Revision

For the group S_3, if we write $\phi = \rho_5 = (12)$ $\chi = \rho_1 = (123)$ we write ρ_0 as e, the identity element in S_3

Then $\phi^2 = e$, $\chi^3 = e$ and $\phi.\chi = \rho_4 = (13)$, Here $\chi^2 = (132)$

and $\chi.\phi = \rho_3 = (23)$ Here $\phi.\chi \neq \chi.\phi$

Here $\chi^{-1} = \chi^2$ as $\chi^3 = e$, so, $\phi.\chi = \chi^{-1}.\phi$ Here

So, $S_3 = \{e, \phi, \chi, \chi^2, \phi.\chi, \chi.\phi\}$

Problem 1 In S_3, give an example of two elements x, y such that $(x.y)^2 \neq x^2.y^2$

Solution: Let $x = \phi$, $y = \chi$ then $x.y = \phi.\chi = (13)$

$(x.y)^2 = (13)(13) = e$ Now $x^2 = \phi^2 = e$ $y^2 = \chi^2 = (132)$

So, $x^2.y^2 = e(132) = (132)$ So, $(x.y)^2 \neq x^2.y^2$

Problem 2 In S_3, show that there are four elements satisfying $x^2 = e$, and three elements satisfying $y^3 = e$

Solution: Here $e^2 = e$, $\phi^2 = e$, $(\phi.\chi)^2 = e$, and $(\chi.\phi)^2 = e$

Also, $e^3 = e$, $\chi^3 = e$, $(\chi^2)^3 = e$. So, we get the required result.

Let G be an non-empty set on which a binary operation o is defined. Then then the algebraic system (G, o) is called a groupoid.

A groupoid (G,o) is said to be a semigroup if o is associative.

A semigroup (G, o) containing the identity element is said to be a monoid.

Scanned with CamScanner

A groupoid (G, o) is said to be a quasigroup if for any two elements $a, b \in G$, each of the equation $a o x = b$ and $y o a = b$ has a unique solution in G.

The set $\mathbb{Z}_n$ forms a commutative monoid under multiplication (modulo n)

In a monoid, an invertible element is said to be a unit.

Let us find the units in the monoid $(\mathbb{Z}_n, \cdot)$ $(n>1)$.

Let $\bar{u}$ be a unit. Then $\exists\ \bar{v} \in \mathbb{Z}_n$ such that $\bar{u} \cdot \bar{v} = \bar{1}$

$\Rightarrow uv - 1 = kn$, or $uv - kn = 1$, where k is an integer.

This shows that $\gcd(u, n) = 1$

Conversely, let u be and integer less than n and prime to n

Then $\exists$ integers p and q such that $up + nq = 1$ or

$up - 1 = -qn$ or $up \equiv 1 \pmod{n}$. Clearly, p is not a multiple of n.

Let $p \equiv r \pmod{n}$, where $0 < r < n$. Then $\bar{r} \in \mathbb{Z}_n$

$r \equiv p \pmod{n} \Rightarrow ur \equiv up \pmod{n} \Rightarrow ur \equiv 1 \pmod{n}$

This gives $\bar{u} \cdot \bar{r} = \bar{1}$. Since the monoid is commutative

$\bar{u} \cdot \bar{r} = \bar{r} \cdot \bar{u} = \bar{1}$. This shows that $\bar{u}$ is a unit.

Thus $\bar{u}$ is a unit if and only u is less than n and prime to n.

Consider the set $U_n = \{ \bar{u} \in \mathbb{Z}_n : \bar{u} \text{ is a unit} \}$

$= \{ \bar{u} \in \mathbb{Z}_n : \gcd(u, n) = 1 \}$

We prove that U_n forms a commutative group under multiplication (modulo n)

(i) Let $\bar{u}, \bar{v} \in U_n$. Then u is prime n and v is prime to n. So, uv is prime to n. So, $\overline{uv} = \bar{u} \cdot \bar{v} \in U_n$.

Scanned with CamScanner

(ii) Multiplication $(\bmod n)$ is associative in $\mathbb{Z}_n$, and U_n is a subset of $\mathbb{Z}_n$. So, it is associative in U_n.

(iii) $\bar{1} \in U_n$ and $\bar{1}.\bar{u} = \bar{u}.\bar{1} = \bar{u}$, $\forall\, \bar{u} \in U_n$. So, $\bar{1}$ is the identity in U_n

(iv) Let $\bar{u} \in U_n$. Then $\bar{u}$ is a unit in the monoid $(\mathbb{Z}_n, \cdot)$ So, $\exists$ an element $\bar{v} \in \mathbb{Z}_n$ such that $\bar{u}.\bar{v} = \bar{v}.\bar{u} = \bar{1}$. This shows that $\bar{u}$ is a unit in $\mathbb{Z}_n$. So, $\bar{v} \in U_n$ and $\bar{v}$ is the inverse of $\bar{u}$.

(v) Multiplication $(\bmod n)$ is commutative on the set $\mathbb{Z}_n$. U_n is a subset of $\mathbb{Z}_n$. So multiplication $(\bmod n)$ is commutative in U_n.

So, U_n forms a commutative group under multiplication $(\bmod n)$.

U_n has $\phi(n)$ elements where $\phi(n)$ = number of positive integers less than n and prime to n.

