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

1 Operazioni

1. Dimostrare che qualunque sia l'insieme S, le applicazioni

$$\cap : (X, Y) \in P(S) \times P(S) \to X \cap Y \in P(S)$$

$$\cup : (X, Y) \in P(S) \times P(S) \to X \cup Y \in P(S)$$

sono delle operazioni in $P(S)$ associative, commutative. Inoltre verificare se $\cap$ è distributiva rispetto a $\cup$, o/e viceversa.

Soluzione 1.1. *Applicare la definizione. Notare che ciascuna delle operazioni $\cap$ e $\cup$ è distributiva rispetto all'altra.*

2. Determinare quali dei sistemi $(G, *)$ qui descritti sono gruppi. In caso negativo dire quali degli assiomi di gruppo non sono verificati.

- $G = \mathbb{Z}$ con $a * b = a - b$
- $G = \mathbb{N}$ con $a * b = ab$
- G = insieme dei numeri razionali con denominatore dispari, $a*b = a + b$
- $G = a_0, a_1, a_2, a_3, a_4, a_5, a_6$ con
  - $a_i * a_j = a_{i+j}$ se $i + j < 7$
  - $a_i * a_j = a_{i+j-7}$ se $i + j \geq 7$.

Soluzione 1.2. *(a) Non è un gruppo, manca l'associatività*

(b) Non è un gruppo, manca l'inverso

(c) É un gruppo

(d) É un gruppo.

3. Sia $M_2(\mathbb{R})$ l'insieme delle matrici 2×2 a valori reali con le seguenti operazioni: dati $a = (a_{ij})$ e $b = (b_{ij})$ si ha

(a) $a + b = (a_{ij} + b_{ij})$

(b) $a \cdot b = (a_{i1}b_{1j} + a_{i2}b_{2j})$

(c) $a \star b = a \cdot b - b \cdot a$

Verificare se

(a) $(M_2(\mathbb{R}), +)$ è un gruppo.

(b) $(M_2(\mathbb{R}), \cdot)$ è un gruppo.

(c) $(M_2(\mathbb{R}), \star)$ è un gruppo.

(d) $(M_2(\mathbb{R}), +, \cdot)$ è un anello.

(e) $(M_2(\mathbb{R}), +, \star)$ è un anello.

(f) $(M_2(\mathbb{R}), \star, \cdot)$ è un anello.

Soluzione 1.3. *La verifica che 3a e 3b sono gruppi è immediata. 3c non è un gruppo perch non verifica la propriet associativa, infatti si ha:*

$$(a \star b) \star c + (b \star c) \star a + (c \star a) \star b = 0$$

Per ogni a, b e c $\in M_2(\mathbb{R})$*. 3d è un anello, mentre 3e e 3f non lo sono, rispettivamente perch* $(M_2(\mathbb{R}), \star)$ *non è un gruppo e non è un semigruppo.*

2 Gruppi

1. Sia G un insieme non vuoto, chiuso rispetto a un prodotto che sia associativo e che soddisfi inoltre le seguenti condizioni:

   (a) Esiste un elemento e tale che $a * e = a$ per ogni $a \in G$

   (b) Dato $a \in G$ esiste un elemento $y(a) \in G$ tale che $a * y(a) = e$

   Dimostrare allora che G è un gruppo rispetto a questo prodotto.

   Soluzione 2.1. $y(a) = y(a) * e = y(a) * a * y(a) \Rightarrow y(a) * a = e$, *segue che* $e * a = a * y(a) * a = a$.

2. Supponiamo che G sia un insieme finito chiuso rispetto ad un prodotto associativo, e che valgano entrambe le leggi di cancellazione. Dimostrare che G è un gruppo.

