e content for students of patliputra university

B. Sc. (Honrs) Part 2paper 3

Subject:Mathematics

Title/Heading:Groups:definition &elementary properties

By Dr. Hari kant singh

Associate professor in mathematics

Rrs college mokama patna

Groups:Definition &Elementary properties

Definition

A **group** $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied.

1. **Associativity**: $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$

2. **Existence of identity element**: There is an element e in G such that $e * x = x * e = x, \forall x \in G$.

3. **Existence of inverse element**: For each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$.

   Here, a' is called the **inverse** of a.

abelian group:definition

A group G is **abelian** if its binary operation is commutative.

A group that is not abelian is called **nonabelian**.

Remark.

In a group G , the identity element and inverse of each element are unique.

For each $a \in G$, the inverse of a is denoted by a^{-1}.

Example

1. The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ under addition are abelian groups.
2. The sets $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*$, and $\mathbb{C}^*$ under multiplication are abelian groups.
3. The set $\mathbb{Z}^+$ under addition is *not* a group, since it has no identity element for $+$ in $\mathbb{Z}^+$.
4. The set $\mathbb{Z}^+ \cup \{0\}$ under addition is *not* a group, even if it has an identity element 0, but no inverse for 1.
5. The set $\mathbb{Z}^+$ under multiplication is *not* a group. It has an identity element 1, but no inverse for 2.

6. The set $M_n(\mathbb{R})$ under matrix addition is an abelian group. The zero matrix is the identity element.

7. The set $M_n(\mathbb{R})$ under matrix multiplication is *not* a group, since the zero matrix has no multiplicative inverse.

Problem

Let $\langle G, * \rangle$ be a group. For $a, b \in G$, prove that $(a * b)^{-1} = b^{-1} * a^{-1}$

Solution.

We have $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$. Since the inverse of any element in a group is unique, this shows that $(a * b)^{-1} = b^{-1} * a^{-1}$.

■

Problem

Let $*$ be defined on $\mathbb{Q}^+$ by $a * b = \dfrac{ab}{2}$. Prove that $\mathbb{Q}^+$ is an abelian group under $*$.

Solution.

It is clear that $\mathbb{Q}^+$ is closed under $*$. Also, $(a * b) * c = a * (b * c) = \dfrac{abc}{4}$, $\forall a, b, c \in \mathbb{Q}^+$, showing that $*$ is associative.
$*$ is commutative, since $a * b = b * a = \dfrac{ab}{2}$, $\forall a, b \in \mathbb{Q}^+$. If e is the identity for $*$, then $a * e = a \implies \dfrac{ae}{2} = a \implies e = 2$. Finally, computation shows that $a^{-1} = \dfrac{4}{a}$, $\forall a \in \mathbb{Q}^+$. ■

Theorem .

In a group G, with binary operation $*$, the left and right cancellation laws *holds. i.e., $a * b = a * c \implies b = c$ and $b * a = c * a \implies b = c$, $\forall a, b, c \in G$.*

Proof.

Suppose $a * b = a * c$. Multiplying from the left with a^{-1} on both sides, we get $a^{-1} * (a * b) = a^{-1} * (a * c)$. Using associativity, $(a^{-1} * a) * b = (a^{-1} * a) * c \implies e * b = e * c \implies b = c$. Similarly,from $b * a = c * a$, we get $b = c$. □

Theorem

If G is a group with binary operation $*$, and if $a, b \in G$ the linear equations $a * x = b$ and $y * a = b$ have unique solutions , x, y in G.

□

Remark.

A set together with an associative binary operation is called a **semigroup**. A **monoid** is a semigroup that has an identity element for the binary operation.

Note that a group is both a semigroup and a monoid.

Note that there is only one group of a single element, namely $\{e\}$ with binary operation $e * e = e$, up to isomorphism . By looking at the table representations, we can conclude that there is only one group of two elements (or three elements) up to isomorphism . In the next section, we will show that there exists two non isomorphic group structures on a set of four elements.

