Corso di Algebra - a.a. 2007-2008

Prova scritta del 6.2.2008

1. Indichiamo con D_h il gruppo diedrale con $2h$ elementi. Quanti sono gli omomorfismi di gruppo da $\mathbb{Z}/4\mathbb{Z}$ a D_8 e quanti di questi sono iniettivi?

2. Sia X un insieme finito, e sia Y un suo sottinsieme. Indichiamo con $S(X)$ il gruppo delle permutazioni di X. Poniamo $G = \{\sigma \in S(X) : \sigma(Y) \subset Y\}$.

   (a) Mostrare che G è un sottogruppo di $S(X)$.

   (b) G è un sottogruppo normale?

   (c) Quanti sono gli elementi di G?

3. Sia A un anello, B un sottoanello di A e

$$I = \{a \in A \,:\, aA \subset B\}.$$

   (a) Dimostrare che I è un ideale destro di A.

   (b) Dimostrare che I è contenuto in B e che I è un ideale bilatero di B.

4. Sia A un dominio a ideali principali. Supponiamo che A abbia un solo ideale massimale.

   (a) Mostrare che l'insieme delle unità di A è il complementare dell'ideale massimale in A.

   (b) Mostrare che esiste un elemento t di A tale che ogni elemento non nullo di A può essere scritto come ut^n, dove n è un intero non negativo e u è una unità di A.

5. Fattorizzare il polinomio $X^3 - 3 \in K[X]$ e trovare il grado del suo campo di spezzamento su K nei seguenti casi:

   (a) $K = \mathbb{Q}$;

   (b) $K = \mathbb{Z}/5\mathbb{Z}$.

Soluzioni

1. Gli omomorfismi di $\mathbb{Z}/4\mathbb{Z}$ in un qualsiasi gruppo G sono in corrispondenza biunivoca con gli elementi di G il cui ordine divide 4. Il gruppo D_8 è generato da elementi ρ, σ tali che ρ ha ordine 8, σ ha ordine 2, e $\rho\sigma = \sigma\rho^{-1}$. Indichiamo con H il sottogruppo ciclico generato da ρ; questo sottogruppo è normale e ha indice 2. Gli elementi di $\sigma H = D_8 \smallsetminus H$ hanno tutti ordine 2. L'unico elemento di ordine 2 di H è ρ^4, mentre gli elementi di ordine 4 sono ρ^2 e ρ^6. Dunque gli elementi di D_8 is cui ordine divide 4 sono: 1 di ordine 1, 9 di ordine 2, 2 di ordine 4. In tutto sono 12, e questo è il numero degli omomorfismi da $\mathbb{Z}/4\mathbb{Z}$ in D_8. Gli omomorfismi iniettivi sono quelli corrispondenti a elementi di D_4 il cui ordine è esattamente 4, e quindi sono in numero di 2.

2. (a) Dato che $S(X)$ è finito e G contiene l'identità, basta vedere che G è chiuso rispetto al prodotto. Se $\sigma, \tau \in G$, allora $\sigma\tau(Y) = \sigma(\tau(Y)) \subset \sigma(Y) \subset Y$; in altre parole, $\sigma\tau \in G$.

(b) In generale no. Ad esempio, se $X = \{1,2,3\}$ e $Y = \{1\}$, allora $(2\ 3) \in G$, ma $(1\ 2\ 3)(2\ 3)(1\ 2\ 3)^{-1} = (1\ 3) \notin G$.

(c) Un elemento di G determina una permutazione di Y e una di $X \setminus Y$, e viceversa. Dunque, se n indica il numero degli elementi di X e k quello degli elementi di Y, G consta di $k!(n-k)!$ elementi.

3. (a) I non è vuoto perchè contiene 0. Siano a, b elementi di I, e sia c un elemento di A. Allora $(a-b)A = aA + bA \subset B + B = B$, e dunque $a - b \in I$, mentre $acA \subset aA \subset B$, e dunque $ac \in I$. Questo mostra che I è un ideale destro di A.

   (b) Se $a \in I$, allora $a = a \cdot 1 \in aA \subset B$. Dunque $I \subset B$. Se poi $c \in B$, allora $caA \subset cB \subset B$, e quindi $ca \in I$. Questo mostra che I, oltre che ideale destro, è anche un ideale sinistro di B.

4. Indichiamo con M l'ideale massimale di A.

   (a) Dire che u è un'unità equivale a dire che $uA = A$. In altre parole, u non è una unità se e solo se uA è un ideale proprio, cioè se e solo se uA è contenuto in un ideale massimale. Visto che vi è un unico ideale massimale M, u non è una unità se e solo appartiene a M. In altre parole, $A^\times = A \setminus M$.

   (b) Se A è un campo, basta prendere $t = 1$. Supponiamo d'ora in poi che A non sia un campo. Dato che A è a ideali principali, gli ideali massimali in A sono gli ideali primi non nulli, cioè gli ideali principali generati da elementi irriducibili; inoltre, se p, q sono irriducibili, allora $pA = qA$ se e solo se p e q sono associati. Dato che nel nostro caso vi è un solo ideale massimale, ne segue che tutti gli elementi irriducibili sono tra loro associati. Sia t un elemento irriducibile di A. Dato che A è a ideali principali, è anche un dominio a fattorizzazione unica. Ogni elemento non nullo di A è quindi associato a un prodotto di elementi irriducibili, cioè è del tipo ut^n, dove u è una unità e n è un intero non negativo.

5. (a) Dato che $X^3 - 3$ non ha radici razionali, è irriducibile in $\mathbb{Q}[X]$. Quindi $[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}] = 3$. Le altre radici di $X^3 - 3$ sono $\zeta\sqrt[3]{3}$ e $\bar{\zeta}\sqrt[3]{3}$, dove $\zeta = (-1 \pm i\sqrt{3})/2$ è una delle radici cubiche non reali di 1. Queste radici non sono reali e quindi non appartengono a $\mathbb{Q}[\sqrt[3]{3}]$; inoltre sono entrambe radici di $X^2 + \sqrt[3]{3}X + \sqrt[3]{9}$. Dunque uno splitting field di $X^3 - 3$ è $F = \mathbb{Q}[\sqrt[3]{3}, \zeta\sqrt[3]{3}] = \mathbb{Q}[\sqrt[3]{3}, \zeta]$, e $[F : \mathbb{Q}[\sqrt[3]{3}]] = 2$. Ne segue che $[F : \mathbb{Q}] = 6$.

   (b) In questo caso una radice di $X^3 - 3$ è 2, e $X^3 - 3 = (X-2)(X^2 + 2X - 1)$. Quindi uno splitting field di $X^3 - 3$ è uno splitting field di $X^2 + 2X - 1$. Dato che $X^2 + 2X - 1$ non ha radici in K, un suo splitting field ha grado 2 su K.