# DG - Binary operations and group theory

|  |  |
| --- | --- |
| **When is a set closed under a binary operation?** | If for any two no.’s from the set, the result \* returns a no. of the set. |
| **What is the set N?** | The set of counting numbers: {1, 2, 3, ...} |
| **What is the set Z?** | The set of real integers: {..., -1, 0, +1, +2} |
| **What is the set Q?** | The set of rational numbers. |
| **What is commutative in binary operations?** | When a \* b = b \* a.  *Things such as addition are commutative where the order of operation doesn’t matter.* |
| **What is associative in binary operations?** | When (a \* b) \* c = a \* (b \* c). |
| **What is an identity element?** | e \* a = a \* e = a  A value for which under an operation \* leaves the output value unchanged from the input.  *For addition, e = 0. For multiplication, e = 1.* |
| **What is an inverse element?** | a \* a-1 = e  When value which combined with its ‘inverse’ gives the identity element.  *For addition, where e = 0, the inverse of 5 is -5. For multiplication, where e = 1, the inverse of 5 is ⅕.* |
| **What are the general rules for addition and subtraction in modular arithmetic?** | *Use the opposite signs for subtraction. Essentially, their residues are combining.* |
| **Give a proof for the addition rule of modular arithmetic** | *Where k,m, n are some integers.* |
| **What is the general rule for multiplication in modular arithmetic?** |  |
| **What is the general rule for exponentiation in modular arithmetic?** | E.g., 7 ≡ 1 (mod 3) so 76 ≡ 16 ≡ 1 (mod 3).  *Think of this as repeated multiplication. Multiply both sides by the same thing.* |
| **What is the order of a group?** | The number of elements within the group. |
| **What is the period (or order) of an element, x, of a group?** | The smallest non-negative integer such that xn = e where e is the identity element.  *Eg, an element may have period 2 since a2 = e and element c has period 3 since c3 = c(cc) = cd = e.* |
| **What are dihedral groups? How are they denoted?** | * A group of all symmetries of a regular n-gon. * Denoted by Dn where n is number of sides in the regular n-gon.   *These symmetries may include rotational or mirror.* |
| **What are cyclical groups? How do they relate to dihedral groups?** | * Groups generated by a single element. * For example, if only rotational groups are considered. The dihedral group is a cyclic group. |
| **What is a generator?** | * An element that when applied to itself, can generate all other elements in the group. * This group is a cyclic group.     *The 5th roots of unity in the complex plane under multiplication form a group of order 5. Each non-identity element by itself is a generator for the whole group.* |
| **What is a subgroup?** | A group that has the same binary operation as the parent group **AND** each element of the subgroup has its inverse in the subgroup.  *A group is a subgroup of itself just like how 7 has a factor of 7.* |
| **What is a proper subgroup?** | Any subgroup that is not the parent group itself. |
| **What is a trivial subgroup?** | A group containing only the identity element of the parent group. |
| **What are the group axioms?** | 1. Closure - the group is a set closed under the binary operation. 2. Has an identity element. 3. Each element has in inverse. 4. Binary operation is associative on all combinations of elements in the group.   Formal notation is… |
| **What is an abelian group?** | A group that also has a commutative binary operation. |
| **What is Lagrange's theorem?** | For any finite group, G, the order of every subgroup of G divides the order of G.  *This can be used to eliminate many potential subgroups.* |
| **When are two groups isomorphic? How is this denote?** | * When there is a **one-to-one mapping** which associates the elements of the first with those of the second. * A ≅ B.   *This is useful since the results proved true for the first holds true for all isomorphic groups.* |
| **How do you show two groups are or are not isomorphic?** | * Ensure the groups have the **same order.**  1. Identify the identity element in each group (this is one mapping). 2. Find the order of each element (corresponding elements will have the same order) using the Cayley Table. 3. Suggest a mapping and check.   **Example:**      *This is used as they may not have the rows and columns arranged neatly to determine it.* |
| **How does modular arithmetic work using negatives?** | * -8 (mod 5) ≡ 2 (mod 5) and **NOT** ≡ 3 (mod 5) * Since you count up. |