2° COMPITINO DI ARITMETICA

20 dicembre 2017

1. (a) Siano G un gruppo abeliano, H un gruppo qualunque e $f\colon G \to H$ un omomorfismo. Dimostrare che $f(G)$ è un sottogruppo abeliano di H.

(b) Sia $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Determinare il numero degli omomorfismi surgettivi da G a $\mathcal{S}_3$. Contare tutti gli omomorfismi da G a $\mathcal{S}_3$.

SOLUZIONE.

(a) *Prima soluzione.* Sappiamo che se $f : G \to H$ è un omomorfismo di gruppi $f(G)$ è sempre un sottogruppo di H, quindi basta vedere che è abeliano, ovvero che dati $y_1, y_2 \in f(G)$ si ha $y_1y_2 = y_2y_1$, dove l'operazione di gruppo è quella di H. Per definizione di $f(G)$, esistono $x_1 \in G, x_2 \in G$ tali che $y_1 = f(x_1)$ e $y_2 = f(x_2)$. Dal momento che G è abeliano si ha $x_1x_2 = x_2x_1$ (dove l'operazione, questa volta, è quella di G), e usando il fatto che f è un omomorfismo otteniamo

$$x_1x_2 = x_2x_1 \Rightarrow f(x_1x_2) = f(x_2x_1) \Rightarrow f(x_1)f(x_2) = f(x_2)f(x_1) \Rightarrow y_1y_2 = y_2y_1$$

come desiderato.

Seconda soluzione. Per il primo teorema di omomorfismo, detto $K = \ker(f)$ si ha $f(G) \cong G/K$. Siano $a+K$ e $b+K$ due classi laterali qualunque di G/K: allora, utilizzando la definizione della moltiplicazione nel gruppo quoziente G/K e il fatto che $ab = ba$ in G, si ha

$$(a + K)(b + K) = ab + K = ba + K = (b + K)(a + K),$$

il che dimostra che G/K è abeliano. Siccome $f(G)$ e G/K sono isomorfi, anche $f(G)$ è abeliano.

(b) Non esiste alcun omomorfismo surgettivo da G a $\mathcal{S}_3$. Supponiamo infatti per assurdo che esista un omomorfismo surgettivo $f : G \to \mathcal{S}_3$: allora per il punto precedente il gruppo $f(G) = \mathcal{S}_3$ sarebbe abeliano, cosa che sappiamo non essere vera. Ne segue che se $f : G \to \mathcal{S}_3$ è un omomorfismo qualunque, allora la sua immagine (che deve essere un sottogruppo di $\mathcal{S}_3$, di ordine 6) può solo avere ordine 1, 2, o 3; in particolare, l'immagine di f è ciclica. Analizziamo i tre casi separatamente:

i. $|f(G)| = 1$. Allora f è necessariamente l'omomorfismo banale che manda ogni elemento di G nell'identità di $\mathcal{S}_3$; in particolare, esiste un unico omomorfismo di questo tipo.

ii. $|f(G)| = 2$. In tal caso $f(G)$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$ (l'unico gruppo di ordine 2 a meno di isomorfismo); $\mathcal{S}_3$ contiene tre sottogruppi isomorfi a $\mathbb{Z}/2\mathbb{Z}$, ovvero quelli generati da una singola trasposizione $(1,2)$, $(1,3)$ o $(2,3)$. Ne segue che il numero degli omomorfismi di questo tipo è 3 volte il numero di omomorfismi surgettivi $G \to \mathbb{Z}/2\mathbb{Z}$. Per contare questi, osserviamo che è sufficiente contare tutti gli omomorfismi da $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ a $\mathbb{Z}/2\mathbb{Z}$ e sottrarre l'unico omomorfismo banale. Un omomorfismo $f : \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ è determinato dall'immagine dei tre elementi $(1,0,0), (0,1,0), (0,0,1)$. L'immagine dei primi due può essere scelta in due modi, mentre l'immagine del terzo deve essere necessariamente l'identità, visto che 2 e 3 sono primi fra loro. Ne segue che esistono esattamente 4 omomorfismi $G \to \mathbb{Z}/2\mathbb{Z}$, di cui 3 non banali. Il numero di omomorfismi $f : G \to \mathcal{S}_3$ con $|f(G)| = 2$ è dunque pari a $3 \times 3 = 9$.

iii. $|f(G)| = 3$. Il gruppo $\mathcal{S}_3$ contiene un unico sottogruppo di ordine 3, ovvero quello costituito dall'identità e dai 3-cicli $(123), (132)$. In particolare, il numero di omomorfismi f di questo tipo è pari al numero di omomorfismi $G \to \mathbb{Z}/3\mathbb{Z}$. Scrivendo come prima $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ e ragionando come sopra, vediamo che un omomorfismo f è completamente determinato dalle immagini di $(1,0,0), (0,1,0)$ e $(0,0,1)$, e che l'immagine dei primi due di questi elementi deve essere banale. In quanto a $f((0,0,1))$, affinché l'immagine di f abbia ordine 3 si deve avere $f((0,0,1)) = (1,2,3)$ o $f((0,0,1)) = (1,3,2)$, e queste sono le uniche due possibilità. Esistono quindi esattamente due omomorfismi $f : G \to \mathcal{S}_3$ con $|f(G)| = 3$.

