Math-123: Galois groups of polynomials

Sebastien Vasey

Harvard University

April 21, 2020

Today we study Galois theory from the point of view of polynomials!

Today we study Galois theory from the point of view of polynomials!

Recall:

Definition

The *Galois group* of a separable polynomial $f(x) \in F[x]$ is the Galois group of the splitting field of $f(x)$ over F.

Today we study Galois theory from the point of view of polynomials!

Recall:

Definition

The *Galois group* of a separable polynomial $f(x) \in F[x]$ is the Galois group of the splitting field of $f(x)$ over F.

For example, the Galois group of $(x^2 - 2)(x^2 - 3)$ is $\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong Z_2 \times Z_2$.

Today we study Galois theory from the point of view of polynomials!

Recall:

Definition

The *Galois group* of a separable polynomial $f(x) \in F[x]$ is the Galois group of the splitting field of $f(x)$ over F.

For example, the Galois group of $(x^2 - 2)(x^2 - 3)$ is $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong Z_2 \times Z_2$.

We will try to study how to compute the Galois group directly from the polynomial.

Observations about Galois groups of polynomials

Let $f(x) \in F[x]$ be separable, with splitting field K. Let $\alpha_1, \ldots, \alpha_n \in K$ be its roots.

Observations about Galois groups of polynomials

Let $f(x) \in F[x]$ be separable, with splitting field K. Let $\alpha_1, \ldots, \alpha_n \in K$ be its roots.

Any $\sigma \in \mathrm{Aut}(K/F)$ permutes $\{\alpha_1, \ldots, \alpha_n\}$, hence permutes $\{1, 2, \ldots, n\}$.

Observations about Galois groups of polynomials

Let $f(x) \in F[x]$ be separable, with splitting field K. Let $\alpha_1, \ldots, \alpha_n \in K$ be its roots.

Any $\sigma \in \mathrm{Aut}(K/F)$ permutes $\{\alpha_1, \ldots, \alpha_n\}$, hence permutes $\{1, 2, \ldots, n\}$.

This gives an injective homomorphism of $\mathrm{Aut}(K/F)$ into S_n.

Observations about Galois groups of polynomials

Let $f(x) \in F[x]$ be separable, with splitting field K. Let $\alpha_1, \ldots, \alpha_n \in K$ be its roots.

Any $\sigma \in \mathrm{Aut}(K/F)$ permutes $\{\alpha_1, \ldots, \alpha_n\}$, hence permutes $\{1, 2, \ldots, n\}$.

This gives an injective homomorphism of $\mathrm{Aut}(K/F)$ into S_n.

Therefore *the Galois group of a polynomial of order n is a subgroup of S_n.*

Observations about Galois groups of polynomials

Let $f(x) \in F[x]$ be separable, with splitting field K. Let $\alpha_1, \ldots, \alpha_n \in K$ be its roots.

Any $\sigma \in \mathrm{Aut}(K/F)$ permutes $\{\alpha_1, \ldots, \alpha_n\}$, hence permutes $\{1, 2, \ldots, n\}$.

This gives an injective homomorphism of $\mathrm{Aut}(K/F)$ into S_n.

Therefore *the Galois group of a polynomial of order n is a subgroup of S_n.*

Recall we showed splitting fields have order at most $n!$. We just gave a group-theoretic proof!

Galois groups of irreducible polynomials

If $f(x)$ is a separable poly of degree n, its Galois group is a subgroup of S_n.

Galois groups of irreducible polynomials

If $f(x)$ is a separable poly of degree n, its Galois group is a subgroup of S_n.

We can be more precise: suppose $f(x) = f_1(x)f_2(x)\dots f_k(x)$, with each f_i irreducible of degree n_i.

Galois groups of irreducible polynomials

If $f(x)$ is a separable poly of degree n, its Galois group is a subgroup of S_n.

We can be more precise: suppose $f(x) = f_1(x)f_2(x)\dots f_k(x)$, with each f_i irreducible of degree n_i.

Each automorphism permutes roots of the f_i's. Thus the Galois group is a subgroup of $S_{n_1} \times S_{n_2} \times \dots \times S_{n_k}$.

Galois groups of irreducible polynomials

If $f(x)$ is a separable poly of degree n, its Galois group is a subgroup of S_n.

We can be more precise: suppose $f(x) = f_1(x)f_2(x)\dots f_k(x)$, with each f_i irreducible of degree n_i.

Each automorphism permutes roots of the f_i's. Thus the Galois group is a subgroup of $S_{n_1} \times S_{n_2} \times \dots \times S_{n_k}$.

For each i, the Galois group is *transitive* on the roots of $f_i(x)$: for any two roots of $f_i(x)$, there is an automorphism sending one to the other.

