Group Theory: algebra of transformations

Evgeny Khukhro

School of Mathematics and Physics

11 July 2017
Transformations

Throughout mathematics, most important are transformations preserving certain structures (sometimes called “symmetries”).

Example

In geometry on the plane, “structure” means distance = shape of figures.

Which transformations of the plane preserve this structure?

Answer: mirror reflections in an axis, rotations about a point, parallel translations, and their combinations.

Example

Equation \(x_1 x_2^2 x_3^3 + x_2 x_3^2 x_1^3 + x_3 x_1^2 x_2^3 = 1\) in three unknowns.

Transformations = changes of variables that do not affect the equation:

e.g. \(x_1 \rightarrow x_2, \quad x_2 \rightarrow x_3, \quad x_3 \rightarrow x_1\) is OK,

but \(x_1 \rightarrow x_2, \quad x_2 \rightarrow x_1, \quad x_3 \rightarrow x_3\) does not preserve the equation.
Groups of transformations

All transformations of a given object form a group – here “group” has precise mathematical meaning (not just any group in common language).

Example

Transformations of a square (as a rigid figure):

(such transformations are also called isometries)

- four rotations about centre $O$: through $0^\circ$, $90^\circ$, $180^\circ$, and $270^\circ$;
- four reflections:
  - with axes: vertical, horizontal,
  - and two diagonals.

These eight elements form the group of isometries $D_8$ of a square.
‘Multiplication’ of elements of a group
(often called group operation, or group composition)

Given two transformations \( g \) and \( h \) of an object \( \mathcal{A} \), we can perform one after another:

every element \( a \) in \( \mathcal{A} \) is sent \( a \xrightarrow{g} g(a) \xrightarrow{h} h(g(a)) \).

The resulting composite transformation is called the **product** \( g \circ h \)
(sometimes denoted by \( h \circ g \)).
Group is closed under multiplication

Clearly, if $g$ and $h$ preserve the structure, then so does $g \circ h$.

In other words, if $G$ is the group of all transformations preserving $A$, then $G$ is closed under multiplication of transformations:

$$g \in G \text{ and } h \in G \implies g \circ h \in G.$$ 

Example (Transformations of a square)

Let $a$ be anticlockwise rotation through $90^\circ$, and $b$ reflection in the vertical axis.

Then what is $a \circ b$?

(look where $A, B$ go!): $A \xrightarrow{a} D \xrightarrow{b} A$, so $A \xrightarrow{a \circ b} A$;

$B \xrightarrow{a} A \xrightarrow{b} D$, so $B \xrightarrow{a \circ b} D$. So $a \circ b$ must be the reflection in $AC$.

Some other products: $a^2 = a \circ a$ is rotation through $180^\circ$, $b^2 = b \circ b = \text{Id}$ is identity, which does not move anything.
Exercise

Recall: \( a \) is the anticlockwise rotation through 90°,

and \( b \) is the reflection in the vertical axis.

Problem: What is \( b \circ a \)?

Solution: \( A \xrightarrow{b} D \xrightarrow{a} C \), so \( A \xrightarrow{b \circ a} C \);

\( B \xrightarrow{b} C \xrightarrow{a} B \), so \( B \xrightarrow{b \circ a} B \);

So \( b \circ a \) must be the reflection in \( BD \).

(But note: \( b \circ a \neq a \circ b \) – reflection in \( AC \)).

Similar calculation for \( a^3 \circ b \): \( A \xrightarrow{a^3} B \xrightarrow{b} C \), so \( A \xrightarrow{a^3 \circ b} C \);

\( B \xrightarrow{a^3} C \xrightarrow{b} B \), so \( B \xrightarrow{a^3 \circ b} B \);

So \( a^3 \circ b \) must be the reflection in \( BD \). (Note: \( b \circ a = a^3 \circ b \)).
Associativity

means that always \((a \circ b) \circ c = a \circ (b \circ c)\) for transformations:

\[
\begin{align*}
\mathcal{A} & \quad \mathcal{A} & \quad \mathcal{A} & \quad \mathcal{A} \\
\text{a} & \quad \text{b} & \quad \text{c} & \\
\text{a} \circ \text{b} & \quad (a \circ b) \circ c
\end{align*}
\]

Nice: we can write without brackets: simply \(a \circ b \circ c\).
Associativity

means that always \((a \circ b) \circ c = a \circ (b \circ c)\) for transformations:

Nice: we can write without brackets: simply \(a \circ b \circ c\).
Abstract group $D_8$

From now on we do not write $\circ$, just $ab$ for $a \circ b$, or $a^3 = a \circ a \circ a$, etc.

