Galois Group and the Solvability of Polynomials

Shabab Ahmed and David Krumm

Department of Mathematics and Statistics, Colby College

September 24, 2018

Overview

Solvability

- We will say that a polynomial, f, is solvable if the solution of the equation $f(x) = 0$ is possible using arithmetic operations and taking square roots, cube roots, etc.
- **Examples:** Quadratic, cubic and quartic polynomials are solvable.

Quadratic Polynomials

- There exists a general for solving the quadratic polynomials, hence, showing that all such polynomials are solvable.
- Notice: the formula uses the coefficients of the polynomial, arithmetic operations and radicals
- Solved first around 300 BC by Euclid using geometric methods and then by Diophantus using more algebraic methods
- Similarly, there exist general formulas for finding the roots of cubic and quartic polynomials which were found around the 1500s

Questions

Question 1:

Are quintic polynomials solvable?

Answer 1:

Nope! We can find a quintic polynomial that is not solvable! (Abel-Ruffini)

Example:

$f(x) = x^5 - 4x + 2$

Questions

Question 2:

What kind of polynomials are solvable? More precisely, can we come up with a method to figure out which polynomials are solvable?

Answer 2:

Galois' algorithm!

Splitting Field

- A field is a set equipped with two operations where certain properties hold (Associativity, Commutativity, Distributivity etc)
- Fields can be seen as algebraic structures with the four arithmetic operations associated with the real numbers
- We can think of polynomials having coefficients in any field. For example, $f(x) = x^2 + 1$ has coefficients in $\mathbb{R}$
- However, the roots of the polynomial might not be in the coefficient field. $f(x) = x^2 + 1$ does not have real roots
- **Splitting field** is an extension of the coefficient field which contains all the roots of the polynomial. So, the polynomial f can be split into its linear factors in the splitting field.
- For example, the splitting field for $f(x) = x^2 + 1$ is $\mathbb{C}$

Theorem

Theorem (Kronecker)

Let $f(x) \in F[x]$, where F is a field. There exists a field E containing F over which $f(x)$ splits.

Galois Theory

- Galois came up with an algorithm to figure out whether a polynomial is solvable or not
- Sometimes problems in group theory are easier to understand and solve than problems in field theory
- Galois realized this connection between field theory and group theory and came up with the idea of associating a group with every polynomial (Galois Groups)
- Uses permutation groups to explain how the roots of a polynomial are related to each other

Solvability of groups

Solvable group

A solvable group is a group which has a normal series such that each normal factor is Abelian. We say that G is a solvable group if there exists a series of subgroups $\mathbb{1} \triangleleft H_1 \triangleleft H_2 \triangleleft ... \triangleleft H_k = G$ and each $H_i + 1/H_i$ is abelian for $i = 1, 2..., k - 1$.

Example:

$\mathbb{1} \triangleleft \mathbb{Z}_2 \triangleleft \mathbb{Z}_4 \triangleleft \mathbb{Z}_{12}$

Important Results

- Every finite group of order < 60 is solvable
- Every Abelian group is solvable
- Every subgroup of a solvable group is solvable
- The symmetric group, S_n is not solvable for $n \geq 5$

Galois Groups

- If $f(x) \in F[x]$ has n distinct roots in its splitting field E, then the Galois group of f is isomorphic to a subgroup of the symmetric group S_n.
- So we can think of Galois groups as some sort of permutation group of the roots of the polynomial
- Galois proved that a polynomial f is solvable if and only if the associacted Galois group is solvable

Galois' construction

- Galois came up with an algorithm to compute the Galois group of a given polynomial
- His construction basically creates the splitting field of the polynomial
- This has largely been ignored probably due to the fact that Galois stated the construction as a lemma in his memoir and made an assumption of the existence of such a splitting field
- Requires a factorization algorithm (Kronecker) and an algorithm to convert symmetric polynomials to functions of elementary symmetric polynomials (Gauss)

Algorithm

- Let a, b and c be the roots of $f(x)$ and let A, B and C be randomly chosen integers
- Let $V = Aa + Bb + Cc$ be a quantity in the splitting field
- Let $V_\sigma = A\sigma(a) + B\sigma(b) + C\sigma(c)$ where σ ranges through all the possible permutations of a, b and c
- Let $F(x,a) = \prod(x - V_\sigma)$ for σ that keeps a fixed and define $F(x,b)$ and $F(x,c)$ be defined similarly
- Construct $G(x) = F(x,a)F(x,b)F(x,c)T$ and let V be the root of $G(x)$
- Use the factorization algorithm to find a irreducible factor of $G(x)$ say $\tau(x)$
- $K[x]/\tau(x)$ gives us a splitting field for f and for G

- The field constructed is $K(V)$, that is, K adjoined with V
- Express a, b and c in terms of V and consider the other roots of G which would also be in terms of V
- View a, b and c as functions of V and plug in the other roots to see how a, b and c are permuted
- These permutations form the Galois group

Worked Out Example:

Example:

Let $A = 1, B = -1, C = 0$. Thus, $V = ab$:

- $F(x, a) = (x - a + b) * (x - a + c) = x^2 - 3ax + 3a^2$
- $G(x) = x^6 + 108$
- $\tau(x) = x^6 + 108$
- $a = (18V - V^4)/36$, $b = (-18V - V^4)/36$, $c = v^4/18$
- Galois group: S_3
- Computation time: 163 milliseconds