Example: $f(x) = (x^2 - 2)(x^2 - 3)$

Let $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$.

Example: $f(x) = (x^2 - 2)(x^2 - 3)$

Let $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$.

Identify the Galois group G with a subgroup of S_4. Any permutation of G must permute 1 and 2, and permute 3 and 4.

Example: $f(x) = (x^2 - 2)(x^2 - 3)$

Let $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$.

Identify the Galois group G with a subgroup of S_4. Any permutation of G must permute 1 and 2, and permute 3 and 4.

We know fixing $\sqrt{3}$ and sending $\sqrt{2}$ to $-\sqrt{2}$ is an automorphism. This corresponds to $\sigma = (12) \in G$. Similarly $\tau = (34) \in G$.

Example: $f(x) = (x^2 - 2)(x^2 - 3)$

Let $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$.

Identify the Galois group G with a subgroup of S_4. Any permutation of G must permute 1 and 2, and permute 3 and 4.

We know fixing $\sqrt{3}$ and sending $\sqrt{2}$ to $-\sqrt{2}$ is an automorphism. This corresponds to $\sigma = (12) \in G$. Similarly $\tau = (34) \in G$.

The Galois group is the group generated by these two (Klein 4-group).

Example: $f(x) = x^3 - 2$

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = e^{2\pi i/3}\sqrt[3]{2}$, $\alpha_3 = e^{4\pi i/3}\sqrt[3]{2}$.

Example: $f(x) = x^3 - 2$

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = e^{2\pi i/3}\sqrt[3]{2}$, $\alpha_3 = e^{4\pi i/3}\sqrt[3]{2}$.

The Galois group G is a subgroup of S_3.

Example: $f(x) = x^3 - 2$

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = e^{2\pi i/3}\sqrt[3]{2}$, $\alpha_3 = e^{4\pi i/3}\sqrt[3]{2}$.

The Galois group G is a subgroup of S_3.

We know sending $\sqrt[3]{2}$ to $\sqrt[3]{2}$ and $e^{2\pi i/3}$ to $e^{4\pi i/3}$ gives an automorphism. This corresponds to $\tau = (23) \in G$.

Example: $f(x) = x^3 - 2$

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = e^{2\pi i/3}\sqrt[3]{2}$, $\alpha_3 = e^{4\pi i/3}\sqrt[3]{2}$.

The Galois group G is a subgroup of S_3.

We know sending $\sqrt[3]{2}$ to $\sqrt[3]{2}$ and $e^{2\pi i/3}$ to $e^{4\pi i/3}$ gives an automorphism. This corresponds to $\tau = (23) \in G$.

We know sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$ and fixing $e^{2\pi i/3}$ gives an automorphism. This corresponds to $\tau = (123) \in G$.

Example: $f(x) = x^3 - 2$

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = e^{2\pi i/3}\sqrt[3]{2}$, $\alpha_3 = e^{4\pi i/3}\sqrt[3]{2}$.

The Galois group G is a subgroup of S_3.

We know sending $\sqrt[3]{2}$ to $\sqrt[3]{2}$ and $e^{2\pi i/3}$ to $e^{4\pi i/3}$ gives an automorphism. This corresponds to $\tau = (23) \in G$.

We know sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$ and fixing $e^{2\pi i/3}$ gives an automorphism. This corresponds to $\tau = (123) \in G$.

They generate the entire S_3, so $G = S_3$.

Question: for each n, is there a polynomial of degree n with S_n as Galois group?

Question: for each n, is there a polynomial of degree n with S_n as Galois group?

The short answer is yes! Intuitively, such polynomials are "generic": they have no relations between their roots.

Question: for each n, is there a polynomial of degree n with S_n as Galois group?

The short answer is yes! Intuitively, such polynomials are "generic": they have no relations between their roots.

The full answer requires some theory.

Let F be a field.

Definition

Let $x_1, x_2, \ldots, x_n$ be "indeterminates". The *elementary symmetric functions* $s_1, \ldots, s_n$ are defined by:

- $s_1 = x_1 + x_2 + \ldots + x_n$.

Let F be a field.

Definition

Let $x_1, x_2, \ldots, x_n$ be "indeterminates". The *elementary symmetric functions* $s_1, \ldots, s_n$ are defined by:

- $s_1 = x_1 + x_2 + \ldots + x_n$.
- $s_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n = \sum_{i<j\leq n} x_ix_j$.

Let F be a field.

Definition

Let $x_1, x_2, \ldots, x_n$ be "indeterminates". The *elementary symmetric functions* $s_1, \ldots, s_n$ are defined by:

- $s_1 = x_1 + x_2 + \ldots + x_n$.
- $s_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n = \sum_{i<j\leq n} x_ix_j$.
- ...
- $s_n = x_1x_2 \ldots x_n$.

