Syllabus

Sets and their Cartesian product (2), Relations, Equivalence Relations and Partitions (4). Mappings (4).

Binary operation, Algebraic system with special reference to field as an example of an algebraic system.

Definition, examples, properties of groups (8) , groups of n th roots of unity, permutation groups, group

of residue modulo classes (5), properties relating to order of an element of a group, order of a group (3),

Subgroups(3), Cyclic groups(3), Cosets (2), Lagrange's Theorem for finite groups(2)

MATHEMATICS HONOURS, SEM I

SECTION I: LECTURE NOTES ON ABSTRACT ALGEBRA

SETS AND FUNCTIONS

In Mathematics, we define a mathematical concept in terms of more elementary concept/s.For example, the definition of perpendicularity between two straight lines is given in terms of the more basic concept of angle between two straight lines. The concept of set is such a basic one that it is difficult to define this concept in terms of more elementary concept. Accordingly, we do not define set but to explain the concept intuitively we say: a set is a collection of objects having the property that given any object, abstract (the thought of getting 100%marks at the term-end examination) or concrete (student of semester II mathematics general having a

particular Roll No), we can say without any ambiguity whether that object belongs to the collection(collection of all thoughts that came to one's mind on a particular day or the collection of all students of this class) or not.For example, the collection of 'good' students of semester II will not be a set unless the criteria of 'goodness' is made explicit!

(This property is called the well defined property).

The objects of which a set A is constituted of are called elements of the set A.

If x is an element of a set A, we write $x \in A$; otherwise $x \notin A$. Subset: If every element of a set X is an element of set Y,X is a subset of Y, written as $X \subseteq Y$.

Proper subset: X is a proper subset of Y if $X \subseteq Y$ and $Y \not\subseteq X$, written as $X \subsetneq Y$.

Equality: For two sets X = Yiff (if and only if, that is bi-implication) $X \subseteq Y$ and $Y \subseteq X$.

Null set: A set having no element is called null set, denoted by $\emptyset$.

Example1.1 $a \neq \{a\}$ (a letter inside envelope is different from a letter without envelope), $\{a\} \in \{a,\{a\}\}$, $\{a\} \subsetneq \{a,\{a\}\}$, $\emptyset \subset A$(the premise $x \in \emptyset$ of the implication $x \in \emptyset \Rightarrow x \in A$ is false but there does not exist any element in $\emptyset$ which is not in A), $A \subseteq A$, for every set A.

Set Operations: formation of new sets

Let X and Y be two sets.

Union: The union of X and Y, denoted by X∪Y, is the set {a| a∈X or a∈Y or both}.

Intersection: The intersection of X and Y, denoted by X∩ *Y*, is the set {a| a∈X and a∈Y}.

Difference: The set differenceof X and Y, denoted by X-Y, is the set {a| a∈X and a∉ Y}.

Complement: The set difference U-X is called complement of the set X, denoted by X/, where U is the universal set.

Symmetric difference: The symmetric set differenceof X and Y, denoted by X*Δ Y*, is the set (X-Y) U(Y-X).

Power set: For any set X, the power setof X, *P*(X), is the set of all subsets of X.

Disjoint sets: Two sets X and Y are disjointiff X∩ *Y*= ∅.

Cartesian product: The Cartesian productof X and Y, denoted by Xx Y, is defined as the set {(x,y)| x∈X, y∈Y} [(x,y) is called an ordered pair.

Two ordered pairs (x,y) and (u,v) are equal, written (x,y) = (u,v), iff x = u and y = v].

If we take X = {1,2} and Y = {3},

then X x Y = {(1,3),(2,3)} ≠{(3,1),(3,2)} = Y xX.

Thus Cartesian product between two distinct sets are not necessarilycommutative .

(Is Øx {1} = {1} x Ø).

Laws governing set operations

For sets X, Y, Z,

- Idempotent laws: X∪ $X = X$, X∩X = X
- Commutative laws: X∪Y = Y∪X, X∩Y = Y∩ X
- Associative Laws: (X∪Y) ∪Z = X∪(Y∪Z), (X∩Y) ∩Z = X∩(Y∩ Z)
- Distributive laws: X∪(Y∩Z) = (X∪ Y) ∩(X∪Z), X∩(Y∪Z) = (X∩ Y) ∪(X∩Z)
- Absorptive laws: X∩(X∪Y)=X, X∪(X∩Y)=X
- De' Morgan's laws: X-(Y∪Z) = (X-Y) ∩(X-Z),
  X-(Y∩Z) = (X-Y) ∪(X-Z)

Note:We may compare between usual addition and multiplication of real numbers on one hand and union and intersection of sets on the other. We see that the analogy is not complete, e.g. union and

intersection both are distributive over the other but addition is not distributive over multiplication though multiplication over addition is. Also A∪ $A = A$, for all set A but a.a = a does not hold for all real a.

Example1.2 Let A, B, C be three sets such that A∩C = B∩C and A∩C/ = B∩C/ holds. Prove that A = B.

Solution: A = A∩U (U stands for the universal set concerned)

= A∩(C∪C/)(definition of complement of a set)

=(A∩C) ∪(A∩C/)(distributivity of ∩ $over$ ∪)

=(B∩C) ∪(B∩C/)(given conditions)

= B∩(C∪C/)(distributivity of ∩ $over$ ∪)

=B

Note: Make a habit of citing appropriate law at each step as far as practicable.

Example1.3 Let A, B, C be three sets such that A∩B = A∩C and A∪B = A∪ C, then prove B = C.

Solution: B= B∪(A∩B) = B∪(A∩ C)

=(B∪A) ∩(B∪C)(distributivity of ∪over∩)

= (C∪A) ∩(B∪C) = C∪(A∩B)= C∪(A∩ C) = C.

Example1.4 $A\Delta C = B\Delta C$ implies A = B: prove or disprove.

Note: Proving any result will involve consideration of arbitrary cases, whereas to disprove a result it is sufficient to give a counter-example.

Solution: This is a true statement. We first prove A⊆B.

Let x∈A.

Case 1: x∈C. Then x∉ (A-C) ∪(C-A) = $A\Delta C$ = $B\Delta C$ = (B-C) ∪(C-B). Thus x∉ $C - B$. Since x∈C , therefore x∈ B.

Case 2: x∉C. x∈ (A-C) ⊆ $A\Delta C$ = $B\Delta C$ = (B-C) ∪(C-B). Since x∉C, x∉C-B.Thus x∈B-C. So x∈ B.

Combining the two cases, we see A⊆ B. Similarly, B⊆A. Combining, A = B.

Example1.5 Prove or disprove:$(A-B)^{/} = (B-A)^{/}$.

Solution: This is a FALSE statement. So we give a counterexample:Let U = A = {1,2}, B = {1}.Then $(A-B)^{/}$ = {1} ≠ $(B-A)^{/}$ = {1,2}.

Example1.6 Prove: [(A-B) ∪(A∩B)] ∩[(B-A) ∪$(A\cup B)^{/}$] = ∅

Solution: By repeated distributivity,

L.H.S. of the given expression

=[(A-B)∩(B-A)] ∪[(A-B) ∩ (A∪B)/] ∪[(A∩B) ∩ (B − A)] ∪[(A∩B) ∩ $(A \cup B)]^{/}$]

= ∅ ∪[(A-B) ∩(A/∩B/)]∪ ∅ ∪ ∅ = ∅.

Example1.7 Prove: A∆(B∆C)=(A∆B) ∆C.

Solution: Let x∈A∆(B∆C)=[A-(B∆C)] ∪[(B∆C)-A]

Case1: x∈A-(B∆C). x∈A, x∉ (B-C) ∪(C-B). Thus x∈A, x∉B∪C. x∈A-B, x∉C.Hence x∈ A∆B, x∉C. Thus x ∈(A∆B)-C⊆ (A∆B) ∆C.

Case 2: x∈(B∆C)-A. x∈ (B-C) ∪(C-B), x∉A. If x∈ (B-C), x∉A, then x∈B-A⊆A∆B, x∉C and hence x∈(A∆B)-C⊆(A∆B) ∆C. If x∈ (C-B), x∉A, then x∈C, x∉B,x∉A; hence x∈C, x∉A∆B and so x∈C-(A∆B) ⊆(A∆B) ∆C.

Combining the two cases, A∆(B∆C) ⊆ (A∆B) ∆C. Similarly other part can be proved.

PRACTICE SUMS

1. Prove or disprove: A∪(B-C) = (A∪B) – (A∪C)
2. Prove or disprove: A-C = B-C iffA∪C = B∪C.(“ iff ” stands for if and only if)
3. Prove :A X (B∪C) = (A X B) ∪ (A X C)

Throughout this discussion, N,Z,Q,R,C will denote set of all positive integers, integers, rational numbers ,real numbers and the complex numbers respectively.

BINARY RELATIONS

Definition1.1 A binary relation R from a set A to a set B is a subset of AxB. A binary relation (we shall often refer to as relation) from A to A is called a binary relation on A. If $(a,b)\in R$, we say a is R-related to b, written as aRb.

Example1.7 Let $A=\{1,2,3\}$ and $R=\{(1,1),(1,3)\}$. Then 1R3 holds but 3R1 does not hold.

Example1.8 Let A be a set and $\mathcal{P}(A)$ denote the power set of A. Given any two subsets X and Y of A, that is, $X,Y\in\mathcal{P}(A)$, either $X\subseteq Y$ or $X\nsubseteq Y$. Thus $\subseteq$ is a binary relation on $\mathcal{P}(A)$.

Example1.9 $R=\{(x,y)\in R^2/\ x^2+y^2=9\}$ is a relation on R.

Definition1.2 Let R be a binary relation on a set A.

- R is reflexive iff aRa holds $\forall a\in A$
- R is symmetric iff $a,b\in A$ and aRb imply bRa
- R is transitive iff $a,b,c\in A$, aRb , bRc imply aRc
- R is an equivalence relationon A iff R is reflexive, symmetric and transitive.

Example1.10 Let R be a relation defined on Z by aRb iff ab≥0. R is reflexive, symmetric but not transitive: -5R0 , 0R7 but -5R7 does not hold.

