# The Theory of Equations and the Birth of Modern Group Theory

## An Introduction to Galois Theory

*B Sury*

**A mathematician whose collected works run to a mere sixty pages, one who did not live to be 21 and yet truly revolutionised modern mathematics through his pioneering discoveries – this uniquely defines Évariste Galois!**

B Sury is now with Indian Statistical Institute in Bangalore after spending about 18 years at the Tata Institute of Fundamental Research in Mumbai. Nonsense writing (present article not included!) and mathematical satire are the principal interests he banks on.

### A Glimpse into his Life and Work

Galois's work was in what was then known as the theory of equations. The principal problem here can be easily described. In school, we learn how to solve quadratic equations $a_0 + a_1x + a_2x^2 = 0$. The solutions are simple expressions in the coefficients and involve only the operations of addition, subtraction, multiplication, division and extraction of square roots. This was discovered in Mesopotamia between 1800 and 1600 BC. For the cubic and the degree four equations, Scipione del Ferro and Ferrari gave solutions in the beginning of the 16th century in terms of the coefficients as expressions involving the above operations and, in addition, the extraction of higher roots. *What about the equations of degree five?* For more than 300 years, mathematicians tried in vain to find such a 'formula' for the general equation of fifth degree. Here, one means by a formula for the roots of a polynomial equation, expressions in the coefficients which involve only the operations of addition, subtraction, multiplication, division and the extraction of various roots. It was Ruffini who first realised that such a formula *may not* exist and Abel followed up Ruffini's ideas to prove this. By this, one should understand that no matter how great the mathematician or how sophisticated the method, one cannot get a 'formula' in the above sense. What is more, one can *prove* that a formula cannot exist! Such non-existence statements occur throughout mathematics and are usually considerably harder to prove than the existence statements.

In other words, it is a 'no go' situation in modern parlance. However, this still does not preclude the possibility of a formula valid for an infinite class of equations. For instance, the great mathematician Gauss proved in 1801 that the roots of the cyclotomic equation $X^n - 1 = 0$ can be expressed by such a formula – the cyclotomic equations will be the subject of another article in a later issue of *Resonance.* Galois's pathbreaking work completely nailed down the whole problem by giving a criterion which is necessary as well as sufficient for a given equation of any degree to yield such a formula. This and more are part of what is known as Galois theory.

Galois's study of a polynomial $p(x)$ was based on the idea that the group of permutations of the roots of $p(x)$ retains all the information on $p(x)$. The theory of groups is such a central part of present-day mathematics that it seems difficult to believe that during Galois's time, group theory, per se, was nonexistent. Indeed, it is a tribute to Galois's genius that group theory has the central place that it has today. If a subgroup of a group has the property that its left cosets and right cosets are the same, Galois recognised quite brilliantly that the subgroup must be distinguished. This paved the way towards his formulation of the theory known now as Galois theory; the fundamental theme here is that to each polynomial one can associate a certain group (called its Galois group) in a bijective fashion so that the theory of equations gets replaced by group theory. *It turns out that for the existence of a formula to find the roots of a polynomial in terms of radicals (i.e. various roots) of the coefficients, it is necessary and sufficient that the corresponding Galois group have the special property that the procedure of writing 'commutators'* $aba^{-1}b^{-1}$, *and commutators of commutators etc. leads after a finite number of repetitions to the identity element. For this reason, such groups are nowadays called solvable (*see *Box* 1*). The general equation of n-th degree has for its Galois group, the full permutation group* $S_n$. *As the symmetric group* $S_n$ *is not solvable when n is greater than or equal to* 5, Abel–Ruffini's theorem about the nonexistence of a 'formula' follows neatly. What is astonishing is that Galois theory solves with equal ease an algebraic problem

**Box 1.**

A *solvable* group $G$ is one for which there is a finite chain of subgroups $\{e\} = G_r \leq \ldots G_1 \leq G_0 = G$ where each $G_i$ is normal in $G_{i-1}$ with the quotient $G_{i-1}/G_i$ being abelian. This easily implies that one has a finite chain in which each $G_i$ is normal in the whole of $G$ rather than just in the next group $G_{i-1}$. For instance, one can define recursively $D_0 = G$, $D_{i+1}$= the smallest subgroup of $D_i$ containing the *commutators* $aba^{-1}b^{-1}$ with $a, b \in D_i$. It can be checked inductively that $D_i \leq G_i$ and the $D_i$ give a chain as asserted.

like the solvability by radicals of a quintic, and classical geometric problems like squaring the circle, trisecting an angle or duplicating the cube. The geometric problems referred to are: (i) to construct a square whose area is that of the unit circle, (ii) to trisect a given angle and, (iii) to construct a cube whose volume is twice that of a given cube, all of which are to be done with the aid of a straight-edge and a compass (for more details, see [1]). Another important discovery by Galois was the determination of the finite fields – these are now called Galois fields.