Let F be a field.

Definition

Let $x_1, x_2, \ldots, x_n$ be "indeterminates". The *elementary symmetric functions* $s_1, \ldots, s_n$ are defined by:

- $s_1 = x_1 + x_2 + \ldots + x_n$.
- $s_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n = \sum_{i<j\leq n} x_ix_j$.
- ...
- $s_n = x_1x_2 \ldots x_n$.

In general, $s_k = \sum_{S\subseteq\{1,\ldots,n\},|S|=k} \prod_{i\in S} x_i$.

Let F be a field.

Definition

Let $x_1, x_2, \ldots, x_n$ be "indeterminates". The *elementary symmetric functions* $s_1, \ldots, s_n$ are defined by:

- $s_1 = x_1 + x_2 + \ldots + x_n$.
- $s_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n = \sum_{i<j\leq n} x_ix_j$.
- ...
- $s_n = x_1x_2 \ldots x_n$.

In general, $s_k = \sum_{S\subseteq\{1,\ldots,n\},|S|=k} \prod_{i\in S} x_i$.

Formally, we think of these as members of the field $F(x_1, x_2, \ldots, x_n)$ of rational functions in $x_1, x_2, \ldots, x_n$.

Let F be a field.

Definition

Let $x_1, x_2, \ldots, x_n$ be "indeterminates". The *elementary symmetric functions* $s_1, \ldots, s_n$ are defined by:

- $s_1 = x_1 + x_2 + \ldots + x_n$.
- $s_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n = \sum_{i<j\leq n} x_ix_j$.
- ...
- $s_n = x_1x_2 \ldots x_n$.

In general, $s_k = \sum_{S\subseteq\{1,\ldots,n\},|S|=k} \prod_{i\in S} x_i$.

Formally, we think of these as members of the field $F(x_1, x_2, \ldots, x_n)$ of rational functions in $x_1, x_2, \ldots, x_n$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2)\ldots(x - x_n)$, a member of $F(x_1, \ldots, x_n)[x]$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2)\dots(x - x_n)$, a member of $F(x_1, \dots, x_n)[x]$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2)\dots(x - x_n)$, a member of $F(x_1, \dots, x_n)[x]$.

Exercise:

$(x - x_1)(x - x_2)\dots(x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2)\ldots(x - x_n)$, a member of $F(x_1, \ldots, x_n)[x]$.

Exercise:

$(x - x_1)(x - x_2)\ldots(x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n$.

Thus the coefficients of the general polynomial of degree n are $\pm$ elementary symmetric functions: $f(x) \in F(s_1, s_2, \ldots, s_n)[x]$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2) \dots (x - x_n)$, a member of $F(x_1, \dots, x_n)[x]$.

Exercise:
$(x - x_1)(x - x_2) \dots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$.

Thus the coefficients of the general polynomial of degree n are $\pm$ elementary symmetric functions: $f(x) \in F(s_1, s_2, \dots, s_n)[x]$.

Thus $F(x_1, x_2, \dots, x_n)$ is a splitting field of $f(x)$ over $F(s_1, s_2, \dots, s_n)$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2)\dots(x - x_n)$, a member of $F(x_1, \dots, x_n)[x]$.

Exercise:
$(x - x_1)(x - x_2)\dots(x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$.

Thus the coefficients of the general polynomial of degree n are $\pm$ elementary symmetric functions: $f(x) \in F(s_1, s_2, \dots, s_n)[x]$.

Thus $F(x_1, x_2, \dots, x_n)$ is a splitting field of $f(x)$ over $F(s_1, s_2, \dots, s_n)$. **Question:** What is its Galois group?

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2) \ldots (x - x_n)$, a member of $F(x_1, \ldots, x_n)[x]$.

Exercise:
$(x - x_1)(x - x_2) \ldots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n$.

Thus the coefficients of the general polynomial of degree n are $\pm$ elementary symmetric functions: $f(x) \in F(s_1, s_2, \ldots, s_n)[x]$.

Thus $F(x_1, x_2, \ldots, x_n)$ is a splitting field of $f(x)$ over $F(s_1, s_2, \ldots, s_n)$. **Question:** What is its Galois group?

The Galois group must be a subgroup of S_n. Moreover for any $\sigma \in S_n$, σ yields an automorphism of $F(x_1, \ldots, x_n)/F$ by permutting the x_i's.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2)\dots(x - x_n)$, a member of $F(x_1, \dots, x_n)[x]$.

Exercise:
$(x - x_1)(x - x_2)\dots(x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \dots + (-1)^n s_n$.

