# Galois, Abel and Jacobi: The development of Group Theory

# Mathematical tragic heroes

- We now enter into a recurrent theme of tragic heroes in mathematics.
- Evariste Galois (1811-1832,) Niels Henrik Abel (1802-1829), and Carl Gustav Jacobi (1804-1851) each did not live very long.
- Galois died in a pistol duel at the age of 20, Abel of tuberculosis at the age of 26 and Jacobi at 46 from smallpox.
- Of these three deaths, certainly Galois's is the most ludicrous seemingly over a love affair or perhaps more accurately, it was political since Galois was somewhat of a political firebrand during the reign of Charles X.
- Having an intuition about his own demise, he wrote a long letter to a friend outlining his mathematical theory, what is now called Galois theory, on the night before his death.

# What is a group?

- To Galois's credit, we must attribute to him the discovery of the concept of a group.
- By the age of 15, he had mastered the works of Legendre and Lagrange.
- He isolated for study permutation groups and remarked that the roots of a polynomial equation are intimately connected with the group that he associated with that polynomial, now called the Galois group of the polynomial.
- So what is a group? It is a set G together with a binary operation denoted by the symbol x such that four axioms are satisfied: (1) for a,b in G, a x b lies in G (closure); (2) for all a,b,c in G, we have a x (b x c) = (a x b) x c (associative property); (3) there is an element e in G (called the identity) such that a x e = e x a = a; (4) for any a in G, there is an element called the inverse and denoted as $a^{-1}$ such that a x $a^{-1}$ = $a^{-1}$ x a = e (existence of inverses). Such a pair (G,x) is called a group.
- Often, we drop the "times" notation x and simply write ab instead of a xb.
- If ab=ba, for all a,b in G, we say the group is an abelian group, named after Niels Henrik Abel who first studied them. Another name for this is a commutative group.

# Examples of groups

- You are of course familiar with groups already and may not know it.
- The set of integers with the operation of addition is an abelian group.
- So is the set of rational numbers as well as the set of real numbers with addition.
- The non-zero rational numbers and non-zero real numbers form an abelian group under multiplication.
- The set of all 2 x 2 matrices with real number entries having non-zero determinant is an example of a non-abelian group, as you can easily verify because matrix multiplication is not commutative.
- The set integers (mod m) is an abelian group under addition, for any natural number m. The set of coprime residue classes under multiplication is another example of an abelian group.
- An important class of groups which some of you may have seen are the permutation groups and we give a brief introduction to these.

# Subgroups and normal subgroups

- What emerges from the work of Galois is the psychology of abstraction, which is an important tool of mathematics.
- Once the concept of a group has been identified as permeating all of nature, then the concept of a subgroup is evident.
- If G is a group, then a subset H of G is called a subgroup if H also satisfies the group axioms. In particular, H is closed under the group operation as well as the map $x \rightarrow x^{-1}$.
- We say a subgroup H is a normal subgroup if $xHx^{-1} = H$ for all x in G.
- A group G always has two normal subgroups namely the trivial group consisting of the identity element and the group itself.
- A group G is called simple if these are the only two normal subgroups of G. This is analogous to the notion of a prime number.

# The concept of a field

- Cognate with the concept of a group is the concept of a field.
- A field F is a set with two operations sometimes denoted + and x such that the pair (F,+) is an abelian group with identity element denoted 0, and (F*,x) an abelian group where F* is the set of non-zero elements of F so that the distributive law is satisfied with these two operations: $a \times (b+c) = a \times b + a \times c$.
- Often, we suppress the multiplication symbol and simply write ab for $a \times b$.
- You are already familiar with examples of fields, such as the field of rational numbers, the field of real numbers and the field of complex numbers.
- If F is a field containing the rational numbers Q, we can talk about the Galois group of F over Q as the set of all bijections $\sigma: F \to F$ such that $\sigma(a+b)=\sigma(a)+\sigma(b)$ and $\sigma(ab)=\sigma(a)\sigma(b)$, and $\sigma(x)=x$ for all rational numbers x.