Example1.11 Let S be a binary relation on the set R of real numbers .

xSy iff	Reflexive	Symmetric	Transitive
y=2x	X	X	X
x<y	X	X	Yes
x≠y	X	Yes	X
xy>0	X	Yes	Yes
y≠ x +2	Yes	X	X
x≤y	Yes	X	Yes
xy≥0	Yes	Yes	X
x=y	Yes	Yes	Yes

Definition 1.2Let R be an equivalence relation on a set A. Let a∈A. [a]={x∈A/xRa} (⊆A) is the equivalence class determined by a with respect to R.

Definition 1.3 Let A be a nonempty set and$\mathcal{P}$be a collection of nonempty subsets of A. Then $\mathcal{P}$ is a partition of A iff

(1) for X,Y∈$\mathcal{P}$, either X=Y or X∩Y=∅ and (2) A=$\bigcup_{X\in \mathrm{P}} X$.

Theorem 1.1 : Let R be an equivalence relation on a set A. Then (1) $[a] \neq \emptyset$, $\forall a \in A$,

(2) $b \in [a]$ iff $[b]=[a]$,

(3) either $[a]=[b]$or $[a] \cap [b]=\emptyset$,

(4) $A=\bigcup_{a \in A}[a]$.

Thus $\{[a]/\ a \in A\}$ is a partition of A.

Proof: (1) since R is reflexive, $(a,a) \in R\ \forall\ a \in A$. Thus $a \in [a]$. Hence $[a] \neq \emptyset$, $\forall a \in A$.

(2) if $[b]=[a]$, then $b \in [b]=[a]$. Conversely, let $b \in [a]$. Then aRb. For $x \in [a]$, xRa holds and , by transitivity of R, xRb holds, that is , $x \in [b]$. Hence $[a] \subseteq [b]$. Similarly $[b] \subseteq [a]$ can be proved . Hence $[b]=[a]$.

(3) Let $[a] \cap [b] \neq \emptyset$. Let $x \in [a] \cap [b]$. Then aRx, xRb imply aRb, that is, $[a]=[b]$.

(4) by definition, $[a] \subseteq A$, $a \in A$. Thus,$\bigcup_{a \in A}[a] \subseteq A$. conversely, let $b \in A$. Then $b \in [b] \subseteq \bigcup_{a \in A}[a]$. Thus $A \subseteq \bigcup_{a \in A}[a]$.Hence $A=\bigcup_{a \in A}[a]$.

Theorem 1.2 :Let $\mathcal{P}$ be a partition of a given set A. Define a relation R on A as follows:

for all $a,b \in A$, aRb iff there exists $B \in \mathcal{P}$ such that $a,b \in B$.

Then R is an equivalence relation on A.

Proof: Left as an exercise.

Example1.12 Verify whether the following relations on the set R of real numbers are equivalence relations: (1) aRbiff$|a-b|>0$, (2) aRb iff 1+ab>0, (3) aRb iff$|a|$≤b

Solution: (1)R is neither reflexive nor transitive but symmetric: 1R0 and 0R1 hold but 1R1 does not hold.

(2) R is reflexive and symmetric but not transitive:

3R(-$\frac{1}{9}$) and (-$\frac{1}{9}$)$R(-6)$hold but 3R(-6) does not hold.

(3)(-2)R(-2)does not hold: not reflexive. -2R5 holds but 5R-2 does not: R not symmetric. Let pRq and qRs hold. Then $|p|$≤q≤$|q|$≤s imply pRs hold.

Example1.13 Verify whether the following relations on the set Z of integers are equivalence relations:

(1) aRb iff $|a-b|\leq 3$,

(2) aRb iff a-b is a multiple of 6,

(3) aRb iff a^2-b^2 is a multiple of 7,

(4) aRb iff $|a|=|b|$,

(5) aRb iff 2a+b=41.

Example1.14 Let X≠ ∅. Prove that the following conditions are equivalent:

(1) Ris an equivalence relation on X,

(2) R is reflexive and for all x,y,z∈X, xRy and yRz imply zRx,

(3)R is reflexive and for all x,y,z∈X, xRy and xRz imply yRz.

Example1.15 A relation R on the set of all nonzero complex numbers is defined by uRv iff $\frac{u-v}{u+v}$ is real. Prove that R is not an equivalence relation .

Solution: Note that iR2i, 2iR(-i) but (i,-i) does not belong to R.

Example1.15 A relation S on R^2 is defined by $(a_1,b_1)S(a_2,b_2)$ iff $\sqrt{{a_1}^2+{b_1}^2}=\sqrt{{a_2}^2+{b_2}^2}$. Prove that S is an equivalence relation and find equivalence class [(1,1)].

Definition 1.4 A function from a set A to a set B, denoted by f: A→B, is a binary relation from A to B satisfying the properties:

- ✓ For every x∈A, there exists y∈B such that (x,y) ∈f. y is called image of x under f and denoted by f(x) . x is called a pre-image of y=f(x) under f . A is called domain and B is called the co-domain of the correspondence.

- ✓ Note that we differentiate between f, the correspondence, and f(x), the image of x under f.
- ✓ For a fixed $x \in A$, $f(x) \in B$ is unique. For two different elements x and y of A, images f(x) and f(y) may be same or may be different.

In brief, a function is a binary relation under which

- ➢ both existence and uniqueness of image of all elements of the domain is guaranteed but
- ➢ neither the existence nor the uniqueness of pre-image of an element of co-domain is guaranteed.

Notation: Let $f:A \to B$. For $y \in B$, if y has no pre-image under f , then $f^{-1}(\{y\}) = \emptyset$, and if y has at least one pre-image under f, $f^{-1}(\{y\})$ stands for the set of all pre-images of y. For two elements $y_1, y_2 \in B$, $f^{-1}(\{y_1, y_2\}) = f^{-1}(\{y_1\}) \cup f^{-1}(\{y_2\})$. For $C \subseteq A$, $f(C) = \{f(c) | c \in C\}$. f(A) is called the range of f.

Example1.16 Prove that $f(A \cap B) \subseteq f(A) \cap f(B)$; give a counterexample to establish that the reverse inclusion may not hold.

Solution: $y \in f(A \cap B) \Rightarrow y = f(x), x \in A \cap B \Rightarrow y = f(x), x \in A$ and $x \in B \Rightarrow y \in f(A)$ and $y \in f(B) \Rightarrow y \in f(A) \cap f(B)$. Hence $f(A \cap B) \subseteq f(A) \cap f(B)$. Consider the counterexample: $f: R \to R, f(x) = x^2$, $A = \{2\}$, $B = \{-2\}$.

Example1.17 Let f: R→R, f(x) = $3x^2$-5. f(x) = 70 implies x = ±5. Thus $f^{-1}\{70\} = \{-5, 5\}$. Hence $f[f^{-1}\{70\}] = \{f(-5), f(-5)\} = \{70\}$. Also, $f^{-1}(\{-11\}) = \emptyset$ $[x \in f^{-1}(\{-11\}) \Rightarrow 3x^2-5=-11 \Rightarrow x^2=-2]$.

Example1.18 Let g: R→R be defined by $g(x) = \frac{x}{x^2+1}$. Find $g^{-1}(\{2\})$.

PRACTICE SUMS

Prove that (1) $f(A \cup B) = f(A) \cup f(B)$, (2) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, (3) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$, (4) $A \subseteq f^{-1}(f(A))$, $f(f^{-1}(B)) \subseteq B$.

Definition 1.5A function under which uniqueness of pre-image is guaranteed is called an injective function. Thus f:A→B is injective iff $a_1, a_2 \in A$, $f(a_1)=f(a_2)$ imply $a_1=a_2$. A function under which existence of pre-image is guaranteed is called a surjective function. f is surjective iff codomain and range coincide, that is, for every y∈B, there exists x∈A such that f(x)=y. A function which is both injective and surjective is called bijective.

Note: The injectivity, surjectivity and bijectivity depends very much on the domain and codomain sets and may well change with the variation of those sets even if the functional rule remains unaltered. e.g.f:Z→Z, $f(x) = x^2$is not injective though g:N→Z, $g(x) = x^2$ is injective.

Example1.19 f: R→R, $f(x) = x^2 - 3x+4$. $f(x_1) = f(x_2)$ implies $(x_1-x_2)(x_1+x_2-3) = 0$. Thus $f(1) = f(2)$ though $1\neq 2$; hence f is not injective.

[Note: for establishing non-injectivity, it is sufficient to consider particular values of x]. Let $y\in R$ and $x\in f^{-1}\{y\}$. Then $y = f(x) = x^2 - 3x+4$. We get a quadratic equation $x^2 - 3x+(4-y) = 0$ whose roots, considered as a quadratic in x, give preimage(s) of y. But the quadratic will have real roots if the discriminant $4y-7\geq 0$, that is , only when $y\geq 7/4$. Thus, for example, $f^{-1}\{1\} =\emptyset$. Hence f is not surjective.

Example1.19 Let $f :X\to Y$ Prove that (1) f is injective iff $A=f^{-1}(f(A))$, for all $A\subseteq X$, (2) f is surjective iff $f(f^{-1}(B))=B$, for all $B\subseteq Y$

(1) Let f be injective. $A\subseteq f^{-1}(f(A))$ holds generally. Let $x\in f^{-1}(f(A))$. Then $f(x) \in f(A)$; so $f(x)=f(a)$,for some $a\in A$. Since f is injective, $x=a\in A$. Thus $f^{-1}(f(A)) \subseteq A$.

Conversely, let $A=f^{-1}(f(A))$, for all $A\subseteq X$. Let $y\in Y$ and let there exist$x\in X$ such that $f(x)=y$. By given condition, $\{x\}=f^{-1}\{f(x)\}$; thus x is the only preimage that f(x) has; hence f is injective.

Definition 1.6If $f:A\to B$ and $g:B\to C$, we can define a function $g_0f:A\to C$, called the composition of f and g, by $(g_0f)(a) = g(f(a))$, $a\in A$.

Example1.20 $f:Z\to Z$ and $g: Z\to Z$ by $f(n) = (-1)^n$ and $g(n) = 2n$. Then $g_0f: Z\to Z$, $(g_0f)(n)=g((-1)^n) = 2(-1)^n$ and $(f_0g)(n) = (-1)^{2n}$. Thus $g_0f\neq f_0g$.Commutativity of composition of functionsneed not hold.

