Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2003/2004
AL2 - Algebra 2, gruppi, anelli e campi
Tutorato - Soluzioni
30 settembre 2003

1. Siano $(G, \star)$ un gruppo e a, b suoi elementi. Provare che $(a \star b)^{-1} = a^{-1} \star b^{-1}$ se e solo se $a \star b = b \star a$.

$a \star b = b \star a \Rightarrow (a \star b)^{-1} = (b \star a)^{-1} = a^{-1} \star b^{-1}$
$a^{-1} \star b^{-1} = (a \star b)^{-1} \Rightarrow (a^{-1} \star b^{-1})^{-1} = a \star b \Rightarrow b \star a = a \star b$

2. Provare che se G è un gruppo con elemento neutro e e tale che $x \star x = e$ per ogni $x \in G$, allora G è abeliano.

$(a \star b) \star (a \star b) = e = a \star a = a \star e \star a = a \star (b \star b) \star a = (a \star b) \star (b \star a) \Rightarrow (a \star b) = (b \star a)$ per la legge di cancellazione destra.

3. Scrivere almeno 4 elementi per ciascuno dei seguenti gruppi ciclici:

1. $18\mathbb{Z}$ rispetto all'addizione;
2. $\{(\frac{1}{3})^n \mid n \in \mathbb{Z}\}$ rispetto alla moltiplicazione;
3. $\{\pi^n \mid n \in \mathbb{Z}\}$ rispetto alla moltiplicazione.

1. $0, 18, -18, 180$
2. $\frac{1}{3}, 3, 1, 9$
3. $1, \pi, \frac{1}{\pi}, \pi^2$

4. Trovare l'ordine del sottogruppo ciclico del dato gruppo generato dall'elemento indicato:

1. il sottogruppo di $\mathbb{Z}_{18}$ generato da $[3]_{18}$;
2. il sottogruppo di $\mathcal{C}_8$ generato da $\cos\frac{3\pi}{2} + i \sin\frac{3\pi}{2}$;

Sia G un gruppo con el. neutro e e g un suo elemento di ordine m. Sia $n \in \mathbb{N}$. Allora $x =$ ordine di $g^n = \frac{m}{MCD(m,n)}$. Infatti $(g^n)^x = e \Rightarrow m|nx \Rightarrow \frac{m}{MCD(n,m)} | \frac{n}{MCD(n,m)} \cdot x \Rightarrow \frac{m}{MCD(n,m)}|x$. Inoltre $(g^n)^{\frac{m}{MCD(n,m)}} = (g^{\frac{n}{MCD(n,m)}})^m = e \Rightarrow x|\frac{m}{MCD(n,m)}$

1. $g = [1]_{18}, m = 18, n = 3$. Quindi l'ordine è 6;

2. $g = \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8}, m = 8, n = 6$. Quindi l'ordine è 4.

5. Nel gruppo $GL_2(\mathbb{Q})$ sono assegnati gli elementi

$$a = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \qquad e \qquad b = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}.$$

Determinare l'ordine di a e quello di b e provare che ab è aperiodico.

L'ordine di a e di b è 2. $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Per induzione si mostra che $\forall n \in \mathbb{N}\ (ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Quindi ab è aperiodico.

6. Siano G un gruppo ed a, b suoi elementi tali che $ab = ba$. Provare che se a è di ordine m, b è di ordine n con m ed n primi tra loro, allora ab è di ordine mn.

Poichè $ab = ba$ si ha che $(ab)^{nm} = a^{nm} \cdot b^{nm} = (a^m)^n \cdot (b^n)^m = e$ (el. neutro di G) , pertanto ab é di ordine finito. Sia s l'ordine di ab; allora $s|nm$. Inoltre $(ab)^s = e \Rightarrow a^s = b^{-s}$. Quindi a^s e $b^s = (b^{-s})^{-1}$ hanno lo stesso ordine. Per quanto visto (cfr. ex. 4 - oppure si consideri l'uguaglianza $(a^s)^m = (a^m)^s = e$) l'ordine di a^s divide m e, analogamente, divide n (poichè è uguale all'ordine di b^s). Perciò l'ordine di a^s divide $MCD(n, m) = 1$. Quindi $ord(a^s) = 1 \Rightarrow a^s = e, b^s = e \Rightarrow s|n, s|m \Rightarrow s|mcm(n, m) = nm$.

7. Siano G un gruppo ed H un suo sottoinsieme non vuoto, $\underline{finito}$ e chiuso rispetto alla operazione (binaria) di G. Provare che H è un sottogruppo di G.

Dato che H è chiuso rispetto all'operazione di G per mostrare che H è effettivamente un sottogruppo di G basta mostrare che $\forall h \in H\ h^{-1} \in H$. Siccome H è finito esistono $n, m \in \mathbb{N}\ t.c.\ h^n = h^m$ con m > n. Perciò $h^{m-n} = e \Rightarrow h^{m-n-1}$ è l'inverso di h e appartiene ad H (se $m - n - 1 = 0$ allora $h = e$).

8. Provare che per ogni $n \geq 3$ ogni elemento di A_n si può scrivere come prodotto di 3-cicli (cicli di lunghezza 3).

Ogni elementi di A_n si può scrivere come prodotto di un numero pari di trasposizioni. Ad ogni coppia di trasposizioni $(n\ m) \circ (p\ q)$ si può sostituire uno o più 3-cicli secondo le seguenti regole:

1. Se $\{n, m\} \cap \{p, q\} = \emptyset$ allora $(n\ m) \circ (p\ q) = (n\ q\ p) \circ (n\ m\ p)$

2. Se $n = p$ allora $(n\ m) \circ (n\ q) = (n\ q\ m)$. Notare che se non vale il caso 1. ci si può sempre ridurre al caso 2.