Corso di Algebra 1 - a.a. 2015-2016

Prova scritta del 23.2.2016

1. Sia $f\colon G \to G'$ un omomorfismo di gruppi e $H := \{(g, f(g)) : g \in G\}$.
   (a) Dimostrare che H è un sottogruppo di $G \times G'$.
   (b) Dimostrare che H è normale in $G \times G'$ se e solo se l'immagine di f è contenuta nel centro di G'.

2. Dimostrare che in S_5 l'equazione
$$gxg^{-1}x^{-1} = h$$
ammette una soluzione x se e solo se gli elementi g e $g^{-1}h$ hanno lo stesso tipo di decomposizione come prodotto di cicli disgiunti.
Stabilire inoltre, in ciascuno dei seguenti casi, se l'equazione ha soluzione e se sì trovarne esplicitamente una.
   (a) $g = (1, 2)$, $h = (1, 2, 3)$.
   (b) $g = (1, 2, 3)$, $h = (1, 2)$.
   (c) $g = (1, 2, 3)$, $h = (3, 4, 5)$.
   (d) $g = (1, 2, 3, 4, 5)$, $h = (1, 5, 4, 3, 2)$.

3. Si considerino i seguenti sottoinsiemi di $\mathbb{Z}[X]$:
$$A = \{\sum_{i\geq 0} a_i X^i \in \mathbb{Z}[X] : a_i \in 2^i\mathbb{Z} \text{ per ogni } i\},$$
$$I = \{\sum_{i\geq 0} a_i X^i \in \mathbb{Z}[X] : a_i \in 2^{i+1}\mathbb{Z} \text{ per ogni } i\}.$$
   (a) Verificare che A è un sottoanello di $\mathbb{Z}[X]$ e che I è un ideale di A.
   (b) Dimostrare che gli anelli A e $\mathbb{Z}[X]$ sono isomorfi.
   (c) Dimostrare che gli anelli A/I e $(\mathbb{Z}/2\mathbb{Z})[X]$ sono isomorfi.

4. Sia $p(X) \in \mathbb{Z}[X]$ un polinomio monico non costante che verrà considerato, per inclusione o quoziente, definito sui seguenti domini: $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$. Stabilire se ciascuna delle seguenti implicazioni è vera o falsa.
   (a) Se p è irriducibile su $\mathbb{Z}$ allora è irriducibile su $\mathbb{Z}[i]$.
   (b) Se p è irriducibile su $\mathbb{Z}[i]$ allora è irriducibile su $\mathbb{Q}$.
   (c) Se p è irriducibile su $\mathbb{Z}/3\mathbb{Z}$ allora è irriducibile su $\mathbb{Z}[i]$.
   (d) Se p è irriducibile su $\mathbb{Z}/3\mathbb{Z}$ e su $\mathbb{Z}/5\mathbb{Z}$ allora è irriducible su $\mathbb{R}$.

Soluzioni

1. (a) $H \neq \emptyset$ perché $(1, 1 = f(1)) \in H$. Inoltre dati $g_1, g_2 \in G$ si ha

$$\begin{aligned}(g_1, f(g_1))(g_2, f(g_2))^{-1} &= (g_1, f(g_1))(g_2^{-1}, f(g_2)^{-1}) \\ &= (g_1 g_2^{-1}, f(g_1) f(g_2)^{-1}) = (g_1 g_2^{-1}, f(g_1 g_2^{-1})) \in H,\end{aligned}$$

   il che dimostra che H è un sottogruppo di $G \times G'$.

   (b) Per definizione H è normale in $G \times G'$ se e solo se per ogni $(a, b) \in G \times G'$ e per ogni $(g, f(g)) \in H$ (con $g \in G$) vale

$$(a, b)(g, f(g))(a, b)^{-1} = (aga^{-1}, bf(g)b^{-1}) \in H,$$

   cioè se e solo se per ogni $a, g \in G$ e per ogni $b \in G'$ si ha

$$bf(g)b^{-1} = f(aga^{-1}). \tag{1}$$

   Se dunque H è normale in $G \times G'$, (1) vale in particolare per $a = 1 \in G$, per cui $bf(g)b^{-1} = f(g)$, o, equivalentemente, $bf(g) = f(g)b$ per ogni $g \in G$ e per ogni $b \in G'$. Ciò significa che $f(g) \in Z(G')$ per ogni $g \in G$, cioè $\mathrm{im}(f) \subseteq Z(G')$.
   Se viceversa $\mathrm{im}(f) \subseteq Z(G')$, l'argomento appena visto mostra che $bf(g)b^{-1} = f(g)$ per ogni $g \in G$ e per ogni $b \in G'$. Allora per ogni $a, g \in G$ si ha anche

$$f(aga^{-1}) = f(a)f(g)f(a)^{-1} = f(g),$$

   quindi (1) è soddisfatta perchè entrambi i membri valgono $f(g)$.

