8th Lecture: 3/2

Binary Operations. This is prerequisite material, but I'll remind you of the most essential things just in case. For further reading, see the file on the Canvas page.

Definition 8.1. A *binary operation* on a set A is a function

$$* : A \times A \to A.$$

Notation 8.2. $*(a_1, a_2)$ is usually denoted $a_1 * a_2$. The default name for a binary operation is "multiplication", even though ordinary multiplication of (complex) numbers is just one example (see Example 8.11) of a binary operation. Thus, $a_1 * a_2$ is read, by default, as "a_1 times a_2".

Definition 8.3. Let $*$ be a binary operation on a set A. We say that $*$ is *commutative* if

$$a_1 * a_2 = a_2 * a_1 \;\; \forall\, a_1,\, a_2 \in A.$$

Definition 8.4. Let $*$ be a binary operation on a set A. We say that $*$ is *associative* if

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3) \;\; \forall\, a_1,\, a_2,\, a_3 \in A.$$

Definition 8.5. Let $*$ be a binary operation on a set A. An element $e \in A$ is said to be an *identity* for $*$ if

$$a * e = e * a = a \;\; \forall\, a \in A.$$

Proposition 8.6. *Let $*$ be a binary operation on a set A. An identity for $*$, if it exists, is unique.*

PROOF: Let e and f be identities for $*$ and consider $e * f$. Since e is an identity, the product must be f. On the other hand, since f is an identity, the product must be e. Hence $e = f$, v.s.v.

Notation 8.7. When we use the default term "multiplication" for a binary operation with identity, we by default write 1 for the latter.

Definition 8.8. Let $*$ be a binary operation with identity 1 on a set A, and let $a \in A$. An element $b \in A$ is said to be an *inverse* of a (with respect to $*$) if

$$a * b = b * a = 1.$$

Proposition 8.9. *Let $*$ be an associative binary operation with identity 1 on a set A, and let $a \in A$. An inverse for a, if it exists, is unique.*

PROOF: Suppose b and c are both inverses of a. Thus

$$a * b = b * a = a * c = c * a = 1.$$

It follows that (note the use of associativity !)

$$b = b * 1 = b * (a * c) \overset{\text{assoc.}}{=} (b * a) * c = 1 * c = c, \quad \text{v.s.v.}$$

Example 8.10. Ordinary addition $+$ is a commutative and associative binary operation on $A = \mathbb{Z}_+$. To get an identity, we need to add zero, thus extend to $A = \mathbb{Z}_+ \cup \{0\} = \mathbb{N}$.

In order for every element to have an inverse, we need to add all negative integers, thus extend to $A = \mathbb{Z}$. We can also consider $+$ as a binary operation on any of the sets $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, for example.

Example 8.11. Ordinary multiplication $\times$ is a commutative and associative binary operation on $A = \mathbb{Z}_+$. We already have an identity, namely 1. But in order for every element to have an inverse, we need to add all non-zero quotients of integers, thus extend to $A = \mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$. We can also consider $\times$ as a binary operation on any of the sets $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$ or $\mathbb{C}^\times = \mathbb{C}\backslash\{0\}$, for example.

Example 8.12. Subtraction $-$ and division $/$ are (silly) examples of non-commutative and non-associative binary operations (on suitably chosen sets of numbers):

$$\begin{aligned} a - b &\neq b - a, \\ (a-b)-c = a-b-c &\neq a-(b-c) = a-b+c, \\ a/b &\neq b/a, \\ (a/b)/c = a/bc &\neq (a/b)/c = ac/b. \end{aligned}$$

Example 8.13. For $n \in \mathbb{Z}_+$, let $\mathbb{M}_n(\mathbb{R})$ denote the set of all $n \times n$ matrices with real entries. Matrix multiplication is a binary operation on this set. As you have learned in linear algebra,

(i) matrix multiplication is associative
(ii) matrix multiplication is non-commutative for all $n \geq 2$
(iii) the matrix $I_n = \text{diag}(1, 1, \ldots, 1)$ is an identity
(iv) a matrix $M \in \mathbb{M}_n(\mathbb{R})$ has an inverse if and only if $\det(M) \neq 0$.

One denotes

$$\mathrm{GL}_n(\mathbb{R}) = \mathbb{M}_n(\mathbb{R})^\times = \{M \in \mathbb{M}_n(\mathbb{R}) : \det(M) \neq 0\}$$

for the so-called *general linear group of order* n *over* $\mathbb{R}$.