Epoch-making as Galois's discoveries are, they didn't get him recognition during his life time. His life was such a succession of misfortunes that it is indeed a miracle that his work came to light at all. Galois was born on the 25th of October, 1811. At the age of 17, he obtained the principal results of Galois theory. (It is remarkable that at that time, Galois had not even heard of Abel.) He submitted two papers on these in May and June of 1829 to Cauchy who promised to present them to the Academy of Sciences in Paris. Cauchy forgot to do so, and, in addition, lost the manuscripts[1]. Galois was so sure of his abilities and of the importance of his researches that he submitted his results for the second time in February 1830, to the Academy of Sciences – this time for the Grand Prize of Mathematics. Fourier, who was secretary then, took them home to examine but died before he could do so and no trace of Galois's manuscripts could be found among Fourier's papers. As a final attempt, Galois submitted a memoir to the Academy once again in January 1831 only to find it turned down by the referee Poisson who found it *incomprehensible*. Such repeated onslaughts of misfortune perhaps engendered in the youngster a hate for society as a whole and drove him to politics on the side of the then forbidden republicanism. He threw himself furiously into the revolution of 1830. He was arrested twice in 1831 on charges of being a radical. Here is a place where the problem was not solvable by radicals! Even after his release from prison, he was hounded by his political enemies. He was challenged to a duel with pistols by a patriot on the 30th of May 1832. He was shot and died

[1] This is according to Van der Waerden's '*History of Modern Algebra*' and E T Bell's '*Men of Mathematics*', for another version, please see T Rothman's 'The Fictionalization of Évariste Galois' in *American Mathematical Monthly*, 89, 84–106, 1982.

early in the morning of the 31st. Realising that he might not survive, he had spent the previous night desperately scribbling down his discoveries, racing against time. He left these papers in the care of his friend Auguste Chevalier. In his letter to Chevalier, he says "Ask Jacobi or Gauss to give their opinion, not as to the truth, but as to the importance of these theorems". This clearly shows how invaluable he believed his work to be. Thanks to Chevalier for preserving the papers, the work done by 17-year old Galois got published eventually – 14 years after Galois died – and proved to be as epoch-making as Galois hoped to see. Look at the Article-in-the-box for more historical details.

## Groups, Rings and Fields

The mathematical formulation of Galois theory involves the languages of groups and fields. We start with the first one which is the one that is more familiar to most people.

Symmetry is a basic phenomenon common to all sciences and the concept of groups was created to understand it. Although the concept was already existent in some form before Galois, the first real place where the power of group theory came to the fore is the theory of equations. *Therefore, one could say that the birth of modern group theory is due to Galois.* Let us get down to brass tacks and say precisely what we are really talking about. As most of the readers would be aquainted with at least finite group theory, we start with a breezy survey of the basic concepts and results of general group theory relevant to us.

**Box 2.**

A *group G* is a set provided with a prescription (called group multiplication) that manufactures from a pair of elements $a$, $b$ (in that order), a third element usually written $ab$ and called their product; this prescription is further required to satisfy the following natural conditions of:

(i) ***Associativity***: $a(bc) = (ab)c$ for all $a$, $b$, $c$,

(ii) *Existence of an identity element e* : $ae = ea = a$ for all $a$,

(iii)*Existence of an inverse element*: for each $a$, there is an element denoted by $a^{-1}$ such that $aa^{-1} = a^{-1}a = e$.

The principal models of groups (see *Box* 2) are the familiar groups of numbers: the integers **Z**, the rational numbers **Q**, the real numbers **R** and the complex numbers **C** under addition. Here are some more examples:

(i) The *non-zero numbers in* **Q**, **R**, **C** under multiplication.

(ii) The unit circle in the complex plane under the multiplication of complex numbers – this just amounts to the addition of angles.

For a positive integer $n$, the set $e^{2i\pi r/n}$ for $r = 1, \cdot \quad, n$, i.e., the set of $n$-th roots of unity, forms a *subgroup* of this group i.e., it is a subset which is a group under the same multiplication. One could also take all the roots of unity corresponding to all positive integers $n$ – this is the torsion subgroup of the circle group (i.e., it comprises all $a$ such that $a^n = 1$ for some $n$).

