Corso di Algebra 1 - a.a. 2009-2010

Prova scritta del 22.2.2010

1. Sia G un gruppo, H un sottogruppo normale di G e $f\colon G \to H$ un omomorfismo tale che $f(a) = a$ per ogni $a \in H$. Dimostrare che l'applicazione
$$\begin{aligned} G &\to H \times G/H \\ a &\mapsto (f(a), aH) \end{aligned}$$
è un isomorfismo.

2. Quanti sono gli omomorfismi di gruppo da $\mathbb{Z}/4\mathbb{Z}$ a $\mathbb{Z}/15\mathbb{Z}^*$ e quanti di questi sono iniettivi?

3. (a) Quanti sono i sottogruppi di ordine 3 di S_4?
   (b) Dimostrare che in S_4 non esistono sottogruppi isomorfi a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. Sia K un campo. Dimostrare che la funzione
$$\begin{aligned} K[X] &\to K \times K \\ f &\mapsto (f(0), f(1)) \end{aligned}$$
è un omomorfismo suriettivo di anelli. Dimostrare inoltre che $K \times K$ è isomorfo a $K[X]/(X^2 - X)$.

5. Sia A un anello e I, J, K tre ideali di A.
   (a) Dimostrare che $(I \cap J) + (I \cap K) \subseteq I \cap (J + K)$.
   (b) Dimostrare che, se $J \subseteq I$ o $K \subseteq I$, allora $(I \cap J) + (I \cap K) = I \cap (J + K)$.

Soluzioni

1. L'applicazione data $F\colon G \to H \times G/H$ è un omomorfismo perché per ogni $a, b \in G$ si ha

$$\begin{aligned} F(ab) = (f(ab), abH) &= (f(a)f(b), aHbH) \\ &= (f(a), aH)(f(b), bH) = F(a)F(b). \end{aligned}$$

Inoltre $F(a) = (1, H)$ se e solo se $f(a) = 1$ e $aH = H$; d'altra parte $aH = H$ se e solo se $a \in H$, e in questo caso, grazie all'ipotesi su f, $f(a) = 1$ se e solo se $a = 1$. Dunque $\ker(F) = \{1\}$ e pertanto F è iniettiva. Infine F è suriettiva perché, dato $(a, bH) \in H \times G/H$, si ha $F(c) = (a, bH)$ con $c = bf(b)^{-1}a$: infatti (tenendo conto che $f(b)^{-1}, a \in H$)

$$f(c) = f(b)f(f(b)^{-1})f(a) = f(b)f(b)^{-1}a = a$$

e $cH = bH$.

2. Ricordando che per ogni intero positivo n gli omomorfismi (iniettivi) da $\mathbb{Z}/n\mathbb{Z}$ a G sono in corrispondenza biunivoca con gli elementi di G il cui ordine divide (è uguale a) n, basta determinare quanti sono gli elementi di $\mathbb{Z}/15\mathbb{Z}^*$ il cui ordine divide (è uguale a) 4. Ora,

$$\mathbb{Z}/15\mathbb{Z}^* = \{\overline{a} \in \mathbb{Z}/15\mathbb{Z}^* \,:\, \mathrm{mcd}(a, 15) = 1\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

e in particolare è un gruppo di ordine 8. Per ogni $\overline{a} \in \mathbb{Z}/15\mathbb{Z}^*$ si ha $\overline{a}^4 = \overline{1}$: infatti $a^4 \equiv 1 \mod 5$ e $a^4 = (a^2)^2 \equiv 1 \mod 3$ per il piccolo teorema di Fermat, dunque anche $a^4 \equiv 1 \mod \mathrm{mcm}(5, 3) = 15$. Ne segue che $\mathrm{ord}(\overline{a})|4$ e $\mathrm{ord}(\overline{a}) = 4$ se e solo se $\overline{a}^2 \neq \overline{1}$. Poiché $\overline{a}^2 = \overline{1}$ se $\overline{a} = \overline{1}, \overline{4}, \overline{11}, \overline{14}$ e $\overline{a}^2 = \overline{4} \neq \overline{1}$ se $\overline{a} = \overline{2}, \overline{7}, \overline{8}, \overline{13}$, se ne deduce che ci sono 8 omomorfismi da $\mathbb{Z}/4\mathbb{Z}$ a $\mathbb{Z}/15\mathbb{Z}^*$ e di questi 4 sono iniettivi.

