Università degli studi di Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2004/2005
AL2 - Algebra 2, gruppi anelli e campi
Soluzioni
22 ottobre 2004

1 Gruppi e Quozienti

1. *Prodotto semidiretto* Sia G un gruppo, H e N sottogruppi con N normale. Sia γ_x la coniugazione per l'elemento $x \in G$.

   (a) Dimostrare che l'applicazione

   $$\begin{array}{rccc} f: & H & \mapsto & Aut(N) \\ & x & \mapsto & \gamma_x \end{array}$$

   è un omomorfismo.

   (b) Se $H \cap N = \{e\}$, dimostrare che la applicazione $H \times N \mapsto HN$ data da $(x, y) \mapsto xy$ è una biezione, e che questa applicazione è un isomorfismo se e solamente se f è triviale, i.e. $f(x) = id_N$ $\forall x \in H$.

   Diremo che G è il *prodotto semidiretto* di H e N, e scriviamo $G = N \times_f H$ se $G = HN$ e $H \cap N = \{e\}$.

   (c) Viceversa siano H e N due gruppi, e sia $\phi : H \mapsto Aut(N)$ un omomorfismo dato. Costruiamo il prodotto semidiretto nel modo seguente. Sia G l'insieme delle coppie (x, h) con $x \in N$ e $h \in H$, definiamo il prodotto nel modo seguente:

   $$(x, h)(y, k) = (x\phi(h)(y), hk)$$

   Dimostrare che questa è una legge di gruppo e che $G = N \times_\phi H$ identificando N con $(x, 1)$ e H con $(1, h)$

   (d) Verificare che $N \times_{id} H \cong N \times H$.

Soluzione 1.1. *(a) Dobbiamo verivicare che $f(xy) = f(x)f(y)$. Sia $g \in G$:*

$$\begin{aligned} f(xy)(g) &= \gamma_{xy}(g) = (xy)^{-1}g(xy) \\ &= x^{-1}(y^{-1}gy)x \\ &= \gamma_x \circ \gamma_y(g) \\ &= f(x) \circ f(y)(g) \end{aligned}$$

(b) Definiamo $\phi : H \times N \to HN$ nel modo seguente

$$\phi(h, n) = hn$$

Osserviamo che

$$\ker \phi = \{(h,n) : hn = e\}$$

Da cui $h = n^{-1} \in N$ *e* $n = h^{-1} \in H$, *quindi* h *e* $n \in H \cap N = \{e\}$, *dunque* $h = n = e$ *e* $\ker \phi = \{(e,e)\}$. *Vediamo che è suriettiva. Sia* $g \in HN$ *allora esistono* $h_0 \in H$ *e* $n_0 \in N$ *tali che* $g = h_0 n_0$, *allora* $\phi(h_0, n_0) = h_0 n_0 = g$. *Inoltre* ϕ *è un omomorfismo di gruppi se e solamente se* f *è banale. Infatti*

$$\phi(h,n)\phi(h',n') = hnh'n' = hh'h'^{-1}nh'n' = hh'\gamma_{h'}(n)n'$$

Mentre

$$\phi((h,n)(h'n')) = hh'nn'$$

Quindi ϕ *è un omomorfismo di gruppi se per ogni* $h \in H$ $\gamma_h \equiv id_N$.

(c) semplice verifica delle proprietà di gruppo.

(d) semplice verifica.

2. Dire quale dei seguenti gruppi è esprimibile come prodotto diretto o semidiretto di due sottogruppi:

   (a) $(\mathbb{Z}, +)$,

   (b) $(\mathbb{Z}_8, +)$,

   (c) $(D_4, \circ)$,

   (d) $(\mathbb{Z}_6, +)$,

   (e) $(\mathbb{C}, +)$,

   (f) $(\mathbb{C}^*, .)$.

   Soluzione 1.2. *(a)* $(\mathbb{Z}, +)$ *no,*

   (b) $(\mathbb{Z}_8, +)$ *no,*

   (c) $(D_4, \circ) \cong <\sigma> \times_\phi <\rho>$ *dove* ρ *è la rotazione di angolo* $\frac{\pi}{2}$, σ *è il ribaltamento orizontale e* ϕ *è l'omomorfismo da* $<\sigma>$ *a* $Aut(<\rho>)$ *tale che* $\phi(\sigma)(x) = \sigma x \sigma^{-1}$,

   (d) $(\mathbb{Z}_6, +) \cong <3> \times <2>$,

   (e) $(\mathbb{C}, +) \cong \mathbb{R} \times i\mathbb{R}$,

   (f) $(\mathbb{C}^*, \cdot) \cong \mathbb{R}^+ \times \{z \in \mathbb{C} : |z| = 1\}$.