Thus the coefficients of the general polynomial of degree n are $\pm$ elementary symmetric functions: $f(x) \in F(s_1, s_2, \dots, s_n)[x]$.

Thus $F(x_1, x_2, \dots, x_n)$ is a splitting field of $f(x)$ over $F(s_1, s_2, \dots, s_n)$. **Question:** What is its Galois group?

The Galois group must be a subgroup of S_n. Moreover for any $\sigma \in S_n$, σ yields an automorphism of $F(x_1, \dots, x_n)/F$ by permutting the x_i's.

It is easy to see σ fixes the s_i's, so σ yields a member of $\mathrm{Aut}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))$.

Definition

The *general polynomial of degree n* is $(x - x_1)(x - x_2) \dots (x - x_n)$, a member of $F(x_1, \dots, x_n)[x]$.

Exercise:

$(x - x_1)(x - x_2) \dots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$.

Thus the coefficients of the general polynomial of degree n are $\pm$ elementary symmetric functions: $f(x) \in F(s_1, s_2, \dots, s_n)[x]$.

Thus $F(x_1, x_2, \dots, x_n)$ is a splitting field of $f(x)$ over $F(s_1, s_2, \dots, s_n)$. **Question:** What is its Galois group?

The Galois group must be a subgroup of S_n. Moreover for any $\sigma \in S_n$, σ yields an automorphism of $F(x_1, \dots, x_n)/F$ by permutting the x_i's.

It is easy to see σ fixes the s_i's, so σ yields a member of $\mathrm{Aut}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))$.

This shows $\mathrm{Aut}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)) \cong S_n$.

Let us call a rational function $f(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

Let us call a rational function $f(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

For example, $\frac{x_1+x_2}{x_1x_2}$ is a symmetric function, but $x_1 + x_2 - x_3$ is not.

Let us call a rational function $f(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

For example, $\frac{x_1+x_2}{x_1 x_2}$ is a symmetric function, but $x_1 + x_2 - x_3$ is not.

Corollary (Fundamental theorem of symmetric functions)

Any symmetric function $f(x_1, \ldots, x_n)$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$:
$f(x_1, \ldots, x_n) \in F(s_1, \ldots, s_n)$.

Let us call a rational function $f(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

For example, $\frac{x_1+x_2}{x_1x_2}$ is a symmetric function, but $x_1 + x_2 - x_3$ is not.

Corollary (Fundamental theorem of symmetric functions)

Any symmetric function $f(x_1, \ldots, x_n)$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$:
$f(x_1, \ldots, x_n) \in F(s_1, \ldots, s_n)$.

Proof.

By definition of a symmetric function, $f(x_1, \ldots, x_n)$ is in the fixed field of the subgroup of $\mathrm{Aut}(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n))$ given by the automorphisms permutting the x_i's.

Let us call a rational function $f(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

For example, $\frac{x_1+x_2}{x_1x_2}$ is a symmetric function, but $x_1 + x_2 - x_3$ is not.

Corollary (Fundamental theorem of symmetric functions)

Any symmetric function $f(x_1, \ldots, x_n)$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$:
$f(x_1, \ldots, x_n) \in F(s_1, \ldots, s_n)$.

Proof.

By definition of a symmetric function, $f(x_1, \ldots, x_n)$ is in the fixed field of the subgroup of $\mathrm{Aut}(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n))$ given by the automorphisms permutting the x_i's.
We have just seen this subgroup is the whole Galois group.

Let us call a rational function $f(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

For example, $\frac{x_1+x_2}{x_1 x_2}$ is a symmetric function, but $x_1 + x_2 - x_3$ is not.

Corollary (Fundamental theorem of symmetric functions)

Any symmetric function $f(x_1, \ldots, x_n)$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$:
$f(x_1, \ldots, x_n) \in F(s_1, \ldots, s_n)$.

Proof.

By definition of a symmetric function, $f(x_1, \ldots, x_n)$ is in the fixed field of the subgroup of $\mathrm{Aut}(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n))$ given by the automorphisms permutting the x_i's.
We have just seen this subgroup is the whole Galois group.
Thus the corresponding fixed field is $F(s_1, \ldots, s_n)$, by the fundamental theorem of Galois theory!

Let us call a rational function $f(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$ *symmetric* if it is not changed by permutting the x_i's.

For example, $\frac{x_1+x_2}{x_1x_2}$ is a symmetric function, but $x_1 + x_2 - x_3$ is not.

Corollary (Fundamental theorem of symmetric functions)

Any symmetric function $f(x_1, \ldots, x_n)$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$:
$f(x_1, \ldots, x_n) \in F(s_1, \ldots, s_n)$.

Proof.

