notion of "generic" polynomial and then it is true that most polynomials have the full symmetric group as Galois group.

For $n \geq 5$ there is only one normal subgroup of S_n, namely the subgroup A_n of index 2. Hence in general there is only one normal subfield of $F(x_1, x_2, \ldots, x_n)$ containing $F(s_1, s_2, \ldots, s_n)$ and it is an extension of degree 2.

Definition. Define the *discriminant* D of $x_1, x_2, \ldots, x_n$ by the formula

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

Define the discriminant of a polynomial to be the discriminant of the roots of the polynomial.

The discriminant D is a symmetric function in $x_1, \ldots, x_n$, hence is an element of $K = F(s_1, s_2, \ldots, s_n)$.

When we first defined the alternating group A_n we saw that a permutation $\sigma \in S_n$ is an element of the subgroup A_n if and only if σ fixes the product

$$\sqrt{D} = \prod_{i<j} (x_i - x_j) \in \mathbb{Z}[x_1, x_2, \ldots, x_n].$$

It follows (by the Fundamental Theorem) that if F has characteristic different from 2 then $\sqrt{D}$ generates the fixed field of A_n and generates a quadratic extension of K. This proves the following proposition.

Proposition 33. If $\mathrm{ch}(F) \neq 2$ then the permutation $\sigma \in S_n$ is an element of A_n if and only if it fixes the square root of the discriminant D.

We now consider the Galois groups of separable polynomials of small degree (≤ 4) over a field F which we assume is of characteristic different from 2 and 3. Note that over $\mathbb{Q}$ or over a finite field (or, more generally, over any perfect field) the splitting field of an arbitrary polynomial $f(x)$ is the same as the splitting field for the product of the irreducible factors of $f(x)$ taken precisely once, which is a separable polynomial.

If the roots of the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ are $\alpha_1, \alpha_2, \ldots, \alpha_n$, then the discriminant of $f(x)$ is[2]

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Note that $D = 0$ if and only if $f(x)$ is not separable, i.e., if the roots $\alpha_1, \ldots, \alpha_n$ are not distinct. Recall that over a perfect field (e.g., $\mathbb{Q}$ or a finite field) this implies $f(x)$ is reducible since every irreducible polynomial over a perfect field is separable.

The discriminant D is symmetric in the roots of $f(x)$, hence is fixed by all the automorphisms of the Galois group of $f(x)$. By the Fundamental Theorem it follows that

[2]If $f(x) = a_n x^n + \cdots + a_0$ is not monic then its discriminant is defined to be a_n^{2n-2} times the D defined above.

$D \in F$. The discriminant can in general be written as a polynomial in the coefficients of $f(x)$ (by Corollary 31) which are fairly complicated for larger degrees (we shall give formulas for $n \leq 4$ below). Finally, note that since

$$\sqrt{D} = \prod_{i<j}(\alpha_i - \alpha_j)$$

we have the useful fact that $\sqrt{D}$ is always contained in the splitting field for $f(x)$.

If the roots of $f(x)$ are distinct, fix some ordering of the roots and view the Galois group of $f(x)$ as a subgroup of S_n as above.

Proposition 34. The Galois group of $f(x) \in F[x]$ is a subgroup of A_n if and only if the discriminant $D \in F$ is the square of an element of F.

Proof: This is a restatement of Proposition 33 in this case. The Galois group is contained in A_n if and only if every element of the Galois group fixes

$$\sqrt{D} = \prod_{i<j}(\alpha_i - \alpha_j)$$

i.e., if and only if $\sqrt{D} \in F$.

This property, together with the fact that $D = 0$ determines the presence of multiple roots, is the reason D is called the *discriminant.*

Polynomials of Degree 2

Consider the polynomial $x^2 + ax + b$ with roots α, β. The discriminant D for this polynomial is $(\alpha - \beta)^2$, which can be written as a polynomial in the elementary symmetric functions of the roots. We did this in Example 1 above:

$$D = s_1^2 - 4s_2 = (-a)^2 - 4(b) = a^2 - 4b,$$

the usual discriminant for this quadratic.

The polynomial is separable if and only if $a^2 - 4b \neq 0$. The Galois group is a subgroup of S_2, the cyclic group of order 2 and is trivial (i.e., A_2 in this case) if and only if $a^2 - 4b$ is a rational square, which completely determines the possible Galois groups.

Note that this restates results we obtained previously by explicitly solving for the roots: if the polynomial is reducible (namely D is a square in F), then the Galois group is trivial (the splitting field is just F), while if the polynomial is irreducible the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ since the splitting field is the quadratic extension $F(\sqrt{D})$.