3. Trovare tutte le immagini omomorfe a:

   (a) $\mathbb{Z}_6$

   (b) $\mathbb{Z}_8$

(c) $\mathbb{Z}_{14}$
(d) $\mathbb{Z}_{18}$
(e) $\mathbb{Z}$
(f) S_3
(g) S_4
(h) D_4
(i) H

Soluzione 1.3. *Per definizione K è un immagine omomorfa di G se esiste un omomorfismo $\phi : G \to K$ suriettivo. Dunque usando il teorema di omomorfismo si ha che $K \cong G/\ker\phi$. Dunque le immagini omomorfe di G sono G/H con H sottogruppo normale di G. Osserviamo che fra le immagini omomorfe ci sono sempre quelle banali $\{0\}$ e tutto il gruppo.*

(a) Le immagini omomorfe di $\mathbb{Z}_6$ non banali sono $\mathbb{Z}_2$ e $\mathbb{Z}_3$. Infatti $\mathbb{Z}_6$ ha due sottogruppi, necessariamente normali perché $\mathbb{Z}_6$ è un gruppo commutativo, $H_1 = \langle 2\rangle$ e $H_2 = \langle 3\rangle$. Allora i rispettivi gruppi quozienti sono:

i. $G/H_1 = \left\{\overline{0}, \overline{1}\right\}$ con $\overline{a} = \{a, a+2, a+4\}$
ii. $G/H_2 = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$ con $\overline{a} = \{a, a+3\}$

(b) Le immagini omomorfe di $\mathbb{Z}_8$ non banali sono $\mathbb{Z}_2$ e $\mathbb{Z}_4$.

(c) Le immagini omomorfe di $\mathbb{Z}_{14}$ non banali sono $\mathbb{Z}_2$ e $\mathbb{Z}_7$.

(d) Le immagini omomorfe di $\mathbb{Z}_{18}$ non banali sono $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_6$ e $\mathbb{Z}_9$.

(e) Le immagini omomorfe di $\mathbb{Z}$ non banali sono $\mathbb{Z}_n$ per ogni $n \in \mathbb{Z}$ positivo

(f) L'immagine omomorfa di S_3 non banale è $\mathbb{Z}_2$. Infatti sappiamo che S_3 ha un solo sottogruppo normale A_3, da cui l'unica immagine omomorfa è $S_3/A_3 = \left\{\overline{id}, \overline{(12)}\right\}$ con:

- $\overline{id} = \{id, (123), (132)\}$
- $\overline{(12)} = \{(12), (13), (23)\}$

(g) Le immagini omomorfe di S_4 sono $\mathbb{Z}_2$ e S_3

(h) Le immagini omomorfe di D_4 sono $\mathbb{Z}_2$ e V_4

(i) Le immagini omomorfe di H sono $\mathbb{Z}_2$ e V_4

4. Trovare i sottogruppi di $U(\mathbb{Z}_n)$ per $n = 6, 7, 15, 21$

Soluzione 1.4. *(a) $U(\mathbb{Z}_6) = \{1, 5\}$, dunque ha solo sottogruppi banali.*

(b) $U(\mathbb{Z}_7) = \{1,2,3,4,5,6\} \cong \mathbb{Z}_6$ *i sottogruppi non banali sono* $\{1,2,4\}$ *e* $\{1,6\}$

(c) $U(\mathbb{Z}_{15}) = \{1,2,4,7,8,11,13,14\} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$*, i sottogruppi non banali sono* $\{1,4\}$, $\{1,2,4,8\}$, $\{1,7,4,13\}$, $\{1,11\}$, $\{1,14\}$ *e* $\{1,4,11,14\}$

(d) $U(\mathbb{Z}_{21}) = \{1,2,4,5,8,10,11,13,16,17,19,20\} \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ *i sottogruppi non banali sono* $\{1,2,4,8,11,16\}$, $\{1,4,16\}$, $\{1,5,4,20,16,17\}$, $\{1,10,16,13,4,19\}$, $\{1,8\}$, $\{1,13\}$, $\{1,20\}$ *e* $\{1,8,13,20\}$

