Group theory - what's beyond

B.Sury

Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560059, India
email : sury@isibang.ac.in

Birth and infancy of group theory

Major progress in group theory occurred in the nineteenth century but the evolution of group theory began already in the latter part of 18th century. Some characteristic features of 19th century mathematics which had crucial impact on this evolution are concern for rigor and abstraction and the view that mathematics is a human activity without necessarily referring to physical situations. In 1770, Joseph Louis Lagrange (1736-1813) wrote his seminal memoir *Reflections on the solution of algebraic equations*. He considered 'abstract' questions like whether every equation has a root and, if so, how many were real/complex/positive/negative? The problem of algebraically solving 5th degree equations was a major preoccupation (right from the 17th century) to which Lagrange lent his major efforts in this paper. His beautiful idea (now going under the name of Lagrange's resolvent) is to 'reduce' a general equation to auxiliary (resolvent) equations which have one degree less. Later, the theory of finite abelian groups evolved from Carl Friedrich Gauss's famous "Disquisitiones Arithmeticae". Gauss (1777-1855) established many of the important properties though he did not use the terminology of group theory. In his work, finite abelian groups appeared in different forms like the additive group $\mathbf{Z}_n$ of integers modulo n, the multiplicative group $\mathbf{Z}_n^*$ of integers modulo n relatively prime to n, the group of equivalence classes of binary quadratic forms, and the group of n-th roots of unity. In 1872, Felix Klein delivered a famous lecture *A Comparative Review of Recent Researches in Geometry*. The aim of his (so-called) Erlangen Program was the classification of geometry as the study of invariants under various groups of transformations. So, the groups appear here "geometrically" as groups of rigid motions, of similarities, or as the hyperbolic group etc. During the analysis of the connections between the different geometries, the focus was on the study of properties of figures invariant under transformations. Soon after, the focus shifted to a study of the transformations themselves. Thus the study of the geometric relations between figures got converted to the study of the associated transformations. In 1874, Sophus Lie introduced his "theory of continuous transformation groups" what we basically call Lie groups today. Poincaré and Klein began their work on the so-called *automorphic functions* and the groups associated with them

around 1876. Automorphic functions are generalizations of the circular, hyperbolic, elliptic, and other functions of elementary analysis. They are functions of a complex variable z, analytic in some domain, and invariant under the group of transformations $x' = \frac{ax+b}{cx+d}$ (a, b, c, d real or complex and $ad - bc \neq 0$), or under some subgroup of this group. We end this introduction with the ancient problem of finding all those positive integers (called congruent numbers) which are areas of right-angled triangles with rational sides. To this date, there is no general result describing all of them precisely. However, the problem can be re-stated in terms of certain groups called elliptic curves and this helps in getting a hold on the problem and in obtaining several partial results. Indeed, if n is a positive integer, then the rational numbers x, y satisfying $y^2 = x^3 - n^2x$ form a group law which can be described geometrically. Then, n is a congruent number if and only if, this group is infinite !

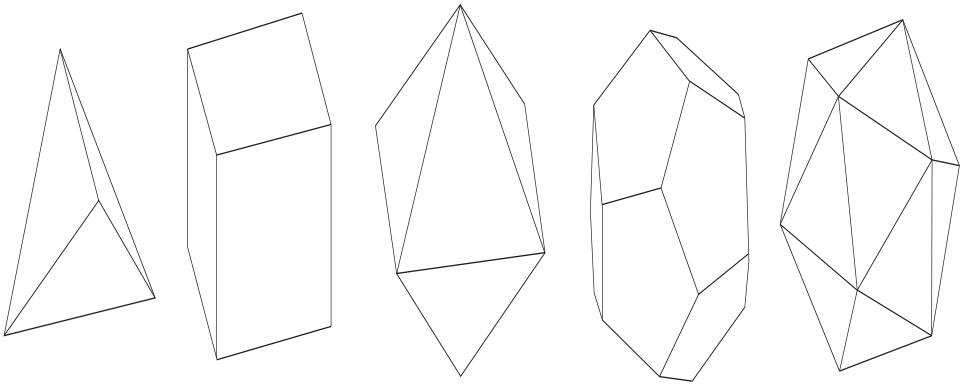
1 Unreasonable effectiveness of group theory

In a first course on group theory, one does not discuss much beyond the Sylow theorems, structure of finitely generated abelian groups, finite solvable groups (in relation to Galois theory), and the simplicity of the alternating groups A_n for $n \geq 5$. For instance, nilpotent groups are hardly discussed and nor is there a mention of other non-abelian simple groups, let alone a proof of their simplicity or a mention of the classification of finite simple groups. Moreover, infinite groups are also hardly discussed although quite a bit could be done at that stage itself. For instance, free groups are barely discussed and profinite are rarely discussed. Even a second course in group theory usually does not give one an inkling as to its depth and effectiveness. Here, we take several brief de-tours to indicate this. Let us start with some familiar aspects first.

