Fields and Galois Theory

George Voutsadakis[1]

[1] Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Groups and Equations
   - Solvability of Galois Group and Solvability by Radicals
   - Insolvable Quintics
   - General Polynomials

Subsection 1

Solvability of Galois Group and Solvability by Radicals

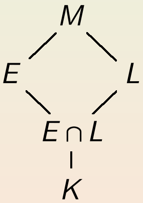
Solvability of Galois Group and Solvability by Radicals

Theorem

Let K be a field of characteristic zero. Let f be a polynomial in $K[X]$ whose Galois group $\mathrm{Gal}(f)$ is solvable. Then f is solvable by radicals.

- Let L be a splitting field of f over K. We are supposing that $\mathrm{Gal}(L:K)$ is solvable. Suppose also that $|\mathrm{Gal}(L:K)| = m$.

  If K does not contain an m-th root of unity, we can adjoin one. Let E be the splitting field over K of the polynomial $X^m - 1$. Now let M be a splitting field for f over E. By a previous theorem, we may regard M as an extension of L, and $\mathrm{Gal}(M:E) \cong \mathrm{Gal}(L:E\cap L)$.



  Now $\mathrm{Gal}(L:E\cap L)$ is a subgroup of the soluble group $\mathrm{Gal}(L:K)$. So, by a previous theorem, $G = \mathrm{Gal}(M:E)$ is soluble.

Solubility of Galois and Solubility by Radicals (Cont'd)

- $G = \mathrm{Gal}(M:E)$ is soluble. Thus there exist subgroups

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G,$$

such that G_{i+1}/G_i is cyclic for $0 \le i \le r-1$. By the Fundamental Theorem, there is a corresponding sequence of subfields of M

$$E = M_r \subseteq M_{r-1} \subseteq \cdots \subseteq M_0 = M,$$

such that $\mathrm{Gal}(M:M_i) = G_i$, and $\mathrm{Gal}(M_i:M_{i+1}) \cong G_{i+1}/G_i$.
Thus M_i is a cyclic extension of M_{i+1}.
Let $[M_i:M_{i+1}] = d_i, i = 0,1,\ldots,r$. Then $d_i \mid [M:E] = |\mathrm{Gal}(M:E)|$.
Also $|\mathrm{Gal}(M:E)| = |\mathrm{Gal}(L:E\cap L)| \mid |\mathrm{Gal}(L:K)| = m$.
Since M_{i+1} contains E, it contains every m-th root ω of unity.
So certainly contains all d_i-th roots of unity, these being powers of ω.
Hence, by a theorem, there exists β_i in M_i, such that $M_i = M_{i+1}(\beta_i)$, where β_i is a root of an irreducible $X^{d_i} - c_{i+1}$, with c_{i+1} in M_{i+1}.
So the polynomial f is solvable by radicals.

Radical Extensions and Solvable Groups

Theorem

Let K be a field of characteristic zero, and let $K \subseteq L \subseteq M$, where M is a radical extension. Then $\mathrm{Gal}(L:K)$ is a solvable group.

- Suppose there is a sequence $K = M_0, M_1, \ldots, M_r = M$, such that $M_{i+1} = M_i(\alpha_i)$, $i = 0, 1, \ldots, r-1$, where α_i is a root of a polynomial $X^{n_i} - a_i$, irreducible in $M_i[X]$.
- The idea of the proof is simple.

  At each stage, where the element α_i is a root of $X^{n_i} - b_i$, we use preceding theorems to get useful information about the Galois groups.
- However, we have to be careful that we have normal extensions at each stage.

Radical Extensions and Solvable Groups: The Start

- First, note that L need not be a normal extension of K.

  Instead of repairing L, we modify the base field K.

  The fixed field $K' = \Phi(\Gamma(K))$ of $\mathrm{Gal}(L:K)$ will in general be larger than K. On the other hand, we know that

  $$\Phi(\Gamma(K')) = (\Phi\Gamma\Phi\Gamma)(K) = (\Phi\Gamma)(K) = K'.$$

  Hence, L is a normal extension of K'.