2. L'equazione data è equivalente a $xg^{-1}x^{-1} = g^{-1}h$, che per definizione ammette una soluzione x se e solo se g^{-1} e $g^{-1}h$ sono coniugati. Ricordando che in S_5 (e più in generale in S_n per ogni intero positivo n) due permutazioni sono coniugate se e solo se hanno lo stesso tipo di decomposizione come prodotto di cicli disgiunti, per dimostrare la prima parte basta allora osservare che g e g^{-1} hanno lo stesso tipo di decomposizione come prodotto di cicli disgiunti. Quest'ultimo fatto è vero perché, se $g = \tau_1 \cdots \tau_m$ con i τ_i cicli disgiunti di lunghezze k_i, allora $g^{-1} = \tau_1^{-1} \cdots \tau_m^{-1}$ con i τ_i^{-1} cicli disgiunti di lunghezze k_i (tenendo conto che τ_i e τ_i^{-1} muovono gli stessi elementi di $\{1, \ldots, n\}$ per ogni i).

(a) $g^{-1}h = (1,2)(1,2,3) = (2,3)$ è una trasposizione come $g = g^{-1}$, dunque ci sono soluzioni. Dato $x \in S_5$, si ha

$$xg^{-1}x^{-1} = x(1,2)x^{-1} = (x(1), x(2)),$$

quindi una soluzione è $x = (1,3)$.

(b) $g^{-1}h = (1,3,2)(1,2) = (2,3)$ è una trasposizione mentre g è un 3-ciclo, dunque non ci sono soluzioni.

(c) $g^{-1}h = (1,3,2)(3,4,5) = (1,3,4,5,2)$ è un 5-ciclo mentre g è un 3-ciclo, dunque non ci sono soluzioni.

(d) $g^{-1}h = (1,5,4,3,2)(1,5,4,3,2) = (1,4,2,5,3)$ è un 5-ciclo come g, dunque ci sono soluzioni. Dato $x \in S_5$, si ha

$$xg^{-1}x^{-1} = x(1,5,4,3,2)x^{-1} = (x(1), x(5), x(4), x(3), x(2)),$$

quindi una soluzione è $x = (2,3,5,4)$.

3. (a) Siano $p = \sum_{i\geq 0} a_i X^i, q = \sum_{i\geq 0} b_i X^i \in \mathbb{Z}[X]$.
Dato che chiaramente $1 \in A$, per dimostrare che A è un sottoanello di $\mathbb{Z}[X]$ basta verificare che, se $p, q \in A$ (cioè $a_i, b_i \in 2^i\mathbb{Z}$ per ogni i), allora anche $p - q, pq \in A$. Ora, $p - q = \sum_{i\geq 0}(a_i - b_i)X^i \in A$ perché $a_i - b_i \in 2^i\mathbb{Z}$ per ogni i (essendo $2^i\mathbb{Z}$ un sottogruppo di $\mathbb{Z}$). D'altra parte, $pq = \sum_{i\geq 0} c_i X^i$ con $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, e quindi per concludere che $pq \in A$ (cioè $c_i \in 2^i\mathbb{Z}$ per ogni i) basta verificare che $a_j b_{i-j} \in 2^i\mathbb{Z}$ per ogni $0 \leq j \leq i$. Infatti, per ipotesi $a_j = 2^j a'_j$ e $b_{i-j} = 2^{i-j} b'_{i-j}$ per opportuni $a'_j, b'_{i-j} \in \mathbb{Z}$, per cui $a_j b_{i-j} = 2^i a'_j b'_{i-j} \in 2^i\mathbb{Z}$.
Per dimostrare che I è un ideale di A, notiamo intanto che $I \subseteq A$ (perché $2^{i+1}\mathbb{Z} \subseteq 2^i\mathbb{Z}$ per ogni i) e che ovviamente $0 \in I$. Inoltre, se $p, q \in I$ (cioè $a_i, b_i \in 2^{i+1}\mathbb{Z}$ per ogni i), allora anche $p + q = \sum_{i\geq 0}(a_i + b_i)X^i \in I$, dato che $a_i + b_i \in 2^{i+1}\mathbb{Z}$ per ogni i. Resta da verificare che $pq \in I$ se $p \in A$ e $q \in I$. Ragionando analogamente a prima, basta verificare che $a_j b_{i-j} \in 2^{i+1}\mathbb{Z}$ per ogni $0 \leq j \leq i$. In questo caso per ipotesi $a_j = 2^j a'_j$ e $b_{i-j} = 2^{i-j+1} b'_{i-j}$ con $a'_j, b'_{i-j} \in \mathbb{Z}$, quindi concludiamo che $a_j b_{i-j} = 2^{i+1} a'_j b'_{i-j} \in 2^{i+1}\mathbb{Z}$.