1.1 Classification of finite simple groups

The basic problem in finite group theory was to 'find' all possible finite groups of a given order. However, this is too difficult/wild a problem - even an estimate (in terms of n) of the number of possible non-isomorphic groups of order n is a rather recent result requiring deep analysis of several years. As simple groups are building blocks, the classification of all finite, simple groups is a more tractable problem. The biggest success story of recent years is an accomplishment of this task. In rough terms, the big classification theorem of finite simple groups (CFSG) asserts :
Every finite simple group is a cyclic group of prime order, an alternating group, a simple group of Lie type or, one of the 26 sporadic finite simple groups.
A self-contained proof at this point would take 10,000 pages and there are serious attempts to simplify several parts of it. For instance, the famous odd-order theorem which is an important part of the CFSG itself takes more than 2000 pages. The odd-order theorem is the beautiful assertion proved by Feit and Thompson : "Any group of odd order is solvable." The CFSG is extremely useful in many situations but, often it is some consequence of the CFSG which is applied. For instance, a consequence of CFSG is that every nonabelian, finite simple group can be generated by two elements, one of which could be an arbitrary nontrivial element. See [1] for further reading.

1.2 Platonic solids



The determination of finite subgroups of the group of 3-dimensional rotations plays an all-important role in proving that there are precisely five Platonic solids - the cube, the tetrahedron, the octahedron, the dodecahedron and the icosahedron. Let us describe this more precisely. The symmetry group of a 3-dimensional figure is the set of all distance preserving maps, or isometries, of $\mathbf{R}^3$ which map the figure to itself, and with composition as the operation. To make this more concrete, we view each Platonic solid centered at the origin. An isometry which sends the solid to itself then must fix the origin. An isometry which preserves the origin is a linear transformation, and is represented by a matrix A satisfying $A^T A = I_3$. Thus, the symmetry group of a Platonic solid is isomorphic to a subgroup of the orthogonal group $O_3(\mathbf{R}) = \left\{A : A^T A = I\right\}$. Elements of $O_3(\mathbf{R})$ are either rotations or reflections across a plane, depending on whether the matrix has determinant 1 or -1. The set of rotations is then the subgroup $SO_3(\mathbf{R})$ of $O_3(\mathbf{R})$. Let G be the symmetry group of a Platonic solid, viewed as a subgroup of $O_3(\mathbf{R})$. If $R = G \cap SO_3(\mathbf{R})$, then R is the subgroup of rotations in G. We note that if $z : \mathbf{R}^3 \to \mathbf{R}^3$ is defined by $z(x) = -x$ for all $x \in \mathbf{R}^3$, then z is a reflection, z is a central element in $O_3(\mathbf{R})$, and $O_3(\mathbf{R}) = SO_3(\mathbf{R}) \times \langle z \rangle \cong SO_3(\mathbf{R}) \times \mathbf{Z}_2$. These facts are all easy to prove. Thus, $[O_3(\mathbf{R}) : SO_3(\mathbf{R})] = 2$. As a consequence, $[G : R] \leq 2$. The element z is a symmetry of all the Platonic solids except for the tetrahedron, and there are reflections which preserve the tetrahedron. Therefore, $[G : R] = 2$ in all cases, and $G \cong R \times \mathbf{Z}_2$ for the four largest solids. Thus, for them, it will be sufficient to determine the rotation subgroup R. The final outcome is given in the following table :

Solid	Rotation Group	Symmetry Group
tetrahedron	A_4	S_4
cube	S_4	$S_4 \times \mathbf{Z}_2$
octahedron	S_4	$S_4 \times \mathbf{Z}_2$
dodecahedron	A_5	$A_5 \times \mathbf{Z}_2$
icosahedron	A_5	$A_5 \times \mathbf{Z}_2$

It is no coincidence that the symmetry group of the octahedron and the symmetry group of the cube are isomorphic, as are the groups for the dodecahedron and icosahedron. There is a notion of *duality* of Platonic solids. If we take a Platonic solid, put a point in the center of each face, and connect all these points, we get another Platonic solid. The resulting solid is called the *dual* of the first. For instance, the dual of the octahedron is the cube, and the

dual of the cube is the octahedron. By viewing the dual solid as being built from another in this way, any symmetry of the solid will yield a symmetry of its dual, and vice-versa. Thus, the symmetry groups of a Platonic solid and its dual are isomorphic. The groups of symmetries of regular polyhedra arise in nature as the symmetry groups of molecules. For instance, $H_3C - CCl_3$ has the symmetry group C_3, S_3 is the symmetry group of the ethane molecule C_2H_6 and S_4 is the symmetry group of uranium hexaflouride UF_6 etc.

1.3 Lattice groups and crystallographic groups

Given a lattice L in $\mathbf{R}^n$ (that is the group of all integer linear combinations of a vector space basis), its group of automorphisms is isomorphic to $GL(n, \mathbf{Z})$. Finite subgroups of such a group arise if we are looking at orthogonal transformations with respect to a positive-definite quadratic form (metric). The (finite) groups of orthogonal transformations which take a lattice in $\mathbf{R}^n$ to itself is called a *crystallographic class*. There are exactly 10 plane crystallographic classes (when $n = 2$) - the cyclic groups of orders $1, 2, 3, 4, 6$ and the dihedral groups of orders $2, 4, 6, 8, 12$. In 3-dimension, there are 32 crystallographic classes. Determination of these groups does not completely solve the problem of finding all the inequivalent symmetry groups of lattices. That is to say, two groups in the same crystallographic class may be inequivalent as symmetry groups (algebraically, two non-conjugate subgroups of $GL(n, \mathbf{Z})$ may be conjugate by an orthogonal matrix. The inequivalent symmetry groups are 13 in the plane case and 72 in the case $n = 3$. The corresponding polygons (resp. polyhedrons when $n = 3$) of which these groups are symmetry groups can be listed and a description of the actions can be given without much difficulty. In general dimension, one can use a general result of Jordan to show that there are only finitely many symmetry groups of lattices.