We had our group of isometries of a square

$$D_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$  
(Here $e = \text{Id}$ is the identity transformation – when nothing is moved)

$$b^2 = e, \quad a^4 = e, \quad ba = a^3b.$$  

Abstract group – when we forget the square and work just with these eight elements using these relations.
Inverses

An inverse of $g$ is an element $g^{-1}$ such that $gg^{-1} = g^{-1}g = e$.

In $D_8$ we have inverses: $b = b^{-1}$ (because $b^2 = e$), $a^{-1} = a^3$ (because $a^4 = e$).

Inverses are useful for solving equations: e.g., solve $ax = b$ in $D_8$:

$$a^{-1}(ax) = a^{-1}b$$ (important on which side multiplying by inverses!);

by associativity: $(a^{-1}a)x = a^{-1}b$; $ex = a^{-1}b$;

so $x = a^{-1}b = a^3b$. 
Exercise

Solve the equation

\[ abxb = ba \] in \( D_8 \)

using our relations

\[
\begin{align*}
  b^2 &= e, & a^4 &= e, & ba &= a^3b, & a^{-1} &= a^3, & b^{-1} &= b
\end{align*}
\]

(remember: important on which side, and in which order, multiplying by inverses!);

Solution: \( x = b^{-1}a^{-1}bab^{-1} \)

\[ = ba^3bab = ba^3(ba)b = ba^3a^3bb \]

\[ = ba^2 = (ba)a = (a^3b)a = a^3a^3b = a^2b. \]
Abstract groups

Definition of a group

A **group** is any set of elements $G$ with an operation called ‘multiplication’ such that

- $g, h \in G \Rightarrow gh \in G$ (closed under multiplication);
- $(ab)c = a(bc)$ (associative);
- there is identity (“neutral”) element $e$ such that $ea = ae = a$ for all $a \in G$;
- for any $g \in G$ there is inverse $g^{-1}$ such that $gg^{-1} = g^{-1}g = e$.

The main example in applications: the group of transformations $G(\mathcal{A})$ preserving a structure $\mathcal{A}$: consists of 1-to-1 mappings of the underlying set of $\mathcal{A}$, the operation on $G(\mathcal{A})$ is the composition (＝‘one-after-another’). All axioms are satisfied “automatically”.

Evgeny Khukhro (SMP UoL) Group Theory: algebra of transformations 11 July 2017 13 / 1
Examples of groups

Set of integers $\mathbb{Z}$ with operation being addition (confusing! :-)), identity is 0, inverse of $a \in \mathbb{Z}$ is $-a$.

The same operations for the sets of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$.

The set of rational numbers $\mathbb{Q}$ w.r.t. ordinary multiplication: associative, there is identity 1, inverses? for all but not for 0, so this is not a group. But removing 0 we get a group $\mathbb{Q} \setminus \{0\}$ w.r.t. multiplication.

All these numerical groups are commutative: $ab = ba$, which is very nice and convenient.

But not all groups are commutative, as we saw for $D_8$, where $ab \neq ba$.

There are many other examples of groups: matrix groups, Lie groups, braid groups, etc.
Exercises

Problem

Which of the following sets form a group w.r.t. multiplication modulo 15?

(a) \{1, 4, 7, 13\}  
(b) \{2, 5, 8, 14\}  
(c) \{3, 6, 9, 12\}

Reminder: multiplication modulo 15 means taking product, then remainder after division by 15; for example, \(5 \cdot 5 \equiv 10 \pmod{15}\).

