Group Theory

Preliminaries

- Let A be a nonempty set. A binary relation on a set A is a subset R of Ax A and we write a~b if (a,b)ϵ R.
- The relation ~ on A is said to be:
  (a) reflexive if a~a, for all a ϵA,
  (b) symmetric if a ~b implies b ~a for all a, b ϵ A,
  (c) transitive if a ~ b and b ~ c implies a ~ c for all a, b, c ϵ A.

- If ~ defines an equivalence relation on A, then the equivalence class of aϵ A is defined to be {xϵ A I x~a}. Elements of the equivalence class of a are said to be equivalent to a. If C is an equivalence class, any element of C is called a representative of the class C.

Let A be a nonempty set.
(1) If ~ defines an equivalence relation on A then the set of equivalence classes of ~ form a partition of A.
(2) If {A_i| I ϵ I} is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i,iϵ I.
Let n be a fixed positive integer. Define a relation on Z by
    a ~b if and only if n I(b- a).
Clearly a~ a, and a ~ b implies b ~ a for any integers a and b, so this relation is trivially reflexive and symmetric. If a~ b and b ~ c then n divides a – b and n divides b - c so n also divides the sum of these two integers, i.e., n divides (a -b) + (b-c) = a - c, so a~ c and the relation is transitive. Hence this is an equivalence relation.
Write a≡ b (mod n) (read: a is congruent to b mod n) if a~b.
For any k E Z we shall denote the equivalence class of a by $\overline{a}$. this is called the congruence class or residue class of a mod n and consists of the integers which differ from a by an integral multiple of n, i.e.,
a = {a + kn I k ϵ Z}
={a, a ± n, a ± 2n, a ± 3n, . . . }.
There are precisely n distinct equivalence classes mod n, namely $\overline{0},\overline{1},...,\overline{(n-1)}$ determined by the possible remainders after division by n and these residue classes partition the integers Z. The set of equivalence classes under this equivalence relation will be denoted by Z/nZ and called the integers modulo n (or the integers mod n).

Group Theory

$\overline{a}+\overline{b}=\overline{a+b}$ and $\overline{a}.\overline{b}=\overline{a.b}$

Basic Definitions:

(1) A binary operation * on a set G is a function * : G x G → G. For any a, b ϵ G we shall write a*b for *(a, b).

(2) A binary operation * on a set G is associative if for all a, b, c ϵ G we have a * (b * c) = (a * b) * c.

(3) If * is a binary operation on a set G we say elements a and b of G commute if a * b = b *a. We say * (or G) is commutative if for all a, b ϵ G, a * b = b * a.

Examples:

(1) + (usual addition) is a commutative binary operation on Z (or on Q, R, or C respectively).

(2) x (usual multiplication) is a commutative binary operation on Z (or on Q, R, or C respectively).

(3) - (usual subtraction) is a non-commutative binary operation on Z, where - (a, b) = a - b. The map a→ -a is not a binary operation (not binary).

Suppose that * is a binary operation on a set G and H is a subset of G. If the restriction of * to H is a binary operation on H, i.e., for all a, b ϵ H, a * b E H, then H is said to be closed under *·

Definition.

(1) A group is an ordered pair (G, *) where G is a set and * is a binary operation on G satisfying the following axioms:

(i) (a * b) * c = a * (b * c), for all a, b, c E G, i.e., * is associative,

(ii) there exists an element e in G, called an identity of G, such that for all a ϵ G we have a * e = e * a = a,

(iii) for each a ϵG there is an element a^{-1} of G, called an inverse of a, such that a * a^{-1} = a^{-1} * a= e.

(2) The group (G , *) is called abelian (or commutative) if a * b = b * a for all a, b ϵ G .

Group Theory

→we say G is a finite group if in addition G is a finite set.

Examples

(1) Z,Q,R and C are groups under + with e = 0 and a^{-1} = -a, for all a.

(2) Q - {0}, R - {0} , C - {0}, Q+ , R+ are groups under x with e = 1 and a^{-1}=(1/a)

(3) For n ϵ z+, Z/nZ is an abelian group under the operation + of addition of residue classes. The identity in this group is the element $\overline{0}$ and for each $\overline{a}$ ϵ Z/nZ, the inverse of $\overline{a}$ is $\overline{-a}$.

