**Definition: Group**

A non-empty set *G*, together with an operation \* i.e., (*G*, \*) is said to be a group if it satisfies the following axioms

(1) **Closure axiom :** *a*, *b*  *G* ⇒ *a* \* *b*  *G*

(2) **Associative axiom :** ∀*a*, *b*, *c*  *G*, (*a* \* *b*) \* *c* = *a* \* (*b* \* *c*)

(3) **Identity axiom :** There exists an element *e*  *G*

such that *a* \* *e* = *e* \* *a* = *a*, ∀*a*  *G*.

(4) **Inverse axiom :** ∀*a*  *G* there exists an element *a*−1*G* such

that *a*−1 \* *a* = *a* \* *a*−1 = *e.*

*e* is called the identity element of *G* and *a*−1 is called the inverse of *a* in *G*.

**Definition: Commutative property**

A binary operation \* on a set *S* is said to be commutative

if *a* \* *b* = *b* \* *a* ∀ *a*, *b*  *S*

**Note:** If a group satisfies the commutative property then it is called an abelian group or a commutative group, otherwise it is called a non-abelian group.

**Definition : Semi-group**

A non-empty set *S* with an operation \* i.e., (*S*, \*) is said to be a semi-group if it satisfies the following axioms.

(1) **Closure axiom :** *a*, *b*  *S* ⇒ *a* \* *b*  *S*

(2) **Associative axiom :** (*a* \* *b*) \* *c* = *a* \* (*b* \* *c*), ∀ *a*, *b*, *c*  *S*.

**Definition :** **Monoid**

A non-empty set *M* with an operation \* i.e., (*M*, \*) is said to be a monoid if it satisfies the following axioms :

(1) **Closure axiom :** *a*, *b*  *M* ⇒ *a* \* *b*  *M*

(2) **Associative axiom :** (*a* \* *b*) \* *c* = *a* \* (*b* \* *c*) ∀*a*, *b*, *c*  *M*

(3) **Identity axiom :** There exists an element *e*  *M*

such that *a* \* *e* = *e* \* *a* = *a*, ∀*a*  *M*.

(*N*, +) is a semi-group but it is not a monoid/group.

(*Z*, .) is a monoid. But it is not a group.

(Z,+) is a group.

***Example :*** Prove that (*Z*, +) is an infinite abelian group.

**Solution:**

(i) **Closure axiom :** We know that sum of two integers is again an integer.

(ii) **Associative axiom :** Addition is always associative in *Z*

i.e., ∀*a*, *b*, *c*  *Z,* (*a* + *b*) + *c* = *a* + (*b* + *c*)

(iii) **Identity axiom :** The identity element O *Z* and it satisfies

*O* + *a* = *a* + *O* = *a*, ∀ *a*  *Z* Identity axiom is true.

(iv) **Inverse axiom :** For every *a*  *Z,* an element − *a*  *Z* such

that − *a* + *a* = *a* + (− *a*) = 0

∴ Inverse axiom is true. ∴ (*Z*, +) is a group.

(v) ∀ *a*, *b*  *Z*, *a* + *b* = *b* + *a*

∴ addition is commutative. ∴ (*Z*, +) is an abelian group.

(vi) Since *Z* is an infinite set (*Z*, +) is infinite abelian group.

***Example:*** Show that (Z6, +6) forms a group.

**Solution:** Let *Z 6* = {[0], [1], [2], ... [*5*]} be the set of all congruence classes modulo 6.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| +*6* | [0] | [1] | [2] | [3] | [4] | [5] |
| [0] | [0] | [1] | [2] | [3] | [4] | [5] |
| [1] | [1] | [2] | [3] | [4] | [5] | [0] |
| [2] | [2] | [3] | [4] | [5] | [0] | [1] |
| [3] | [3] | [4] | [5] | [0] | [1] | [2] |
| [4] | [4] | [5] | [0] | [1] | [2] | [3] |
| [5] | [5] | [0] | [1] | [2] | [3] | [4] |

(i) **Closure axiom :**

{[0], [1], [2], [3], [4],[*5*]} *Z 6*. ∴Closure axiom is true.

