Lett Mat Int (2017) 5:75–80
DOI 10.1007/s40329-017-0164-6

A for Algebra

Algorithms, formulas or structures?

Claudio Procesi[1]

Published online: 1 June 2017

Abstract This is a very brief overview of some of the main ideas of algebra through history, from the decomposition of a binomial identity, to the degree of a complex number, Euler's formula, transcendental numbers, skew fields, the Abel–Ruffini theorem, permutation groups, Lie algebras and more.

Keywords Algebra · Number theory · Quaternions · Lie algebras

I think my first encounter with algebra occurred in the lower secondary school, with the *binomial identity* $a^2 - b^2 = (a - b)(a + b)$.

I remember lots of exercises in computing with literal variables, where we had to develop intricate polynomial identities. There were also strange identities (which now I do not remember) involving square roots.

Those first lessons in algebra, given by talented professor Andreanelli, taught me one thing: while in Euclidean geometry we could always proceed by intuition and there was no single way to do things, in algebra could, and indeed had to, follow a purely algorithmic path, one that a machine could follow.

At that time computers were in their infancy and I knew them only through science fiction; that formula was the first of countless formulas that I would encounter in my life as a mathematician. Only many years later would I come to understand how to tackle analogous formulas, such as the decomposition of $a^n - b^n$ for any natural number n, and see algebra from completely different standpoints.

This decomposition is a good example for discussion because it carries with it many algebraic ideas. There are two standard formulas, the first one using the roots of unity:

$$\boxed{a^n - b^n = \prod_{k=0}^{n-1}(a - \zeta_n^k b)}, \quad \zeta_n := e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}. \tag{1}$$

The second and more interesting one is a unique factorisation via irreducible polynomials on the integers, and precisely the *irreducible cyclotomic polynomials* with integer coefficients, given by:

$$(x^n - 1) = \prod_{d|n}\phi_d(x), \quad \phi_d(x) := \prod_{(k,d)=1}(x - \zeta_d^k), \tag{2}$$

where $(k, d) = 1$ means that k has greatest common divisor with d equal to 1.

Examples of formula (2): $n = 6$, whose divisors are 1, 2, 3, 6; and $n = 9$ whose divisors are 1, 3, 9.

$$\begin{aligned} x^6 - 1 &= (x-1)(x+1)(x^2+x+1)(x^2-x+1), \\ x^9 - 1 &= (x-1)(x^2+x+1)(x^6+x^3+1). \end{aligned} \tag{3}$$

These formulas are connected to a great enigma of Greek geometry, that is, if it is possible to *square the circle*, *duplicate the cube* or *trisect an angle* using a ruler and a compass.

Carl Friedrich Gauss (1777–1855) proved that the last two constructions are impossible, using the notion of *degree* of a number.

Definition 1 The degree of a complex number α is the degree k of an irreducible polynomial with rational

✉ Claudio Procesi
procesi@mat.uniroma1.it

[1] Via Bolzano 32, 00198 Rome, Italy

coefficients $f(x) = x^k + a_1 x^{k-1} + \cdots + a_k$ of which α is a root, that is, $f(\alpha) = 0$. If there is such a polynomial, it is unique and is said to be a *minimal polynomial* of α; if it is does not exist, we say α is *transcendental*.

Gauss proved that if a point in the plane given by a complex number α is constructible using ruler and compass, then the degree of α must be a power of 2. The duplication of the cube is impossible since the number $\alpha = \sqrt[3]{2}$, the length of the side of the cube of volume 2, satisfies the irreducible polynomial $x^3 - 2$ and so has degree 3.

From formula (3) we see that the root ζ_n is the second vertex of a regular n-gon with first vertex 1 and centred at 0. Hence, such a n-gon is constructible if and only if the degree of the cyclotomic polynomial $\phi_n(x)$ is a power of 2.

This is why cyclotomic polynomials appear in the solution of the problem. From formula (3), the minimal polynomial of ζ_6 is $x^2 - x + 1$; then it has degree 2.