5. Descrivere i seguenti gruppi:

   (a) $(\mathbb{C}^\star, \cdot) \,/\, \{z \in \mathbb{C} : |z| = 1\}$

   (b) $(\mathbb{C}^\star, \cdot) \,/\, \{z \in \mathbb{C}^\star : z - \overline{z} = 0\}$

   (c) $(\mathbb{C}, +) \,/ \mathbb{Z} + i\mathbb{Z}$

   Soluzione 1.5. *Descriviamo solo gli elementi del gruppo quoziente*

   (a) $\overline{z} = \{\zeta \in \mathbb{C}^\star : |\zeta| = |z|\}$

   (b) $\overline{z} = \{\zeta \in \mathbb{C}^\star : Arg(\zeta) = \pm Arg(z)\}$

   (c) $\overline{z} = \{\zeta \in \mathbb{C}^\star : Re(\zeta) - Re(z) \in \mathbb{Z} \text{ e } Im(\zeta) - Im(z) \in \mathbb{Z}\}$

2 Gruppo Simmetrico

1. Per ogni divisore p, primo, di $Ord(S_4)$ trovare un elemento di ordine p.

   Soluzione 2.1. *I divisori prini di* $Ord(S_4)$ *sono 2 e 3.*

   (a) Ordine 2: (1,2).

   (b) Ordine 3: (1,2,3).

2. Per quali divisori n di $Ord(S_4)$ esiste un elemento di ordine n ?

   Soluzione 2.2. *I divisori di* $Ord(S_4)$ *sono 1, 2, 3, 4, 6 e 8.*

   (a) Ordine 1: identità.

   (b) Ordine 2: (1,2).

   (c) Ordine 3: (1,2,3).

   (d) Ordine 4: (1,2,3,4).

   (e) Ordine 6 e 8: non ci sono.

3. Verificare l'equazione delle classi per S_4 e S_3.

Soluzione 2.3. *L'equazione delle classi è*

$$Ord\,(G) = \sum \frac{Ord\,(G)}{Ord\,(C\,(a))}$$

dove la somma è estesa ad elementi $a \in G$, uno per ogni classe di coniugio.Nel caso di S_3 si ottiene.

$$\begin{aligned} 6 = Ord\,(S_3) &= \frac{Ord\,(S_3)}{Ord\,(C\,(id))} + \frac{Ord\,(S_3)}{Ord\,(C\,((1,2)))} + \frac{Ord\,(S_3)}{Ord\,(C\,((1,2,3)))} \\ &= \frac{6}{6} + \frac{6}{3} + \frac{6}{2} = 1 + 2 + 3. \end{aligned}$$

Analogamente per S_4.

4. Dimostrare che due qualsiasi sottogruppi di ordine 3 di S_4 sono coniugati.

Soluzione 2.4. *I sottogruppi di ordine 3 in S_4 sono:*

(a) $< (1,2,3) >$
(b) $< (1,2,4) >$
(c) $< (1,3,4) >$
(d) $< (2,3,4) >$.

Allora

(a) $< (1,2,4) >= (34) < (1,2,3) > (34)$
(b) $< (1,3,4) >= (23)(34) < (1,2,3) > (34)(23) = (234) < (1,2,3) > (243)$
(c) $< (2,3,4) >= (12)(23)(34) < (1,2,3) > (34)(23)(12) = (1234) < (1,2,3) > (1432)$.

Poichè il coniugio è una relazione di equivalenza abbiamo che due qualsiasi sottogruppi di ordine 3 sono coniugati.

3 Gruppo Diedrale

1. Consideriamo D_4 il gruppo dei movimenti rigidi del quadrato.
   (a) Trovare tutti i sottogruppi di D_4,
   (b) Trovare le classi di coniugio di D_4.

