

SOLUZIONI DEL COMPITO DI ALGEBRA 1

9 luglio 2013

1. a) Siano A, B, C gruppi abeliani. Dimostrare che

$$\text{Hom}(A \oplus B, C) \cong \text{Hom}(A, C) \oplus \text{Hom}(B, C).$$

b) Sia G un gruppo abeliano di ordine n ; dimostrare che $G \cong \text{Hom}(G, \mathbb{Z}/n\mathbb{Z})$.

Soluzione esercizio 1. a) Consideriamo la mappa:

$$\varphi : \text{Hom}(A, C) \oplus \text{Hom}(B, C) \mapsto \text{Hom}(A \oplus B, C)$$

definita da $\varphi((f, g)) = h$ dove $h(x, y) = f(x) + g(y)$ per ogni $x \in A, y \in B$.

E' immediato vedere che l'applicazione φ è ben definita (si tratta di vedere che $h \in \text{Hom}(A \oplus B, C)$) inoltre è un omomorfismo, cioè $\varphi((f, g) + (f', g')) = \varphi((f, g)) + \varphi((f', g'))$, infatti $\forall (x, y) \in A \oplus B$ si ha $\varphi((f, g) + (f', g'))(x, y) = \varphi((f + f', g + g'))(x, y) = (f + f')(x) + (g + g')(y) = f(x) + f'(x) + g(y) + g'(y) = f(x) + g(y) + f'(x) + g'(y) = \varphi((f, g))(x, y) + \varphi((f', g'))(x, y) = (\varphi((f, g)) + \varphi((f', g')))(x, y)$.

Inoltre $\varphi(f, g) = 0$ se e solo se $f(x) + g(y) = 0$ per ogni $x \in A$ e per ogni $y \in B$. In particolare prendendo $y = 0$ si ottiene $\varphi(f, g) = 0 \Rightarrow f(x) = 0 \forall x \in A$, quindi $f = 0$ e quindi anche $g = 0$. Ne segue che $\text{Ker}(\varphi) = \{0\}$, cioè φ è iniettiva.

L'omomorfismo φ è anche surgettivo in quanto $\forall h \in \text{Hom}(A \oplus B, C)$ si ha $\varphi((f, g)) = h$ per f e g definite da $f(x) = h(x, 0)$ e $g(y) = h(0, y)$.

b) Dal teorema di struttura dei gruppi abeliani abbiamo che $G \cong \bigoplus_{i=1}^r \mathbb{Z}/d_i\mathbb{Z}$, quindi per il punto (a) vale

$$\text{Hom}(G, \mathbb{Z}/n\mathbb{Z}) \cong \bigoplus_{i=1}^r \text{Hom}(\mathbb{Z}/d_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}),$$

basta quindi dimostrare che se $d|n$ si ha $\text{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$.

Sappiamo che un omomorfismo definito su $\mathbb{Z}/d\mathbb{Z}$ è completamente definito dall'immagine di $\bar{1}$ e che questa può essere un qualsiasi elemento di $\mathbb{Z}/n\mathbb{Z}$ di ordine che divide d . Ne segue che $|\text{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})| = d$, ed è ciclico in quanto la mappa $f \rightarrow f(1)$ lo immerge in $\mathbb{Z}/n\mathbb{Z}$. Questo dimostra quanto richiesto.

2. Determinare, a meno di isomorfismo, i sottogruppi di S_6 di ordine 8.

Soluzione esercizio 2. Sappiamo che un gruppo di ordine 8 è isomorfo a uno dei seguenti gruppi: $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_4, Q$ = gruppo dei quaternioni. Vediamo quale di questi è isomorfo ad un sottogruppo di S_6 .

S_6 non ha sottogruppi isomorfi a $\mathbb{Z}/8\mathbb{Z}$ in quanto S_6 non ha elementi di ordine 8.

Sia H il sottogruppo di S_6 generato da $\{(1, 2, 3, 4), (5, 6)\}$: poiché i generatori commutano si ha $H \cong \langle (1, 2, 3, 4) \rangle \times \langle (5, 6) \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Analogamente $K = \langle (1, 2), (3, 4), (5, 6) \rangle = \langle (1, 2) \rangle \times \langle (3, 4) \rangle \times \langle (5, 6) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Anche D_4 si immerge in S_4 : questo si può mostrare osservando che D_4 si immerge in S_4 in quanto le isometrie del quadrato inducono una permutazione dei suoi quattro vertici, e quindi anche in S_6 , oppure osservando che $\langle (1, 2, 3, 4), (1, 2)(3, 4) \rangle \cong D_4$ (infatti $(1, 2, 3, 4)(1, 2)(3, 4) = (1, 2)(3, 4)(4, 3, 2, 1)$).

