

Asian Resonance

Some Results on Group Elements

Abstract

Order of group elements give some information about its structure, such as about center of group. We can construct non-abelian p-groups with order of each non-identity element is p etc.

Keywords: Cyclic Group, p-Group, Heisenberg Group, Center of Group

Introduction

Let G be a nonempty set and $*$ be a binary operation on G , i.e. $a*b \in G$ for all $a, b \in G$. Then $(G, *)$ is a group or simply G is a group (under the operation $*$) if

1. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$ (Associative law)
2. $\exists e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (e is called an identity of G)
3. For each $a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$ (a^{-1} is called inverse of a). For the sake of simplicity we use ab for $a * b$ and a^{-1} for a^{-1} .

A group G is said to be abelian (commutative) if $ab = ba \quad \forall a, b \in G$.

A group G is said to be finite if G is a finite set, otherwise G is an infinite group.

The number of elements in G is denoted by $|G|$ (or $o(G)$) and it is called the order of G .

If G has exactly n distinct elements then $|G| = n$.

Example 1

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are infinite abelian groups with identity 0. $(\mathbb{Q}^+, \cdot), (\mathbb{R}^+, \cdot), (\mathbb{C}^+, \cdot)$ are infinite abelian groups with identity 1,

where $\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\}$

$$\mathbb{Q} = \mathbb{Q} - \{0\}$$

For $n \in \mathbb{N}, (\mathbb{Z}_n, +_n)$ is a group of order n , under $+_n$ where $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ and $a +_n b =$ the least nonnegative integer when $a + b$ is divided by n .

For a prime number $p, \mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ is a group under \cdot_n , and \mathbb{Z}_p is a field. For $n > 1,$

$U(n) = \{k \in \mathbb{N} \mid k < n \text{ and } \gcd(k, n) = 1\}$ is an abelian group under \cdot_n and order is denoted by $\phi(n)$,

$GL(n, \mathbb{R}), SL(n, \mathbb{R})$ are groups under matrix multiplication with identity I , the $n \times n$ unit matrix.

Properties

Let G be a group with identity e . Then,

1. The identity element of G is unique.
2. Every $a \in G$ has unique inverse.
3. $(a^{-1})^{-1} = a$ for all $a \in G$.
4. $(ab)^{-1} = b^{-1} a^{-1} \quad \forall a, b \in G$. More general $(a_1 a_2 \dots a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \dots a_2^{-1} a_1^{-1}$ for all $a_i \in G$.
5. Cancellations laws: For $a, u, w \in G,$
 $au = aw \Rightarrow u = w$ LCL
 $ua = wa \Rightarrow u = w$ RLC.
6. For any $a, b \in G,$ the equations $ax = b$ and $ya = b$ have unique solutions in G .
7. If $a^2 = e$ (i.e. $a = a^{-1}$) $\forall a \in G$ then G is abelian.

Definition

Let G be a group with identity e and $n \in \mathbb{N}$, we define integral powers of a as follows

$$a^0 = e, a^1 = a \text{ and for any } a \in G;$$

$$a^{n+1} = a^n a \text{ i.e. } a^n = a a \dots a \text{ (n times), } a^{-n} = (a^{-1})^n.$$

Properties

In a group G with identity e ; for any $a \in G$ and $m, n \in \mathbb{Z},$

1. $a^{-n} = (a^n)^{-1} = (a^{-1})^n$
2. $a^m a^n = a^{m+n}$

J. N. Salunke

School of Mathematical Sciences
SRTM University, Nanded.

S. P. Basude

School of Mathematical Sciences
SRTM University, Nanded.

Asian Resonance

3. $(a^m)^n = a^{mn} = (a^n)^m$

4. $e^n = e$.

Note that a group G is abelian iff $(ab)^2 = a^2 b^2 \forall a, b \in G$ and if G is abelian, then $(ab)^n = a^n b^n \forall n \in \mathbb{Z}$

Definition

Let $(G, *)$ be a group and H be a nonempty subset of G. If $(H, *)$ is a group, then H is called a subgroup of G.

Note that if $\emptyset \neq H \subseteq G$ and G is a group then (subgroup tests):

H is a subgroup of G iff $ab, a^{-1} \in H \forall a, b \in H$

iff $ab^{-1} \in H \forall a, b \in H$

iff $ab \in H$ for all $a, b \in H$, for a finite set H.

