1 Two applications of group theory

In this extended abstract, we give the definition of a group and 3 theorems in group theory. We also have 2 important examples of groups, namely the permutation group and symmetry group, together with their applications.

1.1 What is a Group?

Given a set G and an operation $*$ on G, we say $(G, *)$ is a *group* if the following 4 requirements are satisfied:

Closure: For all $a, b \in G$, $a * b \in G$.

Associativity: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

Identity: There exists $e \in G$, such that for all $a \in G$, $e * a = a * e = a$, and e is called an identity element.

Inverse: For all $a \in G$, there is an element $b \in G$, such that $b * a = a * b = e$. Here b is called an inverse of a.

1.2 Quick examples and non-examples

In fact lots of structures we are familiar with form a group. In particular, the following two:

1. The integers $\mathbb{Z}$ under operation "+" form a group $(\mathbb{Z}, +)$.
2. The set of invertible n by n matrices M under operation "$\times$", i.e. matrix multiplication, form a group.

Here are two cases that they don't form a group:

1. The integers $\mathbb{Z}$ under operation "$\times$" does not form a group. Because $\frac{1}{2} \notin \mathbb{Z}$, so 2 doesn't have an inverse.
2. The set of all n by n matrices M under operation "$\times$" does not form a group. Because a non-invertible matrice doesn't have an inverse.

1.3 Two theorems

Merely from the definition, there are already some non-trivial properties of groups that we can prove. For example, given a group $(G, *)$, by definition we know there must exist an identity element e. However, no where in the definition indicate the uniqueness of the identity! Now lets prove the following 2 properties.

Theorem 1. *The identity element in $(G, *)$ is unique.*

Theorem 2. *Let $(G, *)$ be a group. Then every element in G has a unique inverse.*

1.4 Two important type of groups

1. **Permutation group**
   Given $X = \{1, 2, ..., n\}$ a finite set of n elements. Let G be the set of all bijective functions from X to X, with the operation defined to be function composition $\circ$, then $(G, \circ)$ forms a group, called the permutation group of order n, and denoted by S_n.
2. **Symmetry group**
   Suppose S is an object, say an image. Let G be the set of all transformations under which the object is invariant. Then G with operation defined to be transformation composition $\circ$, forms a group, called the symmetry group of this object.

1.5 A theorem related to S_n

Theorem 3 (Cayley's theorem)**.** *Every finite group G is isomorphic to a subgroup of S_n, for some $n \in \mathbb{Z}$.*

Note! we didn't formally define the notion "isomorphism", but loosely speaking, if two groups are "isomorphic", then they are essentially the same group with different names. Just like you wearing two different clothes, although you look slightly different, but you are still you.

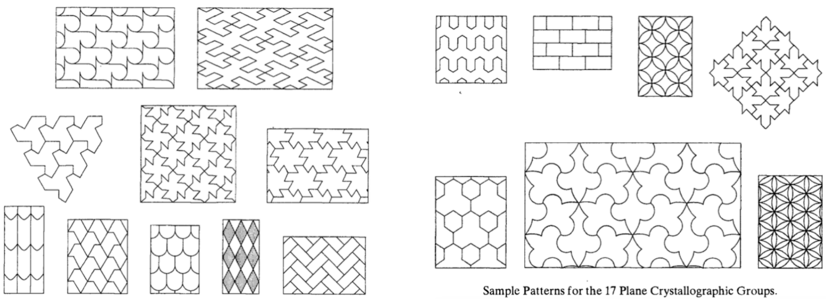
Cayley's theorem is cool, because it tells us that any group, no matter how strange, is contained in a symmetric group S_n. On the other hand, you may start thinking: then group theory is easy, we just need to know S_n and then we know everything about any group! Theoretically it is true, but a symmetric group S_n contains $n!$ many elements, i.e. the size of S_n grows factorially, which is even faster than exponential functions. This is too big to analyse.

Of course, people developed lots of clever theorems to study groups, see [1], [2] and link [3].

1.6 Cool applications and potential study projects

While the formal study of group theory may sounds very abstract when first time encounter it, it has wild applications.

1. A wallpaper usually contain a repetitive pattern. A wallpaper group, or a plane symmetry group, is a group of isometries (translation, rotation, reflection, and glide reflection) that acts on a two-dimensional repeating pattern, i.e. a wallpaper. You may think of there are infinitely many types of wallpapers (with repetitive patterns), however, the Russian mathematician Evgraf Fedorov proved that there were only 17 possible patterns, i.e. there are 17 different wallpaper groups, and no more! (see figure below [2]) Those beautiful works of wallpaper art illustrate very nicely group-theoretic aspects of the symmetry groups. Moreover, studying the symmetry groups helps to understand the geometric restrictions those artists have to discover in order to create their patterns.



Sample Patterns for the 17 Plane Crystallographic Groups.

2. Another bit of math you may remember from school is the quadratic formula, which provides analytic solutions of the quadratic equations. It took people a lot of effort to find the analytic solutions for the cubic and quartic equations (degree 3 and 4 polynomials). After that, the progress stopped at solving the quintic equations (degree 5 polynomials). It turns out that it is not because we are too stupid to find the analytic solutions, it is because there aren't any, which is proved in Galois theory. Specifically, Galois theory says a polynomial is solvable if and only if its related symmetric group S_n is solvable. And it turns out quintic (degree 5) polynomials relate to A_5, the symmetric group of order 5, which is not a solvable group.

2 References

Resources for Abstract algebra:

[1] Joseph Gallian, Contemporary Abstract Algebra 9th edition.

[2] Michael Artin, Algebra 2nd edition.

[3] http://web.bentley.edu/empl/c/ncarter/vgt/media.html

Resources for Wallpaper symmetry:

[1] Maxwell Levine, Plane Symmetry Groups

[2] Patrick J. Morandi, Symmetry Groups: The Classication of Wallpaper Patterns Mathematics 482/526, New Mexico State University