(ii) Addition modulo *n* is always **associative** in the set of congruence classes modulo *n*.

([4] +6 [5]) +6 [3] = [3] +6 [3] = [0]

[4] +6 ([5] +6 [3]) = [4] +6 [2] = [0]

(iii) The **identity** element [0] *Z 6* and it satisfies the identity axiom.

[0] +6 [5] = [5] and [5] +6 [0] = [5]

(iv) The **inverse** of [0] *Z*6is [0]

[0] is the inverse of [0]

[5] is the inverse of [1]

[4] is the inverse of [2]

[3] is the inverse of [3]

[2] is the inverse of [4]

[1] is the inverse of [5]

∴ The inverse axiom is also true. Hence (*Z 6*, +*6*) is a group.

***Example:*** Show that (*Zn*, +*n*) forms group.

**Solution:** Let *Z n* = {[0], [1], [2], ... [*n* − 1]} be the set of all congruence classes modulo *n*. and let [*l*], [*m*], *Z n* 0 ≤ *l*, *m* < *n*

(i) **Closure axiom :** By definition of addition modulo *n,*

[*l*] +*n* [*m*] =

where *l* + *m* = *q* . *n* + *r,* 0 ≤ *r* < *n*

In both the cases, [*l* + *m*] *Z n* and [*r*] *Z n*

∴ Closure axiom is true.

(ii) Addition modulo *n* is always **associative** in the set of congruence classes modulo *n*.

(iii) The **identity** element [0] *Z n* and it satisfies the identity axiom.

(iv) The **inverse** of [*l*] *Zn* is [*n* − *l*]

Clearly [*n* − *l*] *Z n* and

[*l*] +*n* [*n* − *l*] = [0]

[*n* − *l*] +*n* [*l*] = [0]

∴ The inverse axiom is also true. Hence (*Z n*, +*n*) is a group.

**Note :** (Z*n*, +*n*) is a finite abelian group of order *n*.

***Example:*** Show that (*Z*7 − {[0]}, **.** 7) forms a group.

**Solution:** Let *G* = [[1], [2], ... [6]]

The Cayley’s table is

**.**7 [1] [2] [3] [4] [5] [6]

[1] [1] [2] [3] [4] [5] [6]

[2] [2] [4] [6] [1] [3] [5]

[3] [3] [6] [2] [5] [1] [4]

[4] [4] [1] [5] [2] [6] [3]

[5] [5] [3] [1] [6] [4] [2]

[6] [6] [5] [4] [3] [2] [1]

From the table :

1. All the elements of the composition table are the elements of *G*.

∴ The closure axiom is true.

(ii) The multiplication modulo 7 is always associative.

(iii) The identity element is [1] *G* and satisfies the identity axiom.

(iv) The inverse of [1] is [1] ; [2] is [4] ; [3] is [5] ; [4] is [2] ; [5] is [3] and

[6] is [6] and it satisfies the inverse axiom.

∴ the given set forms a group under multiplication modulo 7.

In general, it can be shown that (*Zp* − {(0)}, **.** *p*) is a group for any prime *p*.

**Subgroup**

A subgroup of a group G is a subset of G that forms a group with the same law of composition. For example, the even numbers form a subgroup of the group of integers with group law of addition.

Any group G has at least two subgroups: the trivial subgroup {1} and G itself. It need not necessarily have any other subgroups however; for example, Z5 has no nontrivial proper subgroup.