Related to the above-mentioned finite groups are certain infinite discrete groups called *crystallographic groups*. Atoms of a crystal are arranged discretely and symmetrically in 3-space. One naturally looks at groups of motions of 3-space which preserve the physical properties of the crystal (in other words, takes atoms to atoms and preserves all relations between the atoms). More generally, one can do this for n-space. Basically, a crystallographic group in n dimension is a discrete group of motions of $\mathbf{R}^n$ such that the quotient of this action is a compact space. For instance, the group $\mathbf{Z}^n$ is such a group. More generally, a classical theorem is :

Bieberbach's theorem. If G is a crystallographic group in dimension n, then the subgroup of all translations in G is a normal subgroup A of finite index in it.

This, along with a result of Jordan implies that the number of non-isomorphic crystallographic groups in a given dimension is finite (Jordan's theorem is that any finite group has only finitely many inequivalent 'integral' representations in any fixed dimension n). This solves the first part of Hilbert's 18th problem. In crystallography, it is important to know the groups in dimension 3. It turns out that there are 219 such groups (230 if we distinguish mirror images) and have a special naming system under the "*International tables for crystallography*". On the plane (that is, in dimension 2) there are 17 crystallographic groups known as *wallpaper groups*. They make very beautiful patterns and can be seen abundantly

in Escher's paintings as well as architectural constructions (see [10]. In 4-dimensions, there are 4783 crystallographic groups. There are also groups appearing in non-euclidean crystallography which involves non-euclidean geometry.

1.4 Reflection groups

The group of permutations of a basis of Euclidean space is a group of orthogonal transformations of the Euclidean space which is generated by reflections about hyperplanes. In general, groups of orthogonal transformations generated by reflections arise in diverse situations; indeed, even in the theory of crystallographic groups. One abstractly studies such groups under the name of Coxeter groups. A *Coxeter group* G is a group generated by elements $s_1, \cdots, s_n$ with relations $(s_i s_j)^{m_{ij}} = 1$ where $m_{ii} = 2$ and $m_{ij} = m_{ji} \geq 2$. If the so-called Gram matrix $a_{ij} = \cos(\pi/m_{ij})$ is positive-semidefinite, the corresponding Coxeter group is a crystallographic group and these have been classified. If the Gram matrix is positive-definite, this Coxeter group is finite; the irreducible ones are classified under the names $A_n, B_n, D_n, E_6, E_7, E_8, F_4, H_3, H_4, I_2(m)$. The subscripts denote the dimensions of the Euclidean space on which the group acts. This classification is the key to classifying the complex simple Lie algebras also. See [4] for further reference.

1.5 Galois groups versus polynomials

Lagrange's method of resolvents can be briefly described as follows : Let f be the original polynomial, with roots $r_1, r_2, \cdots, r_n$. For any rational function F of the roots and the coefficients of f, look at all the different values which F takes when we go through the various permutations of the roots of f. Denoting these values by $s_1, s_2, \cdots, s_k$, he considers the (resolvent) polynomial $g(x) = (x - s_1)(x - s_2) \cdots (x - s_k)$.
The coefficients of g are symmetric functions of the roots of f; so, they are polynomials in the elementary symmetric functions in them. In other words, the coefficients of g are polynomials in the coefficients of f. Lagrange showed that the number k divides $n!$. This is the origin of the so-called Lagranges theorem in group theory. For example, if f has roots r_1, r_2, r_3, r_4 (and so degree of f is 4), then the function $F = r_1 r_2 + r_3 r_4$, assumes 3 different values under the 4! permutations of the r_i's. So, the resolvent polynomial of a quartic (degree 4 polynomial) is a cubic polynomial. When Lagrange tried to apply this to quintics (the polynomials of degree 5), Lagrange found the resolvent polynomial to be of degree 6 (!) Even though he did not succeed in going further in the problem of quintics, his method was path-breaking as it was the first time that solutions of polynomial equations and permutations of roots were related to each other. The theory of Galois has its germ in Lagrange's method. Galois theory is now a basic subject taught in undergraduate programmes as it plays a role in all branches of mathematics. Here is a nice application of Galois theory to the study of polynomials over integers.

Let $f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ be a monic, integral polynomial of degree $n > 1$. Suppose that for every prime p, the polynomial f considered as a polynomial with coefficients in $\mathbf{Z}/p\mathbf{Z}$ has a root. Then, f must be reducible over $\mathbf{Z}$.
Here is how it is proved. For a prime p, the decomposition type of f is the set of numbers

$n_1 \leq n_2 \cdots \leq n_r$ where the polynomial f - when considered modulo p - is a product of irreducible polynomials of degrees $n_1, \cdots, n_r$. For an infinite set P of primes, one has often a well-defined notion of density. We briefly recall it although we will not need any details except the statement of the following theorem. The theory of the Riemann zeta function tells us that for any complex number s with Re $s > 1$, the infinite product $\prod_{p\ prime}(1 - 1/p^s)^{-1}$ converges to a finite number denoted by the sum $\sum_n 1/n^s$. Also,

$$\prod_{p\ prime} (1 - 1/p^s)^{-1} - \frac{1}{s-1}$$

has a finite limit as $s \to 1$ from the right. Then, one defines the density of a set P of primes to be the limit as $s \to 1^+$ of the ratio

