Corso di Algebra 1 - a.a. 2016-2017

Prova scritta del 23.1.2017

1. Sia G il gruppo $S_3 \times D_4$.
   (a) Per quali $x \in D_4$ il sottogruppo H_x di G generato da $((1,2,3), x)$ ha ordine 6?
   (b) Dimostrare che esiste unico $y \in D_4$ tale che H_y ha ordine 6 ed è normale in G.
   (c) Determinare l'ordine di ogni elemento in G/H_y.

2. Sia n un intero positivo e G un gruppo non ciclico di ordine $2n$. Sia inoltre $f\colon G \to \mathbb{Z}/n\mathbb{Z}$ un omomorfismo suriettivo di gruppi e $a \in G$ tale che $f(a) = \overline{1}$.
   (a) Dimostrare che a ha ordine n.
   (b) Indicando con H il sottogruppo generato da a e con K il nucleo di f, dimostrare che $HK = G$ e $H \cap K = \{1\}$.
   (c) Dimostrare che G è isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e che n è pari.

3. Sia A il gruppo additivo $\mathbb{R} \times \mathbb{R}$ con moltiplicazione definita da
$$(a,b)(c,d) = (ac, ad + bc)$$
per ogni $a, b, c, d \in \mathbb{R}$.
   (a) Dimostrare che A è un anello commutativo.
   (b) Dimostrare che A è isomorfo come anello a $\mathbb{R}[X]/(X^2)$.
   (c) Trovare tutti gli ideali non banali di A.

4. Per ogni $a \in \mathbb{Z}$ sia $p_a = X^4 + (a-1)X + 2a$.
   (a) Dimostrare che, se a è dispari, allora p_a è irriducibile in $\mathbb{Q}[X]$.
   (b) Esiste $a \in \mathbb{Z}$ tale che p_a ha una radice multipla in $\mathbb{Q}$?
   (c) Dimostrare che esiste unico $b \in \mathbb{Z}$ tale che p_b è divisibile per $X^2 + X + 4$. Dimostrare inoltre che esistono due campi K_1 e K_2 tali che l'anello quoziente $\mathbb{Q}[X]/(p_b)$ è isomorfo a $K_1 \times K_2$.

Soluzioni

1. (a) Posto $\sigma = (1,2,3)$, per ogni $x \in D_4$ si ha

$$\#H_x = \mathrm{ord}((\sigma, x)) = \mathrm{mcm}(\mathrm{ord}(\sigma), \mathrm{ord}(x)) = \mathrm{mcm}(3, \mathrm{ord}(x)),$$

per cui $\#H_x = 6$ se e solo se $\mathrm{ord}(x) = 2$ o $\mathrm{ord}(x) = 6$. In D_4 non ci sono elementi di ordine 6, mentre quelli di ordine 2 (e quindi gli x cercati) sono R^2 e R^iS per $i = 0, 1, 2, 3$.

(b) Per ogni i intero H_{R^iS} non è normale in G, dato che

$$(1, R)(\sigma, R^iS)(1, R)^{-1} = (\sigma, RR^iSR^{-1}) = (\sigma, R^{i+2}S)$$

e $R^{i+2}S \notin \langle R^iS \rangle = \{1, R_iS\}$, per cui $(\sigma, R^{i+2}S) \notin H_{R^iS}$. Per il punto precedente può allora essere solo $y = R^2$ e basta dimostrare che H_{R^2} è normale in G. Va cioè dimostrato che $ghg^{-1} \in H_{R^2}$ per ogni $g \in G$ e per ogni $h \in H_{R^2}$. Essendo $H_{R^2} = \langle a \rangle$ con $a = (\sigma, R^2)$, esiste $i \in \mathbb{Z}$ tale che $h = a^i$, e quindi $ghg^{-1} = (gag^{-1})^i \in H_R^2$ se $gag^{-1} \in H_{R^2}$. Basta allora verificare che $gag^{-1} \in H_{R^2}$ per ogni $g \in G$. Se $g = (\tau, x)$, si ha in effetti

$$gag^{-1} = (\tau, x)(\sigma, R^2)(\tau, x)^{-1} = (\tau\sigma\tau^{-1}, xR^2x^{-1}).$$