**Example: Subgroups of Z8**

Let *G* be the cyclic group Z8 whose elements are {\displaystyle G=\left\{0,2,4,6,1,3,5,7\right\}}G = {0, 2, 4, 6, 1, 3, 5, 7}and whose group operation is addition modulo eight. Its Cayley table is

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **+** | **0** | **2** | **4** | **6** | **1** | **3** | **5** | **7** |
| **0** | 0 | 2 | 4 | 6 | 1 | 3 | 5 | 7 |
| **2** | 2 | 4 | 6 | 0 | 3 | 5 | 7 | 1 |
| **4** | 4 | 6 | 0 | 2 | 5 | 7 | 1 | 3 |
| **6** | 6 | 0 | 2 | 4 | 7 | 1 | 3 | 5 |
| **1** | 1 | 3 | 5 | 7 | 2 | 4 | 6 | 0 |
| **3** | 3 | 5 | 7 | 1 | 4 | 6 | 0 | 2 |
| **5** | 5 | 7 | 1 | 3 | 6 | 0 | 2 | 4 |
| **7** | 7 | 1 | 3 | 5 | 0 | 2 | 4 | 6 |

This group has two nontrivial subgroups: *J*={0,4} and *H*={0,2,4,6}, where *J* is also a subgroup of *H*. The Cayley table for *H* is the top-left quadrant of the Cayley table for *G*. The group *G* is cyclic, and so they are its subgroups. In general, subgroups of cyclic groups are also cyclic.

**Example: Coset of Z8**

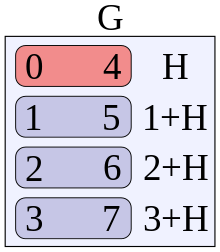
Given a subgroup *H* and some *a* in G, we define the **left coset** *aH* = {*ah* : *h* in *H*}. Because *a* is invertible, the map φ : *H* → *aH* given by φ(*h*) = *ah* is a bijection. Furthermore, every element of *G* is contained in precisely one left coset of *H*; the left cosets are the equivalence classes corresponding to the [equivalence relation](https://en.wikipedia.org/wiki/Equivalence_relation) *a*1 ~ *a*2 if and only if *a*1−1*a*2 is in *H*. The number of left cosets of *H* is called the index of *H* in *G* and is denoted by [*G* : *H*].

[Lagrange's theorem](https://en.wikipedia.org/wiki/Lagrange%27s_theorem_(group_theory)) states that for a finite group *G* and a subgroup *H*,

where |*G*| and |*H*| denote the [orders](https://en.wikipedia.org/wiki/Order_(group_theory)) of *G* and *H*, respectively. In particular, the order of every subgroup of *G* (and the order of every element of *G*) must be a [divisor](https://en.wikipedia.org/wiki/Divisor) of |*G*|.

**Right cosets** are defined analogously: *Ha* = {*ha* : *h* in *H*}. They are also the equivalence classes for a suitable equivalence relation and their number is equal to [*G* : *H*].

If *aH* = *Ha* for every *a* in *G*, then *H* is said to be a [normal subgroup](https://en.wikipedia.org/wiki/Normal_subgroup). Every subgroup of index 2 is normal: the left cosets, and also the right cosets, are simply the subgroup and its complement.



G is the group formed by the integers mod 8 under addition, ie (G, +8). The subgroup H contains only 0 and 4. There are four left cosets of H: H, 1+H, 2+H, and 3+H. Together they partition the entire group G into equal-size, non-overlapping sets. The index [G : H] is 4.

**Example**: Consider the group Z15 = {0, 1, 2, 3, …,14} and its subgroup H = {0, 3, 6, 9, 12}. Then |H| = 5, which divides | Z15| = 15, and there are 15 / 5 = 3 distinct left cosets. They are H = {0, 3, 6, 9, 12}, 1 + H = {1, 4, 7, 10, 13}, and 2 + H = {2, 5, 8, 10, 14}.

**Order of an element:**

Let *G* be a group and *a*  *G*. The order of ‘*a*’ is defined as the least positive integer *n* such that *an* = *e*, *e* is the identity element. If no such positive integer exists, then *a* is said to be of infinite order. The order of *a* is denoted by 0(*a*).