If (A , *) and (B, <>) are groups, we can form a new group A x B, called their direct product, whose elements are those in the Cartesian product

A x B = { (a , b) I a ϵ A , b ϵ B)

and whose operation is defined component wise:

$(a_1 , b_1) (a_2, b_2) = (a_1 * a_2 , b_1 <> b_2)$

Proposition 1. If G is a group under the operation * , then

(1) the identity of G is unique

(2) for each a ϵ G, a^{-1} is uniquely determined

(3) $(a^{-1})^{-1}$ = a for all a ϵ G

(4) $(a * b)^{-1} = (b^{-1}) * (a^{-1})$

(5) for any $a_1 , a_2, \ldots , a_n$ ϵ G the value of $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed (this is called the generalized associative law).

Proof : (1) If f and g are both identities, then by axiom (ii) of the definition of a group f * g = f (take a = f and e = g). By the same axiom f * g = g (take a = g and e = f). Thus f = g, and the identity is unique.

(2) Assume b and c are both inverses of a and let e be the identity of G . By axiom (iii), a * b = e and c * a = e. Thus

c=c*e (definition of e - axiom (ii))

= c * (a * b) (since e = a * b)

= (c * a) * b (associative law)

= e * b (since e = c * a)

= b (axiom (ii)).

Group Theory

(3) To show $(a^{-1})^{-1} = a$ is exactly the problem of showing a is the inverse of a^{-1} (since by part (2) a has a unique inverse). Reading the definition of a^{-1} , with the roles of a and a^{-1} mentally interchanged shows that a satisfies the defining property for the
inverse of a^{-1}, hence a is the inverse of a^{-1} .

(4) Let $c = (a * b)^{-1}$ so by definition of c, $(a * b) * c = e$. By the associative law
$a * (b * c) = e$.
Multiply both sides on the left by a^{-1} to get
$a^{-1} * (a * (b * c)) = a^{-1} * e$.
The associative law on the left hand side and the definition of e on the right give
$(a^{-1} * a) * (b * c) = a^{-1}$
so
$e * (b * c) = a^{-1}$
hence
Now multiply both sides on the left by b^{-1} and simplify similarly:
$b^{-1} * (b * c) = b^{-1} * a^{-1}$
$(b^{-1} * b) * c = b^{-1} * a^{-1}$
$e * c = b^{-1} * a^{-1}$
$c = b^{-1} * a^{-1}$,
as claimed.

(5) Can be proved using mathematical induction.

→ Throughout the proof of this proposition we have not changed the order of any products since G may be non abelian.
Notation: In place of ' *' we will use '.' , we will write a.b as ab.
Let $x^0 = 1$, the identity of G.

Proposition 2: Let G be a group and let a, b ϵ G. The equations ax = b and ya = b have unique solutions for x , y ϵ G. In particular, the left and right cancellation laws
hold in G, i.e.,
(1) if au = av, then u = v, and
(2) if ub = vb, then u = v.

Proof: We can solve ax = b by multiplying both sides on the left by a - 1 and

simplifying to get $x = a^{-1}b$. The uniqueness of x follows because a^{-1} is unique. Similarly, if ya = b, $y = ba^{-1}$. If au = av, multiply both sides on the left by a^{-1} and simplify to get u = v. Similarly, the right cancellation law holds.
One consequence of Proposition 2 is that if a is any element of G and for some b ϵ G, ab = e or ba = e, then $b = a^{-1}$, i.e., we do not have to show both equations hold. Also, if for some b ϵ G, ab = a (or ba = a), then b must be the identity of G, i.e., we do not have to check bx = xb = x for all x ϵ G.

Definition. For G a group and x E G define the order of x to be the smallest positive
integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of
order n. If no positive power of x is the identity, the order of x is defined to be infinity
and x is said to be of infinite order.

Examples: 1) In the additive group Z/9Z the element 6 has order 3.
2) An element of a group has order 1 if and only if it is the identity.

Definition. Let $G = \{g_1 , g_2, . . . , gn \}$ be a finite group with $g_1 = 1$. The

multiplication table or group table of G is the n x n matrix whose i, j entry is the

group element $g_i\, g_j$.

Solution of Exercise questions:

Determine which of the following binary operations are associative:
(a) the operation * on Z defined by a *b = a - b
Solution. (1 * 2) * 3 = - 4 while 1 *(2 * 3) = 2, so * is not associative.

(b) the operation * on R defined by a * b = a + b + ab
Solution. * is associative: let a, b, c be real numbers. Then
(a * b) * c = (a + b + ab) * c
= (a + b + ab) + c + (a + b + ab)c
= a + b + c + ab + ac + bc + abc
= a + (b + c + bc) + a(b + c + bc)

= a * (b + c + bc)
= a * (b * c).

(c) the operation * on Q defined by a * b = (a + b)/5
Solution. (5 * 20) * 15 = 4 while 5 * (20 * 15) = 12/5. Therefore * is not associative.
(d) the operation * on Z × Z defined by (a , b) * (c, d) = (ad + bc, bd)
Solution. * is associative: let (a, b), (c, d), (e, f) be members of Z × Z.