$$\frac{\prod_{p \in P}(1 - 1/p^s)^{-1}}{\prod_{p\ prime}(1 - 1/p^s)^{-1}}$$

if this limit exists. For instance, finite sets P have density zero. The theorem of Dirichlet on infinitude of primes in arithmetic progressions has the analytic statement that if $P(c, d)$ is the set of primes in an arithmetic progression $dn + c$ with $(c, d) = 1$, then the density of $P(c, d)$ is $1/\phi(d)$. We will not need any properties of the density excepting the following statement which is a weaker form of the so-called Frobenius Density Theorem:
Let f be a monic, irreducible, integral polynomial. The set of primes p modulo which f has decomposition type $n_1, n_2, \cdots, n_r$ has density equal to $|\frac{N}{Gal(f))}|$ where $N = \{\sigma \in Gal(f) : \sigma$ has a cycle pattern $n_1, n_2, ..., n_r\}$.
Recall an elementary fact about finite groups :
If H is a proper subgroup of a finite group G, then the union of all the conjugate subgroups of H cannot be the whole of G.
Let us now prove the assertion made in the beginning under the heading. Suppose f is an irreducible polynomial such that f has root modulo every prime. Then the Frobenius Density Theorem shows that every σ has a cycle pattern of the form $1, n_2, \cdots$ This means that every element of $Gal(f)$ fixes a root, say β. Since f is irreducible, the group $Gal(f)$ acts transitively on the roots of f. Thus, this group would be the union of the conjugates of its subgroup H consisting of those elements which fix the root β. But the above fact on finite groups implies H cannot be a proper subgroup. Hence $Gal(f)$ fixes each root of f and is therefore trivial. So we get f to be a linear polynomial. This proves the assertion.

More generally, suppose that f is an integral polynomial and let $f = f_1 f_2 \cdots f_r$ be its decomposition into irreducible, integral polynomials. For each $i \leq r$, let θ_i be a fixed root of f_i and consider the field K_i obtained by adjoining θ_i. If G is the Galois group of f and G_i is the subgroup of all those permutations in G which fix θ_i, then look at the set $S = \bigcup_{i=1}^r G_i$. Finally, look at the product of the resultants of f_i and f_i'; let $p_1^{b_1} \cdots p_r^{b_r}$ be the prime decomposition of this product. Then, we can prove similarly as above that :
f has a root modulo the single integer $p_1^{2b_1+1} \cdots p_r^{2b_r+1}$ and $G = \bigcup_{g \in G} gSg^{-1}$ if and only if f has a root modulo every integer.

1.6 Combinatorial applications - Polya's theory

Groups evidently help in counting problems. In fact, this goes a very long way as the so-called Polya's theory shows. Here we illustrate it by an example. Consider the problem of painting the faces of a cube either red or green. He wants to know how many such distinct coloured cubes he can make. Since the cube has 6 faces, and he has 2 colours to choose from, the total number of possible coloured cubes is 2^6. But, painting the top face red and all the other faces green produces the same result as painting the bottom face red and all the other faces green. The answer is not so obvious but turns out to be 10. Let us see how. To find the various possible colour patterns which are inequivalent, we shall exploit the fact that the rotational symmetriesof the cube have the structure of a group. Let us explain the above in precise terms. Let D denote a set of objects to be coloured (in our case, the 6 faces of the cube) and R denote the range of colours (in the above case {red, green}). By a colouring of D, one means a mapping $\phi : D \to R$. Let X be the set of colourings. If G denotes a group of permutations of D, we can define a relation on the set of colourings as follows:
$\phi_1 \sim \phi_2$ if, and only if, there exists some $g \in G$ such that $\phi_1 g = \phi_2$.
By using the fact that G is a group, it is easy to prove that $\sim$ is an equivalence relation on X, and so it partitions X into disjoint equivalence classes. Now for each $g \in G$, consider the map $\pi_g : X \to X$ defined as $\pi_g(\phi) = \phi g^{-1}$; it is a bijection from X to itself. In other words, for each $g \in G$, we have $\pi_g \in$ Sym X, where Sym X = the group of all permutations on X. The map $f : G \to$ Sym X as $f(g) = \pi_g$ is a homomorphism; i.e., G can be regarded as a group of permutations of X.
It is clear that the orbits of the action described above are precisely the different colour patterns i.e., the equivalence classes under $\sim$. Therefore, we need to find the number of inequivalent colourings, i.e. the number of equivalence classes of $\sim$, i.e. the number of orbits of the action of G on X. Note that, like in the example of the cube we shall consider only finite sets D, R. The answer will be provided by a famous theorem of Polya. Polya's theorem was published first in a paper of J.H.Redfield in 1927 and, apparently no one understood this paper until it was explained by F.Harary in 1960. Polya's theorem is considered one of the most significant papers in 20th-century mathematics. The article contained one theorem and 100 pages of applications. For a group G of permutations on a set of n elements and variables $s_1, s_2, \ldots, s_n$, one defines a polynomial expression (called the cycle index) for each $g \in G$. If $g \in G$, let $\lambda_i(g)$ denote the number of i-cycles in the disjoint cycle decomposition of g. Then, the cycle index of G, denoted by $z(G; s_1, s_2, \ldots, s_n)$ is defined as the polynomial expression

$$z(G; s_1, s_2, \ldots, s_n) = \frac{1}{|G|} \sum_{g \in G} s_1^{\lambda_1(g)} s_2^{\lambda_2(g)} \ldots s_n^{\lambda_n(g)}.$$

For instance,

$$z(S_n; s_1, s_2, \ldots, s_n) = \sum_{\lambda_1 + 2\lambda_2 + \ldots + k\lambda_k = n} \frac{s_1^{\lambda_1} s_2^{\lambda_2} \ldots s_k^{\lambda_k}}{1^{\lambda_1} \lambda_1! 2^{\lambda_2} \lambda_2! \ldots k^{\lambda_k} \lambda_k!}$$

Polya's theorem asserts :
Suppose D is a set of m objects to be coloured using a range R of k colours. Let G be the group of symmetries of D. Then, the number of colour patterns $= \frac{1}{|G|} z(G; k, k, \ldots, k)$.