**Note :**

* Here *an* = *a* \* *a* \* *a* ... \**a* (*n* times). If \* is usual multiplication ‘**.**’ Then *an* is *a . a .a ...* (*n* times) i.e., *an* .
* If \* is usual addition then *an* is *a* + *a* + *a* + ... + *a* (*n* times) i.e., *na*.
* Thus *an* is not “*a* to the power *n*”, it is a symbol to denote *a* \* *a* \* *a* ... \* *a* (*n* times).
* Clearly *an*  *G*, if *a*  *G* .

***Example :*** Find the order of each element of the group (*G*, **.**) where *G* = {1, − 1, *i*, − *i*}.

**Solution:** In the given group, the identity element is 1. ∴ 0(1) = 1.

0(− 1) = 2 [ (− 1) (− 1) = 1]

0(*i*) = 4 [ (*i*) (*i*) (*i*) (*i*) = 1]

0(− *i*) = 4 [(-*i*) (-*i*) (-*i*) (-*i*) = 1].

***Example :*** Find the order of each element in the group *G* = {1, ω, ω2}, consisting of cube roots of unity with usual multiplication.

**Solution:** We know that the identity element is 1. ∴ 0(1) = 1.

0(ω) = 3. Since ω *.* ω *.* ω = ω3 = 1

0(ω2) = 3 since (ω2) (ω2) (ω2) = ω6 = 1

***Example :*** Find the order of each element of the group (*Z*4, +4)

**Solution:** *Z*4 = {[0], [1], [2], [3]} is an abelian group under the addition modulo 4. The identity element is [0] and note that [4] = [8] = [12] = [0]

0([0]) = 1 [identity element]

0([1]) = 4 [add [1] four times to get [4] or [0]]

0 ([2]) = 2 [add [2] two times to get [4] or [0]]

0 ([3]) = 4 [add [3] four times to get [12] or [0]]

**Ring**

A ring is a set *R* and two binary operations, called addition and multiplication, with the following properties:

* The ring is a commutative group under addition.
* Multiplication is associative: *a(bc) = (ab)c*
* Multiplication distributes over addition: *a(b+c) = ab + ac* and *(a+b)c = ac + bc*

**Commutative ring**

A commutative ring is a ring with commutative multiplication.

**Integral Domains**

An integral domain is a commutative ring with unit (and *0 ≠ 1*) in which there are no zero divisors; i.e., *xy = 0* implies that *x=0* or *y=0* (or both).

**Field**

An integral domain is a field if every nonzero element *x* has a reciprocal *x-1* such that *xx-1 = x-1x = 1*. Notice that the reciprocal is just the inverse under multiplication; therefore, the nonzero elements of a field are a commutative group under multiplication.

**Exercise:**

1. Verify that H = {[1]60, [13]60, [37]60, [49]60} is a subgroup of G under multiplication modulo 60.
2. If f : G → H is a surjective homomorphism of groups and G is abelian, prove that H is abelian.
3. Let G be a cyclic group order of n, and let r be an integer dividing n. Prove that G contains exactly one subgroup of order r.
4. Let G be a cyclic group of order 6. How many of its elements generate G?
5. Let G be a group with identity element e. Show that e is the unique identity element.
6. Let G be the group of all invertible n × n matrices (under matrix multiplication). Let H be the subset consisting of n×n matrices with determinant 1. Show that H is a subgroup of G.
7. Let G be a group and suppose that H and K are subgroups. Prove that H ∩ K is a subgroup.
8. Let G be a cyclic group of order 6. What are the orders of the elements of G? How many of the elements of G generate all of G?
9. Let G be the set of all rational numbers except 1(exclude 1) and \* be defined on G by a \* b = a + b − ab for all a, b ∈ G. Show that (G, \*) is an infinite abelian group.
10. Show that the set G = {a + b √2 / a, b ∈ Q} is an infinite abelian group with respect to addition.

