Binary operations

Aim lecture: We introduce the language of groups which unifies algebraic properties & ideas found in various aspects of linear algebra & the study of symmetry.

Defn

Let G be a set. A *binary operation* $*$ on G is a function $* : G \times G \longrightarrow G$. We use the following notation: for $g, g' \in G$, the binary operation $*$ maps (g, g') to $g * g'$. Given such a binary operation we say $*$ is

1. *associative* if for all $g, g', g'' \in G$ we have $(g * g') * g'' = g * (g' * g'')$.
2. *commutative* if for all $g, g' \in G$ we have $g * g' = g' * g$.

E.g. Let $G = \mathbb{N}, \mathbb{Z}, \mathbb{R}$ or $\mathbb{C}$. Then $+$ is a binary operation on G which is associative & commutative.

Examples of binary operations

E.g. 1 Let G be either $\mathbb{R}^\times = \mathbb{R} - 0$ or $\mathbb{C}^\times = \mathbb{C} - 0$. Then $* =$ usual multiplication of real or complex numbers is a binary operation which is

E.g. 2 Matrix multn is a binary operation on $M_{nn}(\mathbb{R})$ & $M_{nn}(\mathbb{C})$ which is

E.g. 3 Composition of permutations defines an associative binary operation on S_n.

E.g. 4 The cross product is a binary operation on $\mathbb{R}^3$ which is

Identity

Prop-Defn

Let $*$ be a binary operation on a set G. We say $e \in G$ is an *identity* for $*$ if $e * g = g = g * e$ for $g \in G$. G can have at most one identity element, so we may speak of *the* identity element (if it exists).

Proof.

E.g.

Definition of group

Defn

A *group* consists of a set G with a binary operation $*$ called the *group law* or *group multiplication* such that the following axioms hold

1. $*$ is associative.
2. There is an identity for $*$ (necessarily unique), often denoted by e_G or just e if no confusion arises. (Other common notn is 1_G). It is called the *group identity*.
3. For every $g \in G$, there exists $g' \in G$ such that $g * g' = e = g' * g$. Such an element is called a *(group) inverse* for g & is usually denoted g^{-1}.

The notation for such a group is $(G, *)$ or just G if no confusion arises as to what the group multn is.
We say the group $(G, *)$ is *abelian* or *commutative* if $*$ is commutative.

Examples of groups involving numbers

E.g. 1 Let $G = \mathbb{Z}, \mathbb{R}$ or $\mathbb{C}$. Then $(G, +)$ is an abelian group with identity $e_G =$
the group inverse

E.g. 2 $(\mathbb{N}, +)$ is not a group since

E.g. 3 $G = \mathbb{R}^\times$ or $\mathbb{C}^\times$

The group S_n

Propn

The set of permutations S_n equipped with the binary operation, composition of permutations, is a group. The identity is $e = \mathrm{id}$, the identity function. The inverse function of any permutation $\sigma \in S_n$ is a permutation which is a group inverse for σ.

Matrix groups

Note that $M_{nn}(\mathbb{R}), M_{nn}(\mathbb{C})$ are not groups when equipped with the binary operation, matrix multn. However

Prop-Defn

Let $GL_n(\mathbb{R})$ (resp $GL_n(\mathbb{C})$) denote the set of invertible matrices in $M_{nn}(\mathbb{R})$ (resp $M_{nn}(\mathbb{C})$). Let $G = GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$ be equipped with the binary operation matrix multn. Then G is a group. The group identity is the identity matrix I_n & the matrix inverse is a group inverse too.

Group inverses

Prop

Let $(G, *)$ be a group with identity e.

1. (Cancellation law) Let $g, g', h \in G$. If $g * h = g' * h$ then $g = g'$. If $h * g = h * g'$ then $g = g'$.
2. (Uniqueness of inverse) An element $g \in G$ has a unique group inverse.
3. Let $g, g' \in G$ be s.t. $g * g' = e$. Then $g' = g^{-1}$.

Proof. 2) If $g * h = g' * h$ & h^{-1} is a group inverse to h then

$$g = g*e = g*(h*h^{-1}) = (g*h)*h^{-1} = (g'*h)*h^{-1} = g'*(h*h^{-1}) = g'*e = g'.$$

Other case is similar.

2) Let h, h' be a groups inverses to g. Result follows on applying cancellation law to

3) Again just apply cancellation law to

Associativity & n-fold products

Consider an associative binary operation $*$ on a set G which we abbreviate to $g * g' = gg'$ (i.e. $*$ = juxtoposition) . For $g_1, g_2, \ldots, g_n \in G$, associativity allows us to define the triple product $g_1g_2g_3$ to be the element $(g_1g_2)g_3 = g_1(g_2g_3)$. More generally,

Propn-Defn

No matter how you bracket to calculate the n-fold product $g_1g_2 \ldots g_n$, the answer is the same (as say for example to $((\ldots((g_1g_2)g_3)\ldots)g_n)$). We may thus define the n-fold product without brackets to be this common element of G.

Proof. You should understand why this is true by observing that the associative law allows you to "push brackets" to the left.
More formally, we argue by induction on n. Choose some way of bracketing so that the last multn is say $g_1 \ldots g_k$ times $g_{k+1} \ldots g_n$ (& by induction, we don't need to bracket these!). We use downward induction on k to show the answer is the same as that for $(g_1 \ldots g_{n-1})g_n$, the case $k = n - 1$ being trivial.

End of proof

Now for $k < n-1$ we have

$$\begin{aligned}(g_1 \dots g_k)(g_{k+1} \dots g_n) &= (g_1 \dots g_k)(g_{k+1}(g_{k+2} \dots g_n)) \\ &= ((g_1 \dots g_k)g_{k+1})(g_{k+2} \dots g_n) \\ &= (g_1 \dots g_{k+1})(g_{k+2} \dots g_n)\end{aligned}$$

so we're done by induction.

Rem The number of ways you can bracket an n-fold product is an interesting number called the n-th Catalan number.

A word about group theory

Groups are interesting mathematical objects which are studied in the third year course MATH3711. They capture many ideas in mathematics, most notably, that of symmetry.

Unfortunately, we will not see much of the general theory, and only use it as a convenient language to describe various notions in linear algebra.

Groups were probably first "invented" by Galois in the early nineteenth century to show that the general quintic polynomial cannot be solved by radicals. This is taught in the 3rd/4th year course MATH5725: Galois theory.