Recall from linear algebra that each matrix $A \in \mathbb{M}_n(\mathbb{R})$ corresponds to a so-called *linear transformation on* $\mathbb{R}^n$, that is, a function $f_A : \mathbb{R}^n \to \mathbb{R}^n$ given by $f_A(\boldsymbol{x}) = A\boldsymbol{x}$. Matrix multiplication thereby corresponds to composition of linear transformations, since

$$(f_A \circ f_B)(\boldsymbol{x}) = A(f_B(\boldsymbol{x})) = A(B\boldsymbol{x}) \overset{\text{assoc.}}{=} (AB)\boldsymbol{x} = f_{AB}(\boldsymbol{x}).$$

Hence, Example 8.13 is just a special case of

Example 8.14. Let S be any set and let $\mathcal{A} = \mathcal{A}_S$ be the set of all functions from S to itself. Composition of functions is a binary operation on $\mathcal{A}$. Note that the standard way to denote composition of functions is with the "after" symbol $\circ$. Thus $f \circ g$ means that one applies the function g first: $(f \circ g)(s) = f(g(s))$. With this convention:

(i) $\circ$ is always associative

$$((f \circ g) \circ h)(s) = (f \circ (g \circ h))(s) = f(g(h(s))).$$

(ii) $\circ$ is non-commutative whenever $|S| > 1$. Let's take $|S| = 2$, say $S = \{1, 2\}$. There are $2^2 = 4$ functions from S to itself, namely

$$f_1(1) = 1,\ f_1(2) = 1; \quad f_2(1) = 2,\ f_2(2) = 2;$$
$$f_3(1) = 1,\ f_3(2) = 2; \quad f_4(1) = 2,\ f_4(2) = 1.$$

We see, for example, that $f_1 \circ f_2 \neq f_2 \circ f_1$ since $f_1 \circ f_2 = f_1$ and $f_2 \circ f_1 = f_2$.

(iii) The identity function $1_S(s) = s\ \forall\, s \in S$ is always an identity for $\circ$.

(iv) A function $f : S \to S$ has an inverse if and only if f is bijective, hence a permutation of S.

Groups. The concept of a group is probably the single most important concept in modern algebra. The definition (see below) imposes just enough structure to lead to a rich theory. You can find many books in the library just on the subject of *Group theory*.

Definition 8.15. Let G be a set and $*$ a binary operation on G. The pair $(G, *)$ is called a *group* if
(i) $*$ is associative
(ii) there exists an identity for $*$ in G
(iii) every element $g \in G$ has an inverse w.r.t. $*$.

When the binary operation $*$ is understood, one usually just writes G rather than $(G, *)$ to denote the group.

Definition 8.16. Let $(G, *)$ be a group. If $*$ is commutative, we say that G is an *abelian group*. If $*$ is not commutative, we say G is *non-abelian*.

Notation 8.17. In a non-abelian group it is conventional to always use multiplicative notation. Hence one denotes the identity element as 1, denotes the inverse of g as g^{-1} and, in general, writes gh for $g * h$.
In an abelian group it is conventional to always use additive notation. Hence one denotes the identity element as 0, denotes the inverse of g as $-g$ and, in general, writes $g + h$ for $g * h$.

Now let's revisit the examples from above.

Example 8.10+ $(\mathbb{Z}, +)$ is an abelian group.

Example 8.11+ $(\mathbb{Q}^\times, \times)$ is an abelian group.

Example 8.13+ $\mathrm{GL}_n(\mathbb{R})$ is a non-abelian group, under matrix multiplication, for each $n \geq 2$. Note, by the way, that $\mathbb{M}_n(\mathbb{R})$ is an abelian group under matrix addition.

Example 8.14+ For a set S, let G_S be the set of all permutations of S. Then G_S is a group under composition of functions. Note that, if S is a finite set, then so is G_S

and $|G_S| = |S|!$. In particular, one denotes by S_n the group of all permutations of $\{1, 2, \ldots, n\}$. It is called the *symmetric group of order* n. We have $|S_n| = n!$.

S_n is non-abelian for all $n \geq 3$. For $n = 3$, the $3! = 6$ elements of S_3 can be visualised as the symmetries of an equilateral triangle, see Figure 8.1. Each geometrical transformation corresponds to a function on the set $\{1, 2, 3\}$, by considering what happens to the three vertices of the triangle. Indeed, there are two ways to translate a geometrical transformation to a function:

$f^1(i) =$ the vertex to which i is moved
$f^2(i) =$ the vertex which replaces i.

It is clear that, as functions on $\{1, 2, 3\}$, f^1 and f^2 will be each others' inverses. In Figure 8.1, I have chosen the first option for the translation.

Important Remark 8.18. When using default multiplicative notation in an abelian group G, the convention is to read products $g_1 g_2$ "from left to right". On the other hand, when the underlying binary operation is composition of functions, the standard $\circ$ notation implies that one should read "from right to left". [1] One must remember this when one uses the group notation and the group elements represent permutations of a set.[2]

When the group elements can be represented geometrically, as in Example 8.14+, there is the additional complication, as mentioned above, that there are two ways to translate from the geometrical transformation to a permutation of a set. One of these is the inverse of the other, which is the same thing as "changing the order of multiplication" since $(gh)^{-1} = h^{-1}g^{-1}$. The important thing is to always be consistent, whatever notation one chooses. In Figure 8.1, the group notation corresponds to performing the geometrical transformations in reverse order. For example:

$$f_5 = f_4 f_2 = f_2 \circ f_4, \qquad T_5 = T_4 \circ T_2.$$

[1]This is a special case of the more general fact that, if $*$ is a binary operation on a set A, then so is the operation $\circ$ given by $a_1 \circ a_2 = a_2 * a_1$. The operation $\circ$ will satisfy any of the properties in Definitions 8.3, 8.4, 8.5, 8.8 if and only if $*$ does so.

[2]In fact, there is a general theorem which says that *any* group is a group of permutations on some set. See Lecture X.