Corso di Algebra - a.a. 2007-2008

Prova scritta del 16.6.2008

1. Sia G il gruppo $S_3 \times \mathbb{Z}/4\mathbb{Z}$.
   (a) Trovare tutti gli interi n tali che il gruppo G contiene un elemento di ordine n.
   (b) Dimostrare che G contiene un sottogruppo di ordine n per ogni intero positivo n che divide l'ordine di G.

2. Siano G un gruppo, X un insieme e Y un sottinsieme non vuoto di X. L'insieme G^X delle applicazioni $X \to G$, con il prodotto definito ponendo $(fg)(x) = f(x)g(x)$ per ogni $x \in X$, è un gruppo. Poniamo $N = \{f \in G^X : f(y) = 1 \text{ per ogni } y \in Y\}$.
   (a) Mostrare che N è un sottogruppo normale di G^X.
   (b) Mostrare che G^X/N è isomorfo a G^Y.

3. Sia A un anello commutativo e $f\colon A \to A$ l'applicazione definita da $f(a) = 2a - a^2$. Dimostrare che f è un omomorfismo di anelli se e solo se $1 + 1 = 0$ in A.

4. Mostrare che l'ideale $I = (3, X^2 + X + 1)$ in $\mathbb{Z}[X]$ non è primo. Trovare tutti gli ideali massimali di $\mathbb{Z}[X]$ contenenti I.

5. Sia K un campo e α un elemento algebrico su K di grado p primo.
   (a) Se $0 < n < p$, dimostrare che $K(\alpha^n) = K(\alpha)$.
   (b) Fornire un esempio in cui $p = 2$ e $K(\alpha^3) \neq K(\alpha)$.

Soluzioni

1. (a) S_3 contiene elementi di ordine 1, 2 e 3, mentre $\mathbb{Z}/4\mathbb{Z}$ contiene elementi di ordine 1, 2 e 4. Ricordando che se (per $i = 1, 2$) g_i è un elemento di ordine n_i in un gruppo G_i allora l'ordine di (g_1, g_2) in $G_1 \times G_2$ è $\mathrm{mcm}(n_1, n_2)$, otteniamo che G contiene un elemento di ordine n se e solo se n è della forma $\mathrm{mcm}(n_1, n_2)$ con $n_1 \in \{1, 2, 3\}$ e $n_2 \in \{1, 2, 4\}$. Concludiamo che i valori cercati di n sono 1, 2, 3, 4, 6 e 12.
   (b) Poiché l'ordine del sottogruppo generato da un elemento è pari all'ordine dell'elemento stesso, G contiene sottogruppi ciclici di ordine n per ogni valore di n trovato al punto precedente. I rimanenti divisori dell'ordine di G (che è 24) sono 8 e 24. Banalmente G stesso è un sottogruppo di ordine 24, mentre, se indichiamo con H un sottogruppo (di ordine 2) di S_3 generato da una trasposizione, $H \times \mathbb{Z}/4\mathbb{Z}$ è un sottogruppo di ordine 8 di G.

2. (a) Se $f, g \in N$ e $y \in Y$, allora $fg^{-1}(y) = f(y)g(y)^{-1} = 1 \cdot 1^{-1} = 1$, quindi $fg^{-1} \in N$. Siccome N non è vuoto, questo mostra che N è un sottogruppo di G^X. Se $f \in N$, $g \in G^X$ e $y \in Y$, allora $gfg^{-1}(y) = g(y)f(y)g^{-1}(y) = g(y)1g^{-1}(y) = 1$, e quindi $gfg^{-1} \in N$. Questo mostra che N è normale.

(b) Per ogni $g \in G^X$ sia $\varphi(g)$ la restrizione di g a Y. L'applicazione φ è un omomorfismo suriettivo. Infatti, data $h \in G^Y$, definiamo $g \in G^X$ ponendo $g(x) = h(x)$ se $x \in Y$ e $g(x) = 1$ se $x \notin Y$; allora $\varphi(g) = h$. Il nucleo di φ è costituito da tutte le applicazioni $g : X \to G$ tali che $g(x) = 1$ per ogni $x \in Y$, e quindi coincide con N. La tesi segue dal primo teorema di omomorfismo.

3. Per $a, b \in A$ si ha

$$f(a+b) - f(a) - f(b) = 2(a+b) - (a+b)^2 - 2a + a^2 - 2b + b^2 = 2ab,$$

quindi f è un omomorfismo di gruppi additivi se e solo se $2ab = 0$ per ogni $a, b \in A$. Essendo $2ab = ab + ab = (1+1)ab$, questo succede se e solo se $1+1 = 0$ (per vedere che la condizione è necessaria basta prendere $a = b = 1$). Per concludere, basta osservare che se $1 + 1 = 0$ allora f è anche un omomorfismo di anelli. Infatti, in ogni caso $f(1) = 1$, mentre $1 + 1 = 0$ implica che $f(a) = -a^2 = a^2$, e dunque

$$f(ab) = (ab)^2 = a^2b^2 = f(a)f(b)$$

per ogni $a, b \in A$.

4. Se indichiamo con F il campo con tre elementi, $\mathbb{Z}[X]/I \cong F[X]/(X^2 + X + 1)$. Questo anello non è un dominio, dato che $X^2 + X + 1 = (X - 1)^2$ in $F[X]$. Quindi I non è un ideale primo.

Sia $\alpha\colon \mathbb{Z}[X] \to F[X]$ la riduzione modulo 3. Gli ideali massimali di $\mathbb{Z}[X]$ contenenti I sono tutti e soli quelli della forma $\alpha^{-1}(M)$, dove M è un ideale massimale di $F[X]$ contenente $X^2 + X + 1$. Gli ideali M di questo tipo sono gli ideali generati da un fattore irriducibile di $X^2 + X + 1$. Il solo fattore è $X - 1$. Quindi il solo ideale massimale di $\mathbb{Z}[X]$ contenente I è $(3, X - 1)$.

5. (a) Dalle estensioni di campi $K \subset K(\alpha^n) \subset K(\alpha)$ si deduce che

$$p = [K(\alpha) : K] = [K(\alpha) : K(\alpha^n)][K(\alpha^n) : K].$$

Poiché p è primo, le uniche possibilità sono $[K(\alpha^n) : K] = p$ (cioè $K(\alpha^n) = K(\alpha)$) o $[K(\alpha^n) : K] = 1$ (cioè $K(\alpha^n) = K$). Per concludere che $K(\alpha^n) = K(\alpha)$ basta allora osservare che $\alpha^n \notin K$: infatti, se per assurdo $\alpha^n \in K$, α sarebbe radice del polinomio non nullo $X^n - \alpha^n \in K[X]$, per cui il suo grado su K sarebbe $\leq n < p$, contro l'ipotesi.

(b) Un esempio è dato da $K = \mathbb{Q}$ e α una radice (complessa) di $X^3 - 1$ diversa da 1. Infatti α ha grado 2 su $\mathbb{Q}$ (è immediato verificare che il suo polinomio minimo è $(X^3 - 1)/(X - 1) = X^2 + X + 1$) e $\mathbb{Q}(\alpha^3) = \mathbb{Q} \neq \mathbb{Q}(\alpha)$.