Similarly, a vertex ζ_3 of an equilateral triangle satisfies $x^2 + x + 1$ and again has degree 2. The construction of these two polygons with ruler and compass is taught in schools.

But if we want to trisect the angle of the equilateral triangle, and hence to build the regular polygon with nine sides, the number ζ_9 now satisfies $x^6 + x^3 + 1$ [see again formula (3)] and ζ_9 has degree 6. So it is not constructible!

In general, the degree of the cyclotomic polynomial $\phi_d(x)$ is given by the *Euler function* $\varphi(d)$ which, if $d = \prod_i p_i^{h_i}$ is the decomposition of d in prime factors, is given by

$$\varphi\left(\prod_i p_i^{h_i}\right) = \prod_i (p_i - 1) p_i^{h_i - 1}.$$

As soon as an odd prime with exponent >1 appears, this number is not a power of 2. For a prime p we have the problem of when $\phi(p) = p - 1 = 2^h$.

For instance, $\varphi(17) = 16 = 2^4$, and indeed the polygon with 17 sides can be constructed with ruler and compass.

It is easy to see that, if a prime number is of the form $p = 2^k + 1$, then $k = 2^n$ is also a power of 2 for some n.

A prime number of the form $2^{2^n} + 1$ is called a *Fermat prime*, but in fact it is not known if infinitely many Fermat primes exist. The only known ones are 3, 5, 17, 257, 65537.

The problem of squaring the circle is far more complex. We also find it mentioned by Dante Alighieri, in Canto XXXIII of *Paradiso*:

> Qual è 'l geomètra che tutto s'affige
> per misurar lo cerchio, e non ritrova,
> pensando, quel principio ond'elli indige...

("As the geometrician, who endeavours/To square the circle, and discovers not,/By taking thought, the principle he wants...", in Henry Wadsworth Longfellow's translation).

The answer is that the circle cannot be squared. Ferdinand von Lindemann (1852–1939) proved that *π is a transcendental number* (Definition 1). This proof is part of the *analytic number theory*.

The two formulas (1) and (2) already allow us to discuss two further steps into algebra. In the first one the *complex numbers* ($\mathbb{C}$) as well as an example of *Euler's formula* appear:

$$e^{i\theta} = \cos\theta + i \sin\theta. \tag{4}$$

It is interesting to understand how complex numbers were discovered. It was in Italy, in mid-Renaissance, when Scipione del Ferro (1465–1526) discovered the formula to solve a cubic equation $x^3 = px + q$. Let's start with the symbolic identity $(a+b)^3 = 3ab(a+b) + a^3 + b^3$. If there are two numbers a, b such that

$$q = a^3 + b^3, \quad p = 3ab, \quad \Longrightarrow \; p^3 = 27a^3b^3, \tag{5}$$

then one solution is

$$x = a + b.$$

From (5) it follows that the two numbers a^3, b^3 are the solutions of the quadratic equation $x^2 - qx + \frac{p^3}{27}$. Then we have the solution of the equation $x^3 = px + q$:

$$x = a + b = \sqrt[3]{\frac{q + \sqrt{q^2 - \frac{4p^3}{27}}}{2}} + \sqrt[3]{\frac{q - \sqrt{q^2 - \frac{4p^3}{27}}}{2}}. \tag{6}$$

Consider now the equation:

$$x^3 - 7x + 6 = 0 \quad (p = 7,\ q = -6).$$

We see immediately that

$$x^3 - 7x + 6 = (x-1)(x-2)(x+3)$$

and, therefore, this equation has as its solutions 1, 2 and −3. By applying formula (6):

$$a + b = \sqrt[3]{-3 + 10\sqrt{-\frac{1}{27}}} + \sqrt[3]{-3 - 10\sqrt{-\frac{1}{27}}} \tag{7}$$

the mysterious term $\sqrt{-\frac{1}{27}}$ appears. This is how complex numbers entered mathematics. They were studied systematically by Rafael Bombelli. By computing with them, one finds that the mysterious formula (7) is indeed equal to 1.