ASSOCIATIVITY OF COMPOSITION OF FUNCTIONS

Theorem 1.3Let $f: A\to B$, $g: B\to C$ and $h: C\to D$. Then $h_0(g_0f)=(h_0g)_0f$.

Proof: Both $h_0(g_0f):A\to D$ and $(h_0g)_0f: A\to D$. For $x\in A$, $[h_0(g_0f)](x) = h[(g_0f)(x)]=h[g(f(x))]$ and $[(h_0g)_0f](x)=(h_0g)(f(x))=h[g(f(x))]$. Hence $[h_0(g_0f)](x)=[(h_0g)_0f](x)$, $\forall x\in A$.

Theorem 1.4Suppose $f: A\to B$ and $g: B\to C$. Then

(1) if f and g are both injective, then g_0f is injective
(2) if g_0f is injective, then fis injective
(3) if f and g are both surjective, then g_0f is surjective
(4) if g_0f is surjective, then g is surjective

Proof: Left as an exercise.

Definition1.7Let $f: A\to A$. Define $f^0(a)=a$, $f^1(a)=f(a)$, $f^{n+1}(a)=(f_0f^n)(a)$ for all $a\in A$ and for all natural number n.

Lemma 1.1Let $f: A\to A$ be injective. Then $f^n: A\to A$ is injective for all natural number n.

Proof: If possible, let there exists positive integer n such that f^n is not injective: let k be the smallest such positive integer(by well-ordering property of N).

Thus there exist a,b∈A, a≠b such that $f^k(a)=f^k(b)$ holds.

Now $f^k(a)=f^k(b)$

$\Rightarrow f[f^{k-1}(a)]=f[f^{k-1}(b)]$

$\Rightarrow f^{k-1}(a)=f^{k-1}(b)$ (since f is injective)

$\Rightarrow a=b$ (since f^{k-1} is injective),

which contradicts the assumption that a≠b . Hence the proof.

Theorem 1.5Let A be finite and f: A→A be injective. Then f is surjective.

Proof: Let a∈A. Let $B=\{a, f(a), f^2(a),\ldots\}\subseteq A$. Since A is finite, there exist positive integers r and s such that r>s and $f^r(a)=f^s(a)$. By injectivity of f^s, $f^{r-s}(a)=a$. If r-s = 1, $a\in f^{-1}\{a\}$. If r-s>1, then $f^{r-s-1}(a)$ is a pre-image of a under f. Hence the result.

Definition 1.8Let f:A→B. f is called left(right) invertibleif there exists g:B→A (resp. h:B→A) such that $g_0f=I_A$(resp. $f_0h=I_B$). f is invertible iff f is both left and right invertible.

Example1.21 (1) Let f, g :N→N , f(n)=n+1; g(1)=1, g(n)=n-1 for n>1. Then $g_0f=I_N$. But $(f_0g)(1)=2$; so $f_0g\neq I_N$. Thus g is a left but not a right inverse of f.

(2) Let f:Z→E (E is the set of all even nonnegative integers), f(x)=x+|x| and g:E→Z, g(x)=x/2. Then $f_0g=I_E$ but $(g_0f)(-1)=0$ hence $g_0f\neq I_Z$. Hence g is right but not left inverse of f.

(3) Let f,g: R→R, f(x)=3x+4, $g(x)=\frac{x-4}{3}$. Then $g_0f = f_0g=I_R$. Thus g is both left and right inverse of f.

Note If g:B→A and h:B→A be a left inverse and a right inverse of f:A→B, then g=h , for $g=g_0I_B=g_0(f_0h)=(g_0f)_0h=I_{A0}h=h$. as we shall see below, a function may have many left (right) inverses without having any right(left respectively) inverse.

Theorem 1.6Let f:A→B. Then (1) f is left invertible iff f is injective, (2) f is right invertible iff f is surjective (3) f is invertible iff f is bijective.

Proof: (1) Let f be left invertible.

Then there exists g:B→A such that $g_0f=I_A$. Then

$f(a_1)=f(a_2),a_1,a_2\in A \Rightarrow g(f(a_1))=g(f(a_2))$

$\Rightarrow(g_0f)(a_1)=(g_0f)(a_2)$

$\Rightarrow I_A(a_1)=I_A(a_2)$

$\Rightarrow a_1=a_2$. Hence f is injective.

Conversely, let f be injective. Fix $a_0 \in A$.

Define g:B→A by : g(b)=a, if a be the unique preimage of b under f

(byinjectivityof f, if preimage of b exists under f, it is unique)

and $g(b)=a_0$,if b has no preimage under f.

Clearly g:B→A is a function and $(g_0f)(a)=g(f(a))=a=I_A(a), \forall a \in A$

(by the definition of g)

Hence g is a left inverse of f.

Example1.22 Verify whether the following functions are injective and/or surjective:(i)f:R→R, $f(x) = x|x|$, (ii)f: (-1,1) →R, $f(x) = \frac{x}{1+|x|}$.

Example1.23Let f:A→B. Prove that (1) f is injective iff $X=f^{-1}(f(X))$ for all X⊆A, (2) f is surjectiveiff $f(f^{-1}(Y))=Y$ for all Y⊆B, (3) if f is injective, then f (Y-Z)⊆f(Y)-f(Z) for Y,Z⊆A.

Example1.24 Prove that $f(X \cup Y)=f(X) \cup f(Y)$, $f(X \cap Y) \subseteq f(X) \cap f(Y)$; give counterexample to show that the inclusion may be strict (f:R→R, $f(x)=x^2$, X={2},Y={-2}).

Definition 1.9 Let f:A→B be a bijective function. We can define a function f^{-1}: B→ A by $f^{-1}(y) = x$ iff f(x) = y. Convince yourself that because of uniqueness and existence of preimage under f(since f is

injective and surjective), f^{-1} is indeed a function. The function f^{-1} is called the inverse functionto f.

Example1.25 Let f: (0,1) →(1/2,2/3) be defined by f(x) = $\frac{x+1}{x+2}$. Verify that f is bijective.

[explanation:f(x)=f(y)⇒$\frac{x+1}{x+2}$=$\frac{y+1}{y+2}$⇒x=y.

Next let c ∈(1/2,2/3).

If possible, let x be a pre-image of c under f, that is, f(x)=c.

Then c=$\frac{x+1}{x+2}$ implying x=$\frac{1-2c}{c-1}$ ∈(0,1)

since -1/2<c-1<-1/3, -1/3<1-2c<0.

f^{-1}: (1/2,2/3) → (0,1)is to be found.

Now, let f^{-1}(y) = x,y∈ (1/2, 2/3).

Then f(x) = y.

So $\frac{x+1}{x+2}$=y and hence x = $\frac{1-2y}{y-1}$ = f^{-1}(y).

BINARY OPERATIONS

Definition 1.10 Let A≠∅. A binary operation'$_0$' on A is a function from Ax A to A. In other words , a binary operation '$_0$' on A is a rule of correspondence that assigns to each ordered pair (a_1,a_2)∈ A x A,

some element of A, which we shall denote by $a_1 \,_0 a_2$. Note that $a_1 \,_0 a_2$need not bedistinct from a_1 or a_2.

Example1.26 Subtraction is a binary operation on Z but not on N; division is a binary operation on the set Q^* of all nonzero rational number but not on Z.

Definition 1.11 Let $_0$be a binary operation on A≠∅.

$(A,_0)$is called a mathematical system.

$_0$ is commutative iff $x_0y = y_0x$ holds ,for all x,y∈A.

$_0$ is associativeiff $x_0(y_0z) = (x_0y)_0z$ holds for all x,y,z∈A.

An element e∈A is aleftidentity of the system $(A,_0)$ iff $e_0x = x$ holds ∀x∈A.

An element e∈A is a right identity of the system $(A,_0)$ iff $x_0e = x$ holds ∀x∈A.

An element in a system which is both a left and a right identity of the system is called anidentityof the sytem.

$(A,_0)$ be a system with an identity e and let x, y∈A such that $x_0y = e$ holds. Then y(x) is called aright inverseto x(x is a left inverseof y respectively) in $(A,_0)$.y ∈ A is an inverse to x∈A iff $x_0y=y_0x=e$.

Example1.27 Consider the system $(R,_0)$ defined by $x_0y = x$, $\forall x,y \in R$ (R stands for the set of real numbers). Verify that $_0$ is non-commutative, associative binary operation and that $(R,_0)$ has no left identity though$(R,_0)$ has infinite number of right identity.

Example1.28 Verify that subtraction is neither associative nor commutative binary operation on Z. (Z,-) does not have any identity.

Example1.29 Consider the system $(Z,*)$ where the binary operation $*$ is defined by $a*b = |a + b|$, $a,b \in Z$. Verify that $*$ is commutative but not associative [note: to show that $*$is not associative, it is sufficient to give an example, say, $\{(-1)*2\}*(-3) \neq (-1)*\{2*(-3)\}$].

$(Z,*)$ does not have an identity.

Example1.30 (R,+) is commutative, associative, possesses an identity element 0 and every element of (R,+) has an inverse in (R,+).

Note: From examples 1.12 to 1.15 it is clear that associativity and commutativity of a binary operation are properties independent of each other, that is, one can not be deduced from the other.

Example1.31 Let 2Z denote set of all even integers. 2Z, under usual multiplication, form a system which is associative, commutative but possesses no identity.

Example1.32 Let $M_2(Z) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in Z \right\}$. $M_2(Z)$ under usual matrix addition forms a system which is commutative, associative. $(M_2(Z),+)$ possesses an identity, namely the null matrix, and every element in $(M_2(Z),+)$ has an inverse in $(M_2(Z),+)$.

Example1.33 Let GL(2,R) denote the set of all 2x2 real non-singular matrices under usual matrix multiplication. The system is associative, non-commutative, possesses an identity and every element has an inverse in the system.

