WHY GROUPS?

KEITH CONRAD

Group theory is the study of *symmetry*. When an object appears symmetric, group theory can help us study it. We apply the label "symmetric" to anything that is invariant under some transformations. This can apply to geometric figures (a circle is highly symmetric, being invariant under all rotations), but also to algebraic objects like functions: $x^2+y^2+z^2$ is invariant under all rearrangements of x, y, and z and the trigonometric functions $\sin t$ and $\cos t$ are invariant when t is replaced by $t + 2\pi$.

Conservation laws in physics are related to the symmetry of physical laws under various transformations. For instance, we expect the laws of physics to be unchanging in time. This is an invariance under "translation" in time, and it leads to the conservation of energy. Physical laws also should not depend on where you are in the universe. Invariance of physical laws under "translation" in space leads to conservation of momentum. Invariance of physical laws under (suitable) rotations leads to conservation of angular momentum. A general theorem that explains how conservation laws of a physical system must arise from its symmetries is due to Emmy Noether.

Modern particle physics would not exist without group theory; in fact, group theory predicted the existence of many elementary particles *before* they were found experimentally.

The structure and behavior of molecules and crystals depends on their different symmetries. This makes group theory an essential tool in some areas of chemistry.

Within mathematics itself, group theory is very closely linked to symmetry in **geometry**. In the Euclidean plane $\mathbf{R}^2$, the most symmetric kind of polygon is a regular polygon: its sides and its interior angles are congruent. For $n > 2$ there is a regular polygon with n sides: the equilateral triangle for $n = 3$, the square for $n = 4$, the regular pentagon for $n = 5$, and so on. In $\mathbf{R}^3$ a regular polyhedron has congruent faces that are each regular polygons, with the same number of faces meeting at each vertex. In contrast to the infinitely many regular polygons in $\mathbf{R}^2$, there are only *five* (convex) regular polyhedra in $\mathbf{R}^3$, called the Platonic solids. See Figure 1. In higher dimensions the analogue of a regular polygon and regular polyhedron is called a regular polytope. What are the possibilities in $\mathbf{R}^d$ for $d > 3$?

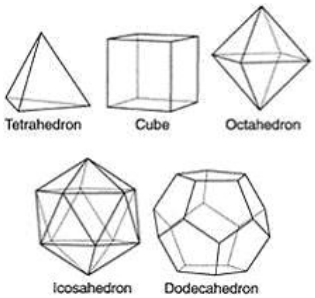

FIGURE 1. The Five Platonic Solids

- In $\mathbf{R}^4$ there are only *six* (convex) regular polytopes.
- For $d > 4$, the number of (convex) regular polytopes in $\mathbf{R}^d$ is always *three*: the higher-dimensional analogues of the tetrahedron, cube, and octahedron in $\mathbf{R}^3$.

The reason there are only a few regular figures in each $\mathbf{R}^d$ for $d > 2$, but there are infinitely many regular polygons in $\mathbf{R}^2$, is connected to the possible finite groups of rotations in Euclidean space of different dimensions.

Consider another geometric topic: regular tilings of the plane. This means a tiling of the plane by copies of congruent regular polygons, with no overlaps except along the boundaries of the polygons. For instance, a standard sheet of graph paper illustrates a regular tiling of $\mathbf{R}^2$ by squares (with 4 meeting at each vertex). See Figure 2.

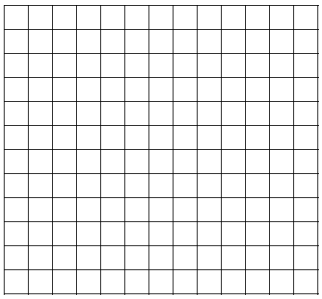

FIGURE 2. Tiling the Plane with Congruent Squares

There are also regular tilings of $\mathbf{R}^2$ by equilateral triangles (with 6 meeting at each vertex) and by regular hexagons (with 3 meeting at each vertex). See Figures 3 and 4.