  Note that:

  - Any polynomial f in $K[X]$ may be regarded as a polynomial in $K'[X]$;
  - $\mathrm{Gal}(L:K) = \mathrm{Gal}(L:K')$.

  So we may replace K by K'.

  To avoid complicating the notation, we suppose that L is a normal extension of K.

Radical Extensions and Solvable Groups (Cont'd)

- If N is a normal closure of M, then N is a radical extension, by a preceding theorem. So we may assume that M is both radical and normal. Note also that:
  - $\text{Gal}(M:L) \lhd \text{Gal}(M:K)$;
  - $\text{Gal}(L:K) \cong \text{Gal}(M:K)/\text{Gal}(M:L)$.

  So, if we prove that $\text{Gal}(M:K)$ is solvable, it will follow, by preceding theorems, that $\text{Gal}(L:K)$ is solvable.

  So we set out to prove that $\text{Gal}(M:K)$ is solvable, our assumption being that M is a normal (separable) radical extension of K.

  Let $M = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, with $\alpha_i^{p_i} \in K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}), i = 1, 2, \ldots, n$.

  We may assume that p_i is prime for all i, at a cost of increasing n.

  If, e.g., we have $\alpha_i^{pq} \in K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, we can define β as α_i^p, and say

$$\beta^q \in K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}) \quad \text{and} \quad \alpha_i^p \in K(\beta, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}).$$

Radical Extensions and Solvable Groups (Cont'd)

- We prove the result by induction on n. We have that $\alpha_1^{p_1} = b_1 \in K$.

  To have enough roots of unity, we let $P = M(\omega)$ be a splitting field for $X^{p_1} - 1$ over M, where ω is a primitive p_1-th root of unity.

  - Certainly, P, being a splitting field, is a normal extension of M.
  - By the Fundamental Theorem, $\text{Gal}(P : M) \lhd \text{Gal}(P : K)$;
  - By the Fundamental Theorem, $\text{Gal}(M : K) \cong \text{Gal}(P : K)/\text{Gal}(P : M)$.

  By a previous theorem, if $\text{Gal}(P : K)$ is solvable, so will be $\text{Gal}(M : K)$.

  Let M_1 be the subfield $K(\omega)$ of P. M_1 is a splitting field over K of $X^{p_1} - 1$. So it is a normal extension. By a previous corollary, $\text{Gal}(M_1 : K)$ is cyclic (and hence solvable). Thus:

  - $\text{Gal}(P : M_1) \lhd \text{Gal}(P : K)$;
  - $\text{Gal}(M_1 : K) \cong \text{Gal}(P : K)/\text{Gal}(P : M_1)$.

  Hence, if $\text{Gal}(P : M_1)$ is solvable, so will be $\text{Gal}(P : K)$.

Radical Extensions and Solvable Groups (Cont'd)

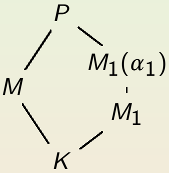
- So, having begun with $\mathrm{Gal}(L:K)$, we have now reduced the problem to showing that $\mathrm{Gal}(P:M_1)$ is solvable.

  We may write $P=M_1(\alpha_1,\alpha_2,\ldots,\alpha_n)$. Denote $\mathrm{Gal}(P:M_1)$ by G. Let $H=\mathrm{Gal}(P:M(\alpha_1))$, a subgroup of G. Use induction on n.

  In $M_1[X]$, $X^{p_1}-1=(X-1)(X-\omega)(X-\omega^2)\cdots(X-\omega^{p_1-1})$. In $(M(\alpha_1))[X]$, $X^{p_1}-b_1=X^{p_1}-\alpha_1^{p_1}=(X-\alpha_1)(X-\omega\alpha_1)(X-\omega^2\alpha_1)\cdots(X-\omega^{p_1-1}\alpha_1)$.