Another interesting story related to these ideas is the investigation by Kummer of *Fermat's last theorem*. The problem is well-known: Fermat claimed that the equation $x^n = y^n + z^n$ has no integer solutions, besides the trivial ones ($y = 0$ or $z = 0$), for $n > 2$, but without providing a proof for his claim. Proving this has long remained one of

the greatest challenges of mathematics. The equation may be rewritten as:

$$x^n - y^n = z^n \iff \prod_{j=1}^{n} \left(x - e^{j\frac{2\pi \mathrm{i}}{n}} y\right) = z^n \tag{8}$$

that is, involving the factorisation of the integer z^n not into integers but into numbers containing the nth roots of 1. Kummer's idea was to use some sort of *unique factorisation* for such non-integer numbers.

The formalization of this method is related to the study of the rings of *algebraic integers* and to the development of the notion of *ideal*, which are fundamental in abstract algebra.

The crucial discovery was that the rings of algebraic integers in a cyclotomic field $\mathbb{Q}(e^{\frac{2\pi \mathrm{i}}{p}})$ with p a prime number are not always unique factorisation rings. When they are, the prime number is said to be *regular*. For instance, all prime numbers less than 100 are regular except 37, 59 and 67.

Kummer was able to prove Fermat's last theorem for n a regular prime. It took more than 100 years and the introduction of very advanced ideas to make it possible for Andrew Wiles to finally solve this mystery in general.

Let us go back to the Euler's formula (i) [see (4)], which together with formula (ii):

(i) $e^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$,

(ii) $e^{\mathrm{i}\theta_1} e^{\mathrm{i}\theta_2} = e^{\mathrm{i}(\theta_1+\theta_2)}$

$$\iff (\cos\theta_1 + \mathrm{i}\sin\theta_1)(\cos\theta_2 + \mathrm{i}\sin\theta_2) = \cos(\theta_1+\theta_2) + \mathrm{i}\sin(\theta_1+\theta_2)$$

yields the basic rules of trigonometry:

$$\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 = \cos(\theta_1+\theta_2),$$
$$\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2 = \sin(\theta_1+\theta_2).$$

The numbers $e^{\mathrm{i}\theta}$ are the complex numbers α having modulus $\alpha\bar{\alpha} = 1$. They form the *group of rotations in the plane* and $e^{\mathrm{i}\theta}$ is the rotation by an angle θ.

Sir William Rowan Hamilton raised the problem of developing a similar calculation for the orthogonal transformations of the space $\mathbb{R}^3$. It was well known, and various formulas had already been developed, that this group is generated by three rotations with respect to the three orthogonal axes given by a Cartesian coordinate system $\mathtt{i}$, $\mathtt{j}$, $\mathtt{k}$. Hamilton tried to develop a multiplication (today we would say a skew field structure) on the space $\mathbb{R}^3$, from which these rotations could be developed. Finally, on 16 October 1843, while walking with his wife, he realised that the solution lay in adding a fourth dimension, given by a number 1 besides the other three ($\mathtt{i}$, $\mathtt{j}$, $\mathtt{k}$), and could not resist doing a graffiti on Brougham Bridge in Dublin (now replaced by a metal plaque) of the fundamental formula of multiplication

$$\mathtt{i}^2 = \mathtt{j}^2 = \mathtt{k}^2 = \mathtt{ijk} = -1. \tag{9}$$

He called such numbers *quaternions*. They form a non-commutative ring $\mathbb{H}$ consisting of elements

$$\mathbb{H} = \{q = a1 + b\mathtt{i} + c\mathtt{j} + d\mathtt{k},\ a, b, c, d \in \mathbb{R}\}.$$

We can define the conjugate $\bar{q} = a1 - b\mathtt{i} - c\mathtt{j} - d\mathtt{k}$ of a quaternion q, obtaining $q\bar{q} = a^2 + b^2 + c^2 + d^2$; from this we define the *modulus* of a quaternion

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2}, \quad q \cdot \bar{q} = |q|^2.$$

Every quaternion other than 0 has an inverse $\bar{q}|q|^{-2}$. We have the first example of what we now call a *skew field*.