In totale, ci sono $1 + 9 + 2 = 12$ omomorfismi $G \to \mathcal{S}_3$.

2. Sia $m \in \mathbb{Z}$ un numero intero diverso da zero e sia $f_a(X) = X^4 - aX - m \in \mathbb{Z}[X]$. Dimostrare che il numero degli elementi $a \in \mathbb{Z}$ per cui $f_a(X)$ è riducibile è finito.

SOLUZIONE: Per il lemma di Gauss, il polinomio $f_a(X)$ è riducibile se e solo se è il prodotto due polinomi di grado positivo a coefficienti interi.

Supponiamo dapprima che $f(x)$ abbia un fattore di primo grado, e quindi una radice. La radice va cercata fra i divisori di m, che sono in numero finito. Se $d|m$ è una radice, allora $d^4 - ad - m = 0$, dunque $d(d^3 - a) = m$ e quindi c'è un'unica possibilità per a, ossia $a = d^3 - \frac{m}{d}$.

Supponiamo ora che $f_a(X)$ si possa scrivere come prodotto di due polinomi di secondo grado, $f_a(X) = g(X)h(X)$. Senza perdita di generalità, i due polinomi $g(X)$ e $h(X)$ si possono supporre monici (il prodotto dei loro primi coefficienti deve essere uguale a 1), e quindi possiamo scrivere

$$g(X) = x^2 + qX + r, \qquad h(X) = X^2 + sX + t$$

per opportuni $q, r, s, t \in \mathbb{Z}$. Moltiplicando ed uguagliando i termini dello stesso grado, otteniamo il sistema di equazioni

$$\begin{cases} q + s = 0 \\ r + qs + t = 0 \\ qt + rs = -a \\ rt = -m \end{cases}$$

La prima equazione dà $s = -q$. Sostituendo nella seconda equazione, si ottiene $r + t = q^2$. L'ultima equazione dice che r e t sono divisori di m, quindi sono in numero finito. Ne segue che anche q ha un numero finito di possibilità.

Infine, sostituendo nella terza equazione, si ottiene che il numero di possibili valori di a per cui questo accade è finito.

3. Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

(a) Dimostrare che $[K : \mathbb{Q}] = 6$.

(b) Dimostrare che $K = \mathbb{Q}(\sqrt[6]{2})$.

(c) Determinare il polinomio minimo di $\sqrt{2} + \sqrt[3]{2}$ su $\mathbb{Q}(\sqrt{2})$ e su $\mathbb{Q}$.

Soluzione.

(a) Per definizione, K è il campo composto di $K_2 = \mathbb{Q}(\sqrt{2})$ e $K_3 = \mathbb{Q}(\sqrt[3]{2})$ su $\mathbb{Q}$. I gradi $[K_2 : \mathbb{Q}]$ e $[K_3 : \mathbb{Q}]$ valgono rispettivamente 2 e 3, dal momento che $\sqrt{2}$ e $\sqrt[3]{2}$ sono radici dei polinomi $x^2 - 2, x^3 - 2$ (che sono irriducibili, in quanto di Eisenstein rispetto al primo 2). Dal momento che gli interi $[K_2 : \mathbb{Q}]$ e $[K_3 : \mathbb{Q}]$ sono primi fra loro, il grado $[K : \mathbb{Q}] = [K_2K_3 : \mathbb{Q}]$ è uguale al prodotto $[K_2 : \mathbb{Q}][K_3 : \mathbb{Q}] = 2 \cdot 3 = 6$.