By definition of a symmetric function, $f(x_1, \ldots, x_n)$ is in the fixed field of the subgroup of $\mathrm{Aut}(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n))$ given by the automorphisms permutting the x_i's.
We have just seen this subgroup is the whole Galois group.
Thus the corresponding fixed field is $F(s_1, \ldots, s_n)$, by the fundamental theorem of Galois theory! □

In fact it is true that symmetric *polynomials* are *polynomials* in the elementary symmetric functions (in any commutative ring).

Examples

- $(x_1 - x_2)^2$ is a symmetric function.

Examples

- $(x_1 - x_2)^2$ is a symmetric function. It is equal to $x_1^2 - 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2$.

Examples

- $(x_1 - x_2)^2$ is a symmetric function. It is equal to $x_1^2 - 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2$.
- $x_1^2+x_2^2+x_3^2 = (x_1+x_2+x_3)^2-2(x_1x_2+x_1x_3+x_2x_3) = s_1^2-2s_2$.

A change of point of view

Recall
$(x - x_1)(x - x_2)\dots(x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n.$

A change of point of view

Recall
$(x - x_1)(x - x_2)\dots(x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \dots + (-1)^n s_n.$

Let us now change notation: think of $s_1, s_2, \dots, s_n$ as indeterminates (formally, we work over $F(s_1, \dots, s_n)$, where the s_i's are just variables).

A change of point of view

Recall
$(x - x_1)(x - x_2)\dots(x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$.

Let us now change notation: think of $s_1, s_2, \dots, s_n$ as indeterminates (formally, we work over $F(s_1, \dots, s_n)$, where the s_i's are just variables).

Look at the polynomial $x^n - s_1 x^{n-1} + \dots + (-1)^n s_n$ over that field. Add roots $x_1, x_2, \dots, x_n$.

A change of point of view

Recall
$(x-x_1)(x-x_2)\dots(x-x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \dots + (-1)^n s_n.$

Let us now change notation: think of $s_1, s_2, \dots, s_n$ as indeterminates (formally, we work over $F(s_1, \dots, s_n)$, where the s_i's are just variables).

Look at the polynomial $x^n - s_1x^{n-1} + \dots + (-1)^n s_n$ over that field. Add roots $x_1, x_2, \dots, x_n$.

The above formula shows that the s_i's are the elementary symmetric functions in $x_1, \dots, x_n$!

A change of point of view

Recall
$(x-x_1)(x-x_2)\dots(x-x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \dots + (-1)^n s_n$.

Let us now change notation: think of $s_1, s_2, \dots, s_n$ as indeterminates (formally, we work over $F(s_1, \dots, s_n)$, where the s_i's are just variables).

Look at the polynomial $x^n - s_1x^{n-1} + \dots + (-1)^n s_n$ over that field. Add roots $x_1, x_2, \dots, x_n$.

The above formula shows that the s_i's are the elementary symmetric functions in $x_1, \dots, x_n$!

For example, consider $f(x) = x^2 + bx + c$. If we know the roots: $f(x) = (x - \alpha_1)(x - \alpha_2)$, then we can get the coefficients: $b = -(\alpha_1 + \alpha_2)$, $c = \alpha_1\alpha_2$.

The generic polynomial, revisited

Think of $s_1, s_2, \ldots, s_n$ as indeterminates and look at the polynomial $x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$ over that field. Add roots $x_1, x_2, \ldots, x_n$.

The generic polynomial, revisited

Think of $s_1, s_2, \ldots, s_n$ as indeterminates and look at the polynomial $x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$ over that field. Add roots $x_1, x_2, \ldots, x_n$.

Observe there are no polynomial relations between $x_1, \ldots, x_n$: if $p(t_1, \ldots, t_n)$ is a polynomial in $F[t_1, \ldots, t_n]$ such that $p(x_1, \ldots, x_n) = 0$, then $p^* := \prod_{\sigma \in S_n} p(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)})$ is a symmetric polynomial in $t_1, \ldots, t_n$ with roots $x_1, \ldots, x_n$.

The generic polynomial, revisited

Think of $s_1, s_2, \ldots, s_n$ as indeterminates and look at the polynomial $x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$ over that field. Add roots $x_1, x_2, \ldots, x_n$.

Observe there are no polynomial relations between $x_1, \ldots, x_n$: if $p(t_1, \ldots, t_n)$ is a polynomial in $F[t_1, \ldots, t_n]$ such that $p(x_1, \ldots, x_n) = 0$, then $p^* := \prod_{\sigma \in S_n} p(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)})$ is a symmetric polynomial in $t_1, \ldots, t_n$ with roots $x_1, \ldots, x_n$.

By the fundamental theorem of symmetric functions, we get a polynomial relation between the s_i's, which is impossible.