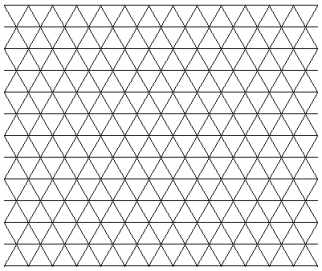

FIGURE 3. Tiling the Plane with Congruent Equilateral Triangles

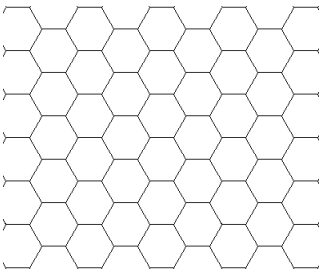

FIGURE 4. Tiling the Plane with Congruent Regular Hexagons

And that is all: there is **no** tiling of $\mathbf{R}^2$ by (congruent) regular n-gons except when $n = 3, 4$, and 6 (how could regular pentagons meet around a point without overlap?). And for each of these three values of n there is essentially just one regular tiling, up to rotation or translation of the plane.

The situation is different if we work with regular polygons in the hyperbolic plane $\mathbf{H}^2$, rather than in the Euclidean plane $\mathbf{R}^2$. The hyperbolic plane $\mathbf{H}^2$ is the interior of a disc in which "lines" are diameters passing through the center of the disc or circular arcs inside the disc that meet the boundary in 90-degree angles. See Figure 5 (the boundary circle is not part of $\mathbf{H}^2$).

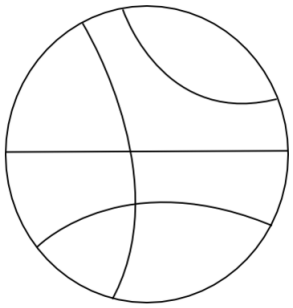

FIGURE 5. Lines in the Hyperbolic Plane $\mathbf{H}^2$

In $\mathbf{H}^2$, unlike in $\mathbf{R}^2$, there are tilings by (congruent) regular n-gons for **every** value of $n > 2$. Figure 6 shows a tiling of $\mathbf{H}^2$ by congruent regular pentagons.

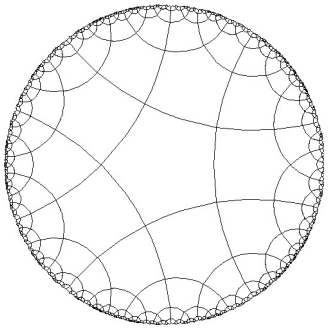

FIGURE 6. Tiling $\mathbf{H}^2$ with Congruent Regular Pentagons

The regions in Figure 6 are pentagons because their boundaries consist of five hyperbolic line segments (intervals along circular arcs meeting the boundary at 90-degree angles). The boundary arcs in each pentagon all have the same hyperbolic length (certainly not the same Euclidean length!), so they are *regular* pentagons, and the pentagons are congruent to each other in $\mathbf{H}^2$ even though they don't appear congruent as figures in the Euclidean plane. Thus we have a tiling of $\mathbf{H}^2$ by congruent regular pentagons with four meeting at each vertex. Nothing like this is possible for tilings of $\mathbf{R}^2$, the Euclidean plane.

There is also more than one tiling of $\mathbf{H}^2$ by regular n-gons for the same n. For instance, taking $n = 3$, there is no tiling of $\mathbf{H}^2$ by congruent equilateral triangles meeting 6 at a vertex, but there are tilings of $\mathbf{H}^2$ with 7 meeting at a vertex and 8 meeting at a vertex. See Figures 7 and 8.

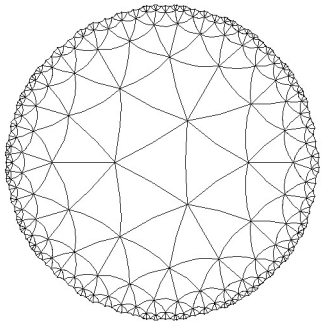

FIGURE 7. Tiling $\mathbf{H}^2$ with Congruent Equilateral Triangles, 7 at a Vertex

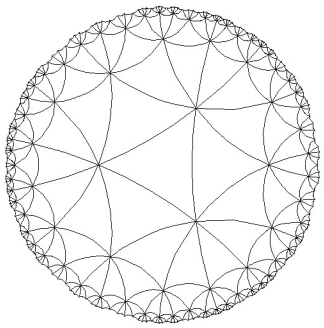

FIGURE 8. Tiling $\mathbf{H}^2$ with Congruent Equilateral Triangles, 8 at a Vertex