  Thus, $M(\alpha_1)$ is a splitting field for $X^{p_1}-b_1$ over M_1.

  Therefore, $\Gamma(M(\alpha_1))=\mathrm{Gal}(M_1(\alpha_1):M_1)$ is cyclic.

  P

  M

  $M_1(\alpha_1)$

  M_1

  K

  $M_1(\alpha)$ is a normal extension (being a splitting field) of M_1.

  So $H\lhd G$ and $G/H\cong\Gamma(M(\alpha_1))$ is cyclic.

  $H=\mathrm{Gal}(P:M(\alpha_1))=\mathrm{Gal}(M_1(\alpha_1)(\alpha_2,\ldots,\alpha_n):M_1(\alpha_1))$.

  P is a normal extension of $M_1(\alpha_1)$.

  By the induction hypothesis, H is solvable.

  Since G/H is certainly solvable, we deduce that G is solvable.

Solvability of Polynomial Equations by Radicals

- The Theorem makes no reference to polynomials or equations, but this omission is easily repaired.
- Let f be a polynomial in $K[X]$, and suppose that it is solvable by radicals.
- Then its splitting field L is contained in a radical extension M of K.
- The theorem tells us that $\mathrm{Gal}(f) = \mathrm{Gal}(L:K)$ is solvable.

Theorem

A polynomial f with coefficients in a field K of characteristic zero is solvable by radicals if and only if its Galois group is solvable.

- Immediate by the preceding two theorems.

Subsection 2

Insolvable Quintics

Galois Group of Irreducible Polynomials of Prime Degree

Theorem

Let p be a prime, and let f be a monic irreducible polynomial of degree p, with coefficients in $\mathbb{Q}$. Suppose that f has precisely two zeros in $\mathbb{C} \backslash \mathbb{R}$. Then the Galois group of f is the symmetric group S_p.

- The polynomial f has a splitting field L contained in $\mathbb{C}$. The roots of f in L are all distinct. The Galois group $G = \text{Gal}(L:\mathbb{Q})$ is a group of permutations on the p roots of f in L. Thus G is a subgroup of S_p.

  In constructing the splitting field of f, the first step is to form $\mathbb{Q}(\alpha)$, where α has minimum polynomial f. Then $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$.

  But $p = |\text{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})| = \frac{|\text{Gal}(L:\mathbb{Q})|}{|\text{Gal}(L:\mathbb{Q}(\alpha))|}$. So p divides $|G|$.

  Thus, G contains an element of order p.

  But the only elements of order p in S_p are cycles of length p.

  So G contains a cycle of length p.

Galois Group of Irreducible Polynomials of Prime Degree

- The two non-real roots of f are complex conjugates of each other.

  So the splitting field contains a transposition, interchanging the two non-real roots and leaving the rest unchanged.

  There is no loss of generality in denoting the transposition by $(1\ 2)$.

  We may also suppose that the p-cycle $\sigma = (a_1\ a_2\ \cdots\ a_p)$ has $a_1 = 1$, for the choice of first element is arbitrary.

  If $a_k = 2$, then $\sigma^{k-1} = (1\ 2\ \cdots)$.

  We may as well write it as $(1\ 2\ \cdots\ p)$.

  By a previous theorem, $(1\ 2)$ and $(1\ 2\ \cdots\ p)$ generate S_p.

  Since G contains $(1\ 2)$ and $(1\ 2\ \cdots\ p)$, $G = S_p$.

Example

- We show that $f(X) = X^5 - 8X + 2$ is not soluble by radicals.

  f is irreducible over $\mathbb{Q}$, by Eisenstein's Criterion.

  A table of values,

X	-2	-1	0	1	2
$f(X)$	-14	9	2	-5	18

  implies that there are roots in the intervals $(-2,-1)$, $(0,1)$ and $(1,2)$.

  So f has at least three real roots.

  The derivative $f'(X) = 5X^4 - 8$ has two real roots.

  By Rolle's theorem, there is at least one real zero of $f'(X)$ between zeros of $f(X)$.