A new, very interesting phenomenon appears. The quaternions of modulus 1 again form a group and give rise to rotations of $\mathbb{R}^3$ via the formula

$$b\mathtt{i} + c\mathtt{j} + d\mathtt{k} \mapsto q\,(b\mathtt{i} + c\mathtt{j} + d\mathtt{k})\,q^{-1}. \tag{10}$$

However, it happens, as seen directly applying formulas (9) and (10), that the quaternion $e^{\mathtt{i}\theta} = \cos\theta + \mathtt{i}\sin\theta$ induces on the plane $\mathtt{j}$, $\mathtt{k}$ a rotation by an angle 2θ and not by θ; analogously, $e^{\mathtt{j}\theta} = \cos\theta + \mathtt{j}\sin\theta$ induces on the plane $\mathtt{k}$, $\mathtt{i}$ a rotation by an angle 2θ (and $e^{\mathtt{k}\theta}$ a rotation on the plane $\mathtt{i}$, $\mathtt{j}$):

$$\begin{aligned}(\cos\theta + \mathtt{j}\sin\theta)\mathtt{k}(\cos\theta - \mathtt{j}\sin\theta) &= (\cos^2\theta - \sin^2\theta)\mathtt{k} + 2\cos\theta\sin\theta\,\mathtt{i}\\ &= \cos(2\theta)\,\mathtt{k} + \sin(2\theta)\,\mathtt{i}.\end{aligned}$$

In modern terms, we have the phenomenon of spin 1/2 (of the electron). The group of quaternions of modulus 1, which from a geometrical point of view is the three-dimensional sphere $a^2 + b^2 + c^2 + d^2 = 1$, is the (double) universal cover of the group $SO(3, \mathbb{R})$ (these ideas are due to Poincaré).

In fact, the calculations involving quaternions for three-dimensional phenomena are now relevant, in disciplines such as computer graphics, machine vision, robotics, control theory, signal processing, attitude control, physics, bioinformatics, molecular dynamics, computer simulations and orbital mechanics.

By the late nineteenth century a process of mathematical abstraction had begun.

We can take as the beginning of abstract algebra the finiteness theorems by Hilbert on the invariants of algebraic forms, submitted to the *Mathematische Annalen* in 1888. Gordan, the leading expert in the theory of invariants, refused to publish the article commenting: "Das ist nicht Mathematik. Das ist Theologie" ("This is not mathematics. This is theology").

This abstract path led to a systematic study of various types of *algebraic structures*, among which the most used are *groups*, *monoids*, *rings*, *(skew) fields*, *Lie algebras*. This abstract approach went in parallel with the development by Cantor of *set theory*, a theory readily supported by Hilbert (1926): "Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können" ("Nobody can drive us out of the paradise that Cantor has created for us").

Usually in mathematics a *structure* is given on a set X. It is an algebraic structure when on X some operations are given, such as binary operations $X \times X \to X$ or more general ones. Then there are geometric structures, such as *topologies* or *differential structures*, given by different sets of axioms.

A *ring* structure is an algebraic structure with two binary operations $+$ and $\times$, with axioms that summarise the formal properties of numbers, but allowing for the possibility that the product is not commutative.

There are infinitely many different rings. Among the rings we have the *skew fields* (or *division algebras*), such as the quaternions, in which each element other than 0 has an inverse, but there are also examples as the rings of matrices, in which there are elements a different from 0 but such that $a^2 = 0$.

We might ask if there are skew fields formed by k coordinates, that is, a skew field structure on $\mathbb{R}^k$. A theorem by Frobenius assures us that there are no other examples except those already known: $k = 1$, $\mathbb{R}$; $k = 2$, $\mathbb{C}$; $k = 4$, $\mathbb{H}$. On the other hand, if we do not require that every nonzero element be invertible, we have on $\mathbb{R}^k$ the associative algebras structures, and there are infinitely many different ones, all related to the matrices.

The group structure is a more primitive one, which is closely linked to a classic problem. After the solution of the third-degree equation, Lodovico Ferrari is credited with the discovery of the solution of fourth-degree equations in 1540.