Answer: (a) is a group: \(1 = e\) identity;

closed: \(4 \cdot 7 = 13,\ 4 \cdot 13 = 7,\ 7 \cdot 13 = 1,\ 7 \cdot 7 = 4\);

inverses: \(4^{-1} = 4,\ 7^{-1} = 13,\ 13^{-1} = 7\).

(b) is not a group: not closed: \(2 \cdot 5 = 10\) not in the set.

(c) is a group with identity 6 . . . . . . . . . . . . .
Exercises

Problem
Prove that 2 × 2 matrices of the form \[
\begin{pmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{pmatrix}
\] form a group w.r.t. matrix multiplication.

Problem
Do all 2 × 2 matrices form a group w.r.t. matrix multiplication?

Problem
Do all 2 × 2 matrices with determinant 1 form a group w.r.t. matrix multiplication?
Permutation groups

A permutation of a finite set is a mapping of this set onto itself; one can think of it as a re-arrangement of a sequence. For example, let the set be \{a, b, c, d, e, f\}, an example of a permutation is

\[
\begin{pmatrix}
  a & b & c & d & e & f \\
  c & a & b & e & d & f \\
\end{pmatrix}.
\]

Usually arrows are not written: \( (a \ b \ c \ d \ e \ f) \). So permutations are transformations of the set preserving only one property: elements remain different.

Automatically form a group, called the symmetric group on these symbols.

Usually numbers are used as symbols. The group of all permutations of the set \{1, 2, \ldots, n\} is denoted by \( S_n \).
Exercise
How many permutations are there in $S_n$ altogether?

Solution: every permutation has the form

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ a_1 & a_2 & a_3 & \ldots & a_{n-1} & a_n \end{pmatrix}.$$ 

Here, $a_1$ can be any of $n$ elements.
Then $a_2$ can be any of the remaining $n-1$ elements (cannot be $a_1$, since different go to different).
Then $a_3$ can be any of the remaining $n-2$ elements (cannot be $a_1$ or $a_2$, since different go to different).
...And so on. Therefore there are $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$ possibilities; this is denoted by $n!$.

Definition
The number of elements in a group $G$ is denoted by $|G|$.

Thus, $|S_n| = n!$. For example, $|S_3| = 3! = 6$; $|S_4| = 4! = 24$, and so on.

Earlier we had $|D_8| = 8$. 
Products of permutations

Compute:

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
5 & 3 & 2 & 1 & 4
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
2 & 3 & 5 & 1 & 4
\end{pmatrix}
= \\
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
5 & 3 & 2 & 1 & 4
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
2 & 3 & 5 & 1 & 4
\end{pmatrix}
= \\
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
5 & 3 & 2 & 1 & 4
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
2 & 3 & 5 & 1 & 4
\end{pmatrix}
= \\
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
4 & 5 & 3 & 2 & 1
\end{pmatrix}
\]

So the answer is 

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
4 & 5 & 3 & 2 & 1
\end{pmatrix}
\]

Permutation groups are not commutative:

\[
\begin{pmatrix}
1 & 2 & 3 \\
2 & 3 & 1
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 2 & 3 \\
2 & 1 & 3
\end{pmatrix}
= \\
\begin{pmatrix}
1 & 2 & 3 \\
1 & 3 & 2
\end{pmatrix},
\]

but 

\[
\begin{pmatrix}
1 & 2 & 3 \\
2 & 1 & 3
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 2 & 3 \\
2 & 3 & 1
\end{pmatrix}
= \\
\begin{pmatrix}
1 & 2 & 3 \\
3 & 2 & 1
\end{pmatrix}.
\]
Inverse permutation

This is easy: flip it!

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
5 & 3 & 2 & 1 & 4 \\
\end{pmatrix}
\cdot
\begin{pmatrix}
5 & 3 & 2 & 1 & 4 \\
1 & 2 & 3 & 4 & 5 \\
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
\end{pmatrix}
= e
\]

So inverse is

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
5 & 3 & 2 & 1 & 4 \\
\end{pmatrix}^{-1}
= \begin{pmatrix}
5 & 3 & 2 & 1 & 4 \\
1 & 2 & 3 & 4 & 5 \\
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
4 & 3 & 2 & 5 & 1 \\
\end{pmatrix}.
\]
Exercise

Solve the equation (find the unknown permutation $X$):

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} \cdot X \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$.