(iii) The set $GL_n$ of all invertible $n \times n$ matrices with entries from $\mathbf{Q}, \mathbf{R}$ or $\mathbf{C}$ under matrix multiplication. In fact, example (i) is the special case of this corresponding to $n = 1$. Note that unlike the earlier examples, when $n \geq 2$, the matrix group is *not abelian* i.e., there are invertible matrices $A, B$ for which $AB \neq BA$. The subsets $B$ of all upper triangular matrices and $T$ of all diagonal matrices in $GL_n$ are also subgroups. The latter is abelian but the former is not abelian if $n \geq 2$.

(iv) For a positive integer $n$, the set of integers modulo $n$ forms a group under addition modulo $n$. More generally, if one considers the equivalence relation $\sim$ among rational numbers defined by $a \sim b$ if $a - b$ is an integer, the equivalence classes form a group (*Ex. What is the group multiplication here?*). These two examples are just the ones mentioned in (ii) under a different guise.

(v) For any set $X$, the set $S(X)$ of all bijections on $X$ is a group under the composition of bijections. If $X$ is a finite set of $n$ elements, $S(X)$ is usually denoted by $S_n$ and is called the symmetric group on $n$ letters. Any subgroup of $S_n$ for some $n$ is called a permutation group. If $\theta : G \to H$ is a homomorphism (see *Box* 3), its image $\{\theta(g) : g \in G\}$ is a subgroup of $H$. For example, the mapping of the circle to itself which raises each element to its $n$-th power (for some fixed $n$) is a homomorphism. Note that this is onto but not 1-1 as each $n$-th root of unity maps to the identity element. A homomorphism which is also a bijection is called an *isomorphism*. As all the properties of a group structure are preserved under any isomorphism, we are interested in only the isomorphism classes of groups. A *cyclic* group is a group generated by a single element of it. The group of

**Box 3.**

A mapping $\theta$ from a group $G$ to a group $H$ which preserves their respective group multiplications is called a *homomorphism*. In other words, $\theta(xy) = \theta(x)\,\theta(y)$ where the two sides of this equation involve products in the two groups.

integers is an infinite cyclic group. As it is the only infinite cyclic group upto isomorphism (why?), one calls it *the* infinite cyclic group. Similarly, for each positive integer $n$, the unique cyclic group with $n$ elements is the group of integers modulo $n$. If a finite, abelian group has at most $n$ elements $g$ such that $g^n = e$ for every $n$, then it is cyclic.

*Exercise. Prove the same without assuming that the group is abelian.*

**Box 4.**

A *subgroup* $H$ of a group $G$ is a subset which is a group in its own right under the multiplication law of $G$. One can define an equivalence relation on $G$ given by $a \sim b$ if $ab^{-1} \in H$. The equivalence classes are called *right cosets*.

Given a subgroup $H$ the right coset (see *Box* 4) corresponding to an element $a$ of $G$ is denoted by $Ha$; it consists of the subset $\{ha : h \in H\}$. As the different right cosets are disjoint and each right coset has exactly as many elements as are in $H$ if $G$ is finite, its order is a multiple (called the index of $H$ in $G$) of the order of $H$; this is known as *Lagrange's theorem*. One defines left cosets analogously and, in general, right cosets may not be left cosets. We shall soon see the role played by normal subgroups (see *Box* 5) in Galois theory. If $G$ is abelian, evidently all subgroups are normal.

Some examples of normal subgroups of nonabelian groups are:

(i) the alternating group $A_n$ of even permutations in $S_n$,

(ii) the special linear group $SL_n$ consisting of $n \times n$ matrices over rationals, reals or complex numbers with determinant 1 and

(iii) the subgroup $U$ of the group $B$ of upper triangular invertible rational, real or complex matrices which consists of $1's$ on the diagonal.

**Box 5.**

It was Galois who recognised the importance of the concept of a subgroup for which left and right cosets are the same. Such a subgroup $H$ is said to be distinguished or *normal* in $G$.

Given a normal subgroup $N$ of a group $G$, the cosets again form a group called the quotient group and denoted by $G/N$. The multiplication here is $(xN)(yN) = xyN$ The group of integers modulo $n$ is just the quotient group of $\mathbf{Z}$ by the subgroup $n\mathbf{Z}$ consisting of all integral multiples of $n$. The torsion subgroup of the circle group is the quotient group $\mathbf{Q}/\mathbf{Z}$.