Our group of rotations of the cube consists of :
90 degree (clockwise or anti-clockwise) rotations about the axes joining the centres of the opposite faces - there are 6 such;
180 degree rotations about each of the above axes - there are 3 such;
120 degree (clockwise or anti-clockwise) rotations about the axes joining the opposite vertices - there are 8 such;
180 degree rotations about the axes joining the midpoints of the opposite edges and;
the identity.
The cycle index of G turns out to be

$$z(G; s_1, \cdots, s_6) = \frac{1}{24}(6s_1^2 s_4 + 3s_1^2 s_2^2 + 8s_3^2 + 6s_2^3 + s_1^6).$$

So, in our example of the cube, the number of distinct coloured cubes

$$= \frac{1}{24}[2^6 + 6 \cdot 2^3 + 8 \cdot 2^2 + 3 \cdot 2^2 \cdot 2^2 + 6 \cdot 2^2 \cdot 2] = 10.$$

There are 10 distinct cubes in all.

2 Some truths about Lie groups

Groups are effective when they also come with additional analytic structure. The prime examples of this marriage of groups and analysis are the so-called Lie (pronounced as 'Lee') groups named so after the Norwegian mathematician Sophus Lie. Lie's idea was to develop a theory for differential equations analogous to what Galois had done for algebraic equations. His key observation was that most of the differential equations which had been integrated by older methods were invariant under continuous groups which could be easily constructed. In general, he considered differential equations which are invariant under some fixed continuous group. He was able to obtain simplifications in the equations using properties of the given group. Lie's work was fundamental in the subsequent formulation of a Galois theory of differential equations by Picard, Vessiot, Ritt and Kolchin. A typical illustration can be given as follows. Consider an n-th order linear differential equation with polynomial coefficients, viz.,

$$\frac{d^n f}{dz^n} + a_{n-1}(z)\frac{d^{n-1} f}{dz^{n-1}} + \cdots + a_0(z)f = 0.$$

Let $f_1, \cdots, f_n$ be $\mathbf{C}$-linearly independent holomorphic solutions. Let K be the field obtained by adjoining the f_i's and their derivatives. If G denotes the group of all $\mathbf{C}(z)$-linear automorphisms of K which commute with taking derivatives. This G is called the Galois group of the differential equation. For $g \in G$, write $g.f_i = \sum_j g_{ji} f_j$ for some complex numbers g_{ji}. Thus, G is a group of matrices and defines what is called an algebraic group. It turns out that the solutions to such a linear homogeneous differential equation are '*elementary*' functions if and only if the corresponding Galois group is a so-called solvable group; this is a consequence of the Lie-Kolchin theorem - a result on triangularizability of connected solvable algebraic groups. As several groups of matrices naturally form Lie groups, it should not be surprising that Lie groups find applications in other subjects like physics and chemistry. In fact, there

are applications to the real world too ! For instance, in navigation, surveillance etc., one needs very sophisticated cameras (called *catadioptric*) to obtain a wide field of view, even greater than 180 degrees. Surprisingly, some of these involve finding dimensions of some quotient spaces of certain Lie groups like the Lorentz group $O(3,1)$ (see [3]). Often, Lie groups arise as groups of real or complex matrices. They appear naturally in geometric ways - the group of rotations of 3-space is $O(3)$. Nowadays, the theory of Lie groups is regarded as a special case of the theory of algebraic groups over real or complex fields. Before discussing Lie groups (which involves a discussion of certain spaces called manifolds), we recall the notion of a topological group.

Given a group G which also happens to be a Hausdorff topological space, this is supposed to yield a *topological group* if the map $(x,y) \mapsto xy^{-1}$ from the product space $G \times G$ to G is a continuous map. Basically, the continuity of the group operations is a powerful tool which often yields group-theoretical consequences. A typical example is the absolute Galois group of the algebraic numbers over the rational numbers; this encodes all the information about all the algebraic number fields at one stroke. Notice that individual finite Galois groups do not have any meaningful topological group structure but only the discrete group structure. So, stringing them all together in this absolute Galois group makes it a topological group which is *totally disconnected* (that is, only the points are connected components) but compact as a space ! This is an example of a profinite group (a *projective limit* of finite groups). In Lie theory which is a special case of a topological group, one will look at the other end of the spectrum where the spaces are connected.

Let us define smooth manifolds briefly. Basically, one has to keep in mind the examples of smooth regular surfaces in 3-space. A Hausdorff space M with a countable basis is said to be a *smooth (real) manifold of dimension* n if :

(i) there is an open cover $\{U_\alpha\}_{\alpha \in \Lambda}$ of M and homeomorphisms
$phi_\alpha : U_\alpha$ onto open sets in $\mathbf{R}^n$,
(ii) the homeomorphisms above are such that the 'transition functions' $\phi_\alpha \circ \phi_\beta^{-1} : \phi_\beta(U_\alpha \cap U_\beta) \to \phi_\alpha(U_\alpha \cap U_\beta)$ are smooth whenever $U_\alpha \cap U_\beta \neq \emptyset$ and
(iii) the collection $(U_\alpha, \phi_\alpha)_\alpha$ is a maximal family satisfying (i) and (ii).

