Let K be a field, char$K \neq 2$, and $f(X)$ be a separable polynomial in $K[X]$ with Galois group G_f over K and $Z_f = \{\alpha_1, \dots, \alpha_n\} \subset K_f$. We know (Proposition 1, lecture 2) that G_f permutes the elements of Z_f, so G_f can be embedded into $S_{Z_f} \simeq S_n$ and can thus, be identified with a subgroup of S_n, which we will do from now on. This embedding has two properties important for us.

Proposition 2. Let $f(X)$ be a separable polynomial of degree n.

(a) $f(X)$ irreducible over $K \Rightarrow n$ divides $|G_f|$.

(b) $f(X)$ irreducible over $K \Leftrightarrow G_f$ is a transitive subgroup of S_n.

Examples:
a) For $f_1(X) = X^4 - 4 \in \mathbb{Q}[X]$, $Z_f = \{\alpha_1 = \sqrt{2},\ \alpha_2 = -\sqrt{2},\ \alpha_3 = i\sqrt{2},\ \alpha_4 = -i\sqrt{2}\}$, $\mathbb{Q}_f = Q[\sqrt{2}, i]$ and $G_f \subset S_4$. G_f is not transitive, which makes sense, as $f_1(X)$ is not irreducible in $\mathbb{Q}[X]$.
b) For $f_4(X) = X^3 - 2 \in Q[X]$, irreducible over $\mathbb{Q}$, $Z_f = \{\alpha_1 = \sqrt[3]{2},\ \alpha_2 = \omega\sqrt[3]{2},\ \alpha_3 = \omega^2\sqrt[3]{2}\}$, $\mathbb{Q}_f = \mathbb{Q}[\sqrt[3]{2}, \omega]$ and $G_f = \langle(123), (23)\rangle = S_3$, which is transitive.

In order to be able to compute G_f , we use what is known as the *discriminant* of f.

Definition. Let char$K \neq 2$, $f(X) \in K[X]$ and $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ in some splitting field. We set $\Delta(f) = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)$. The *discriminant* of $f(X)$ is defined to be $\mathrm{Disc}(f) = \Delta(f)^2 = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2$.

For example, $\mathrm{Disc}(X^2 + aX + b) = a^2 - 4b$. But, how do we compute $\mathrm{Disc}(f)$ when we don't know the exact value of the roots of f? We do it by means of the formula

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} Res(f, f')$$

where, given any two polynomials $h(X) = a_0 + a_1 X + ... + a_n X^n$, and $g(T) = b_0 + b_1 T + ... + b_m T^n$ in $K[X]$, with $a_n \neq 0, b_m \neq 0$, we define the resultant $R(h, g)$ as the determinant of size $(m + n) \times (m + n)$,

$$R(h,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & ... & a_0 & 0 & 0 & ... \\ 0 & a_n & a_{n-1} & ... & a_1 & a_0 & 0 & ... \\ 0 & 0 & a_n & ... & a_2 & a_1 & a_0 & ... \\ ... & ... & ... & ... & ... & ... & ... & ... \\ b_m & b_{m-1} & b_{m-2} & ... & b_0 & 0 & 0 & ... \\ 0 & b_m & b_{m-1} & ... & b_1 & b_0 & 0 & ... \\ 0 & 0 & b_m & ... & b_2 & b_1 & b_0 & ... \\ 0 & 0 & 0 & ... & ... & ... & ... & ... \end{vmatrix}$$

Using Euclidean Division, we may write $f = qg + r$, with $\deg(q) = n - m$, and $r = 0$ or $\deg(r) < m$. If $r = 0, R(f, g) = 0$. If $r \neq 0$ and $\deg(r) = k < m$,

$$R(f, g) = (-1)^{nm} b_m^{n-k} R(g, r).$$

Examples: $\mathrm{Disc}(X^3 + aX + b) = -4a^3 - 27b^2$; $\mathrm{Disc}(X^4 + aX + b) = -27a^4 + 256b^3$; $\mathrm{Disc}(X^4 + aX^2 + b) = 16b(a^2 - 4b)^2$.

We recall that every permutation can be writen as composition of traspositions in many different ways, all of which share the parity of the number of traspositions involved. If a permutation can be written as an even number of traspositions, we say that it is even, with signature +1. If it can be written as an odd number of traspositions, we say that it is odd with signature -1.

Definition: The set of all even permutations in S_n is call A_n with $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.