II

Algebraic Preliminaries

Def. A group $\langle G, \circ \rangle$ is an algebraic structure, where G is a set and $\circ$ is a composition on that set such that the following hold:

i) closure $\quad g \circ h \in G \quad \forall g, h \in G$

ii) associativity $\quad g \circ (h \circ k) = (g \circ h) \circ k \quad \forall g, h, k \in G$

iii) identity $\quad \exists e \in G$ such that $e \circ g = g \circ e = g$ $\forall g \in G$.

iv) inverses $\quad \forall g \in G,\ \exists g^{-1} \in G$ such that
$$g \circ g^{-1} = g^{-1} \circ g = e.$$

Def. An Abelian group, or commutative group is a group for which the commutative axiom holds. i.e., $g \circ h = h \circ g \quad \forall g, h \in G$.

Def. The order, or cardinality of a group, denoted $|G|$, is the number of elements in the set G.

Examples of groups:

$\langle \mathbb{Q} - \{0\}, \cdot \rangle$,

$\langle \mathbb{Z}, + \rangle$,

$\langle \mathbb{R} - \{0\}, \cdot \rangle$,

$\langle \mathbb{R}, + \rangle$,

$\langle \mathbb{Z}_n, +_n \rangle$ addition of integers modulo n.

Examples of $\langle \mathbb{Z}_n, +_n \rangle$

$n = 2$: $\langle \mathbb{Z}_2, +_2 \rangle$ where $\mathbb{Z}_2 = \{0, 1\}$

Composition table

$+_2$	0	1
0	0	1
1	1	0

Observe that the identity $e = 0$.

$n = 3$: $\langle \mathbb{Z}_3, +_3 \rangle$: $\mathbb{Z}_3 = \{0, 1, 2\}$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

1 is actually $[1] = \{\ldots, -2, 1, 4, 7, \ldots\}$ equivalence class

Several observations

- $1^{-1} = 2$ as $1 +_3 2 = 0$
- Each element in $\mathbb{Z}_3$ appears once in each row and each column.

Lemma: The identity of a group is unique

Proof: Assume that two identities exist. Call them e_1, e_2 ... Now what

Lemma: Every element of a group has a unique inverse.

Proof: Once again, assume the premise is false. i.e. Assume $g \in G$ has two inverses, say g_1, g_2.

then $g_1 \circ g = e = g_2 \circ g$

hence $(g_1 \circ g) \circ g_1 = (g_2 \circ g) \circ g_1$

$g_1 \circ (g \circ g_1) = g_2 (g \circ g_1)$ //assoc.

$g_1 \circ e = g_2 \circ e$ // definition of inverse

$g_1 = g_2$

Lemma: $\forall a, b$ in a group $\langle G, \circ \rangle$

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$$

Proof:

$$(b^{-1} \circ a^{-1}) \circ (a \circ b)$$
$$= b^{-1} \circ (a^{-1} \circ a) \circ b$$
$$= b^{-1} \circ b$$
$$= e$$

we're only half done! ... What remains?

Lemma: $\forall a, b \in G$, the equation $a \circ x = b$ has a unique solution x in G.

Proof:

$a \circ x = b$

$a^{-1} \circ (a \circ x) = a^{-1} \circ b$ // existence of inverses

$(a^{-1} \circ a) \circ x = a^{-1} \circ b$ // associativity

$e \circ x = a^{-1} \circ b$ // def. of inverse

$x = a^{-1} \circ b$ // def. of identity

There is only one composition table (up to isomorphism) for a 3-element group.

$\circ$	e	α	β
e	e	α	β
α	α	?	?
β	β	?	?

We cannot have repeats in a row (or column)

e.g. Let $\beta \circ \alpha = \beta$

then $\beta^{-1} \circ (\beta \circ \alpha) = \beta^{-1} \circ \beta$

$(\beta^{-1} \circ \beta) \circ \alpha = e$

$e \circ \alpha = e$

$\alpha = e$

but then this group has only two elements!