Thus, the manifold is a topological space which is locally like $\mathbf{R}^n$ on which it makes sense to do differential calculus. Hence, one can define smooth functions between smooth manifolds. It turns out that a smooth manifold can always be 'embedded' in $\mathbf{R}^N$ for a large enough N. The unit sphere is a typical example where one may take 4 open sets to cover. If there is a curve (image of a smooth map α from $[0,1]$ to M) on M, one has its tangent vector at a point. One may define the tangent space to M at a point as the set of tangent vectors to curves passing through that point. However, one must take some care because different curves may give the same tangent vector. It turns out that the tangent space at any point is a vector space of dimension n.

A *Lie group* is a group G which is a smooth manifold as well as a topological group and, the group multiplication and the inverse map are smooth. Some Lie groups are $\mathbf{R}^n, \mathbf{C}^*, S^1 \times \cdots S^1$, GL($n, \mathbf{R}$), GL(n,$\mathbf{C}$), SL(n,$\mathbf{R}$), SL(n,$\mathbf{C}$), O(n), SO(n), U(n), SU(n). Also, every closed subgroup of GL(n,$\mathbf{R}$) is a Lie group. The tangent space to G at the identity plays a very important role. In particular, this vector space is equipped with a (non-associative) multiplication operation, the Lie bracket, that makes it into what is called a Lie algebra. The theory of Lie groups begun by Lie was continued by Killing and Elie

Cartan. The big result of the classical theory was a classification of the complex simple (note the combination of these two words !) Lie algebras. Later, Hermann Weyl proved that every complex semisimple Lie algebra has a compact real form. This amounted to a classification of certain geometric objects called the real symmetric spaces. These are special Riemannian manifolds which possess certain distance-preserving maps inverting geodesics. We do not discuss Lie groups in more detail here but the interested reader may refer to [11] and [12].

2.1 Algebraic groups - a(f)fine concept

Matrix groups are usually studied under the aegis of the so-called linear algebraic groups. These are more refined versions of Lie groups in the sense that they have more structure; in particular, they can be studied over any field. Here, the advantage is that one can use techniques from algebraic geometry. We do not go into the technical definitions here. Suffice it to say that these are subsets of n-tuples over a field k defined as zero sets of polynomials in n variables over k and have compatible group structures as well. Facts about polynomials play key roles. Some examples of algebraic groups over a field k are :

(i) The additive group of k.
(ii) The multiplicative group k^* identified with the set of zeroes of the polynomial $x_1x_2 - 1$ in k^2.
More generally, $G = T(n,k)$ is the group of $n \times n$ diagonal matrices over k with nonzero diagonal entries, viewed as

$$\{(x_1, \cdots, x_{n+1}) \in k^{n+1} : x_1x_2 \cdots x_{n+1} = 1\}.$$

(iii) The set $G = GL(n,k)$ of all invertible matrices over k, viewed as the set

$$\{(x_{ij}, y) \in k^{n^2+1} : det(x_{ij})y = 1\}.$$

(iv) Let (V,q) be an n-dimensional vector space with a non-degenerate quadratic form $q : V \times V \to k$. The orthogonal group

$$O(V,q) = \{g \in GL(V) : q(gv) = q(v)\}$$

can be viewed as an algebraic group as follows. Choose a basis $\{v_1, \cdots, v_n\}$ of V and write $B = (q(v_i, v_j)$ for the symmetric matrix associated to q. Note that for vectors $x = \sum_i x_iv_i, y = \sum_i y_iv_i \in V$, we have $q(x,y) =^t xBy$ where $^t = (x_1, \cdots, x_n) \in k^n$. Then, $O(V,q)$ can be identified with

$$\{g \in GL(n,k) :^t gBg = B\}.$$

(v) For any skew-symmetric matrix $\Omega \in GL(2n,k)$, the symplectic group

$$Sp(\Omega) = \{g \in GL(2n,k) :^t g\Omega g = \Omega\}.$$

(vi) Let D be a division algebra with center k (its dimension as a k-vector space must be n^2 for some n). Let $v_i; 1 \leq i \leq n^2$ be a k-basis of D. The right multiplication by v_i gives a linear transformation $R_{v_i} \in GL(n^2, \bar{k})$ for $i = 1, 2, \cdots, n^2$ where $\bar{k}$ is the algebraic closure of

k. This is because when the scalars are extended to $\bar{k}$, the algebra D 'becomes' isomorphic to the algebra $M(n^2)$ of all $n^2 \times n^2$ matrices. The group

$$\{g \in GL(n^2, \bar{k}) : gR_{v_i} = R_{v_i} g \ \forall \ i = 1, 2, \cdots, n^2\}$$

is an algebraic group which can be identified over k with the group D^*.
We point out that applications to other subjects like differential geometry, number theory and finite geometries involve more general fields like the real field, finite fields and algebraic number fields.

