Università degli studi di Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2003/2004
AL2 - Algebra 2, gruppi anelli e campi
Soluzioni
3 ottobre 2004

1 Definizione di gruppo

1. 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 1.1. *(a) Non è un gruppo, manca l'associatività*
   (b) Non è un gruppo, manca l'inverso
   (c) É un gruppo
   (d) É un gruppo.

2. Se G è un gruppo nel quale $(ab)^2 = a^2b^2$ per ogni $a, b \in G$ allora G è abeliano.

   Soluzione 1.2. $abab = aabb \Rightarrow ba = ab$.

3. Se G è un gruppo nel quale $(ab)^i = a^ib^i$ per tre interi i consecutivi e per ogni $a, b \in G$, allora G è abeliano.

   Soluzione 1.3. *Abbiamo che*

$$\underbrace{ab\cdots ab}_{i-1} = \underbrace{a\cdots a}_{i-1}\underbrace{b\cdots b}_{i-1} \tag{1}$$

$$\underbrace{ab\cdots ab}_{i} = \underbrace{a\cdots a}_{i}\underbrace{b\cdots b}_{i} \tag{2}$$

$$\underbrace{ab\cdots ab}_{i+1} = \underbrace{a\cdots a}_{i+1}\underbrace{b\cdots b}_{i+1} \tag{3}$$

Da 1 e 2 otteniamo che $ab^{i-1} = b^{i-1}a$*, usando quest'ultima nella 3 otteniamo che* $a^{i+1}b^{i+1} = (ab)^{i+1} = a^ib^iab = a^ibab^i \Rightarrow ab = ba$.

4. Se G è un gruppo finito, dimostrare che esiste un intero N tale che $a^N = e$.

   Soluzione 1.4. *Consideriamo $A = \langle a \rangle$ sottogruppo ciclico generato da a, per assurdo non esista N tale che $a^N = e$, allora $|A| = \infty \Rightarrow |G| = \infty$ assurdo.*

5. Se G è un guppo di ordine pari, dimostrare che in G esiste un elemento $a \neq e$ tale che $a^2 = e$.

   Soluzione 1.5. *Consideriamo le coppie (a, a^{-1}) con $a \in G \setminus \{e\}$. Per assurdo $a \neq a^{-1}$ per ogni $a \in G \setminus \{e\} \Rightarrow |G|$ è dispari, assurdo.*

6. 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 1.6. $y(a) = y(a) * e = y(a) * a * y(a) \Rightarrow y(a) * a = e$, *segue che* $e * a = a * y(a) * a = a$.

7. 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 1.7. *Le regole di cancellazione ci dicono che*

$$ab = ac \Rightarrow b = c \tag{4}$$
$$ba = ca \Rightarrow b = c \tag{5}$$

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:

$$(b * e) * a = b * (e * a) = b * a \Rightarrow b * e = b \tag{6}$$
$$a * (e * b) = (a * e) * b = a * b \Rightarrow e * b = b \tag{7}$$

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 può fare perché cancelliamo a m volte). E' facile verificare che $ea = ae = a$ Rimane da vedere che esiste l'inverso. Consideriamo $b * x$ al variare di $x \in G$, poiché G è finito esiste $x_0 \in G$ tale che $b * x_0 = e$, ne segue che $x_0 = b^{-1}$.

8. Usando il risultato dell'esercizio 7 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 1.8. *Semplice verifica*

9. Si provi che un gruppo non abeliano non è mai ciclico.

   Soluzione 1.9. *Si provi che ogni gruppo ciclico è abeliano*

2 Sottogruppi

1. Quali sono le condizioni perché un sottoinsieme di un gruppo sia un sottogruppo.

   Soluzione 2.1. *Vedere libro di testo p.207 definizione 5.1.7*

2. Se H e K sono sottogruppi di G allora HK è un sottogruppo di G se e solo se $HK = KH$.

   Soluzione 2.2. *Supponiamo* $HK = KH$

   Dato $x \in HK$ *esistono* $h, h' \in H$ *e* $k, k' \in K$ *tali che* $x = hk = k'h'$
   Siano $x\, e\, y \in HK$*. Dobbiamo verificare che:*

   (a) $xy \in HK$

   (b) $x^{-1} \in HK$

   Consideriamo

   $$xy = h_x k_x h_y k_y = h_x h' k' k_y \in HK \tag{8}$$
   $$x^{-1} = (h_x k_x)^{-1} = k_x^{-1} h_x^{-1} \in KH = HK. \tag{9}$$

   Da cui HK è un gruppo.

   Viceversa supponiamo che HK sia un gruppo. Consideriamo $h \in H$ *e* $k \in K$*.*

   $$(hk)^{-1} \in HK \tag{10}$$
   $$(hk)^{-1} = k^{-1}h^{-1} \in KH \tag{11}$$

   Da cui $HK = KH$

3. Siano H e K due sottogruppi finiti di G, sia $|HK|$ la cardinalità di HK come insieme allora
$$|HK| = \frac{Ord(H)Ord(K)}{Ord(H\bigcap K)}. \tag{12}$$

Soluzione 2.3. *Per semplicità supponiamo che $Ord(H\bigcap K) = 1$, i.e. $H\bigcap K = \{e\}$. Dobbiamo dimostrare che $|HK| = Ord(H)Ord(K)$.*