Then
((a, b) * (c, d))* (e, f) = (ad + bc, bd) *(e,f)
=((ad + bc)f + bde, bdf)
= (adf + bcf + bde,bdf)
=(adf + b(cf + de), bdf)
= (a, b) * (cf + de,df)
= (a,b) *((c, d) * (e, f))

(e) the operation * on Q –{.0} defined by a * b = a/b
Solution. (125 * 25) * 5 = 1 while 125 * (25 * 5) = 25, so * is not associative.

2) Similarly check that which of the binary operations in the Q1 are commutative that is to check a*b=b*a is satisfied or not.

a) the operation * on Z defined by a*b=a-b,
Solution: 1-2= -1 , 2-1=1 .So * is not commutative.

b) the operation * on R defined by a * b = a + b + ab
Solution. * is commutative since, for any a, b ϵ R,
a * b = a + b + ab
= b + a + ba
= b * a

c) the operation * on Q defined by a * b = (a + b)/5
Solution. * is commutative since + is commutative in Q.

d) the operation ? on Z ×Z defined by (a, b) * (c,d) = (ad + bc, bd)
Solution. * is commutative: Let (a, b) and (c, d) be elements of Z × Z.

Then

(a, b) * (c, d) = (ad + bc, bd)
= (cb + da, db)
= (c, d) * (a, b).

(e) the operation * on Q $-\{0\}$ defined by a * b = a/b
Solution. * is not commutative since 1 * 2 = 1/2 but 2 * 1 = 2.

4) Prove that multiplication of residue classes in Z/nZ is associative (you may assume it is well defined).
Solution:
Let $\overline{a},\overline{b},\overline{c}$ be residue classes in Z/nZ. Then we have $\overline{a_1 a_2} = \overline{a_1}.\overline{a_2}$
along with the associativity of × in Z, we may write

$$\left(\overline{a}.\overline{b}\right).\overline{c} = \overline{(a.b).c}$$
$$= \overline{a.(b.c)}$$
$$= \overline{a}.\left(\overline{b}.\overline{c}\right)$$

Group Theory

1.3 Symmetric Groups :

Let Ω be any nonempty set and let S_{Ω} be the set of all bijections from Ω to itself (i.e. , the set of all permutations of Q). S_{Ω} is group under function composition:

The set S_{Ω} is a group under function composition: o.

i) Note that o is a binary operation on S_{Ω} since if $\sigma : \Omega \to \Omega$ and $\tau : \Omega \to \Omega$ are both bijections, then $\sigma o \tau$ is also a bijection from $\Omega \to \Omega$. Since function composition is associative in general, o is associative.

ii) The identity of S_{Ω} is the permutation 1 defined by 1(a) = a, for all a $\in \Omega$.

iii) For every permutation σ there is a (2-sided) inverse function, $\sigma^{-1} : \Omega \to \Omega$ satisfying $\sigma^{-1} o \sigma = \sigma o \sigma^{-1} = 1$

Thus, all the group axioms hold for (S_{Ω} , o). This group is called the ***symmetric group*** on the set Ω.

*elements of S_{Ω} are the permutations Ω.

-> When Ω = { 1 , 2, 3 , . . . , n}, the symmetric group on Ω is denoted S_{Ω} , the symmetric group of degree n.

To show that the order of S_n is n!.

Proof: The permutations of { 1 , 2, 3 , . . . , n} are precisely the injective functions of this set to itself because it is finite and we can count the number of injective functions. An injective function σ can send the number 1 to any of the n elements of { 1 , 2, 3 , . . . , n}; σ(2) can then be any one of the elements of this set except σ (1) (so there are n - 1 choices for σ (2)); σ (3) can be any element except σ (1) or σ (2) (so there are n - 2 choices for σ (3)), and so on. Thus there are precisely n · (n - 1) · (n - 2) . . . 2 · 1 = n! possible injective functions from { 1 , 2, 3 , . . . , n} to itself. Hence there are precisely n ! permutations of { 1 , 2, 3 , . . . , n} so there are precisely n! elements in S_n .

Cycle Decomposition:

A cycle is a string of integers which represents the element of S_n which cyclically permutes these integers. The cycle (a_1 a_2 . . . a_m) is the permutation which sends a_i to a_{i+l}, $1 \leq i \leq m - 1$ and sends a_m to a_1 .

For Example: (2 1 3) is the permutations that maps : 2 to 1, 1 to 3 and 3 to 2.

