Algebra 1

Prof. A. D'Andrea, A. De Sole, G. Mondello

Soluzioni della prova scritta del 1 luglio 2022

Esercizio 1. Per quali interi n esiste un omomorfismo tra gruppi $\phi : \mathbb{Z}/48 \to C_{36} = \langle x \rangle$ tale che $\phi(\bar{1}) = x^n$? Per quali interi n tale omomorfismo è suriettivo?

Risposta: ϕ esiste $\iff n \equiv 0 \pmod 3$, e non è mai suriettivo.

Soluzione: Costruire un omomorfismo di gruppi $\mathbb{Z}/(n) \to G$ è equivalente a descrivere un omomorfismo $\mathbb{Z} \to G$ che abbia (n) nel suo nucleo. Inoltre un omomorfismo $f : \mathbb{Z} \to G$ è noto una volta che sia nota l'immagine $f(1)$ del generatore $1 \in \mathbb{Z}$.

Nella nostra situazione, l'omomorfismo $\phi : \mathbb{Z}/(48) \to C_{36}$ è determinato se riusciamo a costruire $f : \mathbb{Z} \to C_{36}$ in modo che $48 \in \ker f$. Ci viene inoltre prescritta l'immagine $f(1) = x^n$.

Si calcola immediatamente che $f(48) = x^{48n}$. Affinché $48 \in \ker f$, deve valere $x^{48n} = 1$ nel gruppo C_{36}; in altre parole va imposto che $48n$ sia un multiplo di 36. A questo punto si procede senza troppi problemi: $48n \equiv 0 \pmod 3 6$ è equivalente a $4n \equiv 0 \pmod 3$, ossia equivalentemente $n \equiv 0 \pmod 3$. Per nessuno di tali valori di n l'omomorfismo ϕ è suriettivo, in quanto l'immagine è contenuta in $\langle x^3 \rangle$.

Non è strettamente necessario procedere con il teorema di omomorfismo. Un modo più diretto è notare che ϕ è noto una volta scelta l'immagine di $\bar{1}$, ma che tale immagine **deve** essere un elemento di ordine che divide 48. L'ordine di x^n in C_{36} è comunque $36/MCD(36, n)$ e affinché tale numero sia un divisore di 48 va imposto che $MCD(36, n)$ sia multiplo di 3. Si arriva immediatamente alla stessa condizione di prima.

Analogamente, si può rispondere alla domanda sulla suriettività anche senza aver compreso la prima parte dell'esercizio: l'immagine di ϕ è un sottogruppo di C_{36} ed è isomorfa ad un quoziente di $\mathbb{Z}/(48)$. Il suo ordine deve pertanto dividere sia 36 che 48 e inevitabilmente anche il loro massimo comun divisore 12. L'omomorfismo non potrà quindi mai essere suriettivo.

Esercizio 2. Determinare tutti i gruppi finiti che contengano al più tre classi di coniugio.

Risposta: a meno di isomorfismo

(1) l'unico gruppo con una classe di coniugio è $G = (1)$

(2) l'unico gruppo con due classi di coniugio è C_2

(3) gli unici gruppi con tre classi di coniugio sono C_3 e S_3.

Soluzione:

Questo esercizio era tra quelli assegnati nei fogli settimanali. Determineremo, ovviamente, tali gruppi a meno di isomorfismo.

Innanzitutto, l'identità fa sempre classe a sé in un gruppo.

(1) Se un gruppo possiede una sola classe di coniugio contiene pertanto la sola identità, ed è il gruppo banale $G = (1)$.

(2) Se le classi di coniugio sono due, e il gruppo ha ordine n, allora una delle classi è quella dell'identità, mentre l'altra contiene i restanti $n-1$ elementi. Abbiamo visto a lezione che la cardinalità di una classe di coniugio divide l'ordine del gruppo e quindi $n-1$ deve dividere n. Questo accade solo se $n-1 = 1$, cioè quando $n = 2$. Il gruppo ha allora ordine 2, ed è ciclico (e quindi abeliano, ed effettivamente le classi di coniugio sono due!!).