  So f has at most 3 real roots.

  Thus, f has precisely three real roots.

  By preceding theorems, $f(X)$ is not solvable by radicals.

Subsection 3

General Polynomials

Algebraic Independence

- Let K be a field of characteristic zero.
- Let L be an extension of K.
- A subset $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of L is said to be **algebraically independent** over K if, for all polynomials $f=f(X_1,X_2,\ldots,X_n)$, with coefficients in K,
$$f(\alpha_1,\alpha_2,\ldots,\alpha_n)=0 \quad \text{implies} \quad f=0.$$
- This is a much stronger condition than linear independence.

  Example: Consider the set $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.
  - It is linearly independent over $\mathbb{Q}$.
  - It is not algebraically independent.
    Let $f(X_1,X_2,X_3,X_4)=X_2X_3-X_4$.
    Then $f(1,\sqrt{2},\sqrt{3},\sqrt{6})=\sqrt{2}\sqrt{3}-\sqrt{6}=0$.

Algebraic Independence (Alternative Formulations)

- Algebraic independence of $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ over K is equivalent to the property that:
  - α_1 is transcendental over K;
  - α_r is transcendental over $K(\alpha_1,\alpha_2,\ldots,\alpha_{r-1})$, for each r in $\{2,3,\ldots,n\}$.
- $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is algebraically independent over K if and only if $K(\alpha_1,\alpha_2,\ldots,\alpha_n)$ is isomorphic to $K(X_1,X_2,\ldots,X_n)$, the field of all rational forms with n indeterminates and coefficients in K.

Finitely Generated Extensions

- An extension L of a field K is said to be **finitely generated** if, for some natural number m, there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_m$, such that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$.
- Every finite extension is certainly finitely generated, but the converse statement is false.

Theorem

Let $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a finitely generated extension of K. Then there exists a field E, such that $K \subseteq E \subseteq L$, such that, for some m such that $0 \leq m \leq n$:

(i) $E = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, where $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is algebraically independent over K;

(ii) $[L : E]$ is finite.

Proof of the Theorem

- Suppose, first, that all elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over K. Then $[L:K]$ is finite. We may take $E = K$ and $m = 0$.

  Suppose not all of $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over K.
  - There exists an α_i which is transcendental over K. Call it β_1.
  - If $[L:K(\beta_1)]$ is not finite, there is an α_j which is transcendental over $K(\alpha_1)$. Call it β_2.
  - The process continues, and must terminate in at most n steps.

  Thus:
  - $E = K(\beta_1, \beta_2, \ldots, \beta_m)$, where $m \leq n$ and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is algebraically independent over K;
  - $[L:E]$ is finite.

Transcendence Degree

Theorem

Keeping the notation of the preceding theorem, suppose that there is another field F, such that $K \subseteq F \subseteq L$, and:

(i) $F = K(\gamma_1, \gamma_2, \ldots, \gamma_p)$, where $\{\gamma_1, \gamma_2, \ldots, \gamma_p\}$ is algebraically independent over K;

(ii) $[L : F]$ is finite.

Then $p = m$.

- Suppose that $p > m$.

  Since $[L : E]$ is finite, the element γ_1 is algebraic over E. Thus, γ_1 is a root of a polynomial with coefficients in $E = K(\beta_1, \beta_2, \ldots, \beta_m)$.

  Equivalently, there is a non-zero polynomial f, such that $f(\beta_1, \beta_2, \ldots, \beta_m, \gamma_1) = 0$. But γ_1 is transcendental over K. So at least one of the β_i's, say β_1, must actually occur in the coefficients of f.

Transcendence Degree (Cont'd)

- Thus, β_1 is algebraic over $K(\beta_2,\ldots,\beta_m,\gamma_1)$.

  Moreover, $[L:K(\beta_2,\ldots,\beta_m,\gamma_1)]$ is finite.

  We continue the argument, replacing each successive β_i by γ_i.

