www.dacrema.com Matematica del discreto App.Uni.Cri

I gruppi ciclici

Sia dato un gruppo (A, @) e un suo elemento a.
Consideriamo gli elementi:
a, a @a, a @ a @ a, a @ a @ a @ a, ...
cioè le potenze di a che indicheremo con i simboli
a^1, a^2, a^3, a^4, ...
Inoltre poniamo per definizione
a^0 = u $a^{-n} = (a^{-1})^n = (a^n)^{-1}$
dove con a^{-1} indichiamo l'inverso di a. Abbiamo così definito tutte le potenze di a ad esponente intero e non solo naturale.

Esempi:

- in $(\mathbb{Z},+)$, posto $a = 5$, e poiché $a^{-1} = -5$, risulta:
  $\ldots, a^{-2} = -10, a^{-1} = -5, a^0 = 0, a^1 = 5, a^2 = 10, a^3 = 15, \ldots$
- in $(\mathbb{Z}^*_7, \times)$, posto $a = 2$, risulta:
  $a^0 = 1,\ a^1 = 2,\ a^2 = 4,\ a^3 = 1,\ a^4 = 2,\ \ldots$ e, poiché $a^{-1} = 4$ (infatti $[4] \times [2] = [1]$):
  $a^{-1} = 4,\ a^{-2} = 2, a^{-3} = 1,\ a^{-4} = 4,\ \ldots$

Dato un elemento a∈(A, @), l'insieme di tutte le potenze di a in A è un sottogruppo di A
DEFINIZIONE. Un gruppo (A, @) si dice ciclico se tutti i suoi elementi si possono esprimere come potenze di uno stesso elemento aÎA.
Si dice che l'elemento a è un *generatore* del gruppo A, oppure che A è generato da a.

(Z,+) è un gruppo ciclico infinito generato da +1
I gruppi (Zn,+) sono tutti gruppi ciclici generati dall'elemento 1.
Ogni gruppo ciclico può avere più di un generatore:
Il gruppo (Z*5,x) = {1, 2, 3, 4} è un gruppo ciclico generato da:

2:	$2^1 = 2$	$2^2 = 4$	$2^3 \equiv 3$	$2^4 \equiv 1$
oppure da 3:	$3^1 = 3,$	$3^2 \equiv 4,$	$3^3 \equiv 2,$	$3^4 \equiv 1$
ma non da 4:	$4^1 = 4,$	$4^2 \equiv 1$		

ESERCIZI

- Trovare un generatore diverso da 1 nel gruppo $(Z_6,+)=\{0, 1, 2, 3, 4, 5\}$.
  $a^1\ a^2\ a^3\ a^4\ a^5\ a^6$
  2 4 0 NO
  3 0 NO
  4 2 0 NO
  5 4 3 2 1 0 Si
- Trovare un generatore diverso da 1 nel gruppo $(Z_8,+)=\{0, 1, 2, 3, 4, 5, 6, 7\}$
  2 4 6 0 NO
  3 6 1 4 7 2 5 0 Si
  4 0 NO
  5 2 7 4 1 6 3 0 Si
  6 4 2 0 NO
  7 .... Si ..... sono generatori gli elementi primi con 8