Poiché $\tau\sigma\tau^{-1} = \sigma$ se $\tau \in A_3 = \langle \sigma \rangle$ e $\tau\sigma\tau^{-1} = (1,3,2) = \sigma^{-1}$ se $\tau \in S_3 \setminus A_3$, mentre $xR^2x^{-1} = R^2$ per ogni $x \in D_4$ (dato che $R^2 \in Z(D_4)$), si ottiene che $gag^{-1} = (\sigma, R^2) = a$ o $gag^{-1} = (\sigma^{-1}, R^2) = a^{-1}$, per cui in ogni caso $gag^{-1} \in H_{R^2}$.
In alternativa, per dimostrare la normalità di H_{R^2} basta notare che $\langle \sigma \rangle = A_3$ è normale in S_3, che $\langle R^2 \rangle = \{1, R^2\}$ è normale in D_4, che quindi $H = \langle \sigma \rangle \times \langle R^2 \rangle$ è normale in $S_3 \times D_4 = G$ e che $H_{R^2} = H$. Quest'ultima uguaglianza segue dal fatto che $\#H_{R^2} = \#H = 6$ e $H_{R^2} = \langle a \rangle \subseteq H$ perché $a \in H$.

(c) A parte l'elemento neutro che ha ordine 1, tutti gli altri elementi di G/H_y hanno ordine 2. Per dimostrarlo basta verificare che $(gH_y)^2 = H_y$, cioè che $g^2 \in H_y$, per ogni $g \in G$. Se $g = (\tau, x)$, si ha $g^2 = (\tau^2, x^2)$ e in ogni caso $\tau^2 \in \langle \sigma \rangle$ ($\tau^2 = \sigma^{-1}$ se $\tau = \sigma$, $\tau^2 = \sigma$ se $\tau = \sigma^{-1}$, altrimenti $\tau^2 = 1$) e $x^2 \in \langle R^2 \rangle$ ($x^2 = R^2$ se $x = R, R^3$, altrimenti $x^2 = 1$). Dunque $g^2 \in H = \langle \sigma \rangle \times \langle R^2 \rangle$ per ogni $g \in G$ e, come osservato nel punto precedente, $H = H_{R^2}$.

2. (a) Chiaramente $\mathrm{ord}(a) \mid 2n = \#G$ per il teorema di Lagrange. Inoltre $n = \mathrm{ord}(\overline{1}) = \mathrm{ord}(f(a)) \mid \mathrm{ord}(a)$ perché f è un omomorfismo di gruppi. Da ciò segue che gli unici possibili valori per $\mathrm{ord}(a)$ sono n e $2n$. Non potendo essere $\mathrm{ord}(a) = 2n$ (altrimenti G sarebbe ciclico), si conclude che $\mathrm{ord}(a) = n$.

   (b) Dato $b \in H$, per definizione esiste $m \in \mathbb{Z}$ tale che $b = a^m$. Allora

$$f(b) = f(a^m) = mf(a) = m\overline{1} = \overline{m},$$

   per cui $b \in K$ se e solo se $\overline{m} = \overline{0}$ se e solo se $n \mid m$. Poiché $\mathrm{ord}(a) = n$ per il punto precedente, si ha $b = a^m = 1$ se e solo se $n \mid m$, e quindi $H \cap K = \{1\}$. Tenendo poi presente che $\#H = \mathrm{ord}(a) = n$ e che

$$\#K = \frac{\#G}{\#(\mathbb{Z}/n\mathbb{Z})} = \frac{2n}{n} = 2$$

   (dato che $G/K \cong \mathbb{Z}/n\mathbb{Z}$ per il primo teorema di isomorfismo), si trova

$$\#(HK) = \frac{(\#H)(\#K)}{\#(H \cap K)} = \frac{n \cdot 2}{1} = 2n = \#G,$$

   per cui $HK = G$.