**Summary**

1. The set of integers is a group under the OPERATION of addition: We have already seen that the integers under the OPERATION of addition are CLOSED, ASSOCIATIVE, have IDENTITY 0, and that any integer x has the INVERSE −x. Because the set of integers under addition satisfies all four group PROPERTIES, it is a group.
2. The set {0,1,2} under addition is not a group, because it does not satisfy all of the group PROPERTIES: it does not have the CLOSURE PROPERTY (see the previous lectures to see why). Therefore, the set {0,1,2} under addition is not a group. (Notice also that this set is ASSOCIATIVE, and has an IDENTITY which is 0, but does not have the INVERSE PROPERTY because −1 and −2 are not in the set!)
3. The set of integers under subtraction is not a group, because it does not satisfy the entire group PROPERTIES: it does not have the ASSOCIATIVE PROPERTY (see the previous lectures to see why). Therefore, the set of integers under subtraction is not a group. (Notice also that this set is CLOSED, but does not have an IDENTITY and therefore also does not have the INVERSE PROPERTY.)
4. The set of natural numbers under addition is not a group, because it does not satisfy the entire group PROPERTIES: it does not have the IDENTITY PROPERTY (see the previous lectures to see why). Therefore, the set of natural numbers under addition is not a group. (Notice also that this set is CLOSED, ASSOCIATIVE, but does not have the INVERSE PROPERTY because none of the negative numbers are in the set.)
5. The set of whole numbers under addition is not a group, because it does not satisfy the entire group PROPERTIES: it does not have the INVERSE PROPERTY (see the previous lectures to see why). Therefore, the set of whole numbers under addition is not a group! (Notice also that this set is CLOSED, ASSOCIATIVE, and has the IDENTITY ELEMENT 0.)
6. The set of rational numbers with the element 0 removed is a group under the OPERATION of multiplication: We have already seen that the set rational numbers with the element 0 removed under the OPERATION of multiplication is CLOSED, ASSOCIATIVE, have IDENTITY 1, and that any integer *x* has the INVERSE (1/*x*). Because the set of rational numbers with the element 0 removed under multiplication satisfies all four group PROPERTIES, it is a group.
7. The set of rational numbers (which contains 0) under multiplication is not a group, because it does not satisfy the entire group PROPERTIES: it does not have the INVERSE PROPERTY (see the previous lectures to see why). Therefore, the set rational numbers under multiplication is not a group. (Notice also that this set is CLOSED, ASSOCIATIVE, and has an IDENTITY which is 1.)
8. The set of rational numbers under division is not a group, because it does not satisfy the entire group PROPERTIES: it does not have the ASSOCIATIVE PROPERTY (see the previous lectures to see why). Therefore, the set of rational numbers under division is not a group. (Notice also that this set is not CLOSED because anything divided by 0 is not in the set, does not have an IDENTITY and therefore also does not have the INVERSE PROPERTY.)
9. The set of natural numbers under division is not a group, because it does not satisfy the entire group PROPERTIES: it does not have the IDENTITY PROPERTY (see the previous lectures to see why). Therefore, the set of natural numbers under division is not a group. (Notice that this set does not have the CLOSURE, ASSOCIATIVE or INVERSE PROPERTIES.)
10. The set of integers under multiplication is not a group, because it does not satisfy all of the group PROPERTIES: it does not have the INVERSE PROPERTY (see the previous lectures to see why). Therefore, the set of integers under multiplication is not a group. (Notice also that this set is CLOSED, ASSOCIATIVE, and has the IDENTITY ELEMENT 1.)

**Cosets**

1. A **left coset** of H in G is gH where g ∈ G (H is on the right).
2. A **right coset** of H in G is Hg where g ∈ G (H is on the left).

**Theorem:** If two left cosets of H in G intersect, then they coincide, and similarly for right cosets. Thus, G is a disjoint union of left cosets of H and also a disjoint union of right cosets of H.

**Corollary(Lagrange’s theorem):** If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. i.e., |H| / |G|.

In particular, the order of every element of G divides the order of G.

**Using of Lagrange’s Theorem, we can state the following:**

1. For any integers n ≥ 0 and 0 ≤ r ≤ n, the number is an integer.
2. For any positive integers a, b the ratios and are integers.
3. For an integer m > 1, let *ϕ*(m) be the number of invertible numbers modulo m. For m ≥ 3 the number *ϕ*(m) is even.