(Remember, it is important on which side you multiply by the inverse!)

Solution:

$X = \left( \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} \right)^{-1} \cdot \left( \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \right) \cdot \left( \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \right)^{-1} =$

$= \begin{pmatrix} 5 & 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} =$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}.$
Cyclic notation

This is just another form of writing a permutation: e.g.

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
2 & 3 & 4 & 8 & 7 & 5 & 6 & 1 \\
\end{pmatrix}
= (12348)(576).
\]

Each cycle, like \((12345)\) means \(1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 1\), that is,

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
2 & 3 & 4 & 5 & 1 \\
\end{pmatrix}.
\]

One-element cycles are usually omitted:

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 1 & 4 & 7 & 6 & 5 \\
\end{pmatrix}
\]
Theorem: every permutation decomposes into independent cycles. Why?
different must go to different!
so a cycle must be formed
different must go to different!
so cycles must be disjoint
Advantages of independent cycles:

- They commute: in particular, if $c, d$ are independent cycles, then
  \[(cd)^k = \underbrace{cd cd \ldots cd}_{k} = c^k d^k\]
  (would not be true if $c, d$ did not commute!).

- Easy to find powers. In particular, $(1 2 \ldots m)^m = e$. 
Example

Problem

How to find \((\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 8 & 7 & 5 & 6 & 1 \end{pmatrix})^{2017}\)?

Use cycles: \((\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 8 & 7 & 5 & 6 & 1 \end{pmatrix})^{2017} = ((12348)(576))^{2017} =\)

because they commute! \((= (12348)^{2017} \cdot (576)^{2017} =\)

(because \(2017 = 5 \cdot 403 + 2\) and \(2016 = 3 \cdot 672 + 1\))

\((= (12348)^2 \cdot (576) = (13824) \cdot (576) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 8 & 1 & 7 & 5 & 6 & 2 \end{pmatrix}.\)
Generators

**Definition**

A group $G$ is said to be generated by a subset $M$ if every element of $G$ is a product of elements in $M$ or their inverses.

Example: $D_8 = \{ e, a, a^2, a^3, b, ab, a^2b, a^3b \}$ is generated by $a, b$ (that is, by the set $M = \{ a, b \}$).
Exercise

Problem

Prove that $S_n$ is generated by all cycles of length 2 (which are called transpositions). In other words, prove that every permutation is a product of some transpositions $(ij)$ (not necessarily independent).

Solution: We already know that every permutation is a product of several cycles. Therefore it is sufficient to represent any cycle $(a_1a_2 \ldots a_k)$ as a product of transpositions. Like this:

$$(a_1a_2 \ldots a_k) = (a_1a_2) \cdot (a_1a_3) \cdot (a_1a_4) \cdots (a_1a_{n-1}) \cdot (a_1a_n).$$

For example,

$$
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 1 & 6 & 7 & 5
\end{pmatrix}
= (1234) \cdot (567) = (12) \cdot (13) \cdot (14) \cdot (56) \cdot (57).
$$
Application

Problem
Prove that the symmetry group of a regular tetrahedron $ABCD$ is $S_4$. Moreover, any permutation of the 4 vertices can be realized as a combination (product) of several mirror reflections.

Solution: Reflection in the plane through $B$, $D$ and midpoint $M$ of $AC$ transposes $A$ and $C$ and leaves $B$, $D$ fixed. So this is a transposition ($AC$) in the group $S_4$ of permutations of the vertices. There are similar transpositions for every pair of vertices. By the previous exercise they generate the whole group $S_4$. 
Parity of a permutation

**Definition**

The parity of a permutation is the parity of the number of transpositions whose product is equal to our permutation.

It is a fact (can be proved) that the parity is independent of the way you express the permutation as a product of transpositions.
15 puzzle

Every move changes the parity of the permutation of the 16 symbols (empty square as “ghost” 16th symbol), and changes the parity of the sum of the row number and column number of the empty square. Therefore the parity of the sum of these parities stays the same.