(b) Sia $K_6 = \mathbb{Q}(\sqrt[6]{2})$. Osserviamo che $[K_6 : \mathbb{Q}] = 6$, perché K_6 è generato su $\mathbb{Q}$ da una radice del polinomio $x^6 - 2$, che è di grado 6 e irriducibile (in quanto Eisenstein rispetto al primo 2). Ne segue che $[K_6 : \mathbb{Q}] = 6 = [K : \mathbb{Q}]$, e

quindi per dimostrare l'uguaglianza $K = K_6$ è sufficiente dimostrare che K è incluso in K_6. Per fare ciò è chiaramente sufficiente mostrare che $\sqrt{2}$ e $\sqrt[3]{2}$ appartengono a K_6, e questo è vero dal momento che

$$\sqrt{2} = (\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2}), \quad \sqrt[3]{2} = (\sqrt[6]{2})^2 \in \mathbb{Q}(\sqrt[6]{2}).$$

(c) Scriviamo per semplicità $\alpha := \sqrt{2} + \sqrt[3]{2}$. Osserviamo che il polinomio $p(x) = (x - \sqrt{2})^3 - 2$ appartiene a $\mathbb{Q}(\sqrt{2})[x]$ e si annulla per $x = \alpha$, dunque $p(x)$ è un multiplo del polinomio minimo di α su $\mathbb{Q}(\sqrt{2})$. D'altro canto, il grado del polinomio minimo di α su $\mathbb{Q}(\sqrt{2})$ è il grado dell'estensione

$$[\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}(\sqrt{2})],$$

e chiaramente si ha

$$\mathbb{Q}(\alpha, \sqrt{2}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = K.$$

Ne segue che $[\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = [K : \mathbb{Q}(\sqrt{2})] = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]} = 3$, e dunque il polinomio minimo di α su $\mathbb{Q}(\sqrt{2})$ ha grado 3. Dato che $p(x) \in \mathbb{Q}(\sqrt{2})[x]$ è un polinomio monico di grado 3 che si annulla in α, esso è il polinomio minimo di α su $\mathbb{Q}(\sqrt{2})$.

Il polinomio minimo di α su $\mathbb{Q}$, d'altra parte, è un multiplo del polinomio minimo di α su $\mathbb{Q}(\sqrt{2})$. Inoltre, siccome è evidente che $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Combinato con il fatto che $3 = [\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$, questo ci dice che il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è 3 oppure 6. Se si avesse $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, il polinomio minimo di α su $\mathbb{Q}$ sarebbe uguale al polinomio minimo $p(x)$ di α su $\mathbb{Q}(\sqrt{2})$. Tuttavia, $p(x) = x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} - 2$ non ha coefficienti razionali, quindi questo non è possibile. Ne segue che il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è uguale a 6. Per trovare un polinomio di grado 6 che si annulli in α, osserviamo che l'uguaglianza $p(\alpha) = 0$ fornisce

$$\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} - 2 = 0,$$

da cui

$$\alpha^3 + 6\alpha - 2 = 3\sqrt{2}\alpha^2 + 2\sqrt{2},$$

ed elevando entrambi i membri al quadrato si trova

$$(\alpha^3 + 6\alpha - 2)^2 = 2(3\alpha^2 + 2)^2.$$

Ne segue che il polinomio

$$q(x) = (x^3 + 6x - 2)^2 - 2(3x^2 + 2)^2 = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$$

si annulla in α, è monico, di grado 6, e a coefficienti razionali. Esso è quindi il polinomio minimo di α su $\mathbb{Q}$.

Commenti.

- È chiaro che $\mathbb{Q}(\alpha)$ è contenuto in K (in quanto somma di $\sqrt{2}$ e $\sqrt[3]{2}$, entrambi elementi di K per definizione). Il fatto che il polinomio minimo di α su $\mathbb{Q}$ sia di grado 6 è equivalente al fatto che $[K(\alpha) : \mathbb{Q}] = 6$, il che (in virtù dell'osservazione fatta sopra) è a sua volta equivalente al fatto che valga l'uguaglianza $K = \mathbb{Q}(\alpha)$. Questo fatto può essere anche dimostrato direttamente senza eccessiva difficoltà: infatti, come stabilito nel corso della soluzione precedente si ha

  $$\alpha^3 + 6\alpha - 2 = 3\sqrt{2}\alpha^2 + 2\sqrt{2},$$

  ovvero

  $$\sqrt{2} = \frac{\alpha^3 + 6\alpha - 2}{3\alpha^2 + 2},$$

  dove ovviamente il denominatore è diverso da zero. Questo dimostra che $\sqrt{2} \in \mathbb{Q}(\alpha)$, e quindi, per differenza, $\sqrt[3]{2} = \alpha - \sqrt{2}$ è anch'esso un elemento di $\mathbb{Q}(\alpha)$. Ne segue che $\sqrt{2}, \sqrt[3]{2}$ sono in $\mathbb{Q}(\alpha)$, e dunque che $K \subseteq \mathbb{Q}(\alpha)$. L'altra inclusione, come già osservato, è chiara.
- Osserviamo esplicitamente che il Criterio di Eisenstein non si applica al polinomio $x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$, perché l'unico primo a dividere tutti i coefficienti (tranne il primo) è $p = 2$, ma il termine noto è divisibile per 2^2.