If $\theta : G \to H$ is a homomorphism, the *kernel* of $\theta$ (the elements mapping to the identity) is a normal subgroup $\mathrm{Ker}(\theta)$ of $G$. Moreover, it is very easy to see that the quotient group $G/\mathrm{Ker}(\theta)$ is isomorphic to the image $\theta(G)$.

(*Ex. What is the isomorphism implicit here?*).

We can now get on to the concept of rings. In our discussion of Galois theory, ring theory plays only a minor role and we shall move on to fields after a very brief interlude with rings. The reader interested in a more detailed study of rings may refer to [2]. For us, all rings (see *Box* 6) are commutative with identity. Conventionally, one writes $ab$ instead of $a.b$ and writes 0 for the additive identity.

**Box 6.**

A commutative *ring* with unity 1 is a set $R$ with two operations + and . (called addition and multiplication) such that $R$ is an abelian group under addition, closed under multiplication and satisfies $a\,.\,1 = a, a\,.\,b = b\,.\,a$, $a\,.\,(b\,.\,c) = (a\,.\,b)\,.\,c$, $a\,.\,(b + c) = a\,.\,b + a\,.\,c$.

The principal examples of rings relevant to us are:

(i) $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ under the usual addition and multiplication of complex numbers. More generally, consider the *subring* generated by a subset $S$ of $\mathbf{C}$; this consists of all finite sums of finite products of elements of $S$.

For instance, for an integer $d$, the sets $\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}$ and $\mathbf{Z}[e^{2i\pi/d}] = \{\sum_{r=1}^{d} a_r e^{2i\pi r/d} : a_r \in \mathbf{Z}\}$ are rings.

(ii) The set $R[X_1, X_2, \cdots, X_n]$ of all polynomials in $n$ variables $X_i$ over any ring $R$ is again a ring, called a polynomial ring over $R$.

**Box 7.**

An *ideal* $I$ in a ring $R$ is a subset which is a subgroup of the additive group of $R$ and satisfies $rs \in I$ for all $r \in R$, $s \in I$. Obviously, $R$ itself is an ideal and is called the unit ideal. The singleton consisting of 0 is called the trivial ideal. Given any ring homomorphism from a ring $R$ to a ring $S$, the kernel $\mathrm{Ker}(\theta) = \{r \in R: \theta(r) = 0\}$ is an ideal of $R$. The image $\theta(R)$ is a subring of $S$.

The notions of a subring, a ring homomorphism and ring isomorphism are defined in the obvious manner. The ring-theoretic concept corresponding to normal subgroups is that of ideals (see *Box* 7). The integral multiples of $n$ form an ideal in the ring $\mathbf{Z}$ It is also the kernel of the ring homomorphism from $\mathbf{Z}$ to the ring of integers modulo $n$. Other examples of ideals are given by looking more generally at the ideal generated by a subset $\Omega$ of a ring $R$; such an ideal consists of finite linear combinations $\sum r_i w_i$ with $r_i \in R, w_i \in \Omega$. This ideal is denoted by $\langle\Omega\rangle$. If $\Omega$ consists of just one element, the ideal $\langle\Omega\rangle$ is said to be *principal*. For instance, every ideal of $\mathbf{Z}$ is principal. So is the case with the polynomial ring $\mathbf{Q}[X]$ as can be seen using the division algorithm –

**Box 8.**

An ideal $I$ of $R$ is *prime* if $ab \in I \Rightarrow$ either $a$ or $b$ is in $I$. An ideal $I$ of $R$ is *maximal* if there is no ideal $J \neq I, R$ such that $I \subseteq J$. An *integral domain* is a ring in which the trivial ideal 0 is a prime ideal i.e., $ab = 0 \Leftrightarrow$ either $a$ or $b$ is zero. A *principal ideal domain* – PID for short – is an integral domain in which all ideals are principal.

any polynomial of least degree in an ideal generates it. The ideal $\langle p \rangle$ of $\mathbf{Z}$ generated by a prime number is a prime ideal as well as a maximal ideal and $\mathbf{Z}$ is an integral domain. The rings $\mathbf{Z}, \mathbf{Q}[X], \mathbf{R}[X]$ and $\mathbf{C}[X]$ are PID's (see *Box* 8).