SEMIGROUP, MONOID AND GROUP

Definition 1.12A nonempty setS with an associative binary operation '.'defined on S forms a semigroup. A semigroup M that contains an identity element is called a Monoid . A monoid in which every element is invertible is called aGroup . Thus (G,.) is a group iff following conditions are satisfied:

(1) .is associative,

(2) (G,.) has an identity element, generally denoted by e and

(3) every element $x \in G$ has an inverse element $x^{-1} \in G$.

If, in addition, (G,.) is commutative , (G,.) is an abelian group.

Note: x^{-1} is not to be confused with $1/x$, which may be a meaningless expression keeping the generality of the underlying set into account.If the group operation is denoted by '+', then inverse of x is denoted by – x.

Example1.34 Verify whether $(Z,_0)$ defined by $a_0b = a+b – ab$ (usual operations on Z on the RHS) forms a group.

» $(a_0b)_0c = (a+b – ab)_0c = (a+b – ab)+c – (a+b-ab)c = a+b+c – ab – bc – ca+ abc$

$a_0(b_0c) = a_0(b+c – bc) = a+(b+c – bc) – a(b+c – bc) = a+b+c – ab – bc – ca+abc.$

So, $(a_0b)_0c = a_0(b_0c)$, for $a,b,c\in Z$. Thus $(Z,_0)$ is associative.

Clearly, $a_00 = 0_0a = a$, $\forall a\in Z$. Thus $(Z,_0)$ possesses an identity $0\in Z$.

Let $a\in z$ and $b\in Z$ be an inverse to a. by definition, $a_0b = b_0a = 0$. Thus $a+b – ab = 0$. Hence , for $a\neq 1$, $b = a/(a-1)$. But , in particular, for $a = 3$, $b = 3/2\notin Z$. Hence $(Z,_0)$ does NOT form a group.

Example1.35 Verify whether $(R,_0)$ defined by $a_0b = |a| + |b|$, $a,b\in R$ forms a group.

» Verify that$(R,_0)$ is associative and commutative. If $(R,_0)$ has an identity $e\in R$, then $a_0e = e_0a = a$ holds for all $a \in R$. Thus $|a| + |e| = a$.

hence $|e| = a - |a|<0$ for a<0, contradiction. Hence $(R,_0)$ has no identity element and hence does not form a group.

Example1.36 Let $A\neq \emptyset$ and $X=\{f/f:A\rightarrow B\}$. The system $(X,_0)$ where $_0$ is composition of functions, is associative but not commutative if A contains at least three elements.

Example1.37 Let n be a natural number. Define a binary relation S on Z by:aSbiff a-b=nk, $\exists k\in Z$. S is an equivalence relation and the set of equivalence classes $Z_n= \{[0],[1],\ldots,[n-1]\}$ form a partition of Z, where $[r] = \{nk+r/\ k\in Z\}$. define a binary operation $+_n$ on Z_n by: $[r]+_n[s]=[r+s]$, $\forall [r],[s]\in Z_n$. the definition is meaningful :If $[r]=[r_1]$ and $[s]=[s_1]$, then $r=nk+r_1$ and $s=nm+s_1$ and hence $r+s=(k+m)n+(r_1+s_1)$ so that $[r+s]=[r_1+s_1]$. $+_n$ is associative: $([r]+_n[s])+_n[t]=[r+s]+_n[t]=[(r+s)+t]=[r+(s+t)]=[r]+_n([s]+_n[t])$. [0] is an identity in $(Z_n,+_n)$. inverse of [0] is [0] and inverse of [r] is [n-r], 0<r<n. Thus $(Z_n,+_n)$ is an anabelian group.

Example1.38 Let n be a prime integer and let $Z_n=\{[1],[2],\ldots,[n-1]\}$. Define $[r]._n[s]=[rs]$. Definition is meaningful: $[r]=[r_1]$ and $[s]=[s_1]$ imply $r=kn+r_1, s=mn+s_1, \exists k,m\in Z$, so that $rs=n(mr_1+ks_1+kmn)+r_1s_1$ implying $[rs]=[r_1s_1]$. Associativity of $._n$ follows from associativity of ..[1] is an identity of $(Z_n,._n)$. Let $[r]\in Z_n$, $1\leq r<n$. since n is prime, r and n are relatively prime so that there exist integers p,q such that

1=pr+qn. Thus [1]=[pr+qn]=[pr]=[p].$_n$[r]=[r].$_n$[p] implying [p] is an inverse of [r]. hence (Z_n,.$_n$) is an abelian group.

Note: If n is not prime, (Z_n,.$_n$) is not a group: if 1<p<n,1<q<n,n=pq , p,q natural, then [p],[q]∈Z_n but [pq]=[n]=[0]∉Z_n.

Example1.39 Let X≠ ∅ and S(X) be the set of all bijective functions from X onto X. Then (S(X),$_0$)is a group. If X contains at least three elements, then S(X) is not commutative. Consider f,g∈ S(X) defined by f(a)=a, f(b)=c,f(c)=b; g(a)=b,g(b)=a,g(c)=c. Then (f_0g)(a)≠(g_0f)(a). Hence f_0g≠g_0f.

Example1.40 consider the group GL(2,R), the set of all 2x2 real nonsingular matrices with usual multiplication of matrices. GL(2,R) is non-commutative.

PRACTICE SUMS

Verify whether following system forms group or not:

(1) (Z,$_0$) , a$_0$b = a|*b*|, a,b∈Z

(2) (Z,$_0$) , a$_0$b = a+b+2

(3) (2Z+1,$_*$), a$_*$b = a+b-1 [2Z+1 stands for set of all odd integers]

(4) Let S≠ ∅ and *P*(S) be the power set of S. Consider (*P*(S),∩).

(5) Let S≠ ∅ and *P*(S) be the power set of S. Consider (*P*(S),*Δ*).

(6) Let $Q[\sqrt{2}] = \{a+\sqrt{2}\, b \mid a,b \in Q\}$. consider $(Q[\sqrt{2}]-\{0\},.)$

Elementary properties of Group

Theorem 1.7 Let (G,.) be a group. The following properties hold:

(1) If G has a left identity e and a right identity f, then e=f. In particular, identity element in G is unique.

(2) If an element x of G has a left inverse y and a right inverse z, then y=z. In particular, x^{-1}, inverse element to x, is unique.

(3) $e^{-1} = e$, $(x^{-1})^{-1} = x$, $\forall x \in G$.

(4) (Cancellation Laws) for a,b,c∈G,

a.c = b.c⇒a = b(right cancellation property)

c.a = c.b⇒a = b(left cancellation property)

(5) $(a.b)^{-1} = b^{-1}.a^{-1}$, a,b∈G.

Proof: (1) Let e,f be two identities of (G,.). Then e = e.f (f is a right identity element) = f (e is a left identity element).

(2) y.x = e and x.z = e. Then y = y.e = y.(x.z) = (y.x).z = e.z = z. Hence x^{-1}, inverse element for given x is unique.

(3) Since e.e= e and $x.x^{-1}=x^{-1}.x$= e, it follows from definition of identity and inverse element.

(4) $a.c = b.c \Rightarrow (a.c).c^{-1} = (b.c).c^{-1} \Rightarrow a.(c.c^{-1}) = b.(c.c^{-1})$ (associativity) $\Rightarrow a.e = b.e \Rightarrow a = b$.

(5) $(a.b).(b^{-1}.a^{-1}) = a.(b.b^{-1}).a^{-1} = (a.e).a^{-1} = a.a^{-1} = e$.

Similarly$(b^{-1}.a^{-1}).(a.b) = e$. Hence the result follows.

Notation: Let G be a group, $a \in G$, $n \in Z$.

Then $a^0 = e$(identity), $a^n = ((a.a)\ldots a)$, (n times, $n \in N$), $a^{-n} = (a^{-1}).(a^{-1})\ldots(a^{-1})$, (n times, $-n \in N$).

Example1.41 Let (G,.) be a group such that $(a.b)^{-1} = a^{-1}.b^{-1}$, $\forall a,b \in G$. Prove that G is abelian.

»For all $a,b \in G$, $(a.b)^{-1} = a^{-1}.b^{-1} = (b.a)^{-1}$. Hence $a.b = [(a.b)^{-1}]^{-1} = [(b.a)^{-1}]^{-1} = b.a$, $\forall a,b \in G$.

Example1.42 Let (G,.) be a finite abelian group and $G=\{a_1,a_2,\ldots,a_n\}$. Let $x = a_1.a_2\ldots.a_n \in G$. Prove that $x^2 = e$.

» using commutativity and associativity of (G,.), x^2 can be expressed as finite product of pairwise product of pair of elements of G, each pair consisting of elements which are mutually inverse to each other. Hence the result.

Example1.43 Let G be a group such that $a^2 = e$, for all $a \in G$. Prove that G is abelian.

» For a∈ G,a.a = a^2=e = a.a^{-1}⇒ a = a^{-1}⇒a.b = $a^{-1}.b^{-1}$ = $(b.a)^{-1}$ = b.a, for a,b∈G. Hence.

Example1.44 Let G be a group such that for a,b,c∈ G , a.b = c.a implies that b = c. Show that G is abelian.

» (a.b).a = a.(b.a), for a,b,c∈G (by associativity)⇒a.b = b.a

Example1.45 Prove that G is abelianiff $(a.b)^2 = a^2.b^2$, ∀a,b∈G.

» Sufficiency: a.(b.a).b = $(a.b)^2$ = (a.a)(b.b) = a.(a.b).b⇒b.a = a.b for a,b∈G.

Necessity: If G is abelian, then $(a.b)^2$ = (a.b).(a.b) = a.(b.a).b = a.(a.b).b = (a.a).(b.b) = $a^2.b^2$.

Theorem 1.8A semigroup (S,.) is a group iff (1) ∃e∈S,∀a∈S such that e.a=a and (2)∀a ∈S,∃b∈S such that b.a=e

Proof: Let Sbe a semigroup which satisfies conditions (1) and (2). Let a∈S. By (2), corresponding to a∈S, there exists b∈S such that b.a=e. For b∈S, by(2), there exists c∈S such that c.b=e. now, a=e.a=(c.b).a=c.(b.a)=c.e and a.b=(c.e).b=c.(e.b)=c.b (by(1))=e. hence a.b=b.a=e(b is not still the inverse to a!). Also, a.e=a.(b.a)=(a.b).a=e.a=a. Thus a.e=e.a=a,∀a∈S. Thus e∈S is an identity and b ∈S is an inverse of a∈S. Thus (S,.) is a group. Converse part follows from definition of a group.