   (c) Sia H che K sono sottogruppi normali di G (il primo perché di indice 2, il secondo perché nucleo di un omomorfismo di gruppi), e dunque dal punto precedente segue che $G \cong H \times K$. D'altra parte $H \cong \mathbb{Z}/n\mathbb{Z}$ (essendo ciclico di ordine n) e $K \cong \mathbb{Z}/2\mathbb{Z}$ (avendo ordine 2), per cui $G \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Inoltre n deve essere pari, perché per n dispari (cioè tale che $\mathrm{mcd}(n, 2) = 1$) si avrebbe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2n\mathbb{Z}$ per il teorema cinese del resto, e quindi G sarebbe ciclico.

3. (a) Per ogni $a, b, c, d, e, f \in \mathbb{R}$ si ha

$$\begin{aligned}[(a,b)(c,d)](e,f) &= (ac, ad+bc)(e,f) = (ace, acf + (ad+bc)e) \\ &= (ace, a(cf+de)+bce) = (a,b)(ce, cf+de) = (a,b)[(c,d)(e,f)]\end{aligned}$$

   (cioè il prodotto è associativo),

$$(a,b)(c,d) = (ac, ad+bc) = (ca, cb+da) = (c,d)(a,b)$$

   (cioè il prodotto è commutativo),

$$(a,b)(1,0) = (a \cdot 1, a \cdot 0 + b \cdot 1) = (a,b)$$

(cioè $(1,0)$ è l'elemento neutro del prodotto) e

$$\begin{aligned}&(a,b)[(c,d)+(e,f)] = (a,b)(c+e,d+f)\\&= (a(c+e), a(d+f)+b(c+e)) = (ac+ae, ad+bc+af+be)\\&\qquad = (ac,ad+bc)+(ae,af+be) = (a,b)(c,d)+(a,b)(e,f)\end{aligned}$$

(cioè vale la proprietà distributiva).

(b) La funzione $f\colon \mathbb{R}[X] \to A$ definita da $f(\sum_{i\geq 0} a_i X^i) = (a_0, a_1)$ è un omomorfismo di anelli perché $f(1) = (1,0)$,

$$\begin{aligned}&f(\sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i) = f(\sum_{i\geq 0}(a_i+b_i)X^i)\\&= (a_0+b_0, a_1+b_1) = (a_0,a_1)+(b_0,b_1) = f(\sum_{i\geq 0} a_i X^i)+f(\sum_{i\geq 0} b_i X^i)\end{aligned}$$

e

$$\begin{aligned}&f((\sum_{i\geq 0} a_i X^i)(\sum_{i\geq 0} b_i X^i)) = f(\sum_{i\geq 0}(\sum_{j=0}^{i} a_j b_{i-j})X^i)\\&= (a_0b_0, a_0b_1+a_1b_0) = (a_0,a_1)(b_0,b_1) = f(\sum_{i\geq 0} a_i X^i) f(\sum_{i\geq 0} b_i X^i)\end{aligned}$$

per ogni $\sum_{i\geq 0} a_i X^i, \sum_{i\geq 0} b_i X^i \in \mathbb{R}[X]$. f è suriettivo perché per ogni $a, b \in \mathbb{R}$ si ha $(a,b) = f(a+bX)$ e $\ker(f) = (X^2)$ perché $f(\sum_{i\geq 0} a_i X^i) = (0,0)$ se e solo se $a_0 = a_1 = 0$ se e solo se $\sum_{i\geq 0} a_i X^i \in (X^2)$. Dunque

$$A = \operatorname{im}(f) \cong \mathbb{R}[X]/\ker(f) = \mathbb{R}[X]/(X^2)$$

per il primo teorema di isomorfismo per anelli.