As we did with normal subgroups, we can define for any ideal $I$ in a ring $R$, an equivalence relation on $R : a \sim b$ if $a - b \in I$. The equivalence classes form a ring called the quotient ring, denoted as $R/I$. One writes $a + I$ for the class corresponding to $a \in R$.

If $\theta : R \rightarrow S$ is a ring homomorphism, then the rings $R/\mathrm{Ker}(\theta)$ and $\theta(R)$ are naturally isomorphic.

*Easy exercises: (i) An ideal $I$ of a ring $R$ is prime if, and only if, $R/I$ is an integral domain; (ii) An ideal $I$ of a ring $R$ is maximal if, and only if, $R/I$ is a field.*

We have used the word *field*; this is nothing but a ring $R$ in which all non-zero elements have multiplicative inverses.

The premier examples of fields are $\mathbf{Q}, \mathbf{R}, \mathbf{C}$; here are more examples.

(i) The smallest field containing a subset $\Omega$ of $\mathbf{C}$ (i.e., the subfield generated by $\Omega$) consists of all the complex numbers $\sum a_i x_i / \sum b_j y_j$ where both are finite sums, $a_i, b_i \in \mathbf{Q}, x_i, y_i \in \Omega$ and $\sum b_j y_j \neq 0$.

**Box 9.**

Fields for which the set $\{n \, . \, 1 : n \in N\}$ is a finite set are said to have *finite characteristic* and the characteristic is defined to be the cardinality of this set. The characteristic has to be a prime number (*Why*?). The other type of fields are said to have *characteristic* 0.

For instance, if $\Omega = \{\sqrt{m}\}$ for some integer $m$, the corresponding field $\mathbf{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbf{Q}\}$.

(ii) The field $K(X_1, \quad , X_n)$ of rational functions $f/g$, $f, g \in K[X_1, \cdot \quad , X_n], g \neq 0$ is a field for any field $K$.

(iii) The set of integers modulo $p$ is a field if $p$ is prime. To stress that one is talking about the field rather than just the additive group, one writes $\mathbf{F}_p$.

In contrast to the number fields (i.e., subfields of $\mathbf{C}$) the last example is different as the set $\{n.1 : n \in \mathbf{N}\}$ is a finite set (of $p$ elements).

The notions of subfields, field homomorphisms and field isomorphisms are once again obviously defined.

*Exercises:*

*(i) Show that a field has characteristic (*see *Box* 9*) $p \neq 0$ (respectively* 0*) if, and only if, $K$ has a subfield isomorphic to $\mathbf{F}_p$ (respectively $\mathbf{Q}$).*

*(ii) For any field $K$, the polynomial ring $K[X_1, \quad \cdot, X_n]$ is a PID if, and only if, $n = 1$.*

**Box 10**

A *field extension* is simply an inclusion of fields $K \subseteq L$ – one writes $L/K$. This is not a quotient of $L$ – a field has no nontrivial ideals! $L$ can then be regarded as a vector space over $K$ and one calls its dimension the *degree* $[L:K]$. If the degree is finite, $L$ is said to be a *finite extension* of $K$.

## Field Extensions and Galois Theory

Let us stop for a moment to review the theory of equations in terms of field theory. One is given a polynomial $f(X)$ in one variable; this may have for its coefficients, numbers like rational numbers or variables like polynomials in some other variables. At any rate, the coefficients are supposed to be known quantities from a given base field. It was tacitly assumed in the days of Galois that there was a bigger field in which the given polynomial $f$ had all its *roots* i.e., $f$ when thought of as a polynomial over the bigger field could be factored into linear polynomials. For polynomials over number fields, this was justified by a rigorous proof due to Gauss of the fundamental theorem of algebra. Be that as it may, the mathematicians of those times assumed the existence of a unique smallest field where $f$ had all its roots and went on to study that field in relation to the base field with a view to expressing the roots of $f$ in terms of the base field. Without further ado, let us consider this as sufficient motivation to study field extensions (see *Box* 10). If $K \subseteq L \subseteq M$ are finite extensions, then for any $K$-basis $\{v_1, \quad \cdot, v_m\}$ of $L$ and $L$-basis $\{w_1, \quad, w_n\}$ of $M$ it is straightforward to check that $\{v_i w_j\}$ is a $K$-basis of $M$. Thus, the very first observation is that *in a chain of finite extensions, the degree multiplies.*

In Galois theory, one studies algebraic elements and algebraic extensions (see *Box* 11) – possibly of infinite degree. For any rational number $d$, the two complex square roots of $d$ are examples of algebraic elements of the field extension $\mathbf{C}/\mathbf{Q}$. The well-known constants $e, \pi$ are not algebraic over $\mathbf{Q}$.

