symmetric if the central symmetry at every point is a local isometry. The central symmetry at a point \( m \) is defined formally as multiplication by \(-1\) in the tangent space to \( m \): one can picture it as taking a very small neighborhood of \( m \) and "reflecting through \( m \)." It turns out that every locally symmetric space is a quotient of a symmetric space: that is, a space such that the central symmetry at every point is a global isometry. Clearly, symmetric spaces have very large isometry groups. The work of Cartan [VI.69] shows that the resulting isometry groups are exactly the semisimple Lie groups [III.48 §1]. We will not say precisely what these are, but they include the classical matrix groups such as \( \text{SL}_n(\mathbb{R}) \), \( \text{SL}_n(\mathbb{C}) \), and \( \text{Sp}_n(\mathbb{R}) \). Other examples, which can also be realized as matrix groups, include the isometry groups of complex and quaternionic hyperbolic spaces.

In general, given a Lie group \( G \) and a discrete subgroup \( \Gamma \), we say that \( \Gamma \) is a cocompact lattice if there is a compact fundamental domain for \( \Gamma \) in \( G \). Cartan's theorem has the consequence that any compact locally symmetric space is a quotient \( \Gamma \backslash G / K \), where \( G \) is the isometry group of the universal cover and \( K \) is the (necessarily compact) set of isometries that fix a specified point. Mostow's theorem says the same here as it said for \( \mathbb{H}^n / \Gamma \): given such a manifold, there is only one way to realize it as \( \Gamma \backslash G / K \). Or, equivalently, any homeomorphism between two such manifolds is homotopic to an isometry unless the relevant locally symmetric space is a product of a flat torus or a hyperbolic surface with some other locally symmetric manifold.

One might well ask how Mostow discovered such a phenomenon. His work certainly did not occur in a vacuum. In fact, earlier work of Calabi, Selberg, Vesentini, and Weil [VI.93] had already shown that the moduli spaces Mostow was studying were discrete: in other words, unlike flat tori or two-dimensional hyperbolic manifolds, higher-dimensional locally symmetric spaces could admit only a discrete set of locally symmetric metrics. Mostow has said explicitly that he was motivated by the desire to find a more geometric understanding of this fact.

Another point worth making is that Mostow's proof is at least as surprising as his theorem. At the time, the study of locally symmetric spaces, or equivalently of semisimple Lie groups and their lattices, was dominated by two sets of techniques: one set that was purely algebraic and another that used classical methods in differential geometry. Mostow's original proof (which was only for \( \mathbb{H}^n \)) uses instead the theory of quasiconformal mappings and some ideas from dynamics.

Raghunathan, another leading figure in the field, has said that when he first read Mostow's paper, he thought it must be by a different man named Mostow. Similar uses of surprising dynamical and analytical ideas to study the same objects occurred almost simultaneously in work of Furstenberg and Margulis. These ideas have had a long and interesting legacy in the study of locally symmetric spaces, semisimple Lie groups, and related objects.

Further Reading


V.24 The \( P \) versus \( NP \) Problem

The \( P \) versus \( NP \) problem is widely considered to be the most important unsolved problem in theoretical computer science, and one of the most important in all of mathematics. \( P \) and \( NP \) are two of the most basic Computational Complexity Classes [III.10]: \( P \) is the class of all computational tasks that can be performed in a time that is polynomial in the length of the input, and \( NP \) is the class of all computational tasks where a correct answer can be verified in a time that is polynomial in the length of the input. An example of the former is multiplying two \( n \)-digit integers (which, even if you use long multiplication, takes roughly \( n^2 \) arithmetical operations). An example of the latter is searching in a Graph [III.34] with \( n \) vertices for a set of \( m \) vertices, any two of which are joined by an edge: if you are presented with \( m \) such vertices, then you just have to check the \( \binom{m}{2} \) pairs of those vertices to make sure that each pair is indeed an edge of the graph.

It appears to be much harder to find \( m \) vertices that are all joined than to check that a given \( m \) vertices are all joined. This suggests that problems in \( NP \) are in
general harder than problems in $P$. The $P$ versus $NP$ problem asks for a proof that the complexity classes $P$ and $NP$ really are distinct. For a detailed discussion of the problem, see Computational Complexity [IV.20].