   Soluzione 2.2. *Le regole di cancellazione ci dicono che*

$$ab = ac \Rightarrow b = c \tag{1}$$
$$ba = ca \Rightarrow b = c \tag{2}$$

   Dobbiamo dimostrare che esiste l'elemento neutro e l'inverso. Per dimostrare che esiste l'elemento nutro fissiamo un elemento a di G e cerchiamo un elemento $e \in G$ *tale che* $e * a = a * e = a$*. Allora se esiste un tale elemento abbiamo che:*

$$(b * e) * a = b * (e * a) = b * a \Rightarrow b * e = b \tag{3}$$
$$a * (e * b) = (a * e) * b = a * b \Rightarrow e * b = b \tag{4}$$

Ricordiamoci che G è finito e chiuso, dunque dato a esistono due naturali n e m, $n \geq m$, tali che $a^n = a^m$, poniamo allora $e = a^{n-m}$ (si pu fare perch cancelliamo a m volte). E' facile verificare che $ea = ae = a$ Rimane da vedere che esiste l'inverso. Consideriamo $b * x$ al variare di $x \in G$, poich G è finito esiste $x_0 \in G$ tale che $b * x_0 = e$, ne segue che $x_0 = b^{-1}$.

3. Usando il risultato dell'esercizio 2 dimostrare che:

   (a) gli interi modulo p primo, diversi da 0, sono un gruppo rispetto alla moltiplicazione modulo p

   (b) gli interi coprimi con n sono un gruppo rispetto alla moltiplicazione modulo n.

   Soluzione 2.3. *Semplice verifica*

4. Calcolare tutti i sottogruppi di $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_{15}$ e $\mathbb{Z}_{21}$.

   Soluzione 2.4. *Applicando la definizione di sottogruppo si ottine che*

   - $\mathbb{Z}_3$ *non ha sottogruppi non banali*
   - $\mathbb{Z}_4$ *ha un solo sottogruppo* $\{\overline{0}, \overline{2}\}$
   - $\mathbb{Z}_{15}$ *ha due sottogruppi*
     (a) $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$
     (b) $\{\overline{0}, \overline{5}, \overline{10}\}$
   - $\mathbb{Z}_{21}$ *ha due sottogruppi*
     (a) $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}\}$
     (b) $\{\overline{0}, \overline{7}, \overline{14}\}$

5. Trovare l'intersezione dei sottogruppi $3\mathbb{Z}$ e $7\mathbb{Z}$ in $(\mathbb{Z}, +)$.

   Soluzione 2.5. *Ricordiamo che*

   $$m\mathbb{Z} = \{n \in \mathbb{Z} : m|n\}$$

   Allora è facile vedere che

   $$3\mathbb{Z} \cap 7\mathbb{Z} = \{n \in \mathbb{Z} : 3|n \ e \ 7|n\} = mcm(3, 7)\mathbb{Z} = 21\mathbb{Z}$$

6. Consideriamo $\mathbb{Z}_n$ con le usuali operazioni, determinare se i seguenti elementi sono zero divisori o invertibili

   (a) Per $n = 7$, $\overline{2}, \overline{3}, \overline{5}, \overline{7}$

   (b) Per $n = 13$, $\overline{4}, \overline{7}, \overline{9}, \overline{12}$

(c) Per $n = 15$, $\overline{3}, \overline{4}, \overline{9}, \overline{13}$

(d) Per $n = 21$, $\overline{4}, \overline{7}, \overline{12}, \overline{15}$

(e) Per $n = 51$, $\overline{2}, \overline{12}, \overline{17}, \overline{31}$

Soluzione 2.6. *Sia* $\overline{m} \in \mathbb{Z}_n$ *allora*

- $\overline{m}$ *è invertibile* $\Leftrightarrow mcd(m,n) = 1$
- $\overline{m}$ *è uno zero divisore* $\Leftrightarrow m = nk$ *per qualche* $k \in \mathbb{Z}$

infatti, supponiamo $\overline{m}$ *invertibile allora esiste* $\overline{m'} \in \mathbb{Z}_n$ *tale che*

$$\overline{1} = \overline{m}\overline{m'} = \overline{mm'}$$

Dunque applicando la definizione di classe modulo n otteniamo che

$$m \text{ è invertibile } \Leftrightarrow \exists m' \in \mathbb{Z} : mm' \equiv 1 \mod n \Leftrightarrow mcd(m,n) = 1$$

Analogamente si ottiene la condizione sugli zero divisori.