**Box 11**

Given a field extension $L/K$, an element $a$ of $L$ is *algebraic over $K$* if there is a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. An *algebraic extension* is one in which all the elements are algebraic.

Another set of examples is provided by any *finite* extension $L/K$. If $t \in L$, look at the set $\{t^i : i \geq 0\}$. If it is a finite set, either $t = 0$ or $t^n = 1$ for some $n$. In either case, $t$ is evidently algebraic over $K$ If it is an infinite set, it has to be linearly dependent in view of the finiteness of $[L : K]$. Thus, once again there is a non-zero polynomial over $K$ which vanishes at $t$. We have proved therefore that: *any finite extension $L/K$ is algebraic.*

Look at an element $t$ of a field extension $L/K$. The smallest subfield $K(t)$ of $L$ containing $K$ and $t$ consists of the fractions $f(t)/g(t)$ for $f, g \in K[X]$ with $g(t) \neq 0$ (Why?). We have the somewhat surprising fact that if $t$ is algebraic, the denominators are not needed!

**Lemma.**

*If $L/K$ is a field extension, then an element $t$ of $L$ is algebraic over $K$ if, and only if, $K(t) = K[t] := \{g(t) : g \in K[X]\}$. Equivalently, the degree $[K(t) : K]$ is finite.*

**Proof.** Consider, for any $t \in L$, the ring $K[t]$ and the ring homomorphism $\phi : K[X] \to K[t]$ defined as $g \mapsto g(t)$. This maps onto $K[t]$. Therefore, the rings $K[X]/\mathrm{Ker}(\phi)$ and $K[t]$ are isomorphic. As $K[t] \subseteq L$, it is an integral domain; hence $\mathrm{Ker}(\phi)$ is a prime ideal of $K[X]$. In other words, $\mathrm{Ker}(\phi)$ is either the zero ideal or the ideal generated by a single polynomial $f$ in $K[X]$. Now, by the very definition, $t$ is algebraic if, and only if, $\mathrm{Ker}(\phi) \neq 0$. But $\langle f \rangle$ is a non-zero prime ideal in $K[X]$ if, and only if, $f$ is irreducible; and this is equivalent to the fact that the ideal $\langle f \rangle$ is a maximal ideal (Why?). Thus, $t$ is algebraic if, and only if, $K[t]$ is a field (i.e., $K[t] = K(t)$). This proves the first equivalence stated. Now, we already know that if $[K(t) : K]$ is finite, then $t$ is algebraic over $K$. Conversely, if $t$ is algebraic over $K$, we have $f(t) = 0$ for some non-zero $f \in K[X]$. The division algorithm produces such an $f$ with the smallest possible degree. Dividing out by the top coefficient, one may take $f$ to be the unique monic polynomial of smallest degree with $f(t) = 0$; one calls $f$ the minimal polynomial of $t$. If $f = a_0 + a_1X + \quad + X^n$, then $\{1, t, \cdot \quad , t^{n-1}\}$ is easily seen (by using again the division algorithm) to be a basis of $K(t)$ over $K$ Thus, $[K(t) : K] = n = \deg(f)$. This completes the proof and allows us the following useful consequence:

**Corollary.**

*Given a field extension $L/K$, the elements of $L$ which are algebraic over $K$ form a subfield.*

**Proof.** If $s, t \in L$ are algebraic over $K$, we need to know that $s+t, s-t, st, st^{-1}$ (if $t \neq 0$) are also algebraic. But, all these elements are in the subfield $K(s,t)$ generated by $s, t$ in $L$. As, obviously $K(s,t) = K(s)(t)$, one calculates the degree $[K(s,t) : K] = [K(s)(t) : K] = [K(s)(t) : K(s)][K(s) : K]$ which is finite. Thus, $K(s,t)$ is algebraic over $K$ by the first observation we made.