(3) Rimane il caso di tre classi di coniugio. La cardinalità di ciascuna divide l'ordine n del gruppo e possiamo quindi scriverle nella forma $n/a, n/b, n/c$ dove a, b, c sono interi. Le classi di coniugio costituiscono una partizione del gruppo e quindi

$$n = \frac{n}{a} + \frac{n}{b} + \frac{n}{c} \implies 1 = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Ricordate che la classe dell'identità contiene un solo elemento, e quindi il più grande tra a, b, c è proprio l'ordine n del gruppo. Possiamo supporre che $a \leq b \leq c$. Se $a \geq 4$, allora $1/a, 1/b, 1/c$ sono tutti $\leq 1/4$ e la loro somma non può raggiungere 1. Possiamo allora limitarci a considerare i casi $a = 2, 3$, dal momento che $a = 1$ è impossibile.

Se $a = 3$, poiché $b, c \geq a$, l'unico possibilità è $a = b = c = 3$. L'equazione delle classi è allora $3 = 1 + 1 + 1$ e il gruppo è abeliano di ordine 3. A meno di isomorfismi, si tratta di C_3.

Se $a = 2$, abbiamo le due possibilità

$$a = 2, b = 3, c = 6, \qquad a = 2, b = 4, c = 4,$$

poiché se $b, c \geq 5$, non riusciamo a raggiungere 1 con la somma. Il secondo caso si esclude immediatamente: l'equazione delle classi sarebbe $4 = 1 + 1 + 2$, ma un gruppo di ordine 4 è sempre abeliano, e tutte le sue classi di coniugio possiedono un unico elemento. Nel primo caso l'equazione delle classi è $6 = 1+2+3$: si tratta di un gruppo non abeliano di ordine 6, che deve essere isomorfo a S_3. In effetti S_3 ha proprio tre classi di coniugio, di cardinalità $1, 2, 3$.

In conclusione, una lista completa, a meno di isomorfismi, di gruppi finiti con al più tre classi di coniugio è C_1, C_2, C_3, S_3.

P.S. a lezione il caso con tre classi di coniugio lo avevamo fatto diversamente, indicando con $1 \leq m \leq n$ le cardinalità delle tre classi di coniugio, e osservando che da $n|(m+n+1) = |G|$ segue $n|(m+1)$. Poiché $n \geq m$ si ottiene $m \leq n \leq m+1$. Se $n = m$, si ha $n|2n+1$ da cui $m = n = 1$. Se $n = m+1$, si ottiene $m|2m+2$, da cui $m = 1, 2$ e quindi $(m, n) = (1, 2)$ oppure $(2, 3)$. Le conclusioni sono poi come prima.

Esercizio 3. Sia $E : \mathbb{Z}[x] \to \mathbb{F}_7$ l'applicazione definita da $E(p(x)) =$ classe di resto modulo 7 di $p(2)$.

(a) Mostrare che E è un omomorfismo di anelli.

(b) Mostrare che $2x + 3$ e $x^2 + x + 1$ appartengono a $\ker E$.

(c) Mostrare che 7 e $x - 2$ appartengono all'ideale $(2x + 3,\ x^2 + x + 1)$ di $\mathbb{Z}[x]$.

(d) Descrivere l'anello quoziente $\mathbb{Z}[x]/(2x + 3,\ x^2 + x + 1)$.

Risposta a (d): $\mathbb{Z}[x]/(2x + 3,\ x^2 + x + 1)$ è isomorfo a $\mathbb{F}_7$.

Soluzione:

(a) $E = \pi \circ \mathrm{ev}_2$ è la composizione degli omomorfismi $\mathrm{ev}_2 : \mathbb{Z}[x] \to \mathbb{Z}$ di valutazione in $x = 2$ e della proiezione canonica $\pi : \mathbb{Z} \to \mathbb{F}_7$. Abbiamo visto a lezione che entrambi sono omomorfismi di anelli, e quindi E è un omomorfismo di anelli.