Definition

Let G be a group. Then $Z(G) = \{ x \in G \mid xy = yx \forall y \in G \}$ is an abelian subgroup of G, called the centre of the group.

G is abelian iff $Z(G) = G$.

Definition

Let G be a group, $a \in G$ and with $a^0 = e$, identity. The least positive integer n such that $a^n = e$ is called order of a and we write $|a| = n$.

Thus $|a| = n \in \mathbb{N}$ means $a^n = e$ and $a^r \neq e$ for any $r \in \mathbb{N}, r < n$.

If no such n exists, i.e. $a^n \neq e$ for all $n \in \mathbb{N}$ then a is said to be of infinite order.

Identity is only group element of order 1.

To find the order of a group element g, compute the sequence of products g, g^2, g^3, \dots until reach the identity for the first time. The exponent of this product is the order of g. If the identity never appears in the sequence, then g has infinite order.

Theorem [2]

Let G be a group with identity e and $a \in G$ with $|a| = n \in \mathbb{N}$. Then

- $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \} = \{ e, a, a^2, \dots, a^{n-1} \}$ is a subgroup of G of order n.
- $a^k = e$ iff $n \mid k$ ($n = |a|$ and $k \in \mathbb{Z}$).

Theorem Fundamental Theorem of Cyclic Groups [1]

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k- namely $\langle a^{n/k} \rangle$.

Some Results About Order of Group Elements

Following proposition and results are well established for more details please refer [2] or any standard book on group theory.

Proposition

Let a be a group element of order n. Then for any $k \in \mathbb{Z}, |a^k| = \frac{n}{\gcd(n, k)}$.

Solution

Let $\gcd(n, k) = d$. Then $n = sd, k = td$ where $s \in \mathbb{N}, t \in \mathbb{Z}$ and $\gcd(s, t) = 1$.

$(a^k)^s = (a^n)^t = e$ and for any $m \in \mathbb{N}$, with $(a^k)^m = e \Rightarrow n = |a| = sd$ divides $km = tdm \mid tm \Rightarrow s \mid m$ since $\gcd(s, t) = 1 \Rightarrow s \mid m$ i.e. $s \leq m$.

Hence $|a^k| = s = \frac{n}{d}$

From above proposition (0) for $a^k \in \langle a \rangle =$

$\{ e, a, a^2, \dots, a^{n-1} \},$

$|a^k| = n$ iff $d = 1$ i.e. $\gcd(n, k) = 1$

i.e. a^k is a generator of $\langle a \rangle$ iff $k \in U(n)$ and hence $\langle a \rangle$ has $\varphi(n)$ generators i.e. elements of order n in $\langle a \rangle$.

1. $|a^{-1}| = \frac{n}{\gcd(n, -1)} = n = |a|$

2. $a^k = e$ iff $|a^k| = 1$ i.e. $\gcd(n, k) = n$ iff $n \mid k$ where $|a| = n$.

3. For a positive divisor k of n, $|a^{n/k}| = \frac{n}{\gcd(n, n/k)} = \frac{n}{\frac{n}{k} \gcd(k, 1)} = k$.

4. For any $k \in \mathbb{Z}, |a^k| = \frac{n}{\gcd(n, k)} = |a^{n/\gcd(n, k)}| = |a^{\gcd(n, k)}|$

5. $\langle a^k \rangle \subseteq \langle a^s \rangle$ iff $\langle a^{\gcd(n, k)} \rangle \subseteq \langle a^{\gcd(n, s)} \rangle$ i.e. $a^{\gcd(n, k)} \in \langle a^{\gcd(n, s)} \rangle$ iff $\gcd(n, s) \mid \gcd(n, k) \cdot \langle a^k \rangle = \langle a^s \rangle$ iff $\gcd(n, s) = \gcd(n, k)$.

Result

$(bab^{-1})^k = ba^k b^{-1}$. So $(bab^{-1})^k = e$ iff $ba^k b^{-1} = e$ i.e. $a^k = e$.

This proves $|bab^{-1}| = |a|$ for all group elements a & b.

From this $|b(ab)b^{-1}| = |ab|$ i.e. $|ba| = |ab|$.

Result

Let G be a group with identity e and $a, b \in G$ of finite order with $ab = ba$

- $|ab|$ divides $\text{lcm}(|a|, |b|)$
- If $\langle a \rangle \cap \langle b \rangle = \{e\}$ then $|ab| = \text{lcm}(|a|, |b|)$
- If $|a|, |b|$ are relatively prime then $|ab| = |a||b|$.