**Example**: Supposea group has 10 elements. Then its subgroup must have 1 element, or 2, or 5, or 10 elements.

**Set Permutations**

In mathematics, the notion of permutation relates to the act of arranging all the members of a set into some sequence or order.

If the set is already ordered, a process of rearranging (reordering) its elements is called permutation.

In group theory, a permutation of a set S is defined as a bijection(one to one and onto) mapping from the set S to itself. That is, it is a function from S to S for which every element occurs exactly once as an image value. This is related to the rearrangement of the elements of S in which each element s is replaced by the corresponding f(s). The collection of such permutations form a group called the **symmetric group of S.**

**Example**: There are six permutations of the set {1,2,3}, namely: (1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), and (3,2,1). These are all the possible orderings of this three element set.

**Note:**

1. The number of permutations of n distinct objects is n factorial, usually written as n!.
2. *k*-permutations of *n* are the different ordered arrangements of a *k*-element subset of an *n*-set. These objects are also known as *partial permutations* or as *sequences without repetition*.
3. The number of circular permutations of a set S with n elements is (n - 1)!.
4. The composition of two bijections always gives another bijection, the product of two permutations is again a permutation.
5. The product of two permutations is obtained by rearranging the columns of the second (leftmost) permutation so that its first row is identical with the second row of the first (rightmost) permutation.
6. Since bijections have inverses, so do permutations.

**Cycle notation**

This alternative notation describes the effect of repeatedly applying the permutation, thought of as a function from a set onto itself. It expresses the permutation as a product of cycles corresponding to the orbits of the permutation; since distinct orbits are disjoint, this is referred to as "decomposition into disjoint cycles".

**Example:** If and , then find *PQ* and *QP*.

Solution: The product *QP* is

(Or)

Similarly,

(Or)

Note:

**Example:** If , then find *P-*1*.*

Solution: Given

(Or)

, .

**Example:** If , then find *P-*1*.*

Solution: Given

(Or)

, .

**Example**: Write the permutation in canonical cycle notation

Solution (312)(54)(8)(976) is a permutation in canonical cycle notation. Note that the canonical cycle notation does not omit one-cycles.

**Orbits and stabilizers**

Consider a group G acting on a set X. The orbit of an element x in X is the set of elements in X to which x can be moved by the elements of G. The orbit of x is denoted by G⋅x:

The defining properties of a group guarantee that the set of orbits of (points x in) X under the action of G form a partition of X. The associated *equivalence relation* is defined by saying x ∼ y if and only if there exists a g in G with g⋅x = y. The orbits are then the *equivalence classes* under this relation; two elements x and y are equivalent *if and only if* their orbits are the same; i.e., G⋅x = G⋅y.

The group action is *transitive* if and only if it has exactly one orbit, i.e., if there exists x in X with G⋅x = X. This is the case if and only if G⋅x = X for all x in X.

The set of all orbits of X under the action of G is written as X/G (or, less frequently: G\X), and is called the quotient of the action. In geometric situations it may be called the orbit space, while in algebraic situations it may be called the space of coinvariants, and written XG, by contrast with the invariants (fixed points), denoted XG: the coinvariants are a quotient while the invariants are a subset.

**Polya’s Theorem**:

The number of colorings of X in *n* colors in equivalent under the action of G is

where c(g) is the number of cycles of g as a permutation of X.

1. Let Xn be the set of colorings of X in n colors. Then we want to compute the number of G-orbits on Xn.
2. Let’s instead count the pairs (g, C) with C ∈ Xn a coloring and g ∈ GC ⊂ G an element of G preserving C.
3. The orbit GC of C has |G| / |GC | elements (used Lemma 1).
4. Each element of GC will appear |GC | times in our counting (used Lemma 2).