(b) È un semplice conto. Per $p = 2x + 3$, si ha $p(2) = 7$. Poiché $E(p)$ è la riduzione modulo 7 di $p(2)$, che fa $E(2x + 3) = \bar{0}$. Allo stesso modo, $q = x^2 + x + 1$ soddisfa $q(2) = 7$. Dunque $E(x^2 + x + 1) = E(q) = \overline{7} = \bar{0}$.

(c) Nell'ideale $(2x + 3, x^2 + x + 1)$ c'è sicuramente l'elemento

$$x(2x + 3) - 2(x^2 + x + 1) = 2x^2 + 3x - 2x^2 - 2x - 2 = x - 2.$$

Ma allora c'è anche

$$2x + 3 - 2(x - 2) = 2x + 3 - 2x + 4 = 7.$$

(d) Alla luce della domanda precedente, sappiamo già che

$$7,\ x - 2 \in (2x + 3,\ x^2 + x + 1) \implies (7,\ x - 2) \subseteq (2x + 3,\ x^2 + x + 1).$$

È lecito sospettare che l'inclusione sia un'uguaglianza. In effetti

$$2x + 3 = 2(x - 2) + 7, \qquad x^2 + x + 1 = (x + 3)(x - 2) + 7$$

e quindi $2x + 3,\ x^2 + x + 1 \in (7,\ x - 2)$. Da cui $(7,\ x - 2) = (2x + 3,\ x^2 + x + 1)$.

Dobbiamo quindi descrivere l'anello quoziente $\mathbb{Z}[x]/(7,\ x - 2)$. Abbiamo fatto questa cosa più volte negli scritti d'esame e sappiamo allora come procedere. Nello specifico:

$$\mathbb{Z}[x]/(2x + 3,\ x^2 + x + 1) = \mathbb{Z}[x]/(7, x - 2) \cong \mathbb{F}_7[x]/(x - 2) \cong \mathbb{F}_7.$$

Un modo indiretto, ma più efficace, di giungere alla stessa conclusione è quello di osservare che $(7,\ x - 2) \subset \ker E$ per (b) e (c). Tuttavia, ogni polinomio che calcolato in 2 assume un valore multiplo di 7 appartiene a $(7,\ x-2)$ e quindi $(7,\ x-2) = \ker E$. Ma allora il quoziente di cui stiamo parlando è $\mathbb{Z}[x]/\ker E$ che è isomorfo all'immagine di E per il teorema di omomorfismo. Questa immagine è appunto $\mathbb{F}_7$.

Esercizio 4. Sia V un modulo sull'anello $\mathbb{Q}[t]$ generato da due elementi v_1 e v_2 soggetti alle relazioni

$$\begin{aligned}(1-t^3)v_1 + tv_2 &= 0\,,\\ (1-t^3)v_2 &= 0\,.\end{aligned}$$

1. Mostrare che V è un modulo ciclico (ovvero generato da un solo elemento) e determinarne un generatore v_0.
2. Determinare un generatore dell'ideale $I \subset \mathbb{Q}[t]$ che consiste dei polinomi $p(t)$ tali che $p(t)v_0 = 0$.
3. Calcolare la dimensione di V come spazio vettoriale su $\mathbb{Q}$.
4. Fissare una base di V come spazio vettoriale su $\mathbb{Q}$ e scrivere la matrice dell'applicazione lineare $T : V \to V$ data da $T(v) = tv$.

Soluzione:

1. V è il quoziente del $\mathbb{Q}[t]$-modulo libero $\mathbb{Q}[t]^2$ quozientato per il sottomodulo generato dalle due relazioni date. Sappiamo come procedere: scriviamo nelle colonne di una matrice i due generatori e procediamo a *diagonalizzare* i generatori con manipolazioni per righe e per colonne. Esplicitamente:

$$\begin{pmatrix}1-t^3 & 0\\ t & 1-t^3\end{pmatrix} \rightsquigarrow \begin{pmatrix}t & 1-t^3\\ 1-t^3 & 0\end{pmatrix} \rightsquigarrow \begin{pmatrix}t & 1\\ 1-t^3 & t^2(1-t^3)\end{pmatrix} \rightsquigarrow \begin{pmatrix}1 & t\\ t^2(1-t^3) & 1-t^3\end{pmatrix} \rightsquigarrow \begin{pmatrix}1 & 0\\ 0 & (1-t^3)^2\end{pmatrix}.$$

