inclusione "$\subset$".

   (*6 punti*)

4. In $R = \mathbb{Z}[x]$ si dia un ideale primo non nullo che non è massimale (con relativa dimostrazione). (*6 punti*)

5. Si dimostri che il polinomio $f = x^3 - 4$ è irriducibile su $\mathbb{Q}$ e che $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{4})$ non è un'estensione di Galois. (*6 punti*)

6. Siano $K = \mathbb{Z}/5\,\mathbb{Z}$ e $f = x^3 - 4x^2 + 2 \in K[x]$. Si dimostri che $K[x]/(f)$ è isomorfo a $GF(125)$. (*6 punti*)

Risposte

3. (a) FALSO: Se fg fosse il polinomio minimo di ab su K, allora sarebbe irriducibile, e quindi uno dei fattori f oppure g dovrebbe essere invertibile, in contraddizione con l'ipotesi che siano entrambi polinomi minimi di un elemento.

   (b) FALSO. Infatti $\mathbb{Q}[x]/(x^2-p) \cong \mathbb{Q}(\sqrt{p})$ e il suo più piccolo sottocampo è $\mathbb{Q}$, quindi la caratteristica è 0.

   (c) FALSO: Se K è un campo finito e P è il suo più piccolo sottocampo, allora $P \subset K$ è un'estensione di Galois il cui gruppo di Galois G è ciclico (generato dall'omomorfismo di Frobenius), quindi isomorfo a $\mathbb{Z}/n\mathbb{Z}$ dove $n = [K : P]$. Per il Teorema Fondamentale della Teoria di Galois esiste quindi una corrispondenza biunivoca fra l'insieme di tutti i sottocampi di K e l'insieme di tutti i sottogruppi di G e questa corrispondenza inverte l'ordine dato dall'inclusione "$\subset$". Ma l'insieme di tutti i sottogruppi di un gruppo ciclico in generale non è totalmente ordinato rispetto a "$\subset$". Si consideri ad esempio $n = 6$, quindi $\mathbb{Z}/6\mathbb{Z}$ con i sottogruppi $< [2] >$ e $< [3] >$.

4. L'ideale $0 \neq (x) \subset R = \mathbb{Z}[x]$ è primo ma non è massimale. Infatti considerando l'epimorfismo

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z},\ f = \sum_{i=0}^{n} a_i\, x^i \mapsto a_0$$

   con nucleo $\operatorname{Ker}\varphi = (x)$ si vede per il Teorema Fondamentale dell'Omomorfismo che $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ è un dominio ma non un campo.

5. Il polinomio $f = x^3 - 4$ è irriducibile su $\mathbb{Q}$. Per verificarlo si procede ad esempio per sostituzione

$$\sigma : \mathbb{Q}[x] \to \mathbb{Q}[x], \quad \sigma(x) = x + 1.$$

   ottenendo $\sigma(f) = (x+1)^3 - 4 = x^3 + 3x^2 + 3x - 3$ che è irriducibile per il Criterio di Eisenstein.

   $\mathbb{Q} \subset F = \mathbb{Q}(\sqrt[3]{4})$ non è un'estensione di Galois, ad esempio perché

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

   Infatti, essendo f il polinomio minimo $\sqrt[3]{4}$ su $\mathbb{Q}$, si ha $[F : \mathbb{Q}] = \deg f = 3$, mentre il gruppo di Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ ha ordine 1 poiché contiene soltanto l'identità: se $\sigma \in G$, allora $\sigma(\sqrt[3]{4})^{\,3} = \sigma(4) = 4$ e $\sigma(\sqrt[3]{4}) \in F \subset \mathbb{R}$, quindi $\sigma(\sqrt[3]{4}) = \sqrt[3]{4}$, dunque σ fissa gli elementi della base $\{1, \sqrt[3]{4}, (\sqrt[3]{4})^2\}$ di F su $\mathbb{Q}$ ed è pertanto l'applicazione identica.

6. Siano $K = \mathbb{Z}/5\,\mathbb{Z}$ e $f = x^3 - 4x^2 + 2 \in K[x]$. Si verifica che f è irriducibile in quanto non ha zeri in K (infatti $f([1]) = f([2]) = [4],\ f([3]) = [3],\ f([4]) = f([0]) = [2]$) ed è un polinomio di grado 3. Dunque $F = K[x]/(f)$ è un campo. Inoltre $[F : K] = \deg f = 3$, quindi $F \cong K^3$ possiede $5^3 = 125$ elementi ed è pertanto isomorfo a $GF(125)$.