Problem

Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ on S by $a * b = a + b + ab$.

(a) Show that $*$ is a binary operation on S.

(b) Show that $\langle S, * \rangle$ is a group.

(c) Find the solution of the equation $2 * x * 3 = 7$ in S.

Solution.

(a) We must show that S is closed under $*$, that is, that $a+b+ab \neq -1$ for $a, b \in S$. Now $a+b+ab=-1$ if and only if $0=ab+a+b+1=(a+1)(b+1)$. This is the case if and only if either $a=-1$ or$b=-1$, which is not the case for $a, b \in S$.

(b) We have $a*(b*c)=a*(b+c+bc)=a+(b+c+bc)+a(b+c+bc)=a+b+c+ab+ac+bc+abc$ and $(a*b)*c=(a+b+ab)*c=(a+b+ab)+c+(a+b+ab)c=a+b+c+ab+ac+bc+abc$. Thus $*$ is associative. Note that 0 acts as identity element for $*$, since $0*a=a*0=a$.

Also, $\frac{-a}{a+1}$ acts as inverse of a, for $a*\dfrac{-a}{a+1}=a+\dfrac{-a}{a+1}+a\dfrac{-a}{a+1}+1=\dfrac{a(a+1)-a-a^2}{a+1}=\dfrac{0}{a+1}=0$. Thus $\langle S, *\rangle$ is a group.

(c) Because the operation is commutative, $2*x*3=2*3*x=11*x$. Now the inverse of 11 is $\dfrac{-11}{12}$, by Part(**b**). From, $11*x=7$, we obtain $x=\dfrac{-11}{12}*7=\dfrac{-11}{12}+7+\dfrac{-11}{12}7=\dfrac{-11+84-77}{12}=\dfrac{-4}{12}=\dfrac{-1}{3}$. ■

Problem

Show that if G is a finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a*a=e$.

Solution.

Let $S=\{x \in G \mid x^{-1} \neq x\}$. Then S has an even number of elements, because its elements can be grouped in pairs x, x^{-1}. Because G has an even number of elements, the number of elements in G but not in S (the set $G-S$) must be even. The set $G-S$ is nonempty because it contains e. Thus there is at least one element of $G-S$ other than e, that is, at least one element other than e that is its own inverse. ■

Problem

Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

Solution.

Let G has m elements. Then the elements $e, a, a^2, a^3, ..., a^m$ are not all different, since G has only m elements. If one of $a, a^2, a^3, ..., a^m$ is e, then we are done. If not, then we must have $a^i = a^j$ where $i < j$. Repeated left cancellation of a yields $e = a^{j-i}$. ■

Problem

Show that if $(a * b)^2 = a^2 * b^2$ for all a, b in a group G, then G is abelian.

Solution.

We have $(a * b) * (a * b) = (a * a) * (b * b)$, so $a * [b * (a * b)] = a * [a * (b * b)]$ and left cancellation yields $b * (a * b) = a * (b * b)$. Then $(b * a) * b = (a * b) * b$ and right cancellation yields $b * a = a * b$. Thus G is abelian. ■

Problem

Let G be a group and let g be one fixed element of G. Show that the map i_g defined by $i_g(x) = gxg^{-1}$ for all x in G, is an isomorphism of G with itself.

Solution.

Let $a, b \in G$. If $g * a * g^{-1} = g * b * g^{-1}$, then $a = b$ by group cancellation, so i_g is a one-to-one map. Because $i_g(g^{-1} * a * g) = g * g^{-1} * a * g * g^{-1} = a$, we see that i_g maps G onto G. We have $i_g(a * b) = g * a * b * g^{-1} = g * a * (g^{-1} * g) * b * g^{-1} = (g * a * g^{-1}) * (g * b * g^{-1}) = i_g(a) * i_g(b)$, so i_g satisfies the homomorphism property also, and is thus an isomorphism. ■