Continuing

$\circ$	e	α	β
e	e	α	β
α	α	β	e
β	β	e	α

there were no choices

Observe that this group is commutative. How do we know?

How many distinct groups are there of order 4?

G_1:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

G_2:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

G_1 is not isomorphic to G_2!

Consider these groups of order 4:

$\boxed{\langle \mathbb{Z}_4, +_4 \rangle}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\boxed{\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle}$

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

They appear different ... however

Consider the bijection $f : \langle \mathbb{Z}_4, +_4 \rangle \to \langle \mathbb{Z}_5, \cdot_5 \rangle$

$\langle \mathbb{Z}_4, +_4 \rangle$		$\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$	
$f(0)$	$=$	1	// identies mapped into each other
$f(1)$	$=$	2	// $\underbrace{1 +_4 1 +_4 1 +_4 1 = 0}_{\text{in } \mathbb{Z}_4}$ $\underbrace{2 \cdot_5 2 \cdot_5 2 \cdot_5 2 = 1}_{\text{in } \mathbb{Z}_5 \setminus 0}$

Def: The order of an element g in a group G is the minimal k such that $g^k = e$.

$1^4 = 0$ in $\langle \mathbb{Z}_4, +_4 \rangle$, the order of 1 is four.
$2^4 = 1$ in $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$, " " " 2 " "

Continuing

$f(2)$	$=$	4	// Why?
$f(3)$	$=$	3	// ditto ...

Exercise: Prove that $\langle \{1, -1, i, -i\}, \cdot \rangle$ is isomorphic to either group above.

Commutative Diagrams to Establish Isomorphisms

$$
\begin{tikzcd}
\mathbb{Z}_4 \times \mathbb{Z}_4 \arrow[rr, "+_4"] \arrow[d, "f"'] & & \mathbb{Z}_4 \arrow[d, "f"] \\
\mathbb{Z}_5 \setminus \{0\} \times \mathbb{Z}_5 \setminus \{0\} \arrow[rr, "\cdot_5"] & & \mathbb{Z}_5 \setminus \{0\}
\end{tikzcd}
$$

Operation performed in $\langle \mathbb{Z}_4, +_4 \rangle$ and then mapped to $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$

Operations performed in $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$

If the structures are isomorphic, then we obtain the same results each way.

For example:

$2 +_4 3 = 1$ in $\langle \mathbb{Z}_4, +_4 \rangle$

$f(1) = 2$ // equivalent result in $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$

OR

$$
\begin{array}{ccccc}
2 & +_4 & 3 & & \\
f\downarrow & & f\downarrow & & \\
4 & \cdot_5 & 3 & = & 2
\end{array}
$$

Instead of performing the computations in $\langle \mathbb{Z}_4, +_4 \rangle$, you can map the operands (by applying the isomorphism f) to their equivalent elements in $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$ And perform operation in the second structure, i.e. $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot_5 \rangle$.

Naturally, to complete the proof, 15 additional commutative diagrams are required.

Why?

Def. A subgroup of a group G is a subset of elements of the set G that forms a group under the composition of the group

example $H = \langle \{0, 2\}, +_4 \rangle$ is a subgroup of $\langle \mathbb{Z}_4, +_4 \rangle$

operator of original group

$+_4$	0	2
0	0	2
2	2	0

There are $\binom{4}{2} = 6$ subsets of size 2. Why does no other subset with 2 elements form a subgroup?

Referring to the definition for subgroup, are there other subgroups of $\langle \mathbb{Z}_4, +_4 \rangle$?

Thm: Let H be a subgroup of G. Then the identity of H is the same as the identity of G. Furthermore, the inverses of the elements of H coincide in G and H.

Thm: Let H be a non-empty subset of G. Then H forms a subgroup of the group G iff $(h_1 \circ h_2^{-1}) \in H \quad \forall h_1, h_2 \in H$.

Thm: Let H be a finite subset of a group G s.t. H is closed under the group composition. Then H forms a subgroup of G.