We have just shown:

Theorem

If $s_1, s_2, \ldots, s_n$ are indeterminates, then the general polynomial $x^n - s_1x^{n-1} + s_2x^{n-2} + \ldots + (-1)^n s_n \in F(s_1, \ldots, s_n)$ is separable with Galois group S_n.

We have just shown:

Theorem

If $s_1, s_2, \ldots, s_n$ are indeterminates, then the general polynomial $x^n - s_1 x^{n-1} + s_2 x^{n-2} + \ldots + (-1)^n s_n \in F(s_1, \ldots, s_n)$ is separable with Galois group S_n.

Intuitively: if there are no polynomial relations between the coefficients $s_1, \ldots, s_n$, then the polynomial with those coefficient is also "generic" in the sense that the Galois group is the entire symmetric group: there are no polynomial relations between the roots.

We have just shown:

Theorem

If $s_1, s_2, \ldots, s_n$ are indeterminates, then the general polynomial $x^n - s_1 x^{n-1} + s_2 x^{n-2} + \ldots + (-1)^n s_n \in F(s_1, \ldots, s_n)$ is separable with Galois group S_n.

Intuitively: if there are no polynomial relations between the coefficients $s_1, \ldots, s_n$, then the polynomial with those coefficient is also "generic" in the sense that the Galois group is the entire symmetric group: there are no polynomial relations between the roots.

If $F = \mathbb{Q}$, let $e_1 \in \mathbb{C}$ be transcendental over $\mathbb{Q}$, $e_2 \in \mathbb{C}$ be transcendental over $\mathbb{Q}(e_1)$, etc. Then the result shows $x^2 - e_1 x^{n-1} + e_2 x^{n-2} + \ldots + (-1)^n e_n$ is separable and has Galois group S_n.

We have just shown:

Theorem

If $s_1, s_2, \ldots, s_n$ are indeterminates, then the general polynomial $x^n - s_1 x^{n-1} + s_2 x^{n-2} + \ldots + (-1)^n s_n \in F(s_1, \ldots, s_n)$ is separable with Galois group S_n.

Intuitively: if there are no polynomial relations between the coefficients $s_1, \ldots, s_n$, then the polynomial with those coefficient is also "generic" in the sense that the Galois group is the entire symmetric group: there are no polynomial relations between the roots.

If $F = \mathbb{Q}$, let $e_1 \in \mathbb{C}$ be transcendental over $\mathbb{Q}$, $e_2 \in \mathbb{C}$ be transcendental over $\mathbb{Q}(e_1)$, etc. Then the result shows $x^2 - e_1 x^{n-1} + e_2 x^{n-2} + \ldots + (-1)^n e_n$ is separable and has Galois group S_n.

It it harder to find rational numbers $a_{n-1}, \ldots, a_0$ so that $x_n + a_{n-1} x^{n-1} + \ldots + a_0$ has Galois group S_n, but it can also be done.

Two warnings

1. Over $\mathbb{Q}$, “generic” polynomials have Galois group S_n. Does it mean that any field has an extension with Galois group S_n?

Two warnings

1. Over $\mathbb{Q}$, "generic" polynomials have Galois group S_n. Does it mean that any field has an extension with Galois group S_n? **No:** For example $\mathbb{C}$ has no nontrivial finite extensions at all! Less trivially, Galois groups of finite extensions of $\mathbb{F}_p$ are all cyclic.

Two warnings

1. Over $\mathbb{Q}$, "generic" polynomials have Galois group S_n. Does it mean that any field has an extension with Galois group S_n? **No:** For example $\mathbb{C}$ has no nontrivial finite extensions at all! Less trivially, Galois groups of finite extensions of $\mathbb{F}_p$ are all cyclic.
2. Any group of order n is a subgroup of S_n, and S_n is the Galois group of an extension of $\mathbb{Q}$. Does it mean any group can be realized as a Galois extension of $\mathbb{Q}$?

Two warnings

1. Over $\mathbb{Q}$, "generic" polynomials have Galois group S_n. Does it mean that any field has an extension with Galois group S_n?
   No: For example $\mathbb{C}$ has no nontrivial finite extensions at all! Less trivially, Galois groups of finite extensions of $\mathbb{F}_p$ are all cyclic.
2. Any group of order n is a subgroup of S_n, and S_n is the Galois group of an extension of $\mathbb{Q}$. Does it mean any group can be realized as a Galois extension of $\mathbb{Q}$?
   No: the Galois correspondence is inclusion-reversing: if $K/\mathbb{Q}$ has Galois group $G = S_n$ and H is a subgroup of G, then the fixed field E satisfies (if H is normal in G) $\mathrm{Aut}(E/\mathbb{Q}) \cong G/H$.