Proof

Let $|a| = m, |b| = n$ where $ab = ba$ i.e. $(ab)^i = a^i b^i \forall i \in \mathbb{Z}$ and $|ab| = |ba| = k, l = \text{lcm}(|a|, |b|) = \text{lcm}(m, n)$.

(a) As $m \mid l, n \mid l$ so $a^l = e = b^l = b^{-l}$

$\Rightarrow (ab)^l = a^l b^l = ee = e$ i.e. $k \mid l$ i.e. $k \mid \text{lcm}(m, n)$

(b) Let $\langle a \rangle \cap \langle b \rangle = \{e\}$. Now $(ab)^k = e \Rightarrow a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = \{e\}$

i.e. $a^k = b^{-k} = e = b^k$

$\Rightarrow m = |a|$ divides $k, n = |b|$ divides k i.e. $l = \text{lcm}(m, n)$ divides k .

$k \mid l$ & $l \mid k$ gives $k = l$

(c) As $|a|, |b|$ are relatively prime, we have $\langle a \rangle \cap \langle b \rangle = \{e\}$

$[1 = mr + ns. \forall x \in \langle a \rangle \cap \langle b \rangle \Rightarrow x = a^{mr} = b^{ns}$ for some $m_1, n_1 \in \mathbb{Z}$

And so $x^1 = x^{mr + ns} = (a^{m_1})^{mr} (b^{n_1})^{ns} = e \Rightarrow \langle a \rangle \cap \langle b \rangle = \{e\}$

By (b), $|ab| = \text{lcm}(|a|, |b|) = |a||b|$.

Example 2

$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$ is a non abelian group under matrix multiplication with identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. (General linear group of 2×2 matrices over \mathbb{R})

$SL(2, \mathbb{R}) = \{A \in GL(2, \mathbb{R}) \mid \det A = 1\}$ is a subgroup of $GL(2, \mathbb{R})$ (Special linear group of 2×2 matrices over \mathbb{R})

Asian Resonance

Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ form $SL(2, \mathbb{R})$

We determine $|A|$, $|B|$ and $|AB|$.

Now $A \neq I, A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I,$
 $A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \neq I, A^4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = I \Rightarrow |A|=4$

$B \neq I, B^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \neq I, B^3 = I \Rightarrow |B|=3.$

$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq I, (AB)^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \neq I, \dots$

$(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \neq I \quad \forall n \in \mathbb{N} \Rightarrow |AB| = +\infty.$

Application

$Z(A_4) = \{(1)\}, Z(A_5) = \{(1)\}, Z(A_6) = \{(1)\}$ etc.

Suppose $Z(A_4) \neq \{(1)\}$. As the orders of elements of A_4 are 1, 2 and 3, So $\exists a \in Z(A_4)$ with $|a| = 2$ or 3

If $|a| = 2$, then for $b \in A_4$ with $|b| = 3$ we have $ab = ba \in A_4$ such that $|ab| = 2 \times 3 = 6$, a contradiction. Similarly if $|a| = 3$ then we get an element of order 6 in A_4 , a contradiction.

So the supposition $Z(A_4)$ is nontrivial subgroup of A_4 is wrong. Hence $Z(A_4) = \{(1)\}$ is a trivial subgroup.

Possible orders of elements of A_5 are 1, 2, 3, 5.

If $Z(A_5) \neq \{(1)\}$ then $\exists a \in Z(A_5)$ with $|a| \in \{2, 3, 5\}$, then we find $b \in A_4$ with $|b| = \{2, 3, 5\} - \{|a|\}$, $ab = ba \in A_4$ with $|ab| \in \{6, 10, 15\}$, a contradiction. Hence $Z(A_5) = \{(1)\}$

Possible orders of elements of A_6 are 1, 2, 3, 4, 5.

If $Z(A_6) \neq \{(1)\}$ then $\exists a \in Z(A_6), a \neq (1)$ and $\exists b \in A_6$ and so $ab = ba \in A_6$ with $|ab| \in \{6, 12, 10, 15, 20\}$ a contradiction.

Hence $Z(A_6) = \{(1)\}$

Possible orders of elements of A_7 are 1, 2, 3, 4, 5, 6, 7.

If $Z(A_7) \neq \{(1)\}$, then $\exists a \in Z(A_7), a \neq (1)$

And $\exists b \in A_7$ and so $ab = ba \in A_7$ with $|ab| \in \{10, 14, 12, 15, 21, 20, 28, 30, 35, 42\}$ a contradiction. Hence $Z(A_7) = \{(1)\}$.