Group Theory

In general, for each $\sigma \in S_n$ the numbers from 1 to n will be rearranged and grouped into k cycles of the form

$(a_1\ a_2 \dots a_{m1})\ (a_{m1+1}\ a_{m1+2} \dots a_{m2}) \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})$

To locate $\sigma(x)$:

→Let $x \in \{1,2,3,\dots,n\}$, If x is not followed immediately by a right parenthesis (i.e., x is not at the right end of one of the k cycles), then $\sigma(x)$ is the integer appearing immediately to the right of x.

→ If x is followed by a right parenthesis, then $\sigma(x)$ is the number which is at the start of the cycle ending with x.

$a_1 \rightarrow a_2 \rightarrow a_3 \dots a_{m1-1} \rightarrow a_{m1}$ Similarly for all others.

- **Length** of the cycle is the number of integers which appear in it.
- A cycle of length t is called *t-cycle*
- Two cycles are called disjoint if they have no numbers in common.

Cycle Decomposition Algorithm :

1) To start a new cycle pick the smallest element of { 1 , 2, ... n} which has not yet appeared in a previous cycle - call it a (if you arc just starting, a = 1) ; begin the new cycle: (a

2) Read off $\sigma(a)$ from the given description of σ - call it b. If b = a, close the cycle with a right parenthesis (without writing b down); this completes a cycle - return to step 1 . If $b \neq a$, write b next t o a in this cycle: (a b

3) Read off σ (b) from the given description of σ - call it c. If c = a, close the cycle with a right parenthesis to complete the cycle - return to step 1 . If $c \neq a$, write c next to b in this

cycle : (a b c Repeat this step using the number c as the new value for b until the cycle closes.

→As per convention 1-cycles will not be written. So If some element does not appear in the cycle decomposition of a permutation σ then $\sigma(i) = i$. The identity permutation of S_n has a cycle decomposition (1)(2)…(n) and will be written simply as 1.

4) Remove all cycles of length 1.

Group Theory

Example: n=13 and let $\sigma \in S_7$ be defined by

$\sigma(1)=7, \sigma(2)=6, \sigma(3)=3, \sigma(4)=5, \sigma(5)=4, \sigma(6)=1, \sigma(7)=2$

Steps to be followed according to Algorithm:

1) (1
2) $\sigma(1)=7=b \neq 1$ so write 7 that is (1 7
3) $\sigma(7)=2 \neq 1$ so continue cycle as (1 7 2

So repeating this algorithm from 1 -3 step we get:

$\sigma = (1\ 7\ 2\ 6)(3)\ (4\ 5)$

4) Here 3 is a cycle of length 1 so remove it . Final cycle decomposition is :

$\sigma = (1\ 7\ 2\ 6)\ (4\ 5)$

Computing products in S_n that is $\sigma o \tau$, one reads the permutations from ***right to left.***

For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order. For Example : $\sigma = (1\ 7\ 2\ 6)\ (4\ 5)$ then

$$\sigma^{-1} = (6\ 2\ 7\ 1\ )\ (5\ 4)$$

Composition of two functions:

Example: (1 2 3) o (1 2)(3 4)

1→2 and 2→3 so 1→3

3→4 and 4→4 so 3→4

4→3 and 3→1 so 4→1

2→1 and 1→2 so 2→2

So the resulting function is: (1 3 4)

Consider another example : (1 2)o(1 3) =(1 3 2) and (1 3)o(1 2)= (1 2 3)

→In Particular this shows that , S_n is a non abelian for all $n \geq 3$.

→ Since disjoint cycles permute numbers which lie in disjoint sets it follows that disjoint cycles commute.

→ Rearranging the cycles in any product of disjoint cycles (in particular, in a cycle decomposition) does not change the permutation. For Example : (1 2 3 4) = (3 4 1 2) .

By convention, the smallest number appearing in the cycle is usually written first.

Group Theory

→The Order of a permutation is l.c.m of the lengths of the cycles in its cycle decomposition.

Exercise Question Solutions:

1) σ: 1→3   2→4   3→5   4→2   5→1
    τ: 1→5   2→3   3→2   4→4   5→1

Cycle decompositions of following permutations;

σ: (1 3 5)(2 4)

τ: (1 5) (2 3)

σ^2: (1 5 3)

στ: (2 5 3 4)

τσ: (1 2 4 3)

$\tau^2\sigma$: 1o(1 3 5)(2 4) =(1 3 5)(2 4)

5. Find the order of (1 12 8 10 4) (2 13) (5 11 7) (6 9) .

Ans : Since the cycles are disjoint the order of the elements in S_{13} is the l.c.m of the cycle lengths: [2,3,5]= 30.

