Corso di Algebra - a.a. 2006-2007

Prova scritta del 18.6.2007

1. Sia H un sottogruppo di S_n, con $n \geq 2$. Mostrare che o tutti gli elementi di H sono permutazioni pari, oppure che lo sono esattamente la metà degli elementi di H.

2. Esiste un omomorfismo suriettivo di gruppi da $\mathbb{Z}/8\mathbb{Z}$ a $(\mathbb{Z}/8\mathbb{Z})^*$? (suggerimento: determinare la struttura di $(\mathbb{Z}/8\mathbb{Z})^*$).

3. Sia A un anello e I il sottoinsieme di A costituito dagli elementi a tali che $na = 0$ per qualche intero positivo n.

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

   (b) Dimostrare che, se A è un dominio, allora $I = A$ o $I = (0)$.

4. Sia $f = 6X^3 + 5X^2 + 5X - 1$.

   (a) Fattorizzare f in $\mathbb{Z}[X]$.

   (b) Determinare i primi p tali che f è irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$.

5. Sia F il campo con 5 elementi, e sia K il campo di spezzamento su F di $X^6 - 1$. Calcolare $[K : F]$ e il numero di elementi di K.

Soluzioni

1. Sia $\varphi : H \to \{\pm 1\}$ la restrizione a H dell'omomorfismo segno. L'insieme H_+ degli elementi di H che sono permutazioni pari è il nucleo di φ. Se $\varphi(H) = \{1\}$, allora $H_+ = H$. Altrimenti φ è suriettiva, e quindi
$$|H| = |\varphi(H)||\ker\varphi| = 2|H_+|\,,$$
cioè $|H_+| = |H|/2$.

2. L'immagine di un gruppo ciclico tramite un omomorfismo è un gruppo ciclico. Invece $(\mathbb{Z}/8\mathbb{Z})^*$ non è ciclico. Infatti i suoi elementi sono le classi di 1, 3, 5 e 7, che hanno tutti quadrato congruo a 1 modulo 8. Dunque non possono esistere omomomorfismi suriettivi da $\mathbb{Z}/8\mathbb{Z}$ a $(\mathbb{Z}/8\mathbb{Z})^*$.

3. (a) Se $a, b \in A$ e $na = 0$, $n > 0$, allora $n(ba) = b(na) = b \cdot 0 = 0$ e $n(ab) = (na)b = 0 \cdot b = 0$; dunque ab e ba appartengono a I. Se inoltre $kb = 0$, $k > 0$ allora $nk(a + b) = k(na) + n(kb) = k \cdot 0 + n \cdot 0 = 0$; dunque $a + b \in I$.

   (b) Se $I \neq (0)$, c'è $a \neq 0$ in I. Quindi c'è $n > 0$ tale che $na = 0$. Questo significa che $0 = na = (n1_A)a$. Visto che A non ha divisori di zero, questo implica che $n1_A = 0$, cioè che $1_A \in I$, e quindi che $I = A$.

4. (a) Le radici razionali di f vanno cercate tra $\pm 1, \pm 1/2, \pm 1/3, \pm 1/6$. Sostituendo al posto di X si trova che l'unico tra questi numeri che è radice di f è $1/6$. Dunque $6X - 1$ divide f, e precisamente $f = (6X - 1)(X^2 + X + 1)$. Si noti che, per quanto osservato prima, $X^2 + X + 1$ è irriducibile.

(b) Se la riduzione di $6X-1$ modulo p ha grado positivo, cioè se $p \neq 2, 3$, la riduzione modulo p della fattorizzazione di f mostra che f non è irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$. Se invece p è uguale a 2 o a 3, la riduzione di f modulo p è $-(X^2+X+1)$, che è irriducibile se $p = 2$, mentre non lo è se $p = 3$, perchè un questo caso $X^2 + X + 1 = (X - 1)^2$.

5. $X^6 - 1 = (X^3 - 1)(X^3 + 1) = (X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1)$. Se α una radice di $X^2 + X + 1$, $-\alpha$ è una radice di $X^2 - X + 1$. Quindi $K = F[\alpha]$. Il polinomio $X^2 + X + 1$ non ha radici in F. Infatti 0 non è una radice, e se $a \in F$ non è nullo, $a^4 = 1$; se supponiamo che a sia radice di $X^2 + X + 1$, allora $a^3 = 1$. Ne segue che $a = 1$, e 1 non è radice di $X^2 + X + 1$ perchè 3 non è congruo a 0 modulo 5. In conclusione, $X^2 + X + 1$ è irriducibile in $F[X]$, e quindi è il polinomio minimo di α. Dunque $[K : F] = \deg(X^2 + X + 1) = 2$ e K ha $5^2 = 25$ elementi.