  So $[L:K(\gamma_1,\gamma_2,\ldots,\gamma_m)]$ is finite.

  We are assuming that $p > m$.

  But γ_{m+1} is transcendental over $K(\gamma_1,\gamma_2,\ldots,\gamma_m)$.

  This gives a contradiction.

  Similarly, we obtain a contradiction if we assume that $m > p$.
- The number m is called the **transcendence degree** of L over K.

Automorphisms Induced by Permutations

- Let K be a field.
- Let L be an extension of K with transcendence degree n.
- Suppose that $L = K(t_1, t_2, \ldots, t_n)$, where $t_1, t_2, \ldots, t_n$ are algebraically independent over K.
- For all σ in the symmetric group S_n we can define a K-automorphism φ_σ of L, given by

  $$\varphi_\sigma(t_i) = t_{\sigma(i)},$$

  and extending in the usual way to L.

  Example: Say $n = 3$ and $L = K(t_1, t_2, t_3)$.

  Let $\sigma = (1\ 2\ 3)$ and $q = \frac{t_1 + 3t_2 - t_3}{t_1^3 t_2} \in L$. Then $\sigma(q) = \frac{t_2 + 3t_3 - t_1}{t_2^3 t_3}$.
- Let us denote by Aut_n the group $\{\varphi_\sigma : \sigma \in S_n\}$.
- The map $S_n \to \mathrm{Aut}_n$; $\sigma \mapsto \varphi_\sigma$ is an isomorphism.

Elementary Symmetric Polynomials

- Consider again $L = K(t_1, t_2, \ldots, t_n)$, where $t_1, t_2, \ldots, t_n$ are algebraically independent over K.
- The fixed field F of Aut_n includes:
  - All the elementary symmetric polynomials

$$\begin{array}{rcl} s_1 & = & t_1 + t_2 + \cdots + t_n, \\ s_2 & = & t_1 t_2 + t_1 t_3 + \cdots + t_{n-1} t_n, \\ & \vdots & \\ s_n & = & t_1 t_2 \cdots t_n; \end{array}$$

  - All rational combinations of these polynomials.

Example:

- $t_1^2 + t_2^2 + \cdots + t_n^2$ is clearly in F.
- Note that we have

$$t_1^2 + \cdots + t_n^2 = (t_1 + \cdots + t_n)^2 - 2(t_1 t_2 + \cdots + t_{n-1} t_n) = s_1^2 - 2s_2.$$

Characterization of the Fixed Field

Theorem

The fixed field F of Aut_n is $F = K(s_1, s_2, \ldots, s_n)$.

- We show, by induction on n, that

$$[K(t_1, t_2, \ldots, t_n) : K(s_1, s_2, \ldots, s_n)] \leq n!.$$

This is obvious for $n = 1$.

Certainly $K(s_1, s_2, \ldots, s_n) \subseteq K(s_1, s_2, \ldots, s_n, t_n) \subseteq K(t_1, t_2, \ldots, t_n)$.

The polynomial $f(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$ factorizes into $(X - t_1)(X - t_2) \cdots (X - t_n)$ over $K(t_1, t_2, \ldots, t_n)$.

Hence, the minimum polynomial of t_n over $K(s_1, s_2, \ldots, s_n)$ divides f.

Consequently $[K(s_1, s_2, \ldots, s_n, t_n) : K(s_1, s_2, \ldots, s_n)] \leq n$.

Characterization of the Fixed Field (Cont'd)

- Let $s_1', s_2', \ldots, s_{n-1}'$ be the elementary symmetric polynomials in $t_1, t_2, \ldots, t_{n-1}$.

  Then $s_1 = s_1' + t_n$, $s_n = s_{n-1}' t_n$, and $s_j = s_{j-1}' t_n + s_j'$, $j = 2, 3, \ldots, n-1$.

  Hence, $K(s_1, s_2, \ldots, s_n) = K(s_1', s_2', \ldots, s_{n-1}', t_n)$.