Polynomials of degree 3

Suppose the cubic polynomial is

$$f(x) = x^3 + ax^2 + bx + c. \tag{14.15}$$

If we make the substitution $x = y - a/3$ the polynomial becomes

$$g(y) = y^3 + py + q \tag{14.16}$$

where

$$p = \frac{1}{3}(3b - a^2) \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c). \tag{14.17}$$

The splitting fields for these two polynomials are the same since their roots differ by the constant $a/3 \in F$ and since the formula for the discriminant involves the *differences* of roots, we see that these two polynomials also have the *same* discriminant.

Let the roots of the polynomial in (16) be α, β, and γ. We first compute the discriminant of this polynomial in terms of p and q. Note that

$$g(y) = (y - \alpha)(y - \beta)(y - \gamma)$$

so that if we differentiate we have

$$D_y g(y) = (y - \alpha)(y - \beta) + (y - \alpha)(y - \gamma) + (y - \beta)(y - \gamma).$$

Then

$$\begin{aligned} D_y g(\alpha) &= (\alpha - \beta)(\alpha - \gamma) \\ D_y g(\beta) &= (\beta - \alpha)(\beta - \gamma) \\ D_y g(\gamma) &= (\gamma - \alpha)(\gamma - \beta). \end{aligned}$$

Taking the product we see that

$$D = [(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)]^2 = -D_y g(\alpha) D_y g(\beta) D_y g(\gamma).$$

Since $D_y g(y) = 3y^2 + p$, we have

$$\begin{aligned} -D &= (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3. \end{aligned}$$

The corresponding expressions in the elementary symmetric functions of the roots were determined in Examples 2 and 3 above. Note that here $s_1 = 0$, $s_2 = p$ and $s_3 = -q$. We obtain

$$-D = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3$$

so that

$$D = -4p^3 - 27q^2. \tag{14.18}$$

This is the same as the discriminant of $f(x)$ in (15). Expressing D in terms of a, b, c using (17) we obtain

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \tag{14.18'}$$

(Galois Group of a Cubic)

a. If the cubic polynomial $f(x)$ is reducible, then it splits either into three linear factors or into a linear factor and an irreducible quadratic. In the first case the Galois group is trivial and in the second case the Galois group is of order 2.

b. If the cubic polynomial $f(x)$ is irreducible then a root of $f(x)$ generates an extension of degree 3 over F, so the degree of the splitting field over F is divisible by 3. Since the Galois group is a subgroup of S_3, there are only two possibilities, namely

A_3 or S_3. The Galois group is A_3 (i.e., cyclic of order 3) if and only if the discriminant D in (18) is a square.

Explicitly, if D is the square of an element of F, then the splitting field of the irreducible cubic $f(x)$ is obtained by adjoining any single root of $f(x)$ to F. The resulting field is Galois over F of degree 3 with a cyclic group of order 3 as Galois group. If D is not the square of an element of F then the splitting field of $f(x)$ is of degree 6 over F, hence is the field $F(\theta, \sqrt{D})$ for any one of the roots θ of $f(x)$. This extension is Galois over F with Galois group S_3 (generators are given by σ, which takes θ to one of the other roots of $f(x)$ and fixes $\sqrt{D}$, and τ, which takes $\sqrt{D}$ to $-\sqrt{D}$ and fixes θ).

We see that in both cases the splitting field for the irreducible cubic $f(x)$ is obtained by adjoining $\sqrt{D}$ and a root of $f(x)$ to F.

We shall give explicit formulas for the roots of (16) (*Cardano's Formulas*) in the next section after introducing the notion of a *Lagrange Resolvent*.

Polynomials of Degree 4

Let the quartic polynomial be

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

which under the substitution $x = y - a/4$ becomes the quartic

$$g(y) = y^4 + py^2 + qy + r$$

with

$$p = \frac{1}{8}(-3a^2 + 8b)$$

$$q = \frac{1}{8}(a^3 - 4ab + 8c)$$

$$r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d).$$

Let the roots of $g(y)$ be α_1, α_2, α_3, and α_4 and let G denote the Galois group for the splitting field of $g(y)$ (or of $f(x)$).

Suppose first that $g(y)$ is reducible. If $g(y)$ splits into a linear and a cubic, then G is the Galois group of the cubic, which we determined above. Suppose then that $g(y)$ splits into two irreducible quadratics. Then the splitting field is the extension $F(\sqrt{D_1}, \sqrt{D_2})$ where D_1 and D_2 are the discriminants of the two quadratics. If D_1 and D_2 do not differ by a square factor then this extension is a biquadratic extension and G is isomorphic to the Klein 4-subgroup of S_4. If D_1 is a square times D_2 then this extension is a quadratic extension and G is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

We are reduced to the situation where $g(y)$ is irreducible. In this case recall that the Galois group is transitive on the roots, i.e., it is possible to get from a given root to any other root by applying some automorphism of the Galois group. Examining the possibilities we see that the only transitive subgroups of S_4, hence the only possibilities