V.25 The Poincaré Conjecture

The Poincaré conjecture is the statement that a compact [III.9] simply connected smooth $n$-dimensional manifold [I.3 §6.9] must be homeomorphic to the $n$-sphere $S^n$. One can think of a compact manifold as a manifold that lives in a finite region of $\mathbb{R}^m$ for some $m$ and that has no boundary: for example, the 2-sphere and the torus are compact manifolds living in $\mathbb{R}^3$, while the open unit disk or an infinitely long cylinder is not. (The open unit disk does not have a boundary in an intrinsic sense, but its realization as the set $\{(x,y) : x^2 + y^2 < 1\}$ has the set $\{(x,y) : x^2 + y^2 = 1\}$ as its boundary.) A manifold is called simply connected if every loop in the manifold can be continuously contracted to a point. For instance, a sphere of dimension greater than 1 is simply connected but a torus is not (since a loop that “goes around” the torus will always go around the torus, however you continuously deform it). Thus, the Poincaré conjecture asks whether two simple properties of spheres, compactness and simple connectedness, are enough to characterize spheres.

The case $n = 1$ is not interesting: the real line is not compact and a circle is not simply connected, so the hypotheses of the problem cannot be satisfied. Poincaré [VI.61] himself solved the problem for $n = 2$ early in the twentieth century, by completely classifying all compact 2-manifolds and noting that in his list of all possible such manifolds only the sphere was simply connected. For a time he believed that he had solved the three-dimensional case as well, but then discovered a counterexample to one of the main assertions of his proof. In 1961, Stephen Smale proved the conjecture for $n \geq 5$, and Michael Freedman proved the $n = 4$ case in 1982. That left just the three-dimensional problem open.

Also in 1982, William Thurston put forward his famous geometrization conjecture, which was a proposed classification of three-dimensional manifolds. The conjecture asserted that every compact 3-manifold can be cut up into submanifolds that can be given metrics [III.56] that turn them into one of eight particularly symmetrical geometric structures. Three of these structures are the three-dimensional versions of Euclidean, spherical, and hyperbolic geometry (see [I.3 §6]). Another is the infinite “cylinder” $S^1 \times \mathbb{R}$; that is, the product of a 2-sphere with an infinite line. (This is not compact, but that is because the pieces into which one cuts up the manifold may have boundaries that are not included in the pieces.) Similarly, one can take the product of the hyperbolic plane with an infinite line and obtain a fifth structure. The other three are slightly more complicated to describe. Thurston also gave significant evidence for his conjecture by proving it in the case of so-called Haken manifolds.

The geometrization conjecture implies the Poincaré conjecture; both were proved by Grigori Perelman, who completed a program that had been set out by Richard Hamilton. The main idea of this program was to solve the problems by analyzing Ricci flow [III.78]. The solution was announced in 2003 and checked carefully by several experts over the next few years. For more details, see Differential Topology [IV.7].

V.26 The Prime Number Theorem and the Riemann Hypothesis

How many prime numbers are there between 1 and $n$? A natural first reaction to this question is to define $\pi(n)$ to be the number of prime numbers between 1 and $n$ and to search for a formula for $\pi(n)$. However, the primes do not have any obvious pattern to them and it has become clear that no such formula exists (unless one counts highly artificial formulas that do not actually help one to calculate $\pi(n)$).

The standard reaction of mathematicians to this kind of situation is to look instead for good estimates. In other words, we try to find a simply defined function $f(n)$ for which we can prove that $\pi(n)$ is always a good approximation to $\pi(n)$. The modern form of the prime number theorem was first conjectured by Gauss [VI.26] (though a closely related conjecture had been made by Legendre [VI.24] a few years earlier). He looked at the numerical evidence, which suggested to him that the “density” of primes near $n$ was about $1/\log n$, in the sense that a randomly chosen integer near $n$ would have a probability of roughly $1/\log n$ of being a prime. This leads to the conjectured approximation of $n/\log n$ for $\pi(n)$, or to the slightly more sophisticated approximation

$$\pi(n) \approx \int_0^n \frac{dx}{\log x}.$$  

The function defined by the integral on the right-hand side is called $\text{l}i(n)$ (which stands for the “logarithmic