# Permutation groups

- Given any set X, the set of all bijections $f:X \to X$ forms a group under composition. This group is denoted Sym(X).
- If X is a finite set of n elements, say 1, 2, …, n, then this group is really the group of permutations of X and is denoted $S_n$ and called the symmetric group on n letters.
- Thus, $S_n$ is a group with n! elements since there are n! permutations of the set 1, 2, …, n.
- Given a polynomial f(x) with integer coefficients having degree n, we know by the fundamental theorem of algebra that it has n complex roots.
- Let F be the smallest subfield of the complex numbers containing all the roots of the polynomial of f.
- The Galois group of the polynomial f is the Galois group of the field F. That is, it is the set of automorphisms $\sigma:F \to F$ fixing Q.

# Galois theory

- Here are the main ideas of Galois theory.
- Give a polynomial f(x) with integer coefficients, let F be the smallest subfield of C which contains all the roots of f.
- The Galois group of F is called the Galois group G of the polynomial.
- Galois's main idea is that this group determines whether or not we can find a "formula" for the roots of f. Here is a more precise statement.
- Given a polynomial $f(x) = a_0 + a_1x + \ldots, + a_nx^n$ we say that there is a formula for the roots if they can be obtained from the coefficients and a finite number of applications of the operations of addition, subtraction, multiplication, division, multiplication by rationals and extraction of roots.
- This was the case for quadratic equations, and we saw in the work of Cardano and Fontana that this holds for cubics and quartics.
- Galois showed that such a formula exists if and only if F can be reached by a finite chain of field extensions of Q obtained by adjoining certain radicals to Q. This is the case if and only if the Galois group G has a chain of subgroups $G \supset G_1 \supset G_2 \ldots \supset G_r = 1$ with $|G_i| / |G_{i+1}|$ a prime each $G_{i+1}$ normal in $G_i$.

# Solvable groups

- If a group G has a chain of subgroups as described above, then we call G a solvable group.
- If we compute the Galois group of a quadratic polynomial, cubic polynomial, or quartic polynomial, then this group turns out to be a subgroup of $S_4$ which is solvable.
- If we have a polynomial of degree 5, generally, the Galois group turns out to be $S_5$ which is not a solvable group. Thus, there is no general formula for the quintic.
- This had been proved earlier by Abel but Abel gave no theoretical basis.

# Niels Henrik Abel

- Niels Henrik Abel was born in Norway and lived in poverty all his life. He died at the age of 26 and his life is another tragic story.
- His most notable contribution is the theorem that there is no formula involving radicals that can determine all the roots of a fifth degree equation or one of higher degree.
- The student will recall that for quadratic polynomials, we have the familiar method of determining the roots.
- For cubic and quartic polynomials, we discussed the Cardano-Fontana solution.
- Abel's theorem is that there is no such general formula for a polynomial of fifth degree and higher.

The underlying reason involves the fact that Galois group of a general fifth degree equation is the symmetric group on 5 letters which has order 5!=120 and is "unsolvable" as explained earlier.

# Group theory and Field theory

- We can see the work of Abel and Galois as solving the ancient problem of finding formulas for the roots of a polynomial, on the one hand, but on the other, it is really the emergence of a new theory that amplifies our understanding.
- It is again an instance of changing one problem into another problem. By this process, we don't solve the problem but understand when we can solve the problem and when we cannot.
- We get a theoretical foundational understanding.

# The ubiquity of group theory

- Nowadays, group theory is everywhere. You are familiar with matrix groups, and now with permutation groups.
- From Galois's work, we see that simple groups are the building blocks of all groups.
- A cyclic group of prime order is an example of a simple group.
- A famous structure theorem is that any finite abelian groups is a "product" cyclic groups. Thus all abelian groups are built out of cyclic groups.
- But until the 20th century, we did not have a complete classification of all the simple groups.
- This was the towering achievement of many mathematicians of the 20th century and we will definitely not go into details.
- The symmetric group contains a subgroup called the alternating group which is the subgroup of "even" permutations and these are all simple for $n \geq 5$.
- There are a few more families like this and some "sporadic" ones that come from a huge finite group called the "Monster" which has intimate connections to modular forms and number theory.

# The work of Jacobi

- Carl Gustav Jacobi (1804-1851) also did not have a long life, dying at the age of 46 from smallpox.
- By the age of 21, he obtained his PhD in mathematics and quickly secured a professorship at Konigsberg University.
- Jacobi worked in analysis and number theory. His major contributions here were extensions of works of Lagrange and Fermat.
- Fermat showed that a prime of the form 4k+1 can be written as a sum of two squares. Lagrange showed that any prime can be written as a sum of four squares.
- Jacobi found analytic formulas for the number of such representations, thus opening the door for the theory of modular forms which involves analysis and group theory.