Remark

If R is a ring and it satisfies any one of the following condition

(a) $x^2 = x \quad \forall x \in R$ (b) $x^3 = x \quad \forall x \in R$ (c) $x^4 = x \quad \forall x \in R$ then R is a commutative. For (a), R is a Boolean ring.

If G is a group and it satisfies anyone of the following condition

(d) $x^2 = x \quad \forall x \in G$ (e) $x^3 = x \quad \forall x \in G$ then G is commutative. For (d), G is a trivial group.

Heisenberg Group

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \text{ is a group}$$

under matrix multiplication with identity $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

This group is called Heisenberg group after the Nobel Prize winning Physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of Quantum Physics.

$$\text{For } A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \in G \text{ we}$$

have $AB \neq BA$;

$$\text{Since } AB = \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}, BA = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \dots (*)$$

$\Rightarrow G$ is non abelian.

For $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G$, by induction we obtain

$$X^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)ac}{2} \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \quad \forall n \in \mathbb{N} \dots \dots (**)$$

Result

For a group H , if $x^2 = e$, identity $\forall x \in H$ then H is abelian.

Here we can not replace 2 by any number greater than 2. That is any fixed integer $n > 2$, we can obtain a non abelian group K with identity e such that $x^n = e \quad \forall x \in K$.

Note

For a prime $p, \mathbb{Z}_p = \{0, 1, \dots, p-1\}$ is a field under addition and multiplication modulo p .

For a prime $p,$

$$G_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\} \text{ is a group under}$$

matrix multiplication (in arithmetic modulo p) of order

$$p^3 \text{ with identity } I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and it is non abelian by}$$

(*).

$$\text{By (**), for } p > 2, \forall X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G_p,$$

$$X^p = \begin{pmatrix} 1 & pa & pb + \frac{p(p-1)ac}{2} \\ 0 & 1 & pc \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I,$$

identity, since $p \mid \frac{p(p-1)}{2}$ etc. Thus for any

prime $p > 2$, we can have a non abelian group G_p of order p^3 such that $x^p = I$, identity, $\forall x \in G_p$.

In group G_p , each nonidentity element has order p and $|Z(G_p)| = p$.

Now consider any integer $n > 2$, then $4 \mid n$ or n has an odd prime factor.

If $4 \mid n$ then G_2 is the nonabelian group of order 8 such that

$$\forall X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G_2, X^4 = \begin{pmatrix} 1 & 4a & 4b + 6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix} = I$$

If an odd prime p is a factor of n then G_p is the nonabelian group of order p^3 such that $x^n = I$, identity $\forall X \in G_p$, since $x^p = I \quad \forall x \in G_p$ and $p \mid n$.

Proposition

Let G be a finite group with the property that every non identity element has prime order and $Z(G)$ is not trivial. Then every non identity element of G has the same order.

Proof

Let G be a finite nontrivial group with identity e , with the property that every non identity element has prime order and $Z(G) \neq \{e\}$.

Consider any $a \in Z(G)$, any $b \in G$ with $a \neq e \neq b$.

By hypothesis $|a| = p$, $|b| = q$ are primes and $ab = ba \in G$

$\Rightarrow |ab| = \text{lcm}(|a|, |b|) = \text{lcm}(p, q)$ is a prime, showing $p = q$.

Thus $\forall x \in G, x \neq e$, we must have $|x| = |a| = p$, prime.

Note 1

(1) For each prime p , D_{2p} is a dihedral nonabelian group of order $2p$ in which one element is identity, $p-1$ elements are of order p and remaining p elements are of order 2.

$\Rightarrow Z(D_{2p}) = \{e\}$

(2) A_4 is a nonabelian group of order 12 and it contains elements of orders 1, 2, 3. So $Z(A_4) = \{(1)\}$.

(3) A_5 is a non-abelian group of order 60 and it contains elements of orders 1, 2, 3 and 5. So $Z(A_5) = \{(1)\}$.

(4) For $n \geq 6$, A_n has elements of composite order and $Z(A_n) = \{(1)\}$.

References

1. Joseph A. Gallian, Contemporary Abstract Algebra, First Narosa Publishing House Reprint (1999).
2. Sudesh Kumari Shah and Asha Gauri Shankar, Group Theory, Pearson second reprint (2014).