(c) Attraverso l'isomorfismo $A \cong \mathbb{R}[X]/(X^2)$ descritto nel punto precedente, gli ideali (non banali) di A corrispondono agli ideali (non banali) di $\mathbb{R}[X]/(X^2)$. D'altra parte, gli ideali di $\mathbb{R}[X]/(X^2)$ sono tutti e soli della forma $I/(X^2)$ con I ideale di $\mathbb{R}[X]$ tale che $(X^2) \subseteq I$. Poiché $\mathbb{R}[X]$ è un dominio a ideali principali (essendo $\mathbb{R}$ un campo), per ogni ideale I di $\mathbb{R}[X]$ esiste (unico a meno di associati) $p \in \mathbb{R}[X]$ tale che $I = (p)$. Dato che X è irriducibile in $\mathbb{R}[X]$, la condizione $(X^2) \subseteq (p)$ (che equivale a $p \mid X^2$) è soddisfatta se e solo se p è associato a uno tra 1, X e X^2. Perciò gli ideali di $\mathbb{R}[X]/(X^2)$ sono solo $(1)/(X^2) = \mathbb{R}[X]/(X^2)$, $(X)/(X^2)$ e

$(X^2)/(X^2) = \{\overline{0}\}$, e quindi l'unico ideale non banale è $(X)/(X^2)$. Dato che (con la notazione del punto precedente) $f(X) = (0,1)$, è facile vedere che $(X)/(X^2)$ corrisponde all'ideale

$$(0,1)A = \{(0,1)(a,b) \,:\, a,b \in \mathbb{R}\} = \{(0,a) \,:\, a \in \mathbb{R}\}$$

di A, che è dunque l'unico ideale non banale di A.

4. (a) Se a è dispari, $2 \nmid 1$, $2 \mid 0$, $2 \mid (a-1)$, $2 \mid (2a)$ e $4 \nmid (2a)$. Allora p_a è irriducibile in $\mathbb{Z}[X]$, e quindi anche in $\mathbb{Q}[X]$, per il criterio di Eisenstein relativo al numero primo 2.

   (b) Non esiste $a \in \mathbb{Z}$ tale che p_a ha una radice multipla. Infatti $q \in \mathbb{Q}$ è radice multipla di p_a se e solo se q è radice sia di p_a che della sua derivata $p'_a = 4X^3 + a - 1$. Ora, se a è dispari, p_a non ha radici razionali per il punto precedente. Se invece a è pari, è facile vedere che p'_a non ha radici razionali. Per dimostrarlo, assumiamo per assurdo che $q \in \mathbb{Q}$ sia radice di p'_a per qualche a pari. Allora $1-a = 4q^3$, e quindi, se $q = \frac{r}{s}$ con $r, s \in \mathbb{Z}$ e $s \neq 0$, $(1-a)s^3 = 4r^3$. Quest'ultima uguaglianza tra interi è però impossibile, dato che, essendo $a-1$ dispari, nel membro di sinistra il primo 2 compare con esponente $\equiv 0 \mod 3$, mentre in quello di destra compare con esponente $\equiv 2 \mod 3$.

   (c) Facendo la divisione con resto di p_a per $X^2 + X + 4$ si trova

$$p_a = (X^2 - X - 3)(X^2 + X + 4) + (a+6)X + 2a + 12,$$

   per cui il resto $(a+6)X+2a+12$ è zero se e solo se $a = -6$. Dunque il valore cercato è $b = -6$. Posto $f_1 = X^2 - X - 3$ e $f_2 = X^2 + X + 4$, si ha allora $p_b = f_1 f_2$ e quindi $(p_b) = (f_1)(f_2)$ come ideali. È immediato verificare che f_1 e f_2 non hanno radici razionali, e perciò, avendo grado 2, sono irriducibili in $\mathbb{Q}[X]$. Poiché $\mathbb{Q}[X]$ è un dominio a ideali principali (dato che $\mathbb{Q}$ è un campo), per $i = 1, 2$ l'ideale (f_i) è massimale e dunque $K_i = \mathbb{Q}[X]/(f_i)$ è un campo. Inoltre f_1 e f_2 non sono associati in $\mathbb{Q}[X]$, per cui (f_1) e (f_2) sono ideali massimali distinti di $\mathbb{Q}[X]$, e da ciò segue che $(f_1) + (f_2) = \mathbb{Q}[X]$. Allora si può applicare il teorema cinese per anelli, ottenendo l'isomorfismo richiesto

$$\mathbb{Q}[X]/(p_b) = \mathbb{Q}[X]/(f_1)(f_2) \cong \mathbb{Q}[X]/(f_1) \times \mathbb{Q}[X]/(f_2) = K_1 \times K_2.$$