Example1.46 Let J=$\left\{\begin{pmatrix} x & y \\ x & y \end{pmatrix}, x, y \in \mathrm{R}, \mathrm{x}+\mathrm{y} \neq 0\right\}$. Show that J is a semigroup under matrix multiplication . Show that J has a left identity and each element of J has a right inverse.

$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$is a left identity. Let $\begin{pmatrix} x & y \\ x & y \end{pmatrix}$ ∈J. $\begin{pmatrix} \frac{1}{x+y} & 0 \\ \frac{1}{x+y} & 0 \end{pmatrix}$is a right inverse of $\begin{pmatrix} x & y \\ x & y \end{pmatrix}$.

Theorem 1.9Asemigroup(S,.) is a group iff∀a,b∈S, the equations a.x=b and y.a=b have solutions for x and y in (S,.).

Proof: Let a∈S. The equation x.a=a has a solution ,say,u∈S. Then u.a=a.Let b∈S. The equation a.x=b has solution,say,c∈S. Thus a.c=b. Now u.b=u.(a.c)=(u.a).c (associativity in (S,.))=a.c=b. Since b∈S was arbitrary, u∈S is a left identity in (S,.). Again, the equation y.a=u has solution , say d∈S. Then d∈S is a left inverse of a in S. Thus (S,.) is a group, by previous theorem.Converse part is obvious.

Theorem 1.10 A finite semigroup (S,.) is a group iff (S,.) satisfies both the cancellation laws: for a,b,c∈S, a.b=a.c⇒b=c (left cancellation law) and b.a=c.a⇒b=c(right cancellation law).

Proof: Let (S,.) be a finite semigroup in which both the cancellation laws hold. By previous theorem, it is sufficient to show that the equations a.x=b and y.a=b have solutions in S, ∀a,b∈S. Let

$S=\{a_1,\ldots,a_n\}$. Let $a,b\in S$. clearly $A=\{a.a_1,\ldots,a.a_n\}\subseteq S$. Also all the elements of A are distinct by left cancellation law. Thus A and S contains same number of elements and $A\subseteq S$. Hence A=S. Thus $b \in S=A=\{a.a_1,\ldots,a.a_n\}$. Hence $b=a.a_i$, for some $i,1\leq i\leq n$. Thus a.x=b has solution in $S,\forall a,b\in S$. Similarly,x.a=b has solution in $S,\forall a,b\in S$. Hence (S,.) is a group. Converse part is trivial.

Note:In a semigroup, cancellation laws may or may not hold. In (N,+), cancellation laws hold. In the semigroup S of all 2x2matrices over integers under multiplication, for $A=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, B=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, C=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$, AB=AC holds but $B\neq C$.

Definition 1.13 Let (G,.) be a group, $a\in G$, $n\in Z$. $a^0=e; a^n=a.a^{n-1}$, if $n\in N$; $a^n=(a^{-1})^{-n}$, if $-n\in N$.

Definition 1.14Let (G,.) be a group and $a\in G$. If there exists positive integer n such that $a^n=e$, then the smallest such positive integern is the order of a, denoted by 0(a). If no such positive integer exist, then a is of infinite order.

NoteIn a group G, the only element of order 1 is identity. All elements in a finite group must be of finite order.

Example1.47(R,+)is an infinite groupin which all elements other than 0 are of infinite order. (P(R),Δ) is an infinite group in which all nonidentity elements are of order 2: that is, every element is of finite

order. In $(Z_6,+_6)$, elements [0],[1],[2],[3],[4],[5] have respective orders 1,6,3,2,3,6.

Theorem 1.11 Let G be a group and a∈G such that 0(a)=n. Then (1) if $a^m=e$ for some positive integer m, then n divides m, (2) for every positive integer t, $0(a^t)=\frac{n}{\gcd(t,n)}$.

Proof(1) By division algorithm of integers, ∃q,r∈Z such that m=nq+r, where 0≤r<n. Now $a^r=a^{m-nq}=a^m.(a^n)^q=e$. Since n is the smallest positive integer such that $a^n=e$ and $a^r=e$ for 0≤r<n, it follows that r=0.Thus m=nq, that is, n divides m.

(2) Let $0(a^t)=k$. then $a^{kt}=e$. By (1), n divides (kt). Then there exists r∈Zsuch that kt=nr.Letgcd(t,n)=d. then ∃u,v∈Z such that t=du, n=dv and gcd(u,v)=1. Now kt=nr implies ku=rv. Thus v divides (ku). Since gcd(u,v)=1, v divides k. thus n/d divides k. Also,

$(a^t)^{n/d}=a^{\frac{nt}{d}}=a^{nu}=(a^n)^u=e$. Since $0(a^t)=k$, k divides n/d. since k and n/d are positive integers, k=n/d. Hence, $0(a^t)=\frac{n}{\gcd(t,n)}$.

Example1.48 In a group of even order, there exists at least one nonidentity element of order 2.

» Let $A=\{g\in G/g\neq g^{-1}\}\subseteq G$. Then e∉ A and g∈ A implies $g^{-1}\in A$. Thus $A=\bigcup_{g\in A}\{g,g^{-1}\}$. Hence number of elements of A is even and so A∪{e} contains odd number of elements. Since the number of

elements of G is even, there exist g∈G such that g∉A∪{e}, so that ,g=g^{-1} and g≠e. thus 0(g)=2.

Example1.49 Let G be a group and a,b∈G, a^2=e,a.b.a=b^7. Prove b^{48}=e.

»b=a^2ba^2=ab^7a=$(aba)^7$=b^{49}. Result follows by cancellation law.

Example1.50 Let S be a semigroup such that for all a∈S, there exist x∈S such that a=a.x.a. If S has a single idempotent element, prove that S is a group.

»Let the single idempotent of S be denoted by e. Let a∈S. Then there exist x∈S such that a=axa so that ax=axax=$(ax)^2$. Thus ax is an idempotent in S and by the uniqueness of idempotent in S, ax=e. Similarly it can be shown that xa=e. Hence a=a(xa)=a.e and a=(ax)a=ea. Thus e is an identity in S. Let b∈S. then there xeisty∈S such that b=byb. Hence by and yb are idempotent and so by=yb=e. Hence S is a group.

Example1.51 Let G be a group and $(a.b)^n$=$a^n.b^n$ holds for alla,b in G and for three consecutive integers n. Prove that G is commutative.

» let $(ab)^n$=a^nb^n, $(ab)^{n+1}$=$a^{n+1}b^{n+1}$, $(ab)^{n+2}$=$a^{n+2}b^{n+2}$,∀a,b∈G.

Then $a^{n+1}b^{n+1}$=$(ab)^{n+1}$=$(a^nb^n)(ab)$⇒ab^n=b^na.

Again$a^{n+2}b^{n+2}$=$(ab)^{n+1}(ab)$=$a^{n+1}b^{n+1}ab$⇒ab^{n+2}=$b^{n+1}ab$=$b(b^na)b$=$b(ab^n)$ b⇒ab=ba. Hence.

Example1.52 Let $G=\{a_1,\ldots,a_n\}$ be a finite abelian group and $x=a_1\ldots a_n\in G$. Prove that $x^2=e$.

»using commutativity and associativity, $x^2=(a_1\ldots a_n)(a_1\ldots a_n)$can be expressed as finite products of expressions like $(a_i.a_{i_k})$, where a_i and a_{i_k} are inverse to each other. Hence $a_i.a_{i_k}=e$ and thus $x^2=e$.

Example1.53 Let G be a group and $x,y\in G$ such that $xy^2=y^3x$, $yx^2=x^3y$. Prove $x=y=e$.

» $xy^2=y^3x\Rightarrow x=y^3xy^{-2}\Rightarrow x^2=xy^3xy^{-2}=(xy^2)yxy^{-2}=(y^3x)yxy^{-2}\Rightarrow x^2y=y^3xyxy^{-1}$(1). Now $yx^2=x^3y\Rightarrow yx^2=xy^3xyxy^{-1}\Rightarrow x^2=y^{-1}xy^3xyxy^{-1}\Rightarrow x^2y=y^{-1}xy^3xyx$ (2). By (1) and (2), $y^3xyxy^{-1}=y^{-1}xy^3xyx\Rightarrow y^4xyx=xy^3xyxy\Rightarrow y^4xyx=xy^2yxyxy=y^3$ $(xy)^3\Rightarrow(yx)^2=(xy)^2$(3). Interchanging x and y in (3),we get $(xy)^2=(yx)^3$ (4). Now (3) and (4) imply $(xy)^2=(yx)^3=(yx)^2(yx)=(xy)^3(yx)\Rightarrow e=xy^2x\Rightarrow x^{-2}=y^2$. Further $xy^2=y^3x\Rightarrow xx^{-2}=yx^{-2}x\Rightarrow x^{-1}=yx^{-1}\Rightarrow y=e$. finally, $yx^2=x^3y\Rightarrow ex^2=x^3e\Rightarrow x=e$.

Example1.54Let S be a finite semi-group. Show that there is an idempotent element e inS .

» Let $x\in S$. Since S is finite, all the elements $x,x^2,x^3,\ldots$ cannot be distinct. Thus there exist integers m,n, m>n, such that $x^m=x^n$. Thus there exists integer k such that $x^{n+k}=x^n$. Now $x^{2n+k}=x^{n+k}.x^n=x^{2n}$. By induction, $x^{tn+k}=x^{tn}$ for any $t\in N$. Also $x^{tn+2k}=x^{tn+k}=x^{tn}$. By induction,

$x^{tn+lk}=x^{tn}$, for any l∈N. In particular, $x^{kn+nk}=x^{kn}$, that is, $e^2=e$, where $e=x^{kn}\in S$.

Example Let G be a group, a,b∈G. Let $(ab)^3=a^3b^3$ and $(ab)^5=a^5b^5$. Prove that ab=ba.