**Orbit-Stabilizer Theorem:** Let G be a finite group of permutations of a set S.

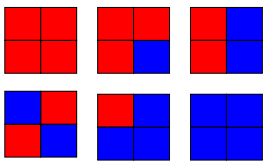
Then, for any *i* from S,



**Burnside’s Theorem:** If G is a finite group of permutations on a set S, then the number of orbits of G on S is



**Example:** Consider an n × n “chessboard” where n ≥ 2. Here we color the squares Red and Blue and two colorings are different only if one cannot be obtained from another by a rotation or a reflection.



For n = 2 there are 6 colorings.

**Example:** Determine the number of ways in which the four corners of a square can be colored with two colors. (It is permissible to use a single color on all four corners.)

Solution: Let S be the set of all colorings before the identification. To color the square with two colors (say A and B), it suffices to indicate vertices with color A. So |S| = 24 = 16.

The symmetry group D4 of the square permutes elements of S. For id ∈ D4, fix(id) = S so |fix(id)| = 16.

For R90◦ , a coloring in fix(R90◦ ) is a coloring with only one color. So |fix(R90◦ )| = 2. By the same reason, |fix(R90◦ )| = 2.

For R180◦ , two opposite vertices are moved to each other. So a coloring in fix(R180◦ ) assigns the same color for two non-adjacent vertices. So |fix(R180◦ )| = 22 = 4. Because of a similar reason, the horizontal flip H or vertical flip V has 4 fixed points set.

Finally, two diagonal flips D and D’ fix two vertices on the axis and move remaining vertices to each other. Therefore if one colors three vertices then the others are determined. Therefore |fix(D)| = |fix(D’ )| = 23 = 8.

In summary, by Burnside’s theorem,



and there are 6 ways to color.

**Example**: In how many ways can the vertices of a regular hexagon (chain with six beads) be colored using c different colors (two colorings are considered to be same if one can be obtained from other through rotation and / or reflection)?

Solution: Consider a hexagon.

1

2

3

5

4

6

6

1

2

4

3

5

5

6

1

3

2

4

e=(123456)

r1=(123456)

R2=(135)(246)

.

.

3

2

1

5

6

4

6

1

2

4

3

5

s1=((1)(26)(35)(4)

t1=(12)(36)(45)

G = {original structure, five rotational structures, three symmetric reflection structures along vertices, three symmetric reflection structures along middle of edges}

G = {e, r1, r2, r3, r4, r5, s1, s2, s3, t1, t2, t3}, |G| = 12, which is number of symmetries of regular hexagon.

Fix(e) = c6, (1)(2)(3)(4)(5)(6) = c6, no rotation, the number of cycles are 6.

Fix(r1) = c, (123456) = c1 = c, 60◦ rotation, the number of cycle is 1.

Fix(r2) = c2, (135)(246) = c1xc1 = c2, 120◦ rotation, the number of cycles are 2.

Fix(r3) = c3, (14)(25)(36) = c1xc1 xc1 = c3, 180◦ rotation, the number of

Fix(r4) = c2, (153)(264) = c1xc1 = c2, 240◦ rotation, the number of cycles are 2.

Fix(r5) = c, (165432) = c, 300◦ rotation, the number of cycle is 1.

Fix(s1) = c4, (1)(26)(35)(4), Reflection along 1 to 4, the number of cycles are 4.

Fix(s2) = c4, (2)(13)(46)(5), Reflection along 2 to 5, the number of cycles are 4.

Fix(s3) = c4, (3)(15)(24)(6), Reflection along 3 to 6, the number of cycles are 4.

Fix(t1) = c3, (12)(36)(45), Reflection &Symmetry, the number of cycles are 3.

Fix(t2) = c3, (14)(23)(56), Reflection &Symmetry, the number of cycles are 3.

Fix(t3) = c3, (16)(23)(34), Reflection &Symmetry, the number of cycles are 3.