Applicando questi risultati si ottiene che:

(a) Per $n = 7$*,* $\overline{2}, \overline{3}, \overline{5}$ *sono invertibili, perch* 7 *è primo, mentre* $\overline{7} = \overline{0}$ *non lo è.*

(b) Per $n = 13$*,* $\overline{4}, \overline{7}, \overline{9}, \overline{12}$ *sono invertibili, perch* 13 *è primo.*

(c) Per $n = 15$*,* $\overline{3}$ *e* $\overline{9}$ *sono zero divisori infatti* $3 \times 5 = 15$ *e* $9 \times 5 = 3 \times 15$*,mentre* $\overline{4}, \overline{13}$ *sono invertibili.*

(d) Per $n = 21$*,* $\overline{7}, \overline{12}, \overline{15}$ *sono zero divisori, mentre* $\overline{4}$ *è invertibile.*

(e) Per $n = 51$*,* $\overline{12}, \overline{17}$ *sono zero divisori, mentre* $\overline{2}, \overline{31}$ *sono invertibili.*

7. Trovare il gruppo delle unità di $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_7$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{27}$, $\mathbb{Z}_{51}$.

Soluzione 2.7. *Ricordiamo che*

$$U(\mathbb{Z}_n) = \{\overline{m} \in \mathbb{Z}_n : mcd(m,n) = 1\}$$

Cioè l'insieme degli elementi invertibili di $\mathbb{Z}_n$ *Si ha che*

- $U(\mathbb{Z}_3) = \{\overline{1}, \overline{2}\}$
- $U(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$
- $U(\mathbb{Z}_7) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$
- $U(\mathbb{Z}_{15}) = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$
- $U(\mathbb{Z}_{27}) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{14}, \overline{16}, \overline{17}, \overline{19}, \overline{20}, \overline{22}, \overline{23}, \overline{25}, \overline{26}\}$

3 Gruppo Simmetrico

1. Calcolare tutti i sottogruppi di S_3.

   Soluzione 3.1. *Osserviamo che*

   $$S_3 = \{id, (12), (13), (23), (123), (132)\}$$

   Allora vediamo che ci sono tre sottogruppi di ordine 2

   $$\{id, (12)\}$$
   $$\{id, (13)\}$$
   $$\{id, (23)\}$$

   e un sottogruppo di ordine 3

   $$\{id, (123), (132)\}$$

2. Determinare le orbite e i cicli delle seguenti permutazioni:

   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$

   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$.

   Soluzione 3.2. *(a) Sia* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$, *allora:*

   $$\begin{aligned} \mathrm{O}_\sigma(1) &= \{1, 2, 3, 4, 5\} \\ \mathrm{O}_\sigma(2) &= \{2, 3, 4, 5, 1\} \\ \mathrm{O}_\sigma(3) &= \{3, 4, 5, 1, 2\} \\ \mathrm{O}_\sigma(4) &= \{4, 5, 3, 4, 5\} \\ \mathrm{O}_\sigma(5) &= \{5, 1, 2, 3, 4\} \\ \mathrm{O}_\sigma(6) &= \{6\} \\ \mathrm{O}_\sigma(7) &= \{7\} \\ \mathrm{O}_\sigma(8) &= \{8, 9\} \\ \mathrm{O}_\sigma(9) &= \{9, 8\} \end{aligned}$$

   (b) Sia $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$, *allora:*

   $$\begin{aligned} \mathrm{O}_\sigma(1) &= \{1, 6, 2, 5\} \\ \mathrm{O}_\sigma(2) &= \{2, 5, 1, 6\} \\ \mathrm{O}_\sigma(3) &= \{3, 4\} \\ \mathrm{O}_\sigma(4) &= \{4, 3\} \\ \mathrm{O}_\sigma(5) &= \{5, 1, 6, 2\} \\ \mathrm{O}_\sigma(6) &= \{6, 2, 5, 1\} \end{aligned}$$

3. Scrivere le permutazioni del problema 2 come prodotto di cicli disgiunti.

   Soluzione 3.3. *(a) (12345)(89)*

   (b) (1625)(34)

4. Dimostrare che il più piccolo sottogruppo di S_n che contiene (1 2) e (1 2 ... n) è S_n.

   Soluzione 3.4. *Sappiamo dalla teoria che ogni elemento di S_n è prodotto di trasposizioni, dunque ci basta verificare che (1 2) e (1 2 ... n) generano tutte le trasposizioni. Osserviamo che*

   $$(1...n)^{-1} = (n...1)$$

   Allora

   $$(i\, i+1) = (1...n)^{i-1} \circ (12) \circ (n...1)^{i-1}$$

   che possiamo riscrivere nel modo seguente

   $$(i\, i+1) = (1...n) \circ (i-1\, i) \circ (n...1)$$

5. Determinare tutti i sottogruppi di Klein di S_3 e S_4.

   Soluzione 3.5. *Ricordiamo che $K = \{id, a, b, c\}$ si dice gruppo di Klein se l'operazione definita su K è associativa e verifica:*