Group Theory

1.4 : Matrix Groups

Definition of Field

1) A field is a set F together with two binary operations + and · on F such that (F, +) is an abelian group (call its identity 0) and (F - {0}, ·) is also an abelian group, and the following distributive law holds:

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,

(2) For any field F let $F^{x} = F - \{0\}$.

For each $n \in \mathbb{Z}^{+}$,

$G L_n (F) = \{A \mid A$ is an n x n matrix with entries from F and $\det(A) \neq 0 \}$,

Where the determinants of any matrix with entries from F can be computed by same formulas used when $F=\mathbb{R}$.

For arbitrary n x n matrices A and B let AB be the product of these matrices as computed by the same rules as when $F = \mathbb{R}$.

i) A(BC)=(AB)C (property of matrices) So product is Associative.

ii) Since $\det(AB) = \det(A) \cdot \det(B)$, it follows that if $\det(A) \neq 0$ and $\det(B) \neq 0$, then $\det(AB) \neq 0$, so $GL_n (F)$ is closed under matrix multiplication.

iii) $\det(A) \neq 0$ if and only if A has a matrix inverse . so each $A \in GL_n (F)$ has an inverse, A^{-1} , in $GL_n(F)$:

$$AA^{-1} = A^{-1} A = I$$

where I is the n x n identity matrix.

Thus $GL_n (F)$ is a group under matrix multiplication, called the general linear group of degree n.

Some Results:

(1) if F is a field and $| F| < \infty$, then $| F | = p^m$ for some prime p and integer m

(2) if $| F | = q < \infty$, then $| GL_n(F) | = (q" - 1) (q" - q) (qn - q^2) \dots (q" - q^{n-1})$.

Group Theory

1.5 The Quaternion Group

The quatemion group, Q_8, is defined by
$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$
with product · computed as follows:
$1 \cdot a = a \cdot 1 = a$, for all $a \in Q_8$
$(-1) . (-1) = 1$, $(-1) \cdot a = a \cdot (-1) = -a$, for all $a \in Q_8$
$i \cdot i = j \cdot j = k \cdot k = -1$
$i. j = k$,
$j \cdot k = i$,
$k . i = j$,
$j . i = -k$
$k . j = -i$
$i . k = -j$.

→Q_8 is a non-abelian group of order 8.

Homomorphisms and Isomorphisms

Definition. Let $(G, *)$ and (H, o) be groups. A map $\varphi : G \to H$ such that
$\Phi(x*y) = \varphi(x) \text{ o } \varphi(y)$, for all $x,y \in G$
is called a ***homomorphism***.

→When the group operations for G and H are not explicitly written, the homomorphism condition becomes simply

$$\varphi(xy) = \varphi(x)\varphi(y)$$

but it is important to keep in mind that the product xy on the left is computed in G
and the product $\varphi(x)\varphi(y)$ on the right is computed in H.

Definition : The map $\varphi : G \to H$ is called an isomorphism and G and H are said to be isomorphic or of the same isomorphism type, written $G \cong H$, if
(1) φ is a homomorphism (i.e., $\varphi(xy) = \varphi(x)\varphi(y)$), and
(2) φ is a bijection.

→Intuitively, G and H are the same group except that the elements and the operations may be written differently in G and H. Thus any property which G has which depends only on the group structure of G (i.e., can be derived from the group axioms - for example, commutativity of the group) also holds in H.

Group Theory

Examples:

1) For any group G,G $\cong$G. The identity map provides an obvious isomorphism but not in general, the only isomorphism from G to itshelf.

2) The exponential map exp: R$\rightarrow$$R^+$ defined by exp(x)=e^x where e is the base of the natural logarithm, is an isomorphism from (R,+) to (R^+,$\times$).

$$e^{x+y} = e^e e^y$$

So exponential map is homomorphism. Exp is bijection since it has an inverse function that is $\log_e$.

$\rightarrow$Any non-abelian group of order 6 is isomorphic to S_3.
Example:- GL_2 (F_2) $\cong$ S_3

if φ: G $\rightarrow$ H is an isomorphism, then, in particular,
(a) I G I = I H I
(b) G is abelian if and only if H is abelian
(c) For all x $\in$ G, |x| = | φ (x) | .

*Note that it is not true that any group of order 6 is isomorphic to S_3.
Ex: i) S_3 is not isomorphic to Z/nZ since one is abelian and the other is not.
ii) (R-{ 0}, x) and (R, +) cannot be isomorphic because in (R-{ 0}, x) the element - 1 has order 2 whereas (R, +) has no element of order 2 , contrary to (c).