Procediamo per assurdo. Supponiamo che esistano $h, h' \in H$ e $k, k' \in K$ distinti tali che $hk = h'k'$
$$hk = h'k' \tag{13}$$
$$h'^{-1}h = k'k^{-1} \tag{14}$$

Dunque $h'^{-1}h \in H\bigcap K$ e $k'k^{-1} \in H\bigcap K$ ne segue che $h = h'$ e $k = k'$ Per fare il caso generale dobbiamo dimostrare che 'hk compare in HK $Ord(H\bigcap K)$ volte'. Vediamo che compare almeno $Ord(H\bigcap K)$ volte: Sia $t \in H\bigcap K$ allora
$$hk = (ht)(t^{-1}k) \tag{15}$$
$$ht \in H\ t^{-1}k \in K. \tag{16}$$

Viceversa, supponiamo che $hk = h'k'$ allora $u = h'^{-1}h = k'k^{-1} \in H\bigcap K$ e $h = h'u$ e $k = u^{-1}k'$, da cui hk può apparire al più $Ord(H\bigcap K)$ volte.

4. Sia H un sottogruppo di G, sia $aHa^{-1} = \{aha^{-1} : h \in H\}$, dimostrare che aHa^{-1} è un sottogruppo di G. Se G è finito calcolare $Ord(aHa^{-1})$.

Soluzione 2.4. *Usiamo la seguente caratterizzazione di un sottogruppo: H è un sottogruppo $\Leftrightarrow \forall x, y \in H\ xy^{-1} \in H$. Allora $x = aha^{-1}$ e $y = aka^{-1}$, dunque $xy^{-1} = ahk^{-1}a^{-1} \in H$.*

Vediamo che $Ord(aHa^{-1}) = Ord(H)$. Sicuramente $Ord(aHa^{-1}) \leq Ord(H)$. Vediamo che vale il viceversa. Supponiamo che $aha^{-1} = aka^{-1}$ allora le proprietà di cancellazione ci dicono che $h = k$, dunque $Ord(aHa^{-1}) \geq Ord(H)$.

5. Scrivere esplicitamente le classi laterali destre di H in G dove:
   (a) $G = (a)$ è un gruppo ciclico di ordine 10 e $H = (a^2)$
   (b) G come sopra e $H = (a^5)$.

Soluzione 2.5. *(a) Le classi laterali destre sono*
$$\begin{aligned} H &= \{1, a^2, a^4, a^6, a^8\} = Ha^2 = Ha^4 = Ha^6 = Ha^8 \\ Ha &= \{a, a^3, a^5, a^7, a^9\} = Ha^3 = Ha^5 = Ha^7 = Ha^9 \end{aligned}$$

(b) Le classi laterali destre sono

$$\begin{aligned} H &= \{1, a^5\} = Ha^5 \\ Ha &= \{a, a^6\} = Ha^6 \\ Ha^2 &= \{a^2, a^7\} = Ha^7 \\ Ha^3 &= \{a^3, a^8\} = Ha^8 \\ Ha^4 &= \{a^4, a^9\} = Ha^9 \end{aligned}$$

6. Sia $a \in G$, definiamo $C(a) = \{x \in G : xa = ax\}$. Dimostrare che C(a) è un sottogruppo di G. C(a) si chiama il centralizzante di a in G.

   Soluzione 2.6. *Osserviamo che* $e \in C(a)$*. Verifichiamo che* $C(a)$ *è chiuso rispetto al prodotto e all'inversione Siano* $x, y \in C(a)$ *allora* $xya = x(ay) = axy$ *dunque* $xy \in C(a)$*. Sappiamo che* $xa = ax$*, dunque*

$$a = x^{-1}ax \tag{17}$$

$$ax^{-1} = x^{-1}a. \tag{18}$$

7. Sia H un sottogruppo di G, definiamo $C(H) = \{x \in G : xh = hx \, \forall h \in H\}$. Dimostrare che C(H) è un sottogruppo di G.

   Soluzione 2.7. *Come in soluzione 2.6. Osserviamo che* $C(G)$ *coincide con il centro di* G

8. Sia H un sottogruppo di G, definiamo $N(H) = \{x \in G : xHx^{-1} = H\}$. Dimostrare che N(H) è un sottogruppo di G e che $N(H) \supseteq H$.

   Soluzione 2.8. *Osserviamo che* $e \in N(H)$*. Verifichiamo la chiusura rispetto al prodotto e all'inversa. Siano* x, $y \in N(H)$ *allora*

$$\begin{aligned} xyHy^{-1}x^{-1} &= xHx^{-1} \text{ perché } yHy^{-1} = H \\ &= H \text{ perché } xHx^{-1} = H \end{aligned}$$

   La chiusura rispetto all'inverso è ovvia, infatti sappiamo che $yHy^{-1} = H \Rightarrow H = y^{-1}Hy$.

3 Gruppo Simmetrico

1. Calcolare tutti i sottogruppi di S_3.

   Soluzione 3.1. *Usiamo il teorema di Lagrange.* $|S_3| = 6$*, dunque ci possono essere solo sottogruppi di ordine 2,3. I sottogruppi di ordine 2 sono della forma* $\langle id, p\rangle$ *con* p *permutazione, mentre c'è un solo sottogruppo di ordine 3 dato da* $\langle id, (123), (132)\rangle = A_3$.

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:*

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

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

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

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

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