Number of orbits for different coloring =

=

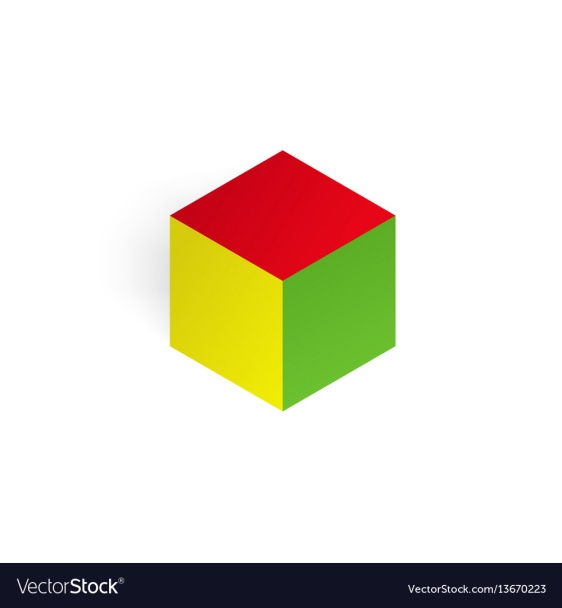
=

For two colors (red and black) = (64+48+32+8+4)/12 = 156/12 = 13.

For three colors (red, green and black) = (729+243+108+18+6)/12 = 1104/12 = 92.

**Example**: How many ways are there to color the sides of a three-dimensional cube with m colors, up to rotation of the cube?

Solution: The rotation group C of the cube acts on the six sides of the cube, which are equivalent to beads.



Consider an ordinary cube in three-space and its group of symmetries (automorphisms), call it C. It permutes the six faces of the cube. (We could also consider edge permutations or vertex permutations.) There are twenty-four automorphisms.

* The identity:

There is one such permutation and its contribution is *a*16.

* Six 90-degree face rotations:

We rotate about the axis passing through the centers of the face and the face opposing it. This will fix the face and the face opposing it and create a four-cycle of the faces parallel to the axis of rotation. The contribution is 6*a*16*a*4.

* Three 180-degree face rotations:

We rotate about the same axis as in the previous case, but now there is no four cycle of the faces parallel to the axis, but rather two two-cycles. The contribution is 3*a*12*a*22.

* Eight 120-degree vertex rotations:

This time we rotate about the axis passing through two opposite vertices (the endpoints of a main diagonal). This creates two three-cycles of faces (the faces incident on the same vertex form a cycle). The contribution is 8*a*32.

* Six 180-degree edge rotations:

These edge rotations rotate about the axis that passes through the midpoints of opposite edges not incident on the same face and parallel to each other and exchanges the two faces that are incident on the first edge, the two faces incident on the second edge, and the two faces that share two vertices but no edge with the two edges, i.e. there are three two-cycles and the contribution is 6*a*23.

The conclusion is that the cycle index of the group C is



Its cycle index is

which is obtained by analyzing the action of each of the 24 elements of C on the 6 sides of

We take all colors to have weight 0 and find that there are

different colorings.

**Exercise:**

1. Let us find the number of benzene rings with cl substituted in the place of H. The symmetry group of the benzene ring is D6 (i.e., the symmetries of a regular hexagon).
2. Count the number of distinct ways to arrange beads on a necklace, where there are 3 different colors of beads, and 3 total beads arranged on the necklace. The same color can appear on more than one bead (or it could appear on none).
3. Suppose D and R are two sets and let G be a permutation group of the set D. We define a binary relation on the set of all functions from D to R. A function f1 is related to a function f2 if and only if there is a permutation π in G such that f1(π(d)) = f2(d) for all d in D. In other words, just as in Problem 3, we are defining a notion of two functions being equivalent under a permutation π if f1 maps π(d) to the same thing as f2 maps d for all d in D. Prove this binary relation is an equivalence relation.
4. Determine the number of ways in which the vertices of an equilateral triangle can be colored with five colors so that at least two colors are used.
5. Determine the number of ways in which the edges of a square can be colored with six colors so that no color is used on more than one edge.
6. Determine the number of ways in which the faces of a cube can be colored with three colors.

**Summary:**