# The Jacobian determinant

- Most of you are familiar with the Jacobian determinant in multivariable calculus. This is due to Jacobi who did extensive research on determinants.
- The Jacobian matrix is one of the ways of generalizing the notion of a derivative to functions of several variables.
- For a function $f:R^m \to R^n$ and a point p, the Jacobian matrix is defined as:

$$J_{\mathbf{p}}\mathbf{f} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_m} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_m} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_m} \end{pmatrix}$$

When we say $\mathbf{f} : \mathbb{R}^m \to \mathbb{R}^n$ is **differentiable** at $\mathbf{q}$ we mean that,

$$\lim_{\mathbf{x}\to\mathbf{q}} \frac{\|\mathbf{f}(\mathbf{x}) - \mathbf{f}(\mathbf{q}) - (J_{\mathbf{q}}\mathbf{f}) \cdot (\mathbf{x} - \mathbf{q})\|}{\|\mathbf{x} - \mathbf{q}\|} = 0$$

where

$$\|\mathbf{x} - \mathbf{q}\| = \sqrt{(x_1 - q_1)^2 + \ldots + (x_m - q_m)^2}.$$

# The length of a curve

- A curve is a map from an interval [a,b] into m-dimensional space. One can write down a formula for the length of the curve. More precisely,

If $I$ is an interval $[a, b]$ in $\mathbb{R}$, and $X : I \to \mathbb{R}^m$ is a curve, with component functions $x_1(t), ..., x_m(t)$ which are differentiable, it is convenient to visualise the domain as a time parameter and the curve being traced out in $m$-dimensional space as $t$ moves from $a$ to $b$. By the usual Pythagorean theorem and the familiar limit process, the **length** of the curve traced out in time $t$ is

$$s(t) := \int_a^t \sqrt{x_1'(u)^2 + \cdots + x_m'(u)^2}\, du.$$

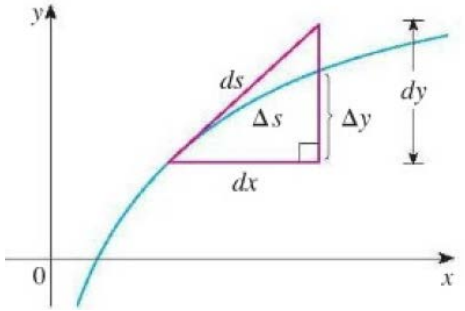
Abel and Jacobi noticed that the calculation of the length of an ellipse leads to new integrals which cannot be expressed in terms of elementary functions. This way the discovered elliptic integrals.

# The perimeter of an ellipse

- In an earlier lecture, we discussed the area of an ellipse with major axis a and minor axis b and found it to be πab.
- There is no simple formula for the perimeter of an ellipse. Both Abel and Jacobi realized that the formula leads to a new theory of elliptic integrals.
- Indeed, let us do this computation. We will write the formula for the previous slide slightly differently and it may be familiar from your first year calculus.

If $f$ is continuous and differentiable on the interval $[a, b]$ and $f'$ is also continuous on the interval $[a, b]$. We have a formula for the length of a curve $y = f(x)$ on an interval $[a, b]$.

$$L = \int_a^b \sqrt{1 + [f'(x)]^2}\,dx \quad \text{or} \quad L = \int_a^b \sqrt{1 + \left[\frac{dy}{dx}\right]^2}\,dx$$




$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \Rightarrow y = \pm\frac{b}{a}\sqrt{a^2 - x^2}$$

By applying the formula of the arc length of a function, we get:

$$L = 4\int_0^a \sqrt{1 + \frac{b^2x^2}{a^2(a^2 - x^2)}}\,dx = 4\int_0^a \sqrt{\frac{a^4 + (b^2 - a^2)x^2}{a^2(a^2 - x^2)}}\,dx$$

$$L = \pi(a+b)\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}^2 h^n \qquad \text{where} \qquad h = \frac{(a-b)^2}{(a+b)^2}$$