We have now got to a point where we can justify the assumption that *for any field $K$ and any $0 \neq f \in K[X]$, there is an extension field $L/K$ such that $f = s\prod_i(X - t_i)$ with $s, t_i \in L$.*

To do this, one first needs to observe: *Given $K, f$ as above, there is an extension $K_0$ in which $f$ has a root.* Why is this so? One may assume that $f$ is irreducible in $K[X]$. But, then the ideal $\langle f \rangle$ is maximal in $K[X]$ and taking $K_0$ to be the quotient $K[X]/\langle f \rangle$, one trivially has $f(t) = 0$ where $t$ is the image $X + \langle f \rangle$ of $X$ in $K_0$. Using this observation along with the remainder theorem and induction on the degree, one can construct an extension $L$ which justifies the assumption quoted above. Moreover, any such extension $L$ of $K$ contains a smallest one called a *splitting field* of $f$. From our natural construction of $L$, it is again a simple argument using induction to show that *any two splitting fields of $f$ are isomorphic by a $K$-isomorphism i.e., an isomorphism which is the identity on $K$*

*Example.* A splitting field of $X^n - 2 \in \mathbf{Q}[X]$ is the field $\mathbf{Q}(2^{1/n}, e^{2i\pi/n}) \subseteq \mathbf{C}$ where $2^{1/n}$ denotes a real root of this polynomial.

An important discovery by Galois was the determination of the finite fields – these are now called Galois fields. As a finite field $F$ has some prime $p$ as its characteristic, it contains a subfield isomorphic to the field $\mathbf{F}_p$ viz., the subfield $\{n.1 : n \in \mathbf{N}\}$. If it has degree $n$ over $\mathbf{F}_p$, then $F$ has exactly $p^n$ elements! What is more, it turns out that *$F$ is just the splitting field of the polynomial $X^{p^n} - X \in \mathbf{F}_p[X]$*; hence *there is only one finite field (upto isomorphism) of a given cardinality.* Moreover, the non-zero elements $F^*$ in $F$ have the property that there are at the most $r$ satisfying $x^r = 1$ for any $r$. By the group-theoretic fact noted earlier, *$F^*$ is a cyclic group.* Thus, $F = \mathbf{F}_p(t)$ for any generator $t$ of $F^*$.

**Box 12.**

An *algebraic closure* of $K$ is an algebraic extension in which the only irreducible polynomials are the linear ones. Any isomorphism from a field $K$ to a field $L$ extends to an isomorphism from any algebraic closure of $K$ to an algebraic closure of $L$.

Given any field $K$, we have produced a splitting field for any polynomial in $K[X]$. However, it is still unclear whether one could get a single splitting field for all the polynomials in $K[X]$. This involves certain set-theoretic difficulties which can be surmounted using the axiom of choice. One thereby gets an *algebraic closure* $\overline{K}$ of $K$. Putting together what we did for two splitting fields of a given polynomial, one shows that $\overline{K}$ is unique upto isomorphisms (see *Box* 12). One defines the group $G(\overline{K}/K)$ of all $K$-isomorphisms of $\overline{K}$ to itself. This group evidently permutes the roots of any given polynomial $f \in K[X]$. It is a simple exercise to show that $a, b \in \overline{K}$ have the same minimal polynomial over $K$ if, and only if, $b = \sigma(a)$ for some $\sigma \in G(\overline{K}/K)$. In other words, *the number of distinct roots of the minimal polynomial of any $a \in \overline{K}$ is the index of the subgroup $G(\overline{K}/K(a))$ in $G(\overline{K}/K)$.* Note that *an extension $L/K$ is normal (*see *Box* 13*) if, and only if, the subgroup $G(\overline{K}/L)$ is a normal subgroup of $G(\overline{K}/K)$.*

**Box 13.**

An algebraic extension $L/K$ is said to be *normal* over $K$ if every element $\sigma$ of $G(K/K)$ maps $L$ into itself. Consequently, a finite normal extension is the splitting field of a polynomial and conversely.

At this point, an important possibility needs to be pointed out. Even though a polynomial $f \in K[X]$ may be irreducible, it could have multiple roots in a splitting field $L$; it could even be of the form $(X - t)^m$ in $L[X]$. One calls an irreducible $f \in K[X]$ *separable over $K$* if all the roots of $f$ in the splitting field are distinct. *This is always so if* char$(K) = 0$ (why?); if char$(K) = p > 0$, $f$ is not separable over $K$ if, and only if, $f = g(X^p)$ for some $g \in K[X]$. One then defines the separability of an element of $\overline{K}$ over $K$ in terms of the separability of its minimal polynomial over $K$.

Thus, $t \in \overline{K}$ *is separable over* $K$ *if, and only if, there are exactly* $[K(t) : K]$ *distinct* $K$*-homomorphisms from* $K(t)$ *to* $\overline{K}$.