   Nei vari passaggi ho prima scambiato le due righe per poi: sommare alla seconda colonna t^2 volte la prima; scambiare le due colonne; sottrarre alla seconda colonna t volte la prima. Ricordate che le manipolazioni per colonne non modificano il sottomodulo che si sta trattando, mentre quelle per righe applicano un automorfismo di $\mathbb{Q}[t]^2$. Nel caso in oggetto, ho scambiato v_1 e v_2 tra loro (scambiando le due righe) e quindi il sottomodulo iniziale V è generato da 1 volta v_2 e da $(1-t^3)^2$ volte v_1.

   Questi conti non sono strettamente necessari se ricordiamo che il coefficiente in prima posizione sulla diagonale è il MCD dei coefficienti della matrice iniziale, e che il determinante non cambia (o viene al più moltiplicato per un invertibile). Evitare i conti, però, non ci permette di sapere in quale $\mathbb{Q}[t]$-base sono poi espressi i generatori del sottomodulo.

   Ad ogni modo, abbiamo appena concluso che

$$V \simeq \mathbb{Q}[t]/(1) \oplus \mathbb{Q}[t]/((1-t^3)^2) \simeq \mathbb{Q}[t]/((1-t^3)^2),$$

   che è un $\mathbb{Q}[t]$-modulo ciclico. Avendo tenuto traccia dei generatori, sappiamo che è generato da v_1.

2. Abbiamo appena visto che $I = ((1-t^3)^2)$.
3. L'ideale I è generato da un polinomio di grado 6 e quindi $\dim_{\mathbb{Q}} V = 6$.
4. La cosa più semplice è scegliere la base $v_1, tv_1, t^2v_1, t^3v_1, t^4v_1, t^5v_1$. La moltiplicazione per t manda ciascun elemento nel successivo, e l'ultimo in t^6v_1. Ricordando che $(t^3-1)^2v_1 = 0$ e calcolando $(t^3-1)^2 = t^6 - 2t^3 + 1$, concludiamo che $T(t^5v_1) = 2t^3v_1 - v_1$. La matrice è allora

$$\begin{pmatrix}0 & 0 & 0 & 0 & 0 & -1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 2\\ 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0\end{pmatrix}.$$

Esercizio 5. Sia $\mathbb{F} \subset \mathbb{K}$ un'estensione algebrica di campi e sia R un anello contenente $\mathbb{F}$ e contenuto in $\mathbb{K}$. Dire se la seguente affermazione è vera (fornendo una dimostrazione) o falsa (fornendo un controesempio): R è un campo.

Risposta: l'affermazione è vera.

Soluzione: Questo esercizio era tra quelli assegnati nei fogli settimanali.

R è sicuramente un sottoanello del campo $\mathbb{K}$ e quindi un dominio d'integrità. Mostriamo che è effettivamente un campo facendo vedere che ogni suo elemento non nullo possiede un inverso in R.

Se $0 \neq a \in R \subset \mathbb{K}$, poiché $\mathbb{F} \subset \mathbb{K}$ è un'estensione algebrica, esisterà un polinomio non nullo $p \in \mathbb{F}[x]$ tale che $p(a) = 0$. Possiamo supporre che tale polinomio sia quello minimo, e quindi che sia irriducibile. Il suo termine noto è allora sicuramente diverso da 0. Se $p = f_n x^n + \cdots + f_1 x + f_0$ allora

$$0 = f_n a^n + \cdots + f_1 a + f_0 = a(f_n a^{n-1} + \cdots + f_1) + f_0,$$

da cui

$$a(f_n a^{n-1} + \cdots + f_1) = -f_0,$$

il che mostra che l'inverso di a è l'elemento

$$-f_0^{-1} \cdot (f_n a^{n-1} + \cdots + f_1)$$

che appartiene sicuramente ad R, visto che $a \in R$ e tutti gli f_i e f_0^{-1} stanno in $\mathbb{F} \subset R$.