From the reduced equation $x^4 + \alpha x^2 + \beta x + \gamma = 0$, we can reduce to solving a cubic equation

$$y^3 + \frac{5}{2}\alpha y^2 + (2\alpha^2 - \gamma)y + \left(\frac{\alpha^3}{2} - \frac{\alpha\gamma}{2} - \frac{\beta^2}{8}\right) = 0.$$

Finding a formula for the fifth-degree equation was a mystery that lasted 250 years.

In 1799 Paolo Ruffini published his *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto* ("General theory of equations in which the algebraic solution of general equations of degree higher than four is proven impossible").

This theorem is known as *Abel-Ruffini theorem*: more precisely, the general equation of degree 5 cannot be solved by radicals.

The systematic study of why and which equations can be solved by radicals is due to Évariste Galois (1811–1832), who developed a general theory through the symmetries of a set of suitable permutations of the roots of the equation, now called *Galois group*. *Group theory* was born.

Why do we have a solution for degree 4? Consider the 24 permutations of 4 numbers; any two of them can be multiplied, or composed (for instance, $(2,4,1,3)\circ(3,1,2,4) = (1,2,4,3)$), forming a group called *symmetric group* and denoted by S_4. We can divide them into six blocks:

$$\begin{aligned} &\mathrm{a}\begin{vmatrix}1,2,3,4\\2,1,4,3\\3,4,1,2\\4,3,2,1\end{vmatrix}, \mathrm{b}\begin{vmatrix}1,2,4,3\\2,1,3,4\\3,4,2,1\\4,3,1,2\end{vmatrix}, \mathrm{c}\begin{vmatrix}1,3,2,4\\2,4,1,3\\3,1,4,2\\4,2,3,1\end{vmatrix}, \mathrm{d}\begin{vmatrix}1,3,4,2\\2,4,3,1\\3,1,2,4\\4,2,1,3\end{vmatrix},\\ &\mathrm{e}\begin{vmatrix}1,4,2,3\\2,3,1,4\\3,2,4,1\\4,1,3,2\end{vmatrix}, \mathrm{f}\begin{vmatrix}1,4,3,2\\2,3,4,1\\3,2,1,4\\4,1,2,3\end{vmatrix} \end{aligned} \tag{11}$$

Multiplying the permutations we observe that we obtain a *multiplication table* between the six blocks; for example, any permutation of block (b) times any one of block (d) gives rise to a permutation of the block (f). The complete table is as follows, renumbered on the right:

$$\begin{array}{cccccc} a & b & c & d & e & f \\ b & a & e & f & c & d \\ c & d & a & b & f & e \\ d & c & f & e & a & b \\ e & f & b & a & d & c \\ f & e & d & c & b & a \end{array} \quad \Longleftrightarrow \quad \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \\ 3 & 4 & 1 & 2 & 6 & 5 \\ 4 & 3 & 6 & 5 & 1 & 2 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{array} \tag{12}$$

The fact that we can assign the 24 permutations of 1, 2, 3, 4 into six blocks in such a way that the multiplication among blocks is well-defined is responsible for the existence of the reduction to a cubic equation, and ultimately for the existence of the solution by radicals of the equation of degree 4. Galois showed that the solubility of an equation depends on the structure of its symmetry group, a property said precisely of a *solvable group*. To explain it let us give a definition.

Definition 2 A *permutation group* is a set of permutations closed under the product $\circ$. A group is *simple* if it cannot be decomposed into *blocks* that multiply by each other.

From a more formal viewpoint, we have to see if a group G has a *normal subgroup* H (the block to which 1 belongs), that is, a subgroup H with $gHg^{-1} = H$, $\forall g \in G$. In this case the blocks in which the group is divided are the cosets $gH = Hg$ that form the *quotient group* G/H.

In our example, the multiplication table (12) of the quotient group coincides with the multiplication table of S_3. The block a) is a *normal subgroup* and the other blocks are its cosets.

This example can be seen geometrically. S_4 is the whole group of symmetries of the tetrahedron or the cube. Each symmetry permutes the three symmetry planes of the cube, inducing the quotient group S_3. There are 4 symmetries fixing these planes.