That we can tile $\mathbf{H}^2$ by regular polygons in more possible ways than $\mathbf{R}^2$ is due to the different structure of the **group** of rigid motions (distance-preserving transformations) in $\mathbf{H}^2$ compared to $\mathbf{R}^2$. Besides Euclidean and hyperbolic geometry, characteristic features of other types of geometry (such as spherical geometry and projective geometry) are also related to the **group** of allowed motions in the space underlying these geometries. The German mathematician Felix Klein gave a famous lecture in Erlangen, in which he asserted that the *definition* of a geometry is the study of the properties of a space that are invariant under a chosen group of transformations of that space. In physics, two of the differences between relativistic spacetime and non-relativistic spacetime are the velocity addition laws in each setting and the motions of each spacetime that preserve the physical laws. Both of these differences are connected to group theory: velocity addition satisfies the axioms for a group operation and the motions preserving the physical laws form a group of transformations of the corresponding spacetime: the Galilean group for non-relativisitic physics and the Poincaré group for relativistic physics,

Group theory is used in geometry not only because the allowed transformations of a geometric space are a group. For instance, besides using numerical invariants (such as the dimension, which is a number) to describe properties of a space, there is the possibility of introducing algebraic invariants of a space. That is, one can attach to a space certain algebraic systems. Examples include different kinds of groups, such as the fundamental group of a space. A plane with one point removed has a commutative fundamental group, while a plane with two points removed has a noncommutative fundamental group. In higher dimensions, where we can't directly visualize spaces that are of interest, mathematicians

often rely on algebraic invariants like the fundamental group to help verify that two spaces are not the same.

Classical problems in **algebra** have been solved using group theory. In the Renaissance, mathematicians found analogues of the quadratic formula for roots of general polynomials of degree 3 and 4. Like the quadratic formula, the cubic and quartic formulas express the roots of all polynomials of degree 3 and 4 in terms of the coefficients of the polynomials and root extractions (square roots, cube roots, and fourth roots). The search for an analogue of the quadratic formula for the roots of all polynomials of degree 5 or higher was unsuccessful. In the 19th century, the failure to find such general formulas was explained by a subtle algebraic symmetry in the roots of a polynomial discovered by Évariste Galois. He found a way to attach a finite group to each polynomial $f(x)$ and there is an analogue of the quadratic formula for all the roots of $f(x)$ exactly when the group associated to $f(x)$ satisfies a certain technical condition (too complicated to explain here, but see a 3Blue1Brown video on group theory for an informal description). Not all groups satisfy the technical condition, and by this method Galois could give explicit examples of fifth degree polynomials, such as $x^5 - x - 1$, whose roots can't be described by anything like the quadratic formula. Learning about this application of group theory to formulas for roots of polynomials would be a suitable subject for a second course in abstract algebra.

The mathematics of **public-key cryptography** uses a lot of group theory. Different cryptosystems use different groups, such as the group of units in modular arithmetic and the group of rational points on elliptic curves over a finite field. This use of group theory derives not from the "symmetry" perspective, but from the ease or difficulty of carrying out certain computations in the groups. Other public-key cryptosystems use other algebraic structures, such as lattices.

Some areas of **analysis** (the mathematical developments coming from calculus) involve group theory. The subject of Fourier series is concerned with expanding a fairly general 2π-periodic function as an infinite series in the special 2π-periodic functions 1, $\sin x$, $\cos x$, $\sin(2x)$, $\cos(2x)$, $\sin(3x)$, $\cos(3x)$, and so on. While Fourier series can be developed solely as a topic within analysis (and at first it was), the modern viewpoint of them uses a fusion of analysis, linear algebra, and group theory called harmonic analysis.

Identification numbers are all around us, such as the ISBN number for a book, the VIN (Vehicle Identification Number) for a car, or the bar code on a UPS package. What makes them useful is their check digit, which helps catch errors when communicating the identification number over the phone or the internet or with a scanner. The different recipes for constructing a check digit for a string of numbers are based on group theory. Usually the group theory is trivial, just addition or multiplication in modular arithmetic. However, a more clever use of other groups leads to a check-digit construction that catches more of the most common types of communication errors. The key idea is to use a noncommutative group.

On the lighter side, there are applications of group theory to puzzles, such as the 15-puzzle and Rubik's Cube. Group theory provides the conceptual framework for solving such puzzles. To be fair, you can learn an algorithm for solving Rubik's cube without knowing group theory, just as you can learn how to drive a car without knowing automotive mechanics. Of course, if you want to understand how a car works then you need to know what is really going on under the hood. Group theory (symmetric groups, conjugations, commutators, and semi-direct products) is what you find under the hood of Rubik's cube.