Soluzione 3.1. *(a) Sia ρ la rotazione di angolo $\pi/4$ e r la riflessione rispetto all'asse x. Allora*

$$D_4 = \left\{id, r, \rho, r\rho, r\rho^2, r\rho^3, \rho^2, \rho^3\right\}$$

I sottogruppi sono

$$\begin{aligned}
Z &= \left\{id, \rho, \rho^2, \rho^3\right\} \\
K_1 &= \left\{id, r, \rho^2, r\rho^2\right\} \\
K_2 &= \left\{id, r\rho, \rho^2, r\rho^3\right\} \\
R_1 &= \left\{id, \rho^2\right\} = Z\left(D_4\right) \\
R_2 &= \{id, r\} \\
R_3 &= \{id, r\rho\} \\
R_4 &= \left\{id, r\rho^2\right\} \\
R_3 &= \left\{id, r\rho^3\right\}
\end{aligned}$$

(b) Osserviamo che $\rho r = r\rho^3$. Le classi di coniugio sono

$$\begin{aligned}
C(r) &= \left\{r, r\rho^2\right\} \\
C(r\rho) &= \left\{r\rho, r\rho^3\right\} \\
C(\rho) &= \left\{\rho, \rho^3\right\} \\
C\left(\rho^2\right) &= \left\{\rho^2\right\}
\end{aligned}$$

2. Determinare il centro di D_n per ogni n.

   Soluzione 3.2. *(a) n dispari: $Z(D_n) = \{id\}$*

   (b) n pari: $Z(D_n) = \left\{id, \rho^{\frac{n}{2}}\right\}$ dove ρ è lo rotazione di angolo $\frac{2\pi}{n}$.

3. Determinare $N(D_4)$ in S_4.

   Soluzione 3.3. $N(D_4) = \langle (2,4), (1,2)(3,4), (1,4)(2,3)\rangle$.

4. Dimostrare che D_n è generato da una riflessione e da una rotazione.

   Soluzione 3.4. *Sia ρ la rotazione di angolo $2\pi/n$, sia $Z = \langle\rho\rangle$. Osserviamo che Z ha indice due, dunque è un sottogruppo normale, sia r_0 un elemento non congruo a ρ, in particolare r_0 ha ordine 2. Sia $x \in D_n$ abbiamo due possibilità:*

   (a) $x \mod Z = 1$, dunque $x = \rho^i$ per qualche i.

   (b) $x \mod Z = -1$ dunque $x = \rho^i r_0 \rho^i$ per qualche i

   Dunque D_n è generato da ρ e r_0.

5. Si dimostri che il gruppo dei movimenti di un rettangolo è il gruppo di Klein.

   Soluzione 3.5. *I movimenti del rettangolo sono dati da i ribaltamenti rispetto all'asse orizzontale, verticale, e la rotazione di angolo π. Ogni elemento ha ordine 2, da cui l'isomorfismo.*

4 Omomorfismi

Poniamo $\phi_h : \mathbb{Z}_n \to \mathbb{Z}_m$ l'omomorfismo tale che $\phi_h(1) = h \in \mathbb{Z}_m$

1. Trovare tutti gli omomorfismi fra $\mathbb{Z}_7$ e $\mathbb{Z}_{21}$

   Soluzione 4.1.

   (a) ϕ_0
   (b) ϕ_3
   (c) ϕ_6
   (d) ϕ_9
   (e) ϕ_{12}
   (f) ϕ_{15}
   (g) ϕ_{18}

2. Trovare tutti gli omomorfismi fra $\mathbb{Z}_{21}$ e $\mathbb{Z}_7$

   Soluzione 4.2.

   (a) ϕ_0
   (b) ϕ_1
   (c) ϕ_2
   (d) ϕ_3
   (e) ϕ_4
   (f) ϕ_5
   (g) ϕ_6

3. Trovare tutti gli omomorfismi fra $\mathbb{Z}$ e $\mathbb{Z}_{13}$

   Soluzione 4.3. *Per ogni $n \in \mathbb{Z}$ sia*

   $$\pi_n : \mathbb{Z} \to \mathbb{Z}_1 3$$

   definito da $\pi_n(m) = \overline{nm}$ Osserviamo che:

   - π_n *è un omomorfismo per ogni* $n \in \mathbb{Z}$

- $\pi_n = \pi_m \Leftrightarrow n \equiv m \mod 13$

Inoltre π_n *è l'omomorfismo nullo* $\Leftrightarrow n \in 13\mathbb{Z}$. *Se* $n \notin 13\mathbb{Z}$ *si ha*

- $\ker \pi_n = 13\mathbb{Z}$
- $\mathtt{Im}\ \pi_n = \mathbb{Z}_{13}$ *In totale abbiamo 13 omomorfismi diversi.*