3. (a) Poiché ogni gruppo di ordine 3 è ciclico, i sottogruppi di ordine 3 di S_4 sono i sottogruppi generati dagli elementi di ordine 3, cioè dai 3-cicli. Ora, il sottogruppo generato da un 3-ciclo (a, b, c) di S_4 è $H = \{(1), (a, b, c), (a, c, b)\}$, e il numero $d = d(H)$ tale che $\{a, b, c, d\} = \{1, 2, 3, 4\}$ dipende solo da H e non dal generatore scelto. Dunque, indicando con T l'insieme dei sottogruppi di ordine 3 di S_4, risulta ben definita una funzione $d\colon T \to \{1, 2, 3, 4\}$, che è biunivoca perché per ogni $i \in \{1, 2, 3, 4\}$ esistono esattamente due 3-cicli (uno l'inverso dell'altro) in S_4 che lasciano fisso i. Pertanto $\#T = 4$, cioè in S_4 ci sono 4 sottogruppi di ordine 3.

(b) Per il teorema cinese del resto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, dunque un sottogruppo isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ conterrebbe elementi di ordine 6, che però non esistono in S_4.

4. Ricordando che per ogni $a \in K$ la valutazione in a è un omomorfismo di anelli da $K[X]$ a K, la data funzione $\alpha\colon K[X] \to K \times K$ è un omomorfismo perché per ogni $f, g \in K[X]$ si ha

$$\begin{aligned}\alpha(f+g) &= ((f+g)(0), (f+g)(1)) = (f(0)+g(0), f(1)+g(1)) \\ &= (f(0), f(1)) + (g(0), g(1)) = \alpha(f) + \alpha(g),\end{aligned}$$

analogamente $\alpha(fg) = \alpha(f)\alpha(g)$ e ovviamente $\alpha(1) = (1,1)$. Inoltre α è suriettiva perché $\alpha((b-a)X + a) = (a, b)$ per ogni $a, b \in K$. Infine $f \in K[X]$ appartiene a $\ker(\alpha)$ se e solo se 0 e 1 sono radici di f, se e solo se (poiché K è un dominio) f è divisibile per $(X-0)(X-1) = X^2 - X$. Dunque $\ker(\alpha) = (X^2 - X)$, e per il primo teorema di isomorfismo si conclude che

$$K \times K = \operatorname{im}(\alpha) \cong K[X]/\ker(\alpha) = K[X]/(X^2 - X).$$

5. (a) Dato $a \in (I \cap J) + (I \cap K)$, per definizione di somma di ideali esistono $b \in I \cap J$ e $c \in I \cap K$ tali che $a = b + c$. Ne segue che $a \in I$ (perché somma di due elementi di I) e $a \in J + K$ (perché somma di un elemento di J e di uno di K), cioè $a \in I \cap (J + K)$.

   (b) Grazie alla simmetria tra J e K si può assumere $J \subseteq I$, e per la prima parte basta dimostrare che $I \cap (J+K) \subseteq (I \cap J) + (I \cap K)$. Dato $a \in I \cap (J + K)$, per definizione di somma di ideali esistono $b \in J$ e $c \in K$ tali che $a = b + c$. Ora, ovviamente $b \in I \cap J = J$, mentre $c = a - b \in I$ (perché differenza di elementi di I) e quindi $c \in I \cap K$. Pertanto $a = b + c \in (I \cap J) + (I \cap K)$.