TEOREMA. Ogni gruppo ciclico è abeliano.
Quindi qualunque gruppo non abeliano non è un gruppo ciclico.
TEOREMA. L'insieme B di tutte le potenze g^n di un elemento di un gruppo (A,@) formano un sottogruppo (ciclico) di A.
TEOREMA. Se l'ordine di un gruppo finito (A,@) è un numero primo p, allora A è un gruppo ciclico (e quindi abeliano).
TEOREMA. Un gruppo ciclico può avere solo sottogruppi ciclici. (Se un gruppo non è ciclico può avere sia sottogruppi ciclici che non ciclici.)
Dimostrazione.
Sia (G,@) un gruppo ciclico generato da un suo elemento g e sia H un suo sottogruppo di G.
$(G,@) = \{g, g^2, \ldots. g^n = u\}$ se è finito
$(G,@) = \{..., g^{-2}, g^{-1}, u, g, g^2, \ldots. g^n \ldots.\}$ se è infinito.
Gli elementi di H sono particolari potenze di g, di cui almeno una ha esponente positivo (perché se $g^{-k} \in H$, con $k>0$, anche $g^k \in H$, poiché H è un gruppo).
$H=\{ \ldots g^{-s}, g^{-r}, g^{-k}, u, g^k, g^r, g^s, \ldots\}$
Mettiamo in ordine crescente tutte le potenze positive di g in H. Avremo: g^k, g^r, g^s…. con $k < r < s$ … Il teorema è dimostrato se mostriamo che $r = 2k$, poiché poi lo stesso ragionamento porta a dire che g^k è generatore di H. Poiché $k < r$ può essere:
$k < r < 2k$ oppure
$r = 2k$ oppure
$r > 2k$.
Mostriamo che la opzione centrale è quella vera, mostrando che le altre due sono false. La terza è falsa perché H è un gruppo, quindi se contiene g^k contiene anche g^{2k}, quindi ci sarebbe una potenza di g tra g^k e g^r contro quanto detto. Se fosse vera la prima, poiché H è un gruppo, anche $g^{r-k} \in H$, mentre abbiamo detto che k è il più piccolo esponente positivo.

Con (Zn*, x) se n è primo, (Zp*, x) ha come elementi {1,…, p-1}, quindi ha ordine p-1. È sempre ciclico; generatori sono tutti i k tali che MCD (p-1,k)=1. Se n non è primo ci sono diversi casi, vediamo qualche esempio:

gruppo	Elementi	ord	Ciclico?	generatori	Sottogruppi non banali
$Z_4^*, \times$	{1, 3}	2	Sì	3→ 3,1	
$Z_6^*, \times$	{1, 5}	2	Sì	5→ 5,1	
$Z_8^*, \times$	{1, 3, 5, 7}	4	No		{3, 1}, {5,1}, {7, 1}
$Z_9^*, \times$	{1, 2, 4, 5, 7, 8}	6	Sì	2 → 2, 4, 8, 7, 5, 1 5 → 5, 7, 8, 4, 2, 1	{8, 1} {4, 7, 1}
$Z_{10}^*, \times$	{1, 3, 7, 9}	4	Sì	3 → 3,9,7,1 7 → 7,9,3,1	{9, 1}
$Z_{12}^*, \times$	{1, 5, 7, 11}	4	No		{5, 1}, {7, 1}, {11, 1}
$Z_{14}^*, \times$	{1, 3, 5, 9, 11, 13}	6	Sì	3 →3,9,13,11,5,1 5 →5,11,13,9,3,1	{1, 13} {1, 9, 11},
$Z_{15}^*, \times$	{1,2,4,7,8,11,13,14}	8	No		{2,4,8,1},{7,4,13,1}, {4,1},{11,1},{14,1}, {11,14,4,1} non ciclico
$Z_{16}^*, \times$	{1,3,5,7,9,11,13,15}	8	No		{3,9,11,1},{5,9,13,1}, {7,1},{9,1},{15,1}, {7,15,9,1} non ciclico
$Z_{18}^*, \times$	{1,5,7,11,13,17}	6	Sì	5 → 5,7,17,13,11,1 11→11,13,17,7,5,1	{17,1} {7,13,1},
$Z_{20}^*, \times$	{1,3,7,9,11,13,17,19}	8	No		{3,9,7,1},{13,9,17,1}, {11,1},{9,1},{19,1}, {11,9,19,1} non ciclico
$Z_{22}^*, \times$	{1, 3, 5, 7, 9, 13, 15, 17, 19, 21}	10	Sì	7→7,5,13,3,21,15,17, 9,19,1	{3,9,5,15,1} {21,1}