4. Trovare tutti gli omomorfismi fra $\mathbb{Z}$ e $\mathbb{Z}_{22}$

   Soluzione 4.4. *Con le notazioni dell'esercizio 3 otteniamo* 22 *omomorfismi differenti tali che*

   - π_n *è l'omomorfismo nullo se* $n \in 22\mathbb{Z}$
   - $\ker \pi_n = 22\mathbb{Z}$ *e* $\mathtt{Im}\ \pi_n = Z_{22}$ *se* $n \mod 22 \in U(\mathbb{Z}_{22})$
   - $\ker \pi_n = 11\mathbb{Z}$ *e* $\mathtt{Im}\ \pi_n = 2Z_{22}$ *se* $n \mod 22 \in 2\mathbb{Z}_{22}$ *e* $n \notin 22\mathbb{Z}$
   - $\ker \pi_n = 2\mathbb{Z}$ *e* $\mathtt{Im}\ \pi_n = 11Z_{22}$ *se* $n \mod 22 \in 11\mathbb{Z}_{22}$ *e* $n \notin 22\mathbb{Z}$

5. Trovare tutti gli omomorfismi fra S_3 e $(\mathbb{Z}_6, +)$

   Soluzione 4.5. *Osserviamo che* S_3 *ha un solo sottogruppo normale, oltre a quelli banali,* A_3. *Dunque i possibili nuclei sono:*

   (a) $\{0\}$
   (b) A_3
   (c) S_3

   Essendo Z_6 *commutativo tutti i sottogruppi sono normali, quindi le possibili immagini sono:*

   (a) $\{0\}$
   (b) $\{0, 3\}$
   (c) $\{0, 2, 4\}$
   (d) Z_6

   Applicando il teorema di omomorfismo abbiamo le seguenti possibilità:

   - $\ker \phi_0 = S_3$ *e* $\mathtt{Im}\ \phi_0 = \{0\}$
   - $\ker \phi_1 = A_3$ *e* $\mathtt{Im}\ \phi_1 = \{0, 3\}$
   - $\ker \phi_2 = \{0\}$ *e* $\mathtt{Im}\ \phi_2 = \mathbb{Z}_6$

   ϕ_0 *è l'applicazione banale.* ϕ_1 *è l'omomorfismo che ad ogni permutazione pari associa* 0 *e ad ogni permutazione dispari associa* 3, *mentre* ϕ_2 *non è ben definita, infatti se* ϕ_2 *fosse ben definita allora avremmo un isomorfismo fra* S_3 *e* $\mathbb{Z}_6$ *il che non può essere essendo* $\mathbb{Z}_6$ *commutativo e* S_3 *non commutativo.*

6. Trovare tutti gli omomorfismi fra $(\mathbb{Z}_6, +)$ e S_3

   Soluzione 4.6. *Usando l'esercizio 5 otteniamo i seguenti omomorfismi*

   - $\ker \phi_0 = Z_6$ *e* `Im` $\phi_0 = \{0\}$
   - $\ker \phi_1 = \{0, 3\}$ *e* `Im` $\phi_1 = A_3$ *tale che* $\phi_1(2) = (123)$

7. Trovare tutti gli omomorfismi fra S_4 e $(\mathbb{Z}_{24}, +)$

   Soluzione 4.7. *Analogo all'esercizio 5*

8. Trovare tutti gli omomorfismi fra $(\mathbb{Z}_{24}, +)$ e S_4

   Soluzione 4.8. *Analogo all'esercizio 5*

9. Trovare tutti gli omomorfismi fra D_4 e $(\mathbb{Z}_8, +)$

   Soluzione 4.9. *Sappiamo dall'esercizio* 3 *1a quali sono i sottogruppi di* D_4*, è facile verificare che i sottogruppi normali sono* Z*,* K_1*,* K_2 *e* R_1*. Dal teorema di omomorfismo sappiamo che la cardinalità dell'immagine è* 2 *o* 4*. Dunque le possibili immagini, non banali, sono* $\{0, 4\}$ *o* $\{0, 2, 4, 6\}$*. Abbiamo le seguenti possibilità:*