2.2 Classification of Lie and algebraic groups

In an algebraic group over an algebraically closed field, one may "strip off" the maximal solvable normal algebraic subgroup and obtain the importance class of the so-called semisimple groups. These are classified in terms of certain associated finite reflection groups (as in § 1.4) called their Weyl groups. The same classification is valid for the complex Lie groups which are semisimple and simply connected. Over a general field, there may be different forms of the same semisimple algebraic group over the algebraic closure and, one uses Galois cohomology to classify and study them. Roughly, one obtains that the (non-exceptional or the) classical groups are the symplectic, Hermitian or skew-Hermitian forms over division algebras over the field. Thus, their classification reduces to the classification of such forms over the underlying field. The classification over a finite field plays a key role in the classification of finite simple groups (see § 1.1). Looking at the classification of Lie groups or algebraic groups, there is a lot in common and this brings forth a unity in mathematics - although the objects are different, their classifications are very similar. The informed reader can refer to [2], [5], [9], [11] for the theory of Lie algebras, algebraic groups and their classification.

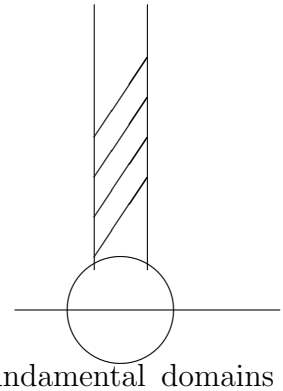
3 Modular group - an arithmetic group

Often, classical number-theoretic problems can be re-phrased in terms of groups; the groups which arise in this context are called arithmetic groups. For instance, the classical Dirichlet unit theorem can be interpreted and generalized in this framework. A prime example of an arithmetic group is the modular group $SL(2, \mathbf{Z})$. It is a discrete subgroup of $SL(2, \mathbf{R})$ such that the quotient space $SL(2, \mathbf{Z}) \backslash SL(2, \mathbf{R})$ is non-compact, but has a finite $SL(2, \mathbf{R})$-invariant measure. One defines a discrete subgroup Γ of a Lie group G to be an arithmetic group if there exists an algebraic group H defined over $\mathbf{Q}$ such that the group $H(\mathbf{R})$ of real points is isomorphic to $G \times K$ for a compact group K and Γ is 'commensurable' with the image of $H(\mathbf{Z})$ in G. Here, commensurability of two groups means that their intersection is of finite index in both. Some examples of arithmetic groups are :
(i) any finite group,
(ii) a free abelian group of finite rank,
(iii) the group of units in the ring of integers of an algebraic number field,
(iv) $GL(n, \mathbf{Z}), SL(n, \mathbf{Z}), Sp_{2n}(\mathbf{Z}), SL_n(\mathbf{Z}[i]), SO(Q)(\mathbf{Z}) := \{g \in SL_n(\mathbf{Z}) : g^t Q g = Q\}$ where Q is a quadratic form in n variables over $\mathbf{Q}$.

When G is a semisimple Lie group, a classical theorem due to A.Borel and Harish-Chandra shows that an arithmetic subgroup Γ has 'finite volume'. This means that there is a G-invariant finite measure on the quotient space G/Γ. The possibility of this quotient space being compact is reflected group-theoretically in terms of existence of unipotent elements in Γ. In general, one has a nice "fundamental domain" for Γ in G and this is given by what is known as reduction theory of arithmetic groups. Reduction theory for $SL(2,\mathbf{Z})$ is (roughly) to find a complement to $SL(2,\mathbf{Z})$ in $SL(2,\mathbf{R})$; a 'nice' complement is called a fundamental domain. Viewing the upper half-plane $\mathbf{H}$ as the quotient space $SL(2,\mathbf{R})/SO(2)$, the subset

$$\{z \in \mathbf{H} : \mathrm{Im}(z) \geq \sqrt{3}/2, \mid Re(z) \mid \leq 1/2\}$$

is (the image in $\mathbf{H}$) of a fundamental domain (figure below) :



Fundamental domains can be very useful in many ways; for example, they give even a presentation for the arithmetic group. Indeed, the above fundamental domain gives the presentation $< x, y | x^2, y^3 >$ for the group $PSL(2,\mathbf{Z}) = SL(2,\mathbf{Z})/\{\pm I\}$; that is, $PSL(2,\mathbf{Z})$ is a free product of cyclic groups of orders 2 and 3. The modular group $SL(2,\mathbf{Z})$ itself is thus an amalgamated free product of cyclic groups of orders 4 and 6 amalgamated along a subgroup of order 2. In this case, such a domain is written in terms of the Iwasawa decomposition of $SL(2,\mathbf{R})$. One has $SL(2,\mathbf{R}) = KAN$ in the usual way. The, reduction theory for $SL(2,\mathbf{Z})$ says $SL(2,\mathbf{R}) = KA_{\frac{2}{\sqrt{3}}}N_{\frac{1}{2}}SL(2,\mathbf{Z})$. Here $A_t = \{diag(a_1,a_2) \in SL(2,\mathbf{R}) : a_i > 0 \text{ and } \frac{a_1}{a_2} \leq t\}$ and $N_u = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N : |x| \leq u\}$.

