Corso di Algebra - a.a. 2007-2008

Prova scritta del 25.9.2008

1. Siano a e b interi positivi. Dire quanti sono gli omomorfismi da C_a a C_b, dove C_h indica il gruppo ciclico con h elementi.

2. Siano G_1 e G_2 due gruppi, H un sottogruppo di $G_1 \times G_2$ e

$$H_1 = \{g \in G_1 \,:\, (g,1) \in H\}, \qquad H_2 = \{g \in G_2 \,:\, (1,g) \in H\}.$$

   (a) Dimostrare che H_i è un sottogruppo di G_i per $i = 1, 2$ e che $H_1 \times H_2 \subset H$.

   (b) Dimostrare che, se G_1 e G_2 sono finiti con ordini primi tra loro, allora $H_1 \times H_2 = H$.

3. Sia A un anello commutativo. Supponiamo che A contenga un elemento nilpotente non nullo, cioè un elemento $a \neq 0$ tale che $a^n = 0$ per qualche intero positivo n. Mostrare che il gruppo delle unità di A è strettamente contenuto nel gruppo delle unità di $A[X]$.

4. Sia K un campo. Per ogni $a \in K$ sia I_a l'ideale di $K[X]$ generato dai polinomi X^2 e $X^2 + (a-1)X + a^2 - 1$.

   (a) Per quali $a \in K$ l'ideale I_a è proprio?

   (b) Per quali $a \in K$ l'ideale I_a è primo?

5. Fattorizzare il polinomio $P(X) = 2X^3 - 5X^2 - X + 1 \in K[X]$ 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. Fissiamo un generatore g di C_a. Se φ è un omomorfismo da C_a a C_b, $\varphi(g)^a = 1$. Viceversa, per ogni elemento h di C_b tale che $h^a = 1$ esiste un omomorfismo $\varphi\colon C_a \to C_b$ tale che $\varphi(g) = h$. Questo omomorfismo è ovviamente unico. Il numero cercato è dunque uguale all'ordine di $\{h \in C_b : h^a = 1\}$, cioè al massimo comun divisore di a e b.

2. (a) Se $h, h' \in H_1$, allora $(h^{-1}h', 1) = (h,1)^{-1}(h',1) \in H$, e quindi $h^{-1}h' \in H_1$. Inoltre $1 \in H_1$. Quindi H_1 è un sottogruppo di G_1. Allo stesso modo si mostra che H_2 è un sottogruppo di G_2. Infine, se $h_1 \in H_1$ e $h_2 \in H_2$, allora $(h_1, h_2) = (h_1, 1)(1, h_2) \in H$, perchè $(h_1, 1)$ e $(1, h_2)$ appartengono ad H.

   (b) Siano r e s gli ordini di G_1 e G_2; poiché sono primi fra loro esistono interi a e b tali che $ar + bs = 1$. Sia (g_1, g_2) un elemento di H. Dato che $g_1^r = 1$, si ha che $g_1 = g_1^{ar+bs} = g_1^{bs}$. D'altra parte $g_2^{bs} = 1$. Quindi $(g_1, g_2)^{bs} = (g_1^{bs}, g_2^{bs}) = (g_1, 1)$. In altre parole, $g_1 \in H_1$. Analogamente si mostra che $g_2 \in H_2$.

3. Sia n il minimo intero positivo tale che $a^n = 0$. Per ipotesi $n > 1$. Se n è dispari, $a^{n+1} = 0$ e $(n+1)/2 < n$. Quindi esiste un intero k (ad esempio $n/2$ se n è pari, $(n+1)/2$ altrimenti) tale che $a^k \neq 0$ e $a^{2k} = 0$. Allora $(1 - a^k X)(1 + a^k X) = 1 - a^{2k} X^2 = 1$, e quindi $(1 - a^k X)$ e $(1 + a^k X)$ sono unità. D'altra parte $(1 - a^k X)$ e $(1 + a^k X)$ non appartengono ad A perchè $a^k \neq 0$.

4. Un altro sistema di generatori di I_a è costituito da X^2 e $P(X) = (a-1)X + a^2 - 1 = X^2 + (a-1)X + a^2 - 1 - X^2$. Se $a = 1$, $P(X) = 0$ e $I_a = (X^2)$. In questo caso I_a è un ideale proprio e non è primo perchè $K[X]/I_a$ non è un dominio. Infatti X non è congruo a zero modulo X^2 ma il suo quadrato sì. D'ora in poi supponiamo che $a \neq 1$. Dato che $a - 1$ è invertibile, I_a è generato da X^2 e $X + a + 1 = (a-1)^{-1} P(X)$. In particolare, se $a = -1$, $I_a = (X)$, e quindi I_a è proprio e primo. Il polinomio $X(X + a + 1) = X^2 + (a+1)X$ appartiene a I_a, e lo stesso è vero per $(a+1)X = X(X + a + 1) - X^2$. Ne segue che, se $a \neq -1$, $X \in I_a$, e quindi anche che $a + 1 = X + a + 1 - X \in I_a$. Dato che $a + 1$ non è nullo, è un'unità in $K[X]$, e dunque I_a coincide con $K[X]$. Riassumendo:

   - se $a = 1$, I_a è proprio ma non primo;
   - se $a = -1$ e $a \neq 1$, I_a è proprio e primo;
   - se $a \neq 1$ e $a \neq -1$, I_a non è proprio.

5. Si vede direttamente che $-1/2$ è radice di $P(X)$, quindi $P(X)$ è divisibile per $2X + 1$ in $\mathbb{Z}[X]$. Dividendo si ottiene che
$$P(X) = (2X + 1)(X^2 - 3X + 1) \tag{1}$$
in $\mathbb{Z}[X]$.

   (a) Il polinomio $Q(X) = X^2 - 3X + 1$ non ha radici intere, quindi, poiché è monico, non ha radici razionali, e dunque è irriducibile in $\mathbb{Q}[X]$. Se α è una radice di $Q(X)$ in qualche estensione di $\mathbb{Q}$, $Q(X)$ è il polinomio minimo di α su $\mathbb{Q}$ e si spezza completamente in $\mathbb{Q}[\alpha]$. Dunque $\mathbb{Q}[\alpha]$ è il campo di spezzamento cercato (è generato da radici di $P(X)$) e $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2$.

   (b) La fattorizzazione (1) vale anche in $K[X]$, dove $K = \mathbb{Z}/5\mathbb{Z}$. In $K[X]$, inoltre, $X^2 - 3X + 1 = X^2 + 2X + 1 = (X + 1)^2$, e quindi $P(X)$ si fattorizza completamente. Dunque il suo campo di spezzamento è K stesso.