So, U_4 has $\phi(4) = 2$ elements and $U_4 = \{\bar{1}, \bar{3}\}$

U_{10} contains $\phi(10) = 4$ elements and $U_{10} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

Theorem 1 A cyclic group of finite order n has one and only one subgroup of order d for every positive divisor d of n.

Proof: Let $G = \langle a \rangle$ be a finite group of order n. Then $o(a) = n$ and $G = \{a, a^2, \ldots, a^{n-1}, a^n (= e)\}$. $\{e\}$ is the only subgroup of order 1 and G is the only subgroup of order n. So the Theorem holds for the divisors 1 and n of n. Let d be a divisor of n such that $1 < d < n$. $\exists$ some positive integer d' such that $dd' = n$ and $1 < d' < n$. Now $a^{d'} \in G$.

and $o(a^{d'}) = \dfrac{n}{\gcd(d', n)} = \dfrac{n}{d'} = d$. Therefore $\langle a^{d'} \rangle$ is

Scanned with CamScanner

a cyclic subgroup of G of order d. Let $H = \langle a^{d'} \rangle$. Let K be another subgroup of G s.t $o(K) = d$. Since G is cyclic, K must be cyclic. Let a^p be a generator of K. Then $o(a^p) = d$

but, $o(a^p) = \frac{n}{\gcd(n,p)}$ So, $\gcd(p,n) = \frac{n}{d} = d'$

This implies that $p = \lambda d'$ for some positive integer λ.

So, $a^p = (a^{d'})^\lambda$. Since λ is an integer, it follows that $\langle a^p \rangle \subset \langle a^{d'} \rangle$. So, $K \subset H$. Since $o(H) = o(K)$, $K = H$ and this proves that H is unique.

Theorem 2 Let a be an element of a group (G, o). Then for integers m and n,

(i) $a^m o a^n = a^{m+n}$ (ii) $(a^m)^n = a^{mn}$ (iii) $(a^n)^{-1} = a^{-n}$

Proof (i) Case 1. Let m and n be both positive integers.

Then $a^m o a^n = (\overbrace{a o a o \dots o a}^{m \text{ times}}) o (\overbrace{a o a o a \dots o a}^{n \text{ times}})$

$= \overbrace{(a o a o \dots a)}^{(m+n) \text{ times}}$, since o is associative.

$= a^{m+n}$

Case 2. Let $m > 0$ and $n < 0$ and let $n = -r$, $r > 0$

If $m > r$, then $a^m o a^n = (\overbrace{a o a o \dots o a}^{m \text{ times}}) o (\overbrace{a^{-1} o a^{-1} o \dots o a^{-1}}^{r \text{ times}})$

$= \overbrace{a o a o \dots o a}^{(m-r) \text{ times}} = a^{m-r} = a^{m+n}$

If $m < r$, then $a^m o a^n = (\overbrace{a o a o \dots o a}^{m \text{ times}}) o (\overbrace{a^{-1} o a^{-1} o \dots o a^{-1}}^{r \text{ times}})$

$= (\overbrace{a^{-1} o a^{-1} o \dots o a^{-1}}^{(r-m) \text{ times}}) = (a^{-1})^{r-m} = a^{m-r} = a^{m+n}$

Case 3. Let $m = -s < 0$ and $n > 0$

This case is similar to Case 2.

Scanned with CamScanner

Case 4 Let $m = -s < 0$ and $n = -r < 0$

Then $a^m \circ a^n = a^{-s} \circ a^{-r} = \underbrace{(\bar{a} \circ \bar{a} \cdots \circ \bar{a}}_{s \text{ times}}) \circ \underbrace{(\bar{a} \circ \bar{a} \circ \cdots \circ \bar{a})}_{r \text{ times}}$

$= \underbrace{\bar{a} \circ \bar{a} \circ \bar{a} \circ \cdots \circ \bar{a}}_{s+r \text{ times}}$ since $\circ$ is associative

$= \bar{a}^{(s+r)} = a^{-s-r} = a^{m+n}$

Case 5. If m or n or both zeroes, the result is easy to show as $a^0 \circ a^n = e \circ a^n = a^n = a^{0+n} = a^{m+n}$ if $m = 0$, etc.

(ii) Exercise

(iii) Case 1 Let n be a +ve integer. We prove the result by induction. For $n = 1$ $(a^1)^{-1} = \bar{a}^1$, So the result is true for $n = 1$. Assume the result is true for $n = k$, k is a positive integer. So,

$$(a^k)^{-1} = a^{-k} \quad \text{---------- (1)}$$

Now $(a^{k+1})^{-1} = (a^k \circ a)^{-1} = \bar{a}^1 \circ (a^k)^{-1}$ $\left[\text{As } (a*b)^{-1} = \bar{b}^1 \circ \bar{a}^1\right]$

$= \bar{a}^1 \circ a^{-k} = a^{-1-k} = a^{-(k+1)}$

So, the result is true for $n = k+1$. So, by the principle of mathematical induction, $(a^n)^{-1} = a^{-n}$, for positive integer n.

Case 2 Let $n = -m < 0$, i.e m is a +ve integer

Now $(a^n)^{-1} = (a^{-m})^{-1} = ((a^{-1})^m)^{-1} = (\bar{a}^1)^{-m}$ (by Case 1)

$= ((a^{-1})^{-1})^m = a^m$

$= a^{-n}$

Case 3 When $n \geq 0$, the proof is easy.

Scanned with CamScanner