»$(ab)^3=a^3b^3\Rightarrow a(ba)^2b=a^3b^3\Rightarrow(ba)^2=a^2b^2$. Interchanging a and b, $(ab)^2=b^2a^2$ (1) Again, $(ab)^5=a^5b^5\Rightarrow(ab)^3(ab)^2=a^5b^5\Rightarrow a^3b^3b^2a^2=a^5b^5\Rightarrow b^5a^2=a^2b^5$(2)

Now
$(ab)^4=(ab)^3(ab)\Rightarrow a(ba)^3b=a^3b^3ab\Rightarrow(ba)^3=a^2b^3a\Rightarrow b^3a^3=a^2b^3a\Rightarrow a^2b^3=b^3a^2$(3).From (2), $b^3b^2a^2=a^2b^3b^2=b^3a^2b^2$(from (3))$\Rightarrow b^2a^2=a^2b^2\Rightarrow(ab)^2=a^2b^2$ (from (1))$\Rightarrow a(ba)b=a(ab)b\Rightarrow ab=ba$.

Example1.55Prove that a finite semigroup G with identity is a group iff G contains only one idempotent. Give a counterexample to show that if we drop the requirement of G possessing identity, then G need not be a group.

» consider the semigroup {[0],[2]} under $+_4$.

Example1.56 If G is a group in which $(ab)^2=a^2b^2$ holds ∀a,b∈G, then G is abelian. Give example to show that the result does not hold for semigroup.

» consider the semigroup (S,.), where S is any nonempty subset and a.b=a,∀a,b∈S. Then S is not a group though $(ab)^2=a^2b^2$ holds ∀a,b∈S.

Example1.57 Show that if G is a finite semigroup with cross-cancellation law, that is, xy=yz implying x=z, for all x,y,z in G, then G is an abelian group.

»xy=xz⇒x(yx)=(xz)x⇒yx=xz⇒y=z. similarly right cancellation law holds. Hence G is a group. Also (xy)x=x(yx) imply xy=yx, for all x,y in G.

Example1.58 Let Sbe a semigroup and for all x,y in S, $x^2y=y=yx^2$ hold. Prove that S is an abelian group.

»Fix x_1∈S.For all y∈S, $x_1^2y=yx_1^2=y$; hence x_1^2 is identity of S,say, e. Thus $x^2=e$, for all x∈S.Hence $x=x^{-1}$; thus every element has an inverse in S. Since $x^2=e$, for all x∈G, the group is abelian.

Example1.59 Let G be a group and a,b∈G such that a.b=b.a and 0(a) and 0(b) are relatively prime. Then prove that 0(ab)=0(a)0(b).

»Let 0(a)=m,0(b)=n,0(ab)=k. So $(ab)^{mn}=(a^m)^n(b^n)^m=e$; hence k/(mn). If k=mn, nothing remains to prove. Let mn=qpk, q positive integer and p be prime. Since p/(mn) , either p/m or p/n; say p/m.Let $m=pm_1$. Now mn=qpk implies $m_1n=qk$. $e=(ab)^k=(ab)^{qk}=(ab)^{m_1n}$ $=a^{m_1n}.(b^n)^{m_1}=a^{m_1n}$. Hence $m/(m_1n)$, that is , $(pm_1)/(m_1n)$. Thus p/n. But then p is a common factor of m and n, contradiction.

Example1.60 Find the number of elements of order 5 in $(Z_{20},+_{20})$.

»Let 0([a])=5. Then 5 is the smallest positive integer such that [0]=5[a]=[5a], that is, 20 divides 5a-0=5a. Thus 4 must divide a,0≤a<20. Hence [a]=[4],[8],[12]or[16].

Example1.61 Suppose a group G contains elements a,b such that 0(a)=4,0(b)=2, $a^3b=ba$. Find 0(ab).

»$a^3b=ba \Rightarrow e=a^4b^2=(ab)^2 \Rightarrow 0(ab)\leq 2$. If 0(ab)=1, then ab=e, $a=b^{-1}$, implying 4=0(a)=0(b)=2, contradiction.

Permutation Groups

Definition 1.15 Let $A\neq \emptyset$. A permutation on A is a bijective mapping of A onto itself. If A={1,2,…,n}, then the group S_n formed by the set of all permutations on A under composition of functions as composition is called Symmetric Group on n symbols . Order of S_n, that is , the number of elements of S_n , is n!

Notation If$\alpha \in S_n$, then we often denote α using two-row notation:$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$. In this notation, if

$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$ and $= \begin{pmatrix} 1 & 2 & \cdots & n \\ \beta(1) & \beta(2) & \cdots & \beta(n) \end{pmatrix}$,

then $\alpha 0\ \beta = \begin{pmatrix} 1 & 2 & \cdots & n \\ \beta(\alpha(1)) & \beta(\alpha(2)) & \cdots & \beta(\alpha(n)) \end{pmatrix}$.

Theorem 1.12 If n is a positive integer ,n≥3, then S_n is a noncommutative group.

Definition 1.16 A permutation α on {1,2,...,n} is a k-cycle iff there exist distinct elements $i_1,...,i_k \in \{1,2,...,n\}$ such that $\alpha(i_1)=i_2,...,\alpha(i_{k-1})=i_k$, $\alpha(i_k)=i_1$ and $\alpha(x) = x$ for all $x \in \{1,2,...,n\}-\{i_1,...,i_k\}$.we denote $\alpha$by $(i_1\ i_2\ ...i_k)$.A transposition is a 2-cycle.

NoteProduct of two cycles need not be a cycle:forα=(5 6) and β=(3 2 4), $\alpha_0\beta$ is not a cycle.

Definition 1.17Two cycles $(i_1...i_m)$ and $(j_1...j_k)$ are disjoint iff $\{i_1,...,i_m\} \cap \{j_1,...,j_k\} = \emptyset$.

Theorem 1.13Let α and β be two disjoint cycles. Then $\alpha_0\beta = \beta_0\alpha$.

Theorem 1.14 Any nonidentity permutation of S_n (n≥2) can be expressed as a product of disjoint cycles , where each cycle is of length ≥2.

Theorem 1.15 Any cycle of length≥2is either a transposition or can be expressed as a product of transpositions.

Proof Note that $(i_1\ i_2 \ldots i_k)=(i_1 i_k)_0(i_1\ i_{k-1})_0 \ldots_0(i_1\ i_2)$.

Theorem 1.16Any nonidentity permutation is either a transposition or can be expressed as a product of transpositions.

Definition 1.18A permutationα is even(odd) iff α can be expressed as product of even (odd respectively)number of transpositions.

Theorem 1.17 Any permutation in S_n is either an even permutation or an odd permutation but never both.

NoteIdentity permutation I is even since $I=(1\ 2)_0\ (2\ 1)$. If α is even, then α^{-1} is even, since $\alpha_0\alpha^{-1}=I$ and I is even. Thus A_n, the set of all even permutations on {1,2,…,n}, forms a group under composition of functions. A_n is called the alternating group.

Theorem 1.18Let $n\geq 2$ and $\alpha\in S_n$ be a cycle. Then α is a k-cycle iff $0(\alpha)=k$.

Theorem 1.19 Let $\alpha\in S_n$, $n\geq 2$, and $\alpha=\alpha_1\ _0 \ldots_0\alpha_k$ be a product of disjoint cycles. Let $0(\alpha_i)=n_i$, i=1,2,…,k. then $0(\alpha)=\text{lcm}\{n_1,n_2,\ldots,n_k\}$.

Example1.62 Show that the number of even permutations in S_n is same as the number of odd permutations in S_n.

ProofDefine $f:A_n\rightarrow(S_n-A_n)$ by $f(\alpha)=\alpha_0\ (1\ 2)$. Verify that f is bijective.

Example1.63 If $\alpha\in S_7$ and $\alpha^4=(2\ 1\ 4\ 3\ 5\ 6\ 7)$, then find α.

»7=$0(\alpha^4)=\frac{0(\alpha)}{\gcd\{4,0(\alpha)\}}$. Thus $0(\alpha)$=7,14,28. Now α is expressible as product of disjoint cycles in S_7. Thus $0(\alpha)\neq$14,28. Hence $0(\alpha)$=7. Thus α^7=I. Thus $\alpha=\alpha^8=(\alpha^4)^2$=(2 1 4 3 5 6 7)$_0$(2 1 4 3 5 6 7).

Example1.64 If α=(1 2 3)$_0$(1 4 5), write α^{99} in cycle notation.

»$\alpha^5 = I$.Thus α^{100}=I and hence $\alpha^{99}=\alpha^{-1}$=(4 1 3 2 5).

Example1.65 In S_6, let α=(1 2 3) and β=(4 5 6). Find a permutation x in S_6 such that xαx^{-1}=β.

»x$_0$ (1 2 3)=(4 5 6)$_0$x.

Attempt 1: x(1)=1.Then [(4 5 6)$_0$x](1)=1=[x$_0$(1 2 3)](1)=x(2), contradiction.

Attempt 2: x(1)=2. Then 2=[(4 5 6)$_0$x](1)=[x$_0$(1 2 3)](1)=x(2), con.

Attempt 3: x(1)=3. Then 3=[(4 5 6)$_0$x](1)=[x$_0$(1 2 3)](1)=x(2), con.

Attempt 4: x(1)=4. [(4 5 6)$_0$x](1)=5=[x$_0$(1 2 3)](1)=x(2). 6=[(4 5 6)$_0$x](2)=[x$_0$(1 2 3)](2)=x(3). Since x is a bijection, x(4),x(5),x(6) will be one of 1,2,3. Thus, [(4 5 6)$_0$x](4)=x(4)=[x$_0$(1 2 3)](4), automatically satisfied. Thus x({4,5,6})={1,2,3}. Hence one choice for x is: x(1)=4,x(2)=5,x(3)=6,x(4)=1,x(5)=2,x(6)=3.

Example1.66 Find the number of elements of order 3 in A_4.