  So, by the induction hypothesis,

$$\begin{aligned}&[K(t_1, t_2, \ldots, t_n) : K(s_1, s_2, \ldots, s_n, t_n)]\\ &= [K(t_n)(t_1, t_2, \ldots, t_{n-1}) : K(t_n)(s_1', s_2', \ldots, s_{n-1}')]\\ &\le (n-1)!.\end{aligned}$$

  This concludes the induction.

  Note that $K(s_1, s_2, \ldots, s_n)$ is contained in the fixed field F of Aut_n.

  By a preceding theorem, $[K(t_1, t_2, \ldots, t_n) : F] = |\mathrm{Aut}_n| = n!$.

  So, by what was just proven, $F = K(s_1, s_2, \ldots, s_n)$.

Algebraic Independence of the Symmetric Polynomials

Theorem

The symmetric polynomials $s_1, s_2, \ldots, s_n$ are algebraically independent.

- $t_1, t_2, \ldots, t_n$ are the roots of $X_n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n$.

  So the field $F(t_1, t_2, \ldots, t_n)$ is a finite extension of $F(s_1, s_2, \ldots, s_n)$.

  Thus, $F(t_1, t_2, \ldots, t_n)$ and $F(s_1, s_2, \ldots, s_n)$ have the same transcendence degree. So $s_1, s_2, \ldots, s_n$ are algebraically independent.

The General Polynomial

- Let K be a field of characteristic 0.
- Consider a set of n algebraically independent elements over K.
- We name these elements as $s_1, s_2, \ldots, s_n$.
- The **general polynomial of degree** n “over K” (its coefficients are actually in $K(s_1, s_2, \ldots, s_n)$) is

$$X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

- We can call it a **general** (or **generic**) **polynomial**, because there is no algebraic connection among the coefficients.

The Splitting Field of the General Polynomial

Theorem

Let K be a field of characteristic zero and

$$g(X)=X^n-s_1X^{n-1}+s_2X^{n-2}-\cdots+(-1)^ns_n.$$

Let M be a splitting field for g over $K(s_1,s_2,\ldots,s_n)$.

- The zeros $t_1,t_2,\ldots,t_n$ of g in M are algebraically independent over K.
- The Galois group of M over $K(s_1,s_2,\ldots,s_n)$ is the symmetric group S_n.

- The degree $[M:K(s_1,s_2,\ldots,s_n)]$ is finite.

  So, over K, the transcendence degree of $M=K(t_1,t_2,\ldots,t_n)$ is the same as that of $K(s_1,s_2,\ldots,s_n)$, namely, n.

  So the elements $t_1,t_2,\ldots,t_n$ must be algebraically independent.

The Splitting Field of the General Polynomial (Cont'd)

- We have

  $$X^n - s_1 X^{n-1} + s_2 X^{n-2} = \cdots + (-1)^n s_n = (X - t_1)(X - t_2)\cdots(X - t_n).$$

  So $s_1, s_2, \ldots, s_n$ are the elementary symmetric polynomials in $t_1, t_2, \ldots, t_n$.

  We have seen that:

  - Aut_n is a group of automorphisms of M;
  - Its fixed field is $K(s_1, s_2, \ldots, s_n)$.

  Thus, by a previous theorem,

  $$[M : K(s_1, s_2, \ldots, s_n)] = [M : \Phi(\mathrm{Aut}_n)] = |\mathrm{Aut}_n| = |S_n| = n!.$$

  Hence $\mathrm{Gal}(M : K(s_1, s_2, \ldots, s_n)) \cong S_n$.

Insolvability of the General Polynomial by Radicals

Theorem

Let K is a field with characteristic zero and $n \geq 5$. The general polynomial

$$X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

is not solvable by radicals.

- By a previous theorem, a polynomial f is solvable by radicals if and only if its Galois group is solvable.

  By the preceding theorem the Galois group of the general polynomial of degree n is S_n.

  By a preceding corollary, S_n is not solvable for $n \geq 5$.