Two warnings

1. Over $\mathbb{Q}$, "generic" polynomials have Galois group S_n. Does it mean that any field has an extension with Galois group S_n?
   No: For example $\mathbb{C}$ has no nontrivial finite extensions at all! Less trivially, Galois groups of finite extensions of $\mathbb{F}_p$ are all cyclic.
2. Any group of order n is a subgroup of S_n, and S_n is the Galois group of an extension of $\mathbb{Q}$. Does it mean any group can be realized as a Galois extension of $\mathbb{Q}$?
   No: the Galois correspondence is inclusion-reversing: if $K/\mathbb{Q}$ has Galois group $G = S_n$ and H is a subgroup of G, then the fixed field E satisfies (if H is normal in G) $\mathrm{Aut}(E/\mathbb{Q}) \cong G/H$. What is true is that $\mathrm{Aut}(K/E) \cong H$, so *any finite group is a Galois group over a finite extension of* $\mathbb{Q}$.

Let's continue studying the extension $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$ (where the s_i's are the elementary symmetric functions in $x_1, \ldots, x_n$).

Let's continue studying the extension $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$ (where the s_i's are the elementary symmetric functions in $x_1, \ldots, x_n$).

It is a Galois extension with Galois group S_n. Are there intermediate Galois extensions?

Let's continue studying the extension $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$ (where the s_i's are the elementary symmetric functions in $x_1, \ldots, x_n$).

It is a Galois extension with Galois group S_n. Are there intermediate Galois extensions?

If $n \geq 5$, S_n has only one normal subgroup: the alternating group A_n of index 2. So what is its fixed field?

Let's continue studying the extension $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$ (where the s_i's are the elementary symmetric functions in $x_1, \ldots, x_n$).

It is a Galois extension with Galois group S_n. Are there intermediate Galois extensions?

If $n \geq 5$, S_n has only one normal subgroup: the alternating group A_n of index 2. So what is its fixed field?

Definition

The *discriminant* D of $x_1, \ldots, x_n$ is:

$$D = \prod_{i<j} (x_i - x_j)^2$$

The *discriminant* of a polynomial is the discriminant of the roots of the polynomial.

Let's continue studying the extension $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$ (where the s_i's are the elementary symmetric functions in $x_1, \ldots, x_n$).

It is a Galois extension with Galois group S_n. Are there intermediate Galois extensions?

If $n \geq 5$, S_n has only one normal subgroup: the alternating group A_n of index 2. So what is its fixed field?

Definition

The *discriminant* D of $x_1, \ldots, x_n$ is:

$$D = \prod_{i<j} (x_i - x_j)^2$$

The *discriminant* of a polynomial is the discriminant of the roots of the polynomial.

Note the discriminant is a symmetric function, so a member of $F(s_1, \ldots, s_n)$.

Alternating group and discriminant

For simplicity, let $F = \mathbb{Q}$.

Exercise: A permutation $\sigma \in S_n$ is in A_n if and only if σ fixes $\sqrt{D} := \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]$.

Alternating group and discriminant

For simplicity, let $F = \mathbb{Q}$.

Exercise: A permutation $\sigma \in S_n$ is in A_n if and only if σ fixes $\sqrt{D} := \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]$.

Thus the fixed field of A_n is generated by $\sqrt{D}$, and is equal to $F(s_1, \ldots, s_n)(\sqrt{D})$.

Discriminant and Galois group of polynomials

Let $f(x) \in \mathbb{Q}[x]$, of degree at least 1. Let $\alpha_1, \ldots, \alpha_n$ be the roots (counted with multiplicity).

Discriminant and Galois group of polynomials

Let $f(x) \in \mathbb{Q}[x]$, of degree at least 1. Let $\alpha_1, \ldots, \alpha_n$ be the roots (counted with multiplicity).

The discriminant of $f(x)$ is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Note $D \neq 0$ if and only if $f(x)$ is separable.

Discriminant and Galois group of polynomials

Let $f(x) \in \mathbb{Q}[x]$, of degree at least 1. Let $\alpha_1, \ldots, \alpha_n$ be the roots (counted with multiplicity).

The discriminant of $f(x)$ is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Note $D \neq 0$ if and only if $f(x)$ is separable.

If $f(x)$ is not separable, can look at the product of the distinct irreducible factors of $f(x)$ and get the same splitting field. This product is separable. Thus without loss $f(x)$ is separable.

Discriminant and Galois group of polynomials

Let $f(x) \in \mathbb{Q}[x]$, of degree at least 1. Let $\alpha_1, \ldots, \alpha_n$ be the roots (counted with multiplicity).