The symmetries of an equation of degree 5 are (often) the 120 permutations of 5 elements. The only well-behaved partition is that into two blocks of 60 elements: the even permutations and the odd ones. This way, we obtain the first non-commutative simple group, the subgroup of even permutations, with 60 elements. It is responsible for the fact that it is impossible to solve the equation of degree 5 by radicals.

Every finite group can be expressed as a *composition*, in a convoluted way, of a series of simple groups, and a group is solvable if and only if these simple groups are commutative.

The study of simple groups was, and still is, one of the great achievements of algebra.

The classification of all finite simple groups is one of the high points of 20th-century algebra. It occupies thousands of pages of complex mathematics, and John G. Thompson and Jacques Tits were awarded the Abel Prize in 2008 for their contributions to the theory.

In addition to the quaternions, in the 19th century two other non-commutative kinds of calculation were developed: the calculation with matrices and Grassmann exterior algebra, both part of *vector calculus*, that is, of linear and multilinear algebra. In addition, a non-associative kind of calculation was developed, that of *Lie algebras*, which originated from the study of non-Euclidean geometries and *continuous groups*, due to Sophus Lie.

By now calculating with matrices is a topic taught in a standard syllabus, but this was not always so. We need only recall that at the beginning of the construction of quantum mechanics Heisenberg had not yet formulated in a completely algebraic way its commutation relations.

From the viewpoint of algebraic structures, we have, as for the groups, the notion of a *simple algebra*; it can be shown that the algebra $M_k(D)$ of all matrices on a skew field D is simple.

Thus we can ask: among the possible structures of associative algebras on $\mathbb{R}^k$, which ones are simple? The answer is due to Wedderburn, who proved that a simple algebra of finite dimension over a field F is necessarily the algebra $M_k(D)$ of the matrices on a skew field D. In particular, when $F = \mathbb{R}$, it is the algebra of all matrices on one of the three skew fields $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$.

Formally a Lie algebra is a vector space (such as $\mathbb{R}^k$) with a bilinear product, denoted by $[a, b]$, that satisfies the two identities:

$$\begin{aligned} &\text{antisymmetry: } [a,b] = -[b,a];\\ &\text{Jacobi identity: } [[a,b],c] + [[b,c],a] + [[c,a],b] = 0. \end{aligned} \tag{13}$$

The notion of a Lie algebra originates from analysis, from the fact that the vector fields

$$X = \sum_{i=1}^{k} f_i(x_1, \dots, x_k)\frac{\partial}{\partial x_i},$$

thought of as linear differential operators, have the property that $[X, Y] := X \cdot Y - Y \cdot X$ is again a vector field. From a dynamic viewpoint, a vector field is the infinitesimal generator of a time evolution of space, the so-called *one-parameter group*.

Formally, a one-parameter group on a space A is a family of transformations $g(t)$: $A \to A$ depending on a parameter $t \in \mathbb{R}$, with the property

$$g(0)(x) = x, \quad \forall x \in A, \qquad g(s+t) = g(s) \circ g(t),$$
$$\forall s, t \in \mathbb{R} \implies g(-t) = g(t)^{-1}.$$

Under suitable assumptions, if $A = \mathbb{R}^k$ or more in general a differentiable manifold, such a one-parameter group is determined by a vector field X, its infinitesimal generator, through the evolution of the functions (e.g., coordinates), by the differential equation

$$\frac{d}{dt} f(t, x_1, \dots, x_k) = X(f(t, x_1, \dots, x_k)),$$

which, at least formally, has as its solution

$$f(t, x_1, \dots, x_k) = e^{tX} f(x_1, \dots, x_k) = \sum_{k=0}^{\infty} t^k \frac{X^k}{k!} f(x_1, \dots, x_k).$$

The product $[X, Y] := X \cdot Y - Y \cdot X$ is said to be a *commutator*, since it vanishes if and only if the two one-parameter groups generated by the two fields commute.

