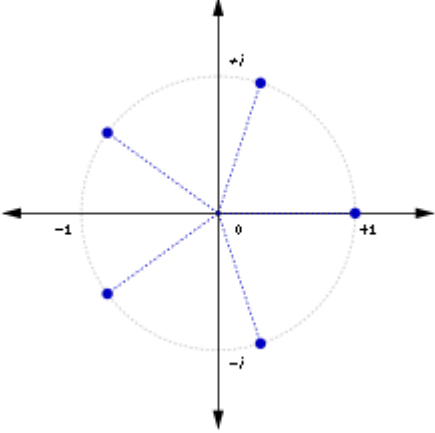


DG - Binary operations and group theory

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: $\{1, 2, 3, \dots\}$
What is the set Z?	The set of real integers: $\{\dots, -1, 0, +1, +2\}$
What is the set Q?	The set of rational numbers.
What is commutative in binary operations?	<p>When $a * b = b * a$.</p> <p><i>Things such as addition are commutative where the order of operation doesn't matter.</i></p>
What is associative in binary operations?	When $(a * b) * c = a * (b * c)$.
What is an identity element?	<p>$e * a = a * e = a$</p> <p>A value for which under an operation $*$ leaves the output value unchanged from the input.</p> <p><i>For addition, $e = 0$. For multiplication, $e = 1$.</i></p>
What is an inverse element?	<p>$a * a^{-1} = e$</p> <p>When value which combined with its 'inverse' gives the identity element.</p> <p><i>For addition, where $e = 0$, the inverse of 5 is -5. For multiplication, where $e = 1$, the inverse of 5 is $\frac{1}{5}$.</i></p>
What are the general rules for addition and subtraction in modular arithmetic?	$a \equiv c \pmod{m}$ $b \equiv d \pmod{m}$ $a + b \equiv c + d \pmod{m}$ <p><i>Use the opposite signs for subtraction. Essentially, their residues are combining.</i></p>

Give a proof for the addition rule of modular arithmetic	$a \equiv b \pmod{n}, c \equiv d \pmod{n}$ $\Rightarrow a = b + kn, c = d + mn$ $\Rightarrow a + c = (b + kn) + (d + mn)$ $= (b + d) + (k + m)n$ $= b + d \pmod{n}$ <p>Where k, m, n are some integers.</p>
What is the general rule for multiplication in modular arithmetic?	$a \equiv c \pmod{m}$ $b \equiv d \pmod{m}$ $a \cdot b \equiv c \cdot d \pmod{m}$
What is the general rule for exponentiation in modular arithmetic?	$a^e \equiv b^e \pmod{m}$ <p>E.g., $7 \equiv 1 \pmod{3}$ so $7^6 \equiv 1^6 \equiv 1 \pmod{3}$.</p> <p><i>Think of this as repeated multiplication. Multiply both sides by the same thing.</i></p>
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?	<p>The smallest non-negative integer such that $x^n = e$ where e is the identity element.</p> <p><i>Eg, an element may have period 2 since $a^2 = e$ and element c has period 3 since $c^3 = c(cc) = cd = e$.</i></p>
What are dihedral groups? How are they denoted?	<ul style="list-style-type: none"> • A group of all symmetries of a regular n-gon. • Denoted by D_n where n is number of sides in the regular n-gon. <p><i>These symmetries may include rotational or mirror.</i></p>
What are cyclical groups? How do they relate to dihedral groups?	<ul style="list-style-type: none"> • Groups generated by a single element. • For example, if only rotational groups are considered. The dihedral group is a cyclic group.

<p>What is a generator?</p>	<ul style="list-style-type: none"> • An element that when applied to itself, can generate all other elements in the group. • This group is a cyclic group.  <p><i>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.</i></p>
<p>What is a subgroup?</p>	<p>A group that has the same binary operation as the parent group AND each element of the subgroup has its inverse in the subgroup.</p> <p><i>A group is a subgroup of itself just like how 7 has a factor of 7.</i></p>
<p>What is a proper subgroup?</p>	<p>Any subgroup that is not the parent group itself.</p>
<p>What is a trivial subgroup?</p>	<p>A group containing only the identity element of the parent group.</p>
<p>What are the group axioms?</p>	<ol style="list-style-type: none"> 1. Closure - the group is a set closed under the binary operation. 2. Has an identity element. 3. Each element has an inverse. 4. Binary operation is associative on all combinations of elements in the group. <p>Formal notation is...</p>

	<div> <div>Key point</div> <p>A group (S, \odot) is a non-empty set S with a binary operation \odot such that:</p> <ul style="list-style-type: none"> \odot is closed in S \odot is associative there is an identity element such that $x \odot e = e \odot x = x$ for all x each element has an inverse x^{-1} such that $x \odot x^{-1} = x^{-1} \odot x = e$ </div>
What is an abelian group?	A group that also has a commutative binary operation.
What is Lagrange's theorem?	<p>For any finite group, G, the order of every subgroup of G divides the order of G.</p> <p><i>This can be used to eliminate many potential subgroups.</i></p>
When are two groups isomorphic? How is this denote?	<ul style="list-style-type: none"> When there is a one-to-one mapping which associates the elements of the first with those of the second. $A \cong B$. <p><i>This is useful since the results proved true for the first holds true for all isomorphic groups.</i></p>
How do you show two groups are or are not isomorphic?	<ul style="list-style-type: none"> Ensure the groups have the same order. <ol style="list-style-type: none"> Identify the identity element in each group (this is one mapping). Find the order of each element (corresponding elements will have the same order) using the Cayley Table. Suggest a mapping and check. <p>Example:</p>

A group G under the binary operation \bullet has the Cayley table

\bullet	p	q	r	s
p	p	q	r	s
q	q	p	s	r
r	r	s	q	p
s	s	r	p	q

A second group $H = (\{i, -i, 1, -1\}, \times)$

Show that H is isomorphic to G and state the corresponding elements in each group.

The Cayley table for H is

\times	i	$-i$	1	-1
i	-1	1	i	$-i$
$-i$	1	-1	$-i$	i
1	i	$-i$	1	-1
-1	$-i$	i	-1	1

The identity element for H is 1 since $1 \times a = a \times 1 = a$

Elements 1 and -1 are self-inverse, so 1 corresponds to p and -1 to q

Reorder the columns and rows in the Cayley table:

\times	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Hence i corresponds to r and $-i$ corresponds to s

The groups are isomorphic.

The corresponding elements for each group are

$1 \leftrightarrow p, -1 \leftrightarrow q, i \leftrightarrow r$ and $-i \leftrightarrow s$

By reordering the columns and rows in the Cayley table, you can see that the pattern of entries here is the same as in the Cayley table for G

Note that this correspondence is not unique. Interchanging i and $-i$ would also give the same pattern of entries as in G

This is used as they may not have the rows and columns arranged neatly to determine it.

How does modular arithmetic work using negatives?

- $-8 \pmod{5} \equiv 2 \pmod{5}$ and **NOT** $\equiv 3 \pmod{5}$
- Since you count up.