   - $a^2 = b^2 = c^2 = 1$
   - $ab = c$

   Grazie all'esercizio 3.1 sappiamo che S_3 non ha un sottogruppi di Klein. Per trovare i sottogruppi di Klein di S_4, cerchiamo per prima cosa tutti gli elementi di ordine 2.

   (a) (12)

   (b) (13)

   (c) (14)

   (d) (23)

   (e) (24)

   (f) (34)

   (g) (12)(34)

   (h) (13)(24)

   (i) (14)(23)

Vediamo subito che possiamo formare 3 *sottogruppi di Klein*

$$\{id, (12), (34), (12)(34)\}$$
$$\{id, (13), (24), (13)(24)\}$$
$$\{id, (14), (23), (14)(23)\}$$

Questi sono gli unici sottogruppi di Klein di S_4*.*

6. In S_5 trovare una permutazione per ogni struttura ciclica seguente:

   (a) (-)

   (b) (- -)(- -)

   (c) (- -)

   (d) (- -)(- - -)

   (e) (- - -)

   (f) (- - - -)

   (g) (- - - - -)

   Soluzione 3.6. *(a) id*

   (b) (12)(23)

   (c) (12)

   (d) (12)(123)

   (e) (123)

   (f) (1234)

   (g) (12345)

7. Trovare un elemento di ordine 2, 3 e 4 in S_4.

   Soluzione 3.7. (12)*,* (123)*,* (1234) *hanno rispettivamente ordine* 2*,* 3 *e* 4*.*

4 Numeri complessi

1. *Notazione Trigonometrica:* Dato un numero complesso $z = a + ib$, dimostrare che esistono $\rho \in \mathbb{R}^+$ e $\theta \in [0, 2\pi)$ tali che

$$z = \rho(\cos(\theta) + i\sin(\theta))$$

   Inoltre se $z \neq 0$, ρ e θ sono unici.

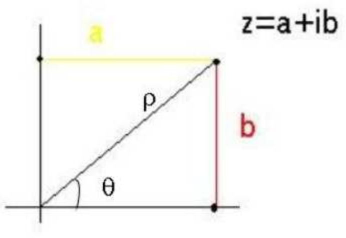

Figura 1: rappresentazione nel piano di un numero complesso.

Soluzione 4.1. *Definiamo:*

$$\begin{aligned}\rho &= \sqrt{z\overline{z}} = |z| = \sqrt{x^2+y^2} \\ \theta &= \arctan\left(\frac{b}{a}\right)\end{aligned}$$

Allora è facile vedere che (usare la figura 4.1 per aiutarsi):

$$\begin{aligned}a &= \rho\cos(\theta) \\ b &= \rho\sin(\theta)\end{aligned}$$

da cui la furmula cercata. Per dimostrare l'unicit, supponiamo che:

$$z = \rho(\cos(\theta) + i\sin(\theta)) = \tau(\cos(\phi) + i\sin(\phi))$$

Allora

$$\tau = |z| = \rho$$

Sostituendo nell'uguaglianza precedente otteniamo

$$\begin{aligned}\cos(\phi) = \cos(\theta) \\ \sin(\phi) = \sin(\theta)\end{aligned}$$

Dunque

$$\phi = \theta + 2k\pi$$

con $k \in \mathbb{Z}$, poich θ e $\phi \in [0, 2\pi)$ si ha

$$\phi = \theta.$$

2. *Notazione Esponenziale:* Dato $\theta \in \mathbb{R}$ definiamo

$$e^{i\theta} := \cos\theta + i\sin\theta$$

Dimostrare che per ogni α e β

(a) $e^{i\alpha} \cdot e^{i\beta} = e^{i\alpha+\beta}$

(b) $e^{i(\alpha+2k\pi)} = e^{i\alpha}$

Inoltre ogni numero complesso z si pu scrivere nella forma

$$z = \rho e^{i\theta}$$

con $\rho \in \mathbb{R}^+$ e $\theta \in [0, 2\pi)$

Soluzione 4.2. *Ricordiamo che*

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

e che

$$\cos(\alpha + 2k\pi) = \cos\alpha$$
$$\sin(\alpha + 2k\pi) = \sin\alpha$$

Cominciamo dalla 2a:

$$\begin{aligned}e^{i\alpha} \cdot e^{i\beta} &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= \cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\ &= e^{i(\alpha+\beta)}\end{aligned}$$

