Outline

1. Galois groups and symmetries
2. Square Roots and the Alternating Group
3. Examples for Degree $\leq 4$
Definition 1 (Review, mostly)

1. If \( K/F \) is Galois, then \( K \) is the splitting field of some separable \( f(x) \in F[x] \).

2. First assume that \( f(x) \) is irreducible:
   - Any \( \sigma \in \text{Gal}(K/F) \) maps roots of \( f \) to roots of \( f \), and is thus determined by its action on \( \alpha_1, \ldots, \alpha_n \).
   - This generates a permutation on the letters \( \{1, 2, \ldots, n\} \) in an obvious manner.
   - This is an injection \( \text{Gal}(K/F) \hookrightarrow S_n \).

3. More generally, if \( f(x) = \prod_{i=1}^{k} f_i(x) \), where \( f_i(x) \) is irreducible of degree \( n_i \), then \( \text{Gal}(K/F) \hookrightarrow S_{n_1} \times \cdots \times S_{n_k} \).
Definition 2

Let \( x_1, \ldots, x_n \) be indeterminants. The \textbf{elementary symmetric functions} \( s_1, \ldots, s_n \) are defined by

\[
\begin{align*}
    s_1 &= \sum_{i=1}^{n} x_i, \\
    s_2 &= \sum_{i<j} x_i x_j, \\
    s_3 &= \sum_{i<j<k} x_i x_j x_k, \\
    \vdots \\
    s_n &= x_1 x_2 \cdots x_n.
\end{align*}
\]
The general polynomial of degree $n$ is

$$(x - x_1)(x - x_2) \cdots (x - x_n),$$

and we can see by expanding that this is

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

**Definition 3**

A **symmetric function** in $x_i$ is a rational function that is not changed by any permutation of the $x_i$.

**Theorem 4**

*If $f(x_1, \ldots, x_n)$ is a symmetric function, then $f$ is a rational function in $(s_1, \ldots, s_n)$.*

**Corollary 5**

*The general polynomial in $F(s_1, \ldots, s_n)$ is separable with Galois group $S_n$.***
Proof (Part 1)

- Consider \( F(x_1, \ldots, x_n) \), rational functions in \( x_1, \ldots, x_n \).
- \( \sigma \in S_n \) acts on such functions in the obvious manner, which is thus an automorphism of \( F(x_1, \ldots, x_n) \).
- Therefore \( S_n \leq \text{Aut}(F(x_1, \ldots, x_n)) \) under this identification.
- Functions of \( s_1, \ldots, s_n \) are fixed by all of these, and therefore \( F(s_1, \ldots, s_n) \subseteq \text{Fix}_{F(x_1, \ldots, x_n)/F(S_n)} \).
- From the Fundamental Theorem,
  \[
  [F(x_1, \ldots, x_n) : \text{Fix}_{F(x_1, \ldots, x_n)/F(S_n)}] = |S_n| = n!.
  \]
- However, since the general polynomial with coefficients in \( s_i \) is the general polynomial with roots \( x_i \), we have that the splitting field of the general polynomial over \( F(s_1, s_2, \ldots, s_n) \) is \( F(x_1, x_2, \ldots, x_n) \) itself.
Proof.

Thus

\[ [F(x_1, \ldots, x_n) : F(s_1, \ldots, s_n)] \leq n!, \]

and thus we cannot have

\[ F(s_1, \ldots, s_n) \subsetneq \text{Fix}_{F(x_1, \ldots, x_n)} / F(S_n), \]

since then

\[ [F(x_1, \ldots, x_n) : F(s_1, \ldots, s_n)] > [F(x_1, \ldots, x_n) : \text{Fix}_{F(x_1, \ldots, x_n)} / F(S_n)] = n!. \]
Examples

1. Clearly \((x_1 - x_2)^2\) is symmetric in \(x_1, x_2\). We note that

\[
(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2.
\]

2. \(x_1^2 + x_2^2 + x_3^2\) is symmetric and we compute

\[
x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = s_1^2 - 2s_2.
\]

3. \(x_1^2x_2 + x_1^2x_3 + x_2^2x_3\) is symmetric and

\[
s_2^2 = (x_1x_2 + x_1x_3 + x_2x_3)^2 = (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) + 2x_1^2x_2x_3 + 2x_1x_2^2x_3 + 2x_1x_2x_3^2
\]

\[
= (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) + 2(x_1 + x_2 + x_3)(x_1x_2x_3),
\]

so

\[
x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = s_2^2 - 2s_1s_3.
\]
1. Galois groups and symmetries

2. Square Roots and the Alternating Group

3. Examples for Degree $\leq 4$
Definition 6

The **discriminant** 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.