This is connected with the theory of quadratic forms as follows. We shall consider only positive definite, binary quadratic forms over $\mathbf{Z}$. Any such form looks like $f(x,y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbf{Z}$; it takes only values > 0 except when $x = y = 0$. Two forms f and g are said to be equivalent (according to Gauss) if $\exists\ A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2,(\mathbf{Z})$ such that $f(x,y) = g(px+qy, rx+sy)$. Obviously, equivalent forms represent the same values. Indeed, this is the reason for the definition of equivalence. One defines the discriminant of f to be $\mathrm{disc}(f) = b^2 - 4ac$. Further, f is said to be primitive if $(a,b,c) = 1$. Note that if f is positive-definite, the discriminant D must be < 0 (because $4a(ax^2+bxy+cy^2) = (2ax+by)^2 - Dy^2$ represents positive as well as negative numbers if $D > 0$.) A primitive, +ve definite, binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is said to be reduced if $|b| \leq a \leq c$ and $b \geq 0$ if either $a = c$ or $|b| = a$. These clearly imply

$$0 < a \leq \sqrt{\frac{|D|}{3}}.$$

For example, the only reduced form of discriminant $D = -4$ is x^2+y^2. The only two reduced forms of discriminant $D = -20$ are $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

$GL(2, \mathbf{R})$ acts on the space S of +ve-definite, binary quadratic forms as follows: Each $P \in S$ can be represented by a +ve-definite, symmetric matrix. For $g \in GL(2, \mathbf{R})$, ${}^t gPg \in S$. This action is transitive and the isotropy at $I \in S$ is $O(2)$. In other words, S can be identified with $GL(2, \mathbf{R})/O(2)$ i.e. $S = \{{}^t gg : g \in GL(2, \mathbf{R})\}$. In general, this works for +ve-definite quadratic forms in n variables.
It is easy to use the above identification and the reduction theory statement for $SL(2, \mathbf{Z})$ to show that each +ve definite, binary quadratic form is equivalent to a unique reduced form. Indeed, writing $f = {}^t gg$ and $g = kan\gamma$, ${}^t gg = {}^t\gamma {}^t n a^2 n\gamma$ with $n \in U_{1/2}$ and $a^2 \in A_{4/3}$; so ${}^t na^2 n$ is a reduced form equivalent to f.
To see how useful this is, let us prove a beautiful discovery of Fermat, viz., that any prime number $p \equiv 1 \bmod 4$ is expressible as a sum of two squares.
Since $(p-1)! \equiv -1 \bmod p$ and since $(p-1)/2$ is even, it follows that $(\frac{p-1}{2}!)^2 \equiv -1 \bmod p$ i.e.,

$$((\frac{p-1}{2})!)^2 + 1 = pq$$

for some natural number q. Now the form $px^2 + 2(\frac{p-1}{2})!xy + qy^2$ is +ve definite and has discriminant -4. Now, the only reduced form of discriminant -4 is $x^2 + y^2$ as it is trivial to see. Since each form is equivalent to a reduced form (by reduction theory), the forms $px^2 + 2\frac{p-1}{2}!xy + qy^2$ and $x^2 + y^2$ must be equivalent. As the former form has p as the value at $(1, 0)$, the latter also takes the value p for some integers x, y.

In fact, reduction theory can also be used to show :
For any $D < 0$, there are only finitely many classes of primitive, positive-definite forms of discriminant D.
The number of classes alluded to is the class number $h(D)$ of the field $\mathbf{Q}(\sqrt{D})$; an isomorphism is obtained by sending $f(x, y)$ to the ideal $a\mathbf{Z} + \frac{-b+\sqrt{D}}{2}\mathbf{Z}$.
The idea is to use reduction theory to show that each form is equivalent to a unique 'reduced' form. 'Reduced' forms can be computed - there are even algorithms which can be implemented in a computer which can determine $h(D)$ and even the $h(D)$ reduced forms of discriminant D.

The initiated reader can refer to [6], [7] and [8] but we end with the statement of a somewhat recent deep application of the theory of arithmetic groups to a classical problem of number theory. The *Oppenheim conjecture* asserts that if Q is a real, indefinite quadratic form in $n \geq 3$ variables which is not a multiple of a rational quadratic form, then its values at integer lattice points form a dense subset of $\mathbf{R}$. This was reformulated in terms of Lie groups by Raghunathan and Dani following which Margulis solved it. The statement in terms of Lie groups is the following :
Let $G = SL(3, \mathbf{R}), \Gamma = SL(3, \mathbf{Z}), H = SO(X_1X_3 - X_2^2)$. Then, for any $g \in G$ such that $Hg\Gamma/\Gamma$ has compact closure, this space $Hg\Gamma/\Gamma$ is actually compact.

References

[1] R.Carter, *Finite groups of Lie type, Conjugacy classes and complex characters*, Reprint of the 1985 original, Wiley Classics Library, John Wiley & Sons, Ltd., Chichester 1993.

[2] R.Carter, *Lie algebras of finite and affine type*, Cambridge Studies in Advanced Mathematics 96, Cambridge University Press 2005.

[3] C.Geyer & K.Daniilidis, *Catadioptric projective geometry*, International Journal of Computer vision 43 (2001), pp.223-243.

[4] J.Humphreys, *Reflection groups and Coxeter groups*, Cambridge University Press 1997.

[5] J.Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics 21, Springer 1975.

[6] G.A.Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 17, Springer-Verlag 1991.

[7] V.P.Platonov & A.S.Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, Pure and Applied Mathematics 139, Academic Press 1994.

[8] M.S.Raghunathan, *Discrete subgroups of Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 68, Springer-Verlag 1972.

[9] T.A.Springer, *Linear algebraic groups*, Progress in Mathematics 9, Birkhauser 1981.

[10] D.Schattschneider, *The Plane Symmetry Groups : Their recognition and notation*, American Mathematical Monthly, Volume 85 (1978), pp. 439-450.

[11] V.S.Varadarajan, *Lie groups, Lie algebras and their representations*, Graduate Texts in Mathematics 102, Springer 1984.

[12] F.Warner, *Foundations of differentiable manifolds and Lie groups*, Scott, Foresman and Co., Glenview, Ill.-London, 1971.