Hence it is impossible to pass from one state to another if this parity is different.
Obtaining greater commutativity

Definition

A group $G$ is said to be commutative (or Abelian) if all elements commute: $ab = ba$ for any $a, b \in G$.

Commutativity is very desirable. So getting more commutativity is good.

Example

Suppose that $G$ is a group such that $g^2 = e$ for every $g \in G$. Then $G$ is commutative.

Proof: for every $a, b \in G$ we have $(ab)(ab) = e$;

times $a$ on the left, times $b$ on the right, use associativity:

$a(ab)(ab)b = aeb; (aa)ba(bb) = ab; ebae = ab; ba = ab$, as required.
Exercises

Problem 1.
Is the group of isometries of a rectangle (not a square) commutative?

Problem 2.
Is the group of isometries of an equilateral triangle commutative?

Problem 3.
How many permutations in \( S_7 \) commute with the cycle \((1\,2\,3\,4\,5\,6\,7)\)?

Problem 4.
Show that the only elements of \( S_n \) commuting with the cycle \((1\,2\,\ldots\,n)\) of length \( n \) are the powers of this cycle.
Generalizations of commutativity

Non-commutative groups may be close to being commutative, to one or another degree (measured in certain ways).

For example, **soluble** groups are defined by saying that a group is constructed from commutative parts (sections), in a certain precise sense.

In Galois Theory (where Group Theory was conceived in its present form), with every equation, a group of permutations of its roots is associated. Then the equation is soluble by radicals if and only if this group is soluble (actually this term “soluble group” comes from this solubility by radicals).

The symmetric group $S_5$ is non-soluble. There are equations with Galois group $S_5$. For example, $x^5 - 6x + 3 = 0$. Therefore there is no formula to express the roots of this equation by radicals.
An example of a recent result

Group theory is one of the strong points of research in pure mathematics at Lincoln School of Mathematics and Physics.
An example of a recent result


Suppose that a finite group $G$ admits an automorphism $\varphi$ of order $2^n$ such that the fixed-point subgroup $C_G(\varphi^{2^{n-1}})$ of the involution $\varphi^{2^{n-1}}$ is nilpotent of class $c$. Let $m = |C_G(\varphi)|$ be the number of fixed points of $\varphi$. Then $G$ has a characteristic soluble subgroup of $(m, n, c)$-bounded index that has $(n, c)$-bounded derived length.
An example of a recent result

The essence is in obtaining greater degree of commutativity (derived length) under certain conditions on automorphisms of a finite group.

Obtained in collaboration with researchers in France and Brazil.

The result lies at a junction of Group Theory and Theory of Lie Rings.

Lie ring methods

hypothesis on a group \( G \) \( \rightarrow \) hypothesis on a Lie ring constructed from the group \( L \)

\[
\begin{align*}
\text{hypothesis on a group} & \quad \text{constructed from the group} \\
\quad \quad G & \quad \quad L \\
\downarrow & \quad \downarrow \\
\text{Lie ring theorem} & \\
\text{result on the group recovered} & \quad \text{result on the Lie ring} \quad L \quad G
\end{align*}
\]
Abstract Group Theory

studies groups in their own right.

Diverse, rich, also developing in interaction with other parts of mathematics.

New results and methods appear all the time.

Many open problems.

Various methods of study.
Group Theory in other parts of Mathematics

Galois Theory

Algebraic topology

Algebraic geometry

Dimension reduction in differential equations, dynamic systems

Cryptography
Group Theory in Natural Sciences

Groups as measures of symmetry are used in crystallography, quantum physics, and in materials science, including molecular and atomic structures.
Group Theory in Art, games, etc.

Regular tessellations on the plane are described by so-called “wallpaper groups”, which are all known, 17 of them. They can only contain rotations of order 2, 3, 4, 6. This means there can be no regular pentagons in such tessellations. In many medieval cultures though it was a kind of “holy grail” to accommodate a pentagon...
Me “working” in Brazil (joke)
Me visiting University of Brasilia