   (a) $\ker \phi = D_4$ *e* `Im` $\phi = \{0\}$
   (b) $\ker \phi = K_1$ *e* `Im` $\phi = \{0, 4\}$
   (c) $\ker \phi = K_2$ *e* `Im` $\phi = \{0, 4\}$
   (d) $\ker \phi = Z$ *e* `Im` $\phi = \{0, 4\}$
   (e) $\ker \phi = R_1$ *e* `Im` $\phi = \{0, 2, 4, 6\}$
   (f) $\ker \phi = \{0\}$ *e* `Im` $\phi = \mathbb{Z}_8$

   Da cui possiamo costruire omomorfismi dai primi quattro, mentre da 9f non è possibile perchè D_4 *non è commutativo mentre* Z_8 *lo è. Infine 9e non è possibile perchè* D_4/R_1 *non è ciclico mentre* $\{0, 2, 4, 6\}$ *lo è.*

10. Trovare tutti gli omomorfismi fra $(\mathbb{Z}_8, +)$ e D_4

    Soluzione 4.10. *I possibili nuclei sono tutti i sottogruppi di* $\mathbb{Z}_8$*. Sappiamo dall'esercizio* 4.9 *che le possibili immagini sono* $\{0\}$*,* R_1*,* Z*,* K_1*,* K_2 *e* D_4*. Dunque abbiamo le seguenti combinazioni*

    (a) $\ker \phi = \mathbb{Z}_8$ *e* `Im` $\phi = \{0\}$
    (b) $\ker \phi = \{0, 4\}$ *e* `Im` $\phi = Z$
    (c) $\ker \phi = \{0, 4\}$ *e* `Im` $\phi = K_1$
    (d) $\ker \phi = \{0, 4\}$ *e* `Im` $\phi = K_2$

(e) $\ker \phi = \{0, 2, 4, 6\}$ e $\texttt{Im}\ \phi = R_1$

(f) $\ker \phi = \{0\}$ e $\texttt{Im}\ \phi = D_4$

Da cui possiamo costruire tre omomorfismi 10a, 10b e 10e.

11. Stabilire se i gruppi $\mathbb{Z}_3 \times \mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ sono isomorfi.

    Soluzione 4.11. *Se* $a = (a_1, a_2, a_3) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$*, allora* $3a = 0$*, per cui ogni elemento di* $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ *ha al massimo ordine 3. Invece* $(0, 1) \in \mathbb{Z}_3 \times \mathbb{Z}_9$ *ha ordine* 9*, per cui i gruppi* $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ *e* $\mathbb{Z}_3 \times \mathbb{Z}_9$ *non sono isomorfi.*

5 Automorfismi

1. Calcolare $Aut\,(V_4)$ e $Inn\,(V_4)$

   Soluzione 5.1.

   - $Aut\,(V_4) = S_3$
   - $Inn\,(V_4) = \{id\}$ *perchè il gruppo è commutativo*

2. Calcolare $Aut\,(\mathbb{Z})$

   Soluzione 5.2. $Aut\,(\mathbb{Z}) = \{1, -1\}$

3. Calcolare $Aut\,(\mathbb{Z}_5)$

   Soluzione 5.3. $Aut\,(\mathbb{Z}_5) = U\,(\mathbb{Z}_5)$ *vedere esercizio 7*

4. Calcolare $Aut\,(\mathbb{Z}_{13})$

   Soluzione 5.4. $Aut\,(\mathbb{Z}_{13}) = U\,(\mathbb{Z}_{13})$ *vedere esercizio 7*

5. Calcolare $Aut\,(\mathbb{Z}_8)$

   Soluzione 5.5. $Aut\,(\mathbb{Z}_8) = U\,(\mathbb{Z}_8)$ *vedere esercizio 7*

6. Calcolare $Aut\,(\mathbb{Z}_{21})$

   Soluzione 5.6. $Aut\,(\mathbb{Z}_{21}) = U\,(\mathbb{Z}_{21})$ *vedere esercizio 7*

7. Calcolare $Aut\,(\mathbb{Z}_n)$ e $Inn\,(\mathbb{Z}_n)$

   Soluzione 5.7.

- *$Aut(\mathbb{Z}_n) = U(\mathbb{Z}_n)$ Costruiamo l'isomorfismo nel modo seguente*

$$\phi : U(\mathbb{Z}_n) \to Aut(\mathbb{Z}_n)$$

  tale che $\phi(m) = f_m$ con

$$f_m : \mathbb{Z}_n \to \mathbb{Z}_n$$

  definito da $f_m(1) = m$.
  Verificare che
  - *f_m è un automorfismo*
  - *ϕ è un isomorfismo*
- *$Inn(\mathbb{Z}_n) = \{id\}$ perchè il gruppo è commutativo*

8. Calcolare $Aut(H)$ e $Inn(H)$

   Soluzione 5.8.