Mentre per la 2b si ha

$$\begin{aligned}e^{i(\alpha+2k\pi)} &= \cos(\alpha+2k\pi) + i\sin(\alpha+2k\pi) \\ &= \cos(\alpha) + i\sin(\alpha) \\ &= e^{i\alpha}\end{aligned}$$

Inoltre sappiamo dall'esercizio 4.1 che

$$z = \rho(\cos\alpha + i\sin\alpha)$$

da cui

$$z = \rho e^{i\alpha}$$

3. *Radici dell'unità* $z \in \mathbb{C}$ si dice radice n-esima dell'unità se esiste $n \in \mathbb{N}$ tale che:

$$z^n - 1 = 0$$

Fissato n dimostrare che:

(a) Ogni radice n-esima dell'unità è della forma $z = e^{i\frac{2k\pi}{n}}$ per $k = 0, 1 \ldots n-1$

(b) L'insieme delle radici n-esime dell'unità forma un gruppo di ordine n.

Una radice n-esima dell'unità si dice *primitiva* se genera il gruppo delle radici n-esime dell'unità. Dimostrare che $z = e^{i\frac{2k\pi}{n}}$ è primitiva se e solamente se $mcd\,(k, n) = 1$.

Soluzione 4.3. *Scriviamo*

$$z = \rho e^{i\theta}$$

e

$$1 = 1 \cdot e^{i \cdot 0}$$

Allora $z^n - 1 = 0$ *diventa:*

$$1 \cdot e^{i \cdot 0} = \left(\rho e^{i\theta}\right)^n = \rho^n \left(e^{i\theta}\right)^n = \rho^n e^{in\theta}$$

Per l'unicit dimostrata nell'esercizio 4.1 si ha

$$\begin{aligned} \rho^n &= 1 \\ n\theta &= 0 + 2k\pi \end{aligned}$$

Da cui

$$\begin{aligned} \rho &= 1 \\ \theta &= \frac{2k\pi}{n} \end{aligned}$$

Osserviamo che $\frac{2k\pi}{n} \in [0, 2\pi) \Leftrightarrow k = 0 \ldots n-1$. *Quindi*

$$z^n - 1 = 0 \Leftrightarrow z = e^{i\frac{2k\pi}{n}} \text{ con } k = 0 \ldots n-1$$

Consideriamo $z = e^{i\frac{2k\pi}{n}}$ *e* $z' = e^{i\frac{2k'\pi}{n}}$ *radici n-esime dell'unità, allora usando l'esercizio 4.2 si ha*

$$zz' = e^{i\frac{2k\pi}{n}} e^{i\frac{2k'\pi}{n}} = e^{i\frac{2(k+k')\pi}{n}}$$

Dunque zz' *è una radice n-esima dell'unità e l'insieme delle radici n-esime dell'unità forma un gruppo rispetto all'operazione indotta dalla moltiplicazione dei numeri complessi. Ricordiamo che* $z = e^{i\frac{2k\pi}{n}}$ *è un generatore del gruppo delle radici n-esime delle unità se per ogni* $z' = e^{i\frac{2k'\pi}{n}}$ *radice n-esima dell'unità esiste* $m \in \mathbb{Z}$ *tale che*

$$z' = e^{i\frac{2k'\pi}{n}} = z^m = e^{i\frac{2mk\pi}{n}}$$

Da cui per l'unicit della scrittura otteniamo

$$\frac{2k'\pi}{n} = \frac{2mk\pi}{n} + 2t\pi$$

Con $t \in \mathbb{Z}$. *Semplificando otteniamo:*

$$k' = mk + tn$$

Cioè l'equazione seguente

$$km \equiv k' \mod (n)$$

deve avere soluzione per ogni k' *con* k *fissato, dunque* $mcd(k, n) = 1$.
Per il viceversa si seguono le implicazioni a ritroso.