»Let $x \in A_4, 0(x)=3$. Let $x=x_1 \, 0 \, x_2 0 \ldots 0 x_k$ be an expression of x in terms of disjoint cycles; hence $3=0(x)=$l.c.m.$\{0(x_1),\ldots,0(x_k)\}$. Thus $0(x_i)=1$ or 3. Since we can drop 1-cycle from the representation, x can be expressed as composition of disjoint 3-cycles; since there are only 4 symbols , x is a 3-cycle. For every choice of three symbols from {1,2,3,4}, there will be two 3-cycles[for example, for symbols 1,3,4, (1 3 4) and (1 4 3)are 2 3-cycles). Hence the number is 8.

Example1.67 Find the number of elements of order 6 in S_4.

Example1.68 Find the number of elements of order 2 in A_4.

SUBGROUP

Let $(G,0)$ be a group and $\emptyset \neq H \subseteq G$. H is closed under 0 iff $\forall \, h_1, h_2 \in H$, $h_1 0 h_2 \in H$. If H be closed under 0, then the restriction of 0 to H x H is a mapping from H x H into H. Thus the binary operation 0 on G induces binary operation, also denoted by 0, on H.

Definition 1.19Let $(G,0)$ be a group and $\emptyset \neq H \subseteq G$. $(H,0)$ is a subgroup of $(G,0)$ iff H is closed under 0 and $(H,0)$ is a group.

Every group G has at least two subgroups , namely, {e} and G. These are called trivial subgroups. Other subgroups, if there be any, are called nontrivial subgroups of G.

Example1.69 $(2Z,+)$ is a subgroup of $(Z,+)$, where 2Z is the set of all odd integers. Since the set 2Z+1 of all odd integers is not closed under addition of integers, (2Z+1,+) is not a subgroup. Though N is closed under addition, (N,+) does not form a group; hence (N,+) is not a subgroup of (Z,+).

Example1.70 $(A_{n,0})$ is a subgroup of $(S_{n,0})$. {[0],[2]} is a subgroup of $(Z_4,+_4)$.

Example 1.71 $\{z \in C / |z| = 1\}$ is a subgroup of the multiplicative group of all nonzero complex numbers.

Theorem 1.20 All subgroups of a group $(G,_0)$ have the same identity element. If H be a subgroup of a group G, $a \in H$ and a_G^{-1}, a_H^{-1} be the inverses of a in G and H respectively, then $a_G^{-1} = a_H^{-1}$.

Proof: Let e_G and e_H be the identities of G and H respectively. Then e_H $_0$ $e_H = e_H$ (consideringe$_H$as identity in $(H,_0)$)

$= e_{H0} e_G$ (since $e_H \in H \subseteq G$ and e_G is identity in $(G,_0)$)

So by cancellation property in $(G,_0)$, $e_H = e_G$.

Using cancellation property of G, from the equality

$a . a_G^{-1} = e_G = e_H = a . a_H^{-1}$, we conclude that $a_G^{-1} = a_H^{-1}$.

Note: $\cap\{H: H \text{ is a subgroup of } G\} \neq \emptyset$

Note: A group may be non-commutative but one of its subgroups may be commutative: $H=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} / ab \neq 0\right\}$ is acommutative subgroup of the non-commutative group GL(2,R).

Theorem 1.21 Let G be a group and $\emptyset \neq H \subseteq G$. Then H is a subgroup of G iff $a.b^{-1} \in H, \forall a,b \in H$.

Proof:Let $\emptyset \neq H \subseteq G$ and let $a.b^{-1} \in H, \forall a,b \in H$.

Since $H \neq \emptyset$, let $a \in H$.

By assumption, $e=a.a^{-1} \in H$.

Let $b \in H$. Then $b^{-1}= e.b^{-1} \in H$.

Also, for $a,b \in H$, $a,b^{-1} \in H$ and hence $a.b=a.(b^{-1})^{-1} \in H$.

Associativity, being a hereditary property, holds in (H,.) since it holds in (G,.).

Thus H is a subgroup of G.

Converse part is trivial.

Theorem 1.22 Let G be a group and $\emptyset \neq H \subseteq G$, H finite. Then H is a subgroup of G iffa.b$\in$H,$\forall$a,b$\in$H.

Proof:(sufficiency)Let h$\in$H.

Then A={h,h^2,h^3,…}$\subseteq$H.

Since H is finite, there exist integers r and s, $0 \leq r < s$ and $h^r = h^s$. Hence by cancellation property in G, $e = h^{s-r} \in H$.

Now $e = h^{s-r} = h.h^{s-r-1}$ implies $h^{-1} = h^{s-r-1} \in H$

[Note that s-r-1 is non-negative integer] .

Let $a,b \in H$. Then $a,b^{-1} \in H$. Hence by hypothesis, $a.b^{-1} \in H$.

Thus by the previous theorem, H is a subgroup of G.

Theorem 1.23The intersection of all subgroups of a group G is a subgroup of G. For two subgroups H and K of a group G, $H \cup K$ is a subgroup of G iff $H \subseteq K$ or $K \subseteq H$.

Proof: Let $\{H_x\}_x$ be the collection of all subgroups of a group G. Since $e \in \bigcap H_x$, $\bigcap H_x \neq \emptyset$. Let $a,b \in \bigcap H_x$. Then $a,b \in H_x$ and since H_x is a subgroup of G, $a.b^{-1} \in H_x$. Thus $a.b^{-1} \in \bigcap H_x$. Hence $\bigcap H_x$ is a subgroup of G.

Let H ,K and $H \cup K$ be subgroups of G. To prove:$H \subseteq K$ or $K \subseteq H$.

If possible, let $H \nsubseteq K$ and $K \nsubseteq H$.

Let $a \in H-K$, $b \in K-H$.

Since $H \cup K$ is a subgroup, $a.b^{-1} \in H \cup K$.

If $a.b^{-1} \in K$, then $a = (ab^{-1})b \in K$, contradiction.

Similarly, if $a.b^{-1} \in H$, then $b = (a.b^{-1})^{-1}.a^{-1} \in H$,contradiction.

Hence $H \cup K$ is a subgroup implies either $H \subseteq K$ or $K \subseteq H$.

Converse part is obvious.

Definition 1.20 Let G be a group. $Z(G)=\{x \in G / x.g=g.x, \forall g \in G\}$ is called the centre of G. If G is commutative, then $G=Z(G)$.

Example1.71Z(G) is a subgroup of G.

»Since $e \in Z(G)$, so $Z(G) \neq \emptyset$. Also Z(G) is a subset of G.

Let $a,b \in Z(G)$.

Then for $g \in G$, $(a.b).g=a.(b.g)=a.(g.b)=(a.g).b=(g.a).b=g.(a.b)$

So $a.b \in G$.

Again, let $a \in Z(G)$. Then $a.g=g.a, \forall g \in G$.

Then $a^{-1}.(a.g)a^{-1}=a^{-1}.(g.a).a^{-1}$ implying $g.a^{-1}=a^{-1}.g$; hence $a^{-1} \in Z(G)$.

Hence Z(G) is a subgroup of G.

Example1.72 Prove that every subgroup of (Z,+) is of the form $nZ=\{na : a \in Z\}$, where n is a non-negative integer.

» Let H be a subgroup of Z. If $H=\{0\}$, then $H=0Z$.

Let $\{0\} \subsetneq H$. Let $0 \neq a \in H$. Since H is a subgroup, $-a \in H$.

Thus H contains positive integers.

By well-ordering principle of N, the set $A=\{a\in H:a\in N\}\subseteq N$ has a smallest element,say, n. We shall prove that $H=\{nr:r\in Z\}$.

Since $n\in H$ and H is a subgroup,$\{nr:r\in Z\}\subseteq H$.

Again, let $b\in H$. By division algorithm for integers, there exist $p,r\in Z$ such that $b=pn+r, 0\leq r<n$.

So $r=b-pn\in H$(since H is a subgroup).

Since $r<n$ and n is the smallest positive integer such that $n\in H$, sor=0.

Thus $b=pn\in nZ$.

Thus $H\subseteq nZ$.

Combining the two, H=Nz.

Practice sums

1. Let G be a group and $a\in G$. Let $C(a)=\{x\in G:a.x=x.a\}$.Show that C(a) is a subgroup of G and Z(G) is contained in C(a).

2. Let G be a commutative group . Prove that the set H of all elements of G of finite order is a subgroup of G.

3. In the group S_3, show that the subset $H=\{\alpha\in S_3:0(\alpha)$ divides $2\}$ is not a subgroup of S_3.

4. In the group S_3, show that H={I,(2 3)} and K={I,(1 2)} are subgroups but H∪K is not a subgroup of S_3.

5. If a group has finitely many subgroups, then G is finite.

6. True or false: the multiplicative group R^+ of nonzero real numbers has no finite subgroups other than {1}.

[solution: Let {1}≠H be a finite subgroup of R^+. Let c∈H, c≠1. Then c^{-1}∈ H; c or c^{-1} is greater than 1. Since c^n∈ H for all integer n, c^n are distinct for distinct integral values n, H is infinite, contradiction.]

7. True or false:Let G be a group and H be a nonempty subset of G such that a^{-1}∈H for all a∈H. Then H is a subgroup.

[False; Z-{0} is not a subgroup of (Z,+).]

8. True or false:There does not exist a proper subgroup H of (Z,+) such that H contains both 5Z and 7Z.

[solution: Let H be such a subgroup; thus 1=5.3-7.2∈H; hence -1∈H. Thus for any integer n, n=1+1+…+1(n times, if n positive) , n=(-1)+…+(-1)(-n times, if n negative),0∈H; hence H=Z.]

CYCLIC GROUPS

A group G is a cyclic group iff there exists a∈G such that G=(a)={a^n:n∈Z}. Such an element a is called a generator of G.

Example1.81 (Z,+) is a cyclic group since Z=(1). (Z_n,+$_n$) is cyclic with [1] as one of its generators. (R,+) is not cyclic: a rational can not generate irrational and vice versa. The multiplicative group of all four fourth roots of unity is cyclic with i as one of its generators.

Theorem 1.24 Every cyclic group is commutative ; converse may not hold.

Proof: Let G=(a) and let b,c∈G. Then b=a^n,c=a^m, there exist integers m,n. Thus bc=a^n.a^m=a^{n+m}=a^{m+n}=a^m.a^n=cb, proving that G is abelian.