   (a) *$Aut(H) = S_3 \times V_4$. Osserviamo che un automorfismo α di H è determinato una volta noti i valori di α in i e j. Definiamo*

$$N = Inn(H) = \{id = \gamma_1 = \gamma_{-1}, \gamma_i = \gamma_{-i}, \gamma_j = \gamma_{-j}, \gamma_k = \gamma_{-k}\}$$

   dove $\gamma_n(g) = n^{-1}gn$, consideriamo l'insieme $I = \{i, j, k\}$ e S_I il gruppo simmetrico associato ad I. Definiamo

$$\sigma : S_I \to Aut(H)$$

   tale che $\sigma(s) = \gamma_s$ e

$$\gamma_s(i) = s(i) \text{ e } \gamma_s(j) = s(j)$$

   Poniamo

$$K = \mathtt{Im}\ (\sigma) = Out(H) \cong S_3$$

   Allora e facile vedere che $N \cap K = \{id\}$ e che $NK = Aut(H)$. Quindi $Aut(H) = N \times K$

   (b) *$Inn(H) = N = V_4$*

9. Verificare che

$$Inn(D_4) \cong D_4/Z(D_4) \cong V_4$$

   Soluzione 5.9. *Semplice verifica.*

6 Matrici e Numeri Complessi

1. Sia M l'insieme delle matrici 3×3 a valori 0 e 1 e tali che ciascuna riga e ciascuna colonna contiene esattamente un 1. Si dimostri che rispetto al prodotto righe per colonne M è un gruppo e che esso è isomorfo a S_3.

   Soluzione 6.1.

$$M = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}.$$

   Consideriamo $a = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *e* $b = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. *È facile verificare che a ha ordine 2, b ha ordine 3 e che a e b generano M. Per costrire l'isomorfismo ricordiamoci che* S_3 *è generato da* $(1, 2)$ *e* $(1, 2, 3)$. *Allora poniamo:* $\phi(a) = (1, 2)$ *e* $\phi(b) = (1, 2, 3)$.

2. Consideriamo l'insieme R delle matrici 2×2 della forma $\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$ per $\theta \in [0, 2\pi)$. Dimostrare che R è un gruppo rispetto al prodotto righe per colonne e che esso è isomorfo a $G = \{z \in \mathbb{C} : |z| = 1\}$

   Soluzione 6.2. *Ricordiamo le formule di addizione per il coseno e il seno.*

$$\begin{aligned} \cos(\alpha + \beta) &= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) \\ \sin(\alpha + \beta) &= \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta). \end{aligned}$$

   Allora

$$\begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} \cos(\beta) & \sin(\beta) \\ -\sin(\beta) & \cos(\beta) \end{pmatrix} =$$
$$= \begin{pmatrix} \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) & \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) \\ -(\sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)) & \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) \end{pmatrix}$$
$$= \begin{pmatrix} \cos(\alpha + \beta) & \sin(\alpha + \beta) \\ -\sin(\alpha + \beta) & \cos(\alpha + \beta) \end{pmatrix}$$

   Dunque R è un gruppo rispetto al prodotto righe per colonne. L'isomorfismo è dato da $\phi\left(\begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}\right) = \cos(\alpha) + i\sin(\alpha)$.

3. È vero che ogni numero complesso di modulo 1 è radice n-esima di 1 per qualche intero positivo n?

Soluzione 6.3. *No, infatti consideriamo* $z = e^{i\theta}$, *tale che* $z^n = 1$ *per qualche* n. *Allora:*

$$1 = e^{i0} = e^{n\theta}$$

Da cui:

$$\theta = \frac{2k\pi}{n} \text{ per qualche } n$$

Quindi

$$\frac{\theta}{\pi} \in \mathbb{Q}$$

Scegliamo $\theta_0 = r\pi$ *con* $r \in \mathbb{R} - \mathbb{Q}$. *Allora* $z_0 = e^{i\theta_0}$ *non è una radice* n*-esima dell'unità per ogni* n.