Perhaps, the first important result of the theory is Galois's beautiful:

### Theorem of the Primitive Element

*A finite, separable extension* $L/K$ *is primitive i.e.,* $L = K(t)$ *for some* $t \in L$.

Galois's proof is the one given even today in all textbooks.

**Proof.** We already noted that an extension of finite fields is primitive. Let us therefore assume that $K$ is infinite and let $[L : K] = n$; by separability, there are distinct $K$-homomorphisms $\sigma_1, \quad ,\sigma_n$ from $L$ to $\overline{K}$. The finitely many proper $K$-vector subspaces $\mathrm{Ker}(\sigma_i - \sigma_j); i \neq j$ of $L$ cannot cover the whole of $L$ (Why?). If $t \in L$ is not in any of these subspaces, $\sigma_i(t); i \leq n$ are at least $n$ different roots of the minimal polynomial of $t$ over $K$. This means that $[K(t) : K] \geq n = [L : K]$; hence $L = K(t)$.

Galois realised that the notions of separability and normality are the only relevant ones needed to study polynomials over any field. One defines a finite extension $L/K$ to be *a Galois extension* if it is both separable and normal. In this case, the finite group $G(L/K)$ is called the Galois group of the extension. In this set-up, it is not hard to prove the so-called fundamental theorem of Galois theory (see *Box* 14). The crucial fact that needs to be verified is that $K = L^{G(L/K)} := \{x \in L : g(x) = x \ \forall \ g \in G(L/K)\}$ i.e., *the Galois group* $G(L/K)$ *fixes* $K$ *and no more.* One also defines the Galois group of a separable polynomial $f \in K[X]$ to be that of the Galois extension defined by the splitting field.

**Box 14.**

**The fundamental theorem of Galois theory asserts that given a finite Galois extension $L/K$, the correspondences $E \mapsto G(L/E)$ and $H \mapsto L^H$ between the intermediate fields $K \subseteq E \subseteq L$ and the subgroups $H$ of $G(L/K)$ are inverses of each other. Further, $E$ is a normal extension of $K$ if, and only if, $G(L/E)$ is a normal subgroup of $G(L/K)$. In this case the corresponding quotient group can be identified with the Galois group of $E$ over $K$.**

Galois discusses two examples of the Galois group of a polynomial.

The first one is the Galois extension $K(X_1, \quad ,X_n)$ over $K(s_1, \quad ,s_n)$ where $s_i$ are the elementary symmetric polynomials in the variables $X_i$. The extension here is just the splitting field of the polynomial $\prod_{i=1}^{n}(X-X_i) \in K(s_1, \cdot \quad , s_n)$ $[X]$. He proves that the corresponding Galois group is the full symmetric group $S_n$.

The other example he discusses is that of the polynomial $X^p - 1 \in \mathbf{Q}[X]$ for some prime $p$. In this case, he shows that the Galois group is the cyclic group of order $p-1$.

## In Conclusion

In summary, what are the applications of Galois theory? The fundamental theorem of algebra is a simple consequence of Galois's theory. The ancient geometric problems alluded to earlier are also easily solved using this theory. However, the most spectacular application is to the solvability of polynomials by radicals, the original motivation due to which the theory was developed in the first place.

*The solvability of a separable polynomial $f$ by radicals amounts to getting a tower of fields $K = K_0 \subseteq K_1 \quad \subseteq K_m = L$ where $L$ is the splitting field of $f$ and each $K_{i+1} = K_i(t_i)$ for some $t_i^{m_i} \in K_i$ with the added proviso that the characteristic of $K$ does not divide $m_i$. In terms of Galois groups, this is equivalent to the Galois group of $f$ being a solvable group as defined earlier. As the symmetric group $S_n$ is not solvable for $n \geq 5$, Galois's discussion of the first example above shows immediately the impossibility of getting a formula for a general equation of degree at least* 5.

Abel died at 26, Eisenstein at 28 and Galois at 20. But, the work of these young giants is so fundamental as to remain relevant perhaps for ever. It might be apt to end our discussion with the anagram **GREAT IS SO ALIVE** !

*Address for Correspondence*
B Sury
Indian Statistical Institute
Bangalore 560 059, India.

## Suggested Reading

[1] **Shashidhar Jagadeesan, Whoever said Nothing is Impossible?, *Resonance*, Vol.4, No.3, p.25, 1999.**

[2] **V Pati, Hilbert's Nullstellensatz and the Beginning of Algebraic Geometry. *Resonance*, Vol.4, No.8, p.36, 1999.**