The discriminant of $f(x)$ is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Note $D \neq 0$ if and only if $f(x)$ is separable.

If $f(x)$ is not separable, can look at the product of the distinct irreducible factors of $f(x)$ and get the same splitting field. This product is separable. Thus without loss $f(x)$ is separable.

Since D is symmetric in the roots of $f(x)$, it is fixed by all the members of the Galois group, so is a member of $\mathbb{Q}$.

Theorem

The Galois group of $f(x)$ is a subgroup of A_n if and only if the discriminant D is the square of a member of F.

Theorem

The Galois group of $f(x)$ is a subgroup of A_n if and only if the discriminant D is the square of a member of F.

Proof.

The Galois group will be contained in A_n if and only if every automorphism fixes $\sqrt{D}$ (as seen before), which means that $\sqrt{D} \in F$. $\square$

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

We think of $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2. Thus $b = -s_1$, $c = s_2$.

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

We think of $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2. Thus $b = -s_1$, $c = s_2$.

These indeterminates are symmetric functions in the roots!
$s_1 = \alpha + \beta$, $s_2 = \alpha\beta$.

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

We think of $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2. Thus $b = -s_1$, $c = s_2$.

These indeterminates are symmetric functions in the roots!
$s_1 = \alpha + \beta$, $s_2 = \alpha\beta$.

The discriminant is $(\alpha - \beta)^2$. We can write it as a polynomial in the elementary symmetric functions:
$(\alpha + \beta)^2 - 4\alpha\beta = s_1^2 - 4s_2 = (-b)^2 - 4c$.

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

We think of $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2. Thus $b = -s_1$, $c = s_2$.

These indeterminates are symmetric functions in the roots!
$s_1 = \alpha + \beta$, $s_2 = \alpha\beta$.

The discriminant is $(\alpha - \beta)^2$. We can write it as a polynomial in the elementary symmetric functions:
$(\alpha + \beta)^2 - 4\alpha\beta = s_1^2 - 4s_2 = (-b)^2 - 4c$.

This is the usual "high school' discriminant" of a quadratic!

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

We think of $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2. Thus $b = -s_1$, $c = s_2$.

These indeterminates are symmetric functions in the roots!
$s_1 = \alpha + \beta$, $s_2 = \alpha\beta$.

The discriminant is $(\alpha - \beta)^2$. We can write it as a polynomial in the elementary symmetric functions:
$(\alpha + \beta)^2 - 4\alpha\beta = s_1^2 - 4s_2 = (-b)^2 - 4c$.

This is the usual "high school' discriminant" of a quadratic!

The polynomial is separable if and only if $D = b^2 - 4c \neq 0$.

Example: Galois group of quadratics

Consider $x^2 + bx + c$, with roots α, β.

We think of $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2. Thus $b = -s_1$, $c = s_2$.

These indeterminates are symmetric functions in the roots!
$s_1 = \alpha + \beta$, $s_2 = \alpha\beta$.

The discriminant is $(\alpha - \beta)^2$. We can write it as a polynomial in the elementary symmetric functions:
$(\alpha + \beta)^2 - 4\alpha\beta = s_1^2 - 4s_2 = (-b)^2 - 4c$.

This is the usual "high school' discriminant" of a quadratic!

The polynomial is separable if and only if $D = b^2 - 4c \neq 0$.

The Galois group is a subgroup of $S_2 = Z_2$. It is trivial if and only if D is the square of a rational: $\sqrt{D} \in \mathbb{Q}$.

See DF for explicit analysis of Galois group of degree 3 and degree 4 polynomials.

Summary

- The Galois group of a polynomial of degree n is a subgroup of S_n. If the polynomial is irreducible, the group is transitive.

Summary

- The Galois group of a polynomial of degree n is a subgroup of S_n. If the polynomial is irreducible, the group is transitive.
- Fundamental theorem of symmetric functions: Every symmetric function is a rational combination of elementary symmetric functions.

Summary

- The Galois group of a polynomial of degree n is a subgroup of S_n. If the polynomial is irreducible, the group is transitive.
- Fundamental theorem of symmetric functions: Every symmetric function is a rational combination of elementary symmetric functions.
- The general polynomial $x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$ has Galois group S_n over $F(s_1, \ldots, s_n)$.

Summary

- The Galois group of a polynomial of degree n is a subgroup of S_n. If the polynomial is irreducible, the group is transitive.
- Fundamental theorem of symmetric functions: Every symmetric function is a rational combination of elementary symmetric functions.
- The general polynomial $x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$ has Galois group S_n over $F(s_1, \ldots, s_n)$.
- The fixed field of A_n is given by adjoining the square root of the discriminant, $\prod_{i<j}(x_i - x_j)$.