Mostriamo ora che S_6 non ha sottogruppi isomorfi a gruppo dei quaternioni Q . Sappiamo che $Q = \{\pm 1, \pm i \pm j \pm k\}$ dove $i^4 = j^4 = k^4 = 1$ e $i^2 = j^2 = k^2 = -1$; se S_6 avesse un sottogruppo isomorfo a Q dovrebbe contenere 3 permutazioni σ, τ, ρ immagine rispettivamente di i, j, k e quindi di ordine 4, che generano sottogruppi diversi, e tali che $\sigma^2 = \tau^2 = \rho^2 = \gamma$ con γ di ordine 2. Le permutazioni di ordine 2 sono prodotto di trasposizioni e tra queste quelle che sono quadrati sono solo quelle di tipo $2+2$. L'equazione $x^2 = (a, b)(c, d)$ in S_6 ha come soluzioni solo (a, c, b, d) il suo inverso e $(a, b, c, d)(e, f)$ e il suo inverso. Da questo segue che in S_6 non esistono 3 permutazioni σ, τ, ρ con le proprietà cercate e quindi S_6 non ha sottogruppi isomorfi a Q .

3. Sia $\gamma = 3 + i \in \mathbb{Z}[i]$ e sia

$$A := \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in \mathbb{Z}[i], (\beta, \gamma) = 1 \right\}.$$

Determinare gli elementi invertibili e gli ideali primi dell'anello A .

Soluzione esercizio 3. Gli elementi invertibili di A sono quelli che nella loro scrittura ridotta ai minimi termini ($\mathbb{Z}[i]$ è UFD) hanno numeratore e denominatore coprimi con γ . Infatti, chiaramente tali elementi sono invertibili in A ; viceversa sia se $\frac{\alpha}{\beta} \in A^*$, allora $\frac{\beta}{\alpha} \in A$. Supponendo che la frazione sia ridotta ai minimi termini, si ha che necessariamente $(\alpha, \gamma) = (\beta, \gamma) = 1$. Ora ogni elemento di A è del tipo $\frac{\alpha}{\beta} = \frac{\alpha_1(\alpha, \gamma)}{\beta}$ con α_1 coprimo con γ e quindi $\frac{\alpha}{\beta}$ è associato a (α, γ) . Fattorizziamo γ : si ha $N(\gamma) = (3 + i)(3 - i) = 10$ quindi γ è prodotto di due fattori irriducibili uno di norma 2 (l'unico a meno di moltiplicazione per invertibili è $1 + i$) e uno di norma 5 e si calcola $\gamma = (1 + i)(2 - i)$.

Da quanto detto segue che ogni elemento di A è associato ad un elemento del tipo $(1 + i)^a(2 - i)^b$. Dico che gli ideali primi di A sono $\{0\}$, $P_1 = (1 + i)$ e $P_2 = (2 - i)$. Questi sono chiaramente ideali primi (si può vedere ad esempio facendo l'anello quoziente che P_1 e P_2 sono anche massimali), inoltre se P è un ideale primo non nullo, sia $(1 + i)^a(2 - i)^b \in P$ allora $(1 + i) \in P$ oppure $(2 - i) \in P$ e solo uno dei due appartiene a P perchè altrimenti P conterrebbe anche 1. Da questo si deduce che $P = (1 + i)$ oppure $P = (2 - i)$, che dimostra quanto affermato.

4. Determinare le sottoestensioni di $\mathbb{Q}(\zeta_{36})$, dando per ognuna un insieme di generatori su \mathbb{Q} .

Soluzione esercizio 4. Ricordiamo che $K = \mathbb{Q}(\zeta_{36})$ è un'estensione di Galois di \mathbb{Q} e $\text{Gal}(\mathbb{Q}(\zeta_{36})) \cong (\mathbb{Z}/36\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. La corrispondenza di Galois assicura che i sottocampi che stiamo cercando sono in corrispondenza biunivoca con i sottogruppi di sottogruppi di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Questo gruppo ha, oltre ai sottogruppi banali, 3 sottogruppi di ordine 2, 1 sottogruppo di ordine 3, 1 sottogruppo di ordine 4 e 3 sottogruppi di ordine 6. Ne segue che, oltre alle sottoestensioni banali \mathbb{Q} e $\mathbb{Q}(\zeta_{36})$, ci sono 3 sottoestensioni di ordine 6 su \mathbb{Q} , 1 di ordine 4, 1 di ordine 3 e 3 di

ordine 2. Dobbiamo determinare i generatori di queste estensioni.

Cominciamo con l'elencare le sottoestensioni note: sappiamo che $\mathbb{Q}(i) \subset K$ e $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_9) \subset K$. Da questo si ricava che $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ e quindi anche $\mathbb{Q}(\sqrt{3})$ sono sottoestensioni di K (e sono tutte quelle di grado 2 su \mathbb{Q}) e $\mathbb{Q}(i, \sqrt{3}) \subset K$ è la sottoestensione di grado 4. Inoltre $\mathbb{Q}(\zeta_9) \subset K$ ha grado 6 su \mathbb{Q} e la sua sottoestensione reale $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ ha grado 3 su \mathbb{Q} . Le sottoestensioni di grado 6 su \mathbb{Q} si ottengono quindi componendo le 3 sottoestensioni di grado 2 con quella di grado 3 e son quindi: $\mathbb{Q}(i, \zeta_9 + \zeta_9^{-1})$, $\mathbb{Q}(\sqrt{3}, \zeta_9 + \zeta_9^{-1})$ e $\mathbb{Q}(\sqrt{-3}, \zeta_9 + \zeta_9^{-1}) = \mathbb{Q}(\zeta_9)$