Lie's ideas developed, in parallel with Felix Klein's *Erlangen Programme*, out of the discovery of *non-Euclidean geometries* and the need to understand the role of the symmetry or isotropy of space (which, by the way, at the beginning of the 20th century was undergoing a crisis, as regards physical space, due to Einstein's general relativity).

Klein's ideas developed the point of view of the *subordination of geometries*, in particular the various geometries

seen as subordinate to projective geometry. In this context, the symmetry groups of the geometries are all contained in the projective group and defined by the property of preserving certain geometric objects.

In a more abstract way, Lie wanted to study transformation groups depending on m parameters and acting on a k-dimensional space. The idea is that such a group (as in the case of the group of rigid motions of space, generated by the three groups of rotations around the three axes and the three translations) can be constructed from m infinitesimal generators $X_1, \dots, X_m$, one for each parameter, which are *multiplied* by each other, or

$$[X_i, X_j] = \sum_{h=1}^{m} a_{i,j}^h X_h, \qquad a_{i,j}^h \in \mathbb{R}.$$

This rule defines, given a basis, the corresponding Lie algebra. In the example of the quaternions of modulus 1, the Lie algebra has as a basis formed by the elements $\mathtt{i}$, $\mathtt{j}$, $\mathtt{k}$, which generate the three one-parameter groups $e^{\mathtt{i}\theta}$, $e^{\mathtt{j}\theta}$, $e^{\mathtt{k}\theta}$ and form a Lie algebra with $[\mathtt{i}, \mathtt{j}] = 2\mathtt{k}$, and similar formulas for other commutators.

The classification of some geometries passes through the classification of simple Lie algebras, which is much easier than the classification of finite simple groups and was obtained by Wilhelm Killing and Élie Cartan. These authors showed that the simple Lie algebras are given by 4 infinite series, associated with the classical groups of matrices, and 5 exceptional algebras, called G_2, F_4, E_6, E_7, E_8.

So we arrive to the 20th century and to the present day. It is impossible to give a true idea of the unrestrained developments of mathematics and algebra, particularly in recent times. At the beginning of the 20th century, at the 1900 International Congress of Mathematicians (ICM) in Paris the participants could be contained in a group picture, while now thousands of scientists from all over the world take part in the ICM. With the advent of the Internet, the TEX typesetting system and the arXiv.org electronic archive,[1] new scientific papers appear every day. It is impossible to follow them all.

The algebra of the 20th century, in addition to the saga of finite groups, mentioned above, has been boosted by geometry in its two aspects of *algebraic geometry* and *algebraic topology*, constructing new theories such as commutative algebra and homological algebra, theories that have merged with the categorical approach that has become increasingly common in the last 50 years.

Abstraction has dominated these theories, often studying objects not really constructible, but whose existence depends on axioms such as that of choice, as for example the *Tarski monster*, an infinite group in which all proper subgroups have order a prime number p.

Another major source of developments has been *quantum mechanics*, which added to the classical methods of mathematical physics, based on differential equations, algebraic methods of operator theory and representations of Lie groups, as the fundamental symmetries of elementary particles.

A very remarkable discovery was that of quarks, by Murray Gell-Mann, from a formal algebraic object called the *Eightfold Way*, consisting of a representation of dimension 3 of the 8-dimensional Lie algebra $su(3)$.

Finally, in recent years the algorithmic and computational approach has regained strength, due to the possibility of using computers to do calculations that are impossible to do by hand. So *computer algebra* was born, along with software packages to perform algebraic calculations.

On the future I'd rather not comment.

Translated from the Italian by Daniele A. Gewurz.

Claudio Procesi is Professor Emeritus at the University of Rome "La Sapienza". He has authored 126 publications in several fields of mathematics, including: K-theory, algebraic geometry, algebraic topology, associative rings and algebras, commutative rings and algebras, convex and discrete geometry, dynamical systems and ergodic theory, field theory and polynomials, general global analysis, analysis on manifolds, group theory and generalizations, history and biography, linear and multilinear algebra, matrix theory, manifolds and cell complexes, non-associative rings and algebras, number theory, partial differential equations, statistical mechanics, topological groups and Lie groups.

[1] https://arxiv.org/find.