(b) La funzione $f\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ definita da $f(p(X)) = p(2X)$ è un omomorfismo di anelli (essendo la valutazione in $2X$). Se $p(X) = \sum_{i\geq 0} a_i X^i$, risulta $p(2X) = \sum_{i\geq 0} 2^i a_i X^i$, ed è quindi chiaro che $\ker(f) = \{0\}$ (per cui f è iniettivo) e $\mathrm{im}(f) = A$, il che dimostra che $\mathbb{Z}[X]$ e A sono isomorfi come anelli.

(c) Sia $g\colon \mathbb{Z}[X] \to A/I$ la composizione dell'isomorfismo $\mathbb{Z}[X] \to A$ indotto da f (visto nel punto precedente) con la proiezione naturale $\pi\colon A \to A/I$. g è un omomorfismo suriettivo di anelli perché composizione di omomorfismi suriettivi. Inoltre, dato $p = \sum_{i\geq 0} a_i X^i \in \mathbb{Z}[X]$, si ha $p \in \ker(g)$ se e solo se $f(p) \in \ker(\pi) = I$. Essendo $f(p) = \sum_{i\geq 0} 2^i a_i X^i$, segue subito dalla definizione di I che $f(p) \in I$ se e solo se $a_i \in 2\mathbb{Z}$ per ogni I. Questo dimostra che $\ker(g) = (2\mathbb{Z})[X]$, e applicando il primo teorema di omomorfismo per anelli all'omomorfismo suriettivo g si trova $A/I \cong \mathbb{Z}[X]/(2\mathbb{Z})[X]$. Ricordando che $\mathbb{Z}[X]/(2\mathbb{Z})[X] \cong (\mathbb{Z}/2\mathbb{Z})[X]$, si conclude che $A/I \cong (\mathbb{Z}/2\mathbb{Z})[X]$ come anelli.

4. (a) Falsa: per esempio $p = X^2+1$ è irriducibile su $\mathbb{Z}$ perché di secondo grado senza radici razionali (nemmeno reali), ma $p = (X-i)(X+i)$ non è irriducibile su $\mathbb{Z}[i]$.

   (b) Vera. Infatti, se p è irriducibile su $\mathbb{Z}[i]$ e $p = qr$ in $\mathbb{Z}[X]$, allora $p = qr$ anche in $\mathbb{Z}[i][X]$. Dunque uno tra q e r sarebbe invertibile, diciamo $q \in \mathbb{Z}[i][X]^* = \mathbb{Z}[i]^*$. Ma $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ e $q \in \mathbb{Z}[X]$, per cui $q = \pm 1 \in \mathbb{Z}^* = \mathbb{Z}[X]^*$, il che dimostra che p è irriducibile su $\mathbb{Z}$. Per concludere basta osservare che, essendo p primitivo (perché monico), p è irriducibile sul dominio a fattorizzazione unica $\mathbb{Z}$ se e solo se lo è sul suo campo dei quozienti $\mathbb{Q}$.

   (c) Falsa: per esempio $p = X^2 + 1$ è irriducibile su $\mathbb{Z}/3\mathbb{Z}$ perché di secondo grado senza radici, ma $p = (X-i)(X+i)$ non è irriducibile su $\mathbb{Z}[i]$.

   (d) Falsa: per esempio $p = X^2 - 2$ è irriducibile sia su $\mathbb{Z}/3\mathbb{Z}$ che su $\mathbb{Z}/5\mathbb{Z}$ perché in ciascuno dei due casi di secondo grado senza radici, ma $p = (X - \sqrt{2})(X + \sqrt{2})$ non è irriducibile su $\mathbb{R}$.