Cosets of a Group

Def: Let K be a subset of elements of a group $\langle G, \circ \rangle$, and let $g \in G$. Then the set $g \circ K$ is the set $\{ g \circ k \mid k \in K \}$

Def: Let H be a subgroup of G. The left cosets of G relative to H are defined to be sets of the form $g \circ H$ where $g \in G$. Right cosets are sets of the form $H \circ g$.

Some examples

Let $G = \langle \mathbb{Z}_4, +_4 \rangle$ and $H = \langle \{0, 2\}, +_4 \rangle$

The left cosets of H in G =
$0 +_4 \{0,2\} = \{0,2\}$
$1 +_4 \{0,2\} = \{1,3\}$
$2 +_4 \{0,2\} = \{2,0\}$
$3 +_4 \{0,2\} = \{3,1\}$

Observe that there are two unique left cosets. $\{0,2\}$ and $\{1,3\}$

The right cosets of H in G =
$\{0,2\} +_4 0 = \{0,2\}$
$\{0,2\} +_4 1 = \{1,3\}$
$\{0,2\} +_4 2 = \{2,0\}$
$\{0,2\} +_4 3 = \{3,1\}$

Once again two of these right cosets are unique : $\{0,2\}$ and $\{1,3\}$

The left cosets equal the right cosets. Why was this predictable?

II

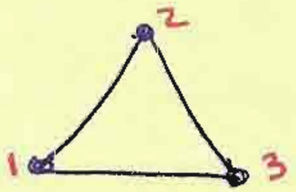
Def: The number of left cosets of G relative to H is called the index of H under G, and is written $[G:H]$.

Thm: (Lagrange 1771) If H is a subgroup of G, then $|H|$ divides $|G|$.

Def: A subgroup H of a group G is said to be a normal subgroup if the left coset partition induced by H is identical to the right coset partition induced by H. Equivalently, H is normal if $g \circ H = H \circ g \ \forall g \in G$.

→ If G is abelian (commutative) then every subgroup is normal.

Examples



Consider an equilateral triangle under clockwise (cw) rotations of $0°$, $120°$, and $240°$
π_0, π_1, π_2

Now, envision each rotation acting upon the set of vertices $\{1,2,3\}$.

permutation notation

π_0 is equivalent to $\begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix}$: each vertex mapped to itself.

π_1 " " " $\begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix}$

and π_2 " " " $\begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}$

Claim: The set of these rotations of an equilateral triangle under the operation - composition of rotations (or equivalently, composition of permutations *)

$\boxed{C_3}$

$\circ$	π_0	π_1	π_2
π_0	π_0	π_1	π_2
π_1	π_1	π_2	π_0
π_2	π_2	π_0	π_1

cyclic group of order 3 - rotations of an equilateral triangle.

where $\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\xrightarrow{}$ left composition *

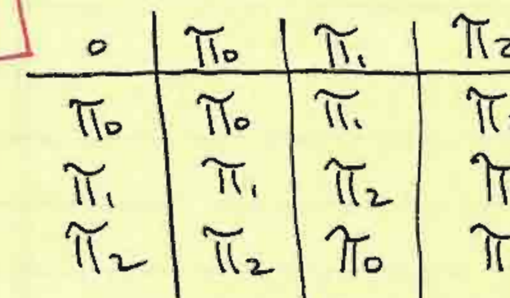
$\pi_1^{-1} = ?$

$\pi_2^{-1} = ?$

What is C_4? C_5?

Next, consider these three rotations as well as the following three flips and complete this table:

$\boxed{D_3}$



dihedral group of degree 3 and order 6. All rigid motions of an equilateral triangle

What is D_4? D_5?

	π_0	π_1	π_2	d_1	d_2	V
π_0	π_0	π_1	π_2			
π_1	π_1	π_2	π_0			
π_2	π_2	π_0	π_1			
d_1				π_0		
d_2					π_0	
V						π_0

1) Complete the composition table
2) Find the left & right cosets of C_3 in D_3.
3) Find a subgroup H in D_3 of order 2.
4) Find the left and right cosets of H in G.
5). Are C_3 and H normal subgroups of D_3?

* N.B. p. 26 in your text - Author composes permutations right to left!