Consider the polynomial \( x^2 + bx + c \) over \( \mathbb{Q} \) (or in fact any field not \( \mathbb{F}_2 \)). Then

\[
x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}
\]

are the roots, and its discriminant is

\[
(x_+ - x_-)^2 = (\sqrt{b^2 - 4ac})^2 = b^2 - 4c.
\]
Note that $D$ is symmetric in $x_1, \ldots, x_n$ and thus is an element of $F(s_1, \ldots, s_n)$.

We have

$$\sqrt{D} = \prod_{i < j} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n].$$

Recall the definition of $A_n$ and note that $\sigma \in A_n$ iff $\sigma$ fixes $\sqrt{D}$.

**Theorem 7**

The Galois group of $f(x) \in F[x]$ is a subgroup of $A_n$ iff $D \in F$ is the square of an element in $F$ (in shorthand, $\sqrt{D} \in F$).

**Proof.**

Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$, and $D = \prod_{i < j} (x_i - x_j)^2$. Since $D$ is symmetric in roots of $f(x)$, it is fixed by all elements of its Galois group, thus in $F$. Also note that $\sqrt{D}$ is in the splitting field of $f(x)$ (it’s an explicit function of the roots) and is fixed by all of the elements of the Galois group iff they are all even permutations.
1. Galois groups and symmetries

2. Square Roots and the Alternating Group

3. Examples for Degree $\leq 4$
- We already computed the discriminant of $x^2 + bx + c$ as $D = b^2 - 4c$.
- This polynomial is separable iff $b^2 - 4c \neq 0$.
- The Galois group is a subgroup of $S_2$. If $b^2 - 4c \in \mathbb{Q}$ then this group is $A_2 = \{1\}$ and if $b^2 - 4c \notin \mathbb{Q}$ then it is $S_2$. 
Consider the general monic cubic over \( \mathbb{Q} \):
\[
f(x) = x^3 + ax^2 + bx + c.
\]
Writing \( x = y - a/3 \), we can remove the quadratic term and obtain
\[
g(y) = y^3 + py + q, \quad p = \frac{3b - a^2}{3}, \quad q = \frac{2a^3 - 9ab + 27c}{27}.
\]
Note that \( a/3 \in \mathbb{Q} \) and we shifted the roots, so the discriminant is unchanged.

We write
\[
g(y) = (y - x_1)(y - x_2)(y - x_3),
g'(y) = (y - x_2)(y - x_3) + (y - x_1)(y - x_3) + (y - x_1)(y - x_2)
g'(x_1) = (x_1 - x_2)(x_1 - x_3),
g'(x_2) = (x_2 - x_1)(x_2 - x_3) = -(x_1 - x_2)(x_2 - x_3),
g'(x_3) = (x_3 - x_1)(x_3 - x_2) = (x_1 - x_3)(x_2 - x_3).
\]
So \( D = -g'(x_1)g'(x_2)g'(x_3) \).
\[ D = -g'(x_1)g'(x_2)g'(x_3) \]

Note \( g'(z) = 3z^2 + p \), so

\[
-D = (3x_1^2 + p)(3x_2^2 + p)(3x_3^2 + p) \\
= 27x_1^2x_2^2x_3^2 + 9p(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) + 3p^2(x_1^2 + x_2^2 + x_3^2) + p^3 \\
= 27s_3^2 + 9p(s_2^2 - 2s_1s_3) + 3p^2(s_1^2 - 2s_2) + p^3
\]

But also notice that \( g(y) = y^3 - s_1y^2 + s_2y - s_3 = y^3 + py + q \),

so \( s_1 = 0, \quad s_2 = p, \quad s_3 = -q \),

and thus

\[
-D = -27(-q)^2 + 9p(p^2) + (3p^2)(-2p) + p^3 \\
= 4p^2 + 27q^2
\]

(Repeated roots iff \( p = q = 0! \))
Repeating,\[ D = -4p^2 - 27q^2 \]
\[ = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \]

- If \( f(x) \) is irreducible, then the degree of \( K \), the splitting field over \( \mathbb{Q} \), is divisible by 3 and bounded above by \( 3! = 6 \), so it is 3 or 6.
- Thus \( \text{Gal}(K/\mathbb{Q}) = S_3 \) or \( A_3 \).
- It is \( A_3 \) iff \( \sqrt{D} \in \mathbb{Q} \).
One can do a similar analysis for the quartic

But we won’t.