For the converse, consider the Klein's 4-group: G={e,a,b,c} with the binary operation $_0$ defined by the property a^2=b^2=c^2=e^2=e. Then G is abelian but not cyclic. [Try to construct the composition table for Klein's 4-group.]

Theorem 1.25 A finite group G is cyclic iff there exists a∈G such that 0(a)=0(G).

(0(A) stands for the number of elements of a finite set A)

Proof: Let G be a finite cyclic group of ordern. Hence there exists element a∈G such that G=(a)={a^i:i∈Z}. Since G is finite, there exist i,j∈Z with i<jsuch that a^i=a^j. Thus a^{j-i}=e, j-i∈N. Let m be the smallest

positive integer such that $a^m=e$. Then $0(a)=m$ and for all integers i,jsuch that $0\leq i<j<m$, $a^i\neq a^j$ or else $a^{j-i}=e$, which contradicts the minimality of m. Hence the elements of the set $S=\{e,a,a^2,\ldots,a^{m-1}\}$ are distinct. Clearly, $S\subseteq(a)$. Conversely, let $a^k\in(a)$. Then there exist $q,r\in Z$ such that $k=qm+r, 0\leq r<m$.

Thus $a^k=a^{qm+r}=(a^m)^q.a^r=a^r\in S$. Hence S=(a).

Since elements of S are distinct and 0((a))=n, m=n. Hence 0(a)=n.

Conversely assume G is a finite group of order n and G has an element a such that 0(a)=n. since o(a)=n, all the elements of $A=\{e,a,a^2,\ldots,a^{n-1}\}$ are distinct ,$A\subseteq G$ and 0(A)=0(G). Hence G=A=(a).

C o r o l l a r y : Let (a) be finite cyclic group. Then 0(a)=0((a)).

Example1.82 Klein's 4-group is not cyclic since it has no element of order 4.

Theorem 1.25 Let G=(a) , 0(G)=n. then for any integer k, $1\leq k<n$, a^k is a generator of G iffgcd(n,k)=1.

Proof:If $G=(a^k)$, then $0(a^k)=0(G)=n$. since G=(a), we have 0(a)=n. Thus $n=0(a^k)=\frac{0(a)}{\gcd(n,k)}=\frac{n}{\gcd(n,k)}$. So gcd(n,k)=1.

Conversely, let gcd(n,k)=1. Then $0(a^k)=\frac{0(a)}{\gcd(n,k)}=0(a)=n=0(G)$. Hence $G=(a^k)$.

Example1.82 For the group G={1,-1.i,-i}, 0(G)=4 and 1 and 3 are the only positive integers less than 4 and relatively prime to 4.Hence i and i^3=-i are the only generators of G.

Theorem 1.26 Every subgroup of a cyclic group is cyclic.

Proof: Let H be a subgroup of a cyclic group G=(a). If H={e}, then H=(e). Suppose H≠{e}. Then there exists b∈H , b≠e. Thus there exist nonzero integer m such that $b=a^m$. Since H is a subgroup, $a^{-m}=b^{-1}$∈H. either m or –m is a positive integer. Hence there exists positive integer i such that a^i∈H. Thus A={n∈N:a^n∈H} ≠ ∅. By well-ordering principle of N, A has a least element n. we prove that H=(a^n). sincea^n∈H and H is a subgroup, (a^n)⊆H. Let h∈H⊆G=(a). thusthere exist integer k such that $h=a^k$. by division algorithm for integers, there exist integers q,r such that k=nq+r,0≤r<n. thus $a^r=a^k.(a^n)^{-q}$∈H (since H is a subgroup). Since n is the smallest positive integer such that a^n∈H and 0≤r<n, r=0. Thus k=nq and so $h=a^k=a^{nq}=(a^n)^q$∈(a^n). Hence H=(a^n).

Example1.83 Find all the generators of (Z_{10},$+_{10}$).

Z_{10}=([m])=(m[1]) iffgcd(m,10)=1. Thus the generators of Z_{10} are [1],[3],[7] and [9].

Example1.84 The group (Q,+) is not cyclic. Hence (R,+) is not cyclic.

If possible, let Q=(x). Clearly, x≠0. Hence x=$\frac{p}{q}$, where p,q are prime to each other and q≠0. But $\frac{p}{2q}$∈Q=($\frac{p}{q}$), contradiction.

COSETS AND LAGRANGE'S THEOREM

Let G be a group and H be a subgroup of G. Define a relation R on G by: a,b∈G, aRbiff $a.b^{-1}$∈H. R is an equivalence relation on G. For a∈G, [a], the equivalence class containing a, is given by: [a]={b∈G:bRa}={b∈G: $b.a^{-1}$∈H}=Ha={ha:h∈H} (Ha is called right coset of H in G generated by a). We know that equivalence classes are nonempty, any two distinct equivalence classes are disjoint and union of all the equivalence classes equals G.Thus Ha∩Hb=Ha, if b∈[a]=Ha and Ha∩Hb=∅, if b∉Ha and G=∪{Ha:a∈G}. Note also that H=He, where e is the identity of G.

Lemma: Let H be a subgroup of a group G. If a∈G, then 0(aH)=0(H).

Proof: f:H→aH, f(h)=a.h, is a bijection. Hence the result.

Theorem 1.27 (Lagrange) Let H be a subgroup of a finite group G. Then0(G)=[G:H]0(H), where [G:H], the index of H in G, is the number of distinct right cosets of H in G.

Proof: Since G is finite, [G:H] is finite. Let [G:H]=r. Let A={Ha_1,Ha_2,…,Ha_r} be the collection of distinct right cosets of H in G.

Since A is a partition of G, $0(G)= 0(Ha_1)+\ldots+0(Ha_r)=r0(H)$(by lemma above). Hence the result.

Converse of Lagrange's Theorem may not hold. It can be proved that 6 divides $0(A_4)$ but A_4 has no subgroup of order 6. But the converse holds for a cyclic group.

Theorem 1.28 Let G =(a), 0(G)=n. If m is a positive integral factor of n, then there exists a unique subgroup of G of order m.

Proof: There exists positive integer k such that n=mk. Now $0(a^k)=\frac{0(a)}{\gcd(k,0(a))}=\frac{n}{k}$=m; hence $0((a^k))=0(a^k)$=m.

Now suppose K is a subgroup of G of order m. $K=(a^t)$, for some $t\in Z$. $0(a^t)=0((a^t))$=m. thus a^{mt}=e. Since 0(a)=n, n divides mt, that is, mt=nr for some integer r. By Lagrange's Theorem, n=km, for some natural k. Hence mt=kmr, so that t=kr. So $a^t=(a^k)^r\in(a^k)$=H. Hence $K=(a^t)\subseteq(a^k)$=H. Both these subgroups have order m. hence H=K.

Example1.85 Let G be a group of order 28. Show that G has a nontrivial subgroup.

»If G is cyclic, G has a subgroup corresponding to every positive integral factor of 28, say, corresponding to 4.

If G is not cyclic, consider the cyclic subgroup (a) generated by $e\neq a\in G$. Clearly $\{e\}\subsetneq(a)\subsetneq G$ (G is not cyclic).

Example1.86 Let G=(a) be an infinite cyclic group. Prove that (1) $a^r=a^t$only if r=t, r,t∈Z , (2) G has only two generators.

»Let $a^r=a^t$, r>t. then there exist natural number m such that $a^{t+m}=a^t$, so that, a^m=e. Thus 0(a) is finite and 0((a)) is infinite, contradiction.

Let (a)=G=(b), for some b∈G. Since a∈(b) and b∈(a), there exist integers r and t such that $a=b^r$, $b=a^t$. thus $a=a^{rt}$, which by part (1) implies rt=1.Thus r=1 or -1. Hence b=a or $b=a^{-1}$. Thus G has exactly two generators.

Example1.87 If a group G has only two subgroups, then G is a cyclic group.

»G≠{e} since G has two subgroups. Let H=(a), e≠a∈G. Since H≠{e} (a∈H), G=H=(a).

Example1.88 Let G be a cyclic group of order 42. Find the number of elements of order 6 and of order 7.

»LetG=(a), 0(a)=42. Let $b=a^r$∈G, o(b)=6. Then a^{6r}=e. Thus 42 must divide 6r, that is, 7 must divide r and r<42. Thus r=7,14,21,28,35. Thus there are five elements of G of order 6.

Example1.89 Let G be a cyclic group such that G has exactly three subgroups: G,{e} and a subgroup of order 5. Find the order of G.

Example1.90 Let G be a cyclic group of infinite order. Find the number of elements of finite order.

Theorem 1.29 Every group of prime order is cyclic.

Proof: Let 0(G)=p, p prime. Thus p≥2. Let e≠a∈G. Then 0((a)) divides 0(G)=p ,0((a))=0(a)>1. Thus 0((a))=p=0(G), (a)⊆G. Hence G=(a).

Theorem 1.30 Let H and K be finite subgroups of a group G. Then 0(HK)=$\frac{0(H)0(K)}{0(H\cap K)}$.

Example1.91 Let G be a group of order p^n, p prime. Prove that G contains an element of order p.

»Let e≠a∈G. Let H=(a). Then 0(a) divides 0(G)=p^n. Thus 0(H)=0(a)=p^m, 1≤m≤n. Now in the cyclic group (a) of order p^m, there exists a cyclic subgroup C=(c) of order p. Thus c∈G and 0(c)=p.

Example1.92 Let G be a group of order pqwhere p and q are prime. show that every subgroup H($\neq G$)is cyclic.

»0(H) divides pq=0(G). Since p,q are primes, 0(H)=1,p,q (note: H≠ G). Sine every group of prime order is cyclic, result follows.

Example1.93 Find all subgroups of Klein's 4-group.

Example1.94 Prove that every proper subgroup of S_3 is cyclic though S_3 is not cyclic.

Example1.95 Prove that every group of order 49 contains a subgroup of order 7.

Example1.96 Let G be a group such that 0(G)<320. Suppose G has subgroups of order 35 and 45. Find the order of G.

Example1.97 Let A and B are two subgroups of a groupG. If 0(A)=p (p prime), then show that $A \cap B=\{e\}$ or $A \subseteq B$.