The Galois group of a polynomial

$\mathbf{K}$ a field, $f \in \mathbf{K}[x]$ a separable monic polynomial, $\mathbf{K}_f = \mathbf{K}[\alpha_1, \ldots, \alpha_n]$ the splitting field of f, $\{\alpha_i\}_i$ zeros of f, $G_f := Gal(\mathbf{K}_f/\mathbf{K})$ the Galois group of f.

Proposition 1. The group G_f permutes the roots of f:
if $\sigma \in G_f$ and $\alpha_i \in Zeros(f)$, then $\sigma(\alpha_i) = \alpha_j \in Zeros(f)$.

There is a homomorphism $\Theta\colon G_f \to S_n$, where S_n is the permutation group of n elements. The homomorphism Θ is injective. Hence $\#G_f$ divides $n!$.

Proposition. $f \in \mathbf{K}[x]$ separable. Then $G_f \cong H \subset S_n$, with H transitive on $\{1, 2, \ldots, n\}$, if and only if f is irreducible over $\mathbf{K}$.

Criterion. $f \in \mathbf{K}[x]$ separable, $char(\mathbf{K}) \neq 2$. Then $G_f \cong A_n$ if and only if $Disc(f)$ is a square in $\mathbf{K}$, where $Disc(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2 \in \mathbf{K}$ (it is G_f-invariant).

Example 1. $\mathbf{K} = \mathbf{Q}$, $f(x) = x^4 - 4 = (x^2 + 2)(x^2 - 2)$;
$\mathbf{K}_f = \mathbf{Q}(\sqrt{2}, i\sqrt{2})$, $G_f \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
Example 2. $\mathbf{K} = \mathbf{Q}$, $f(x) = x^4 - 2$;
$\mathbf{K}_f = \mathbf{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$, $G_f \cong D_4$.

Example 3. (degree 2 case). $f \in \mathbf{K}[x]$ separable of degree 2; $G_f \subset S_2 = \{id, (12)\}$.
(a) $G_f = id \quad \Leftrightarrow \quad [\mathbf{K}_f : K] = 1 \quad \Leftrightarrow \quad \mathbf{K}_f = K$ if and only if f factors in $\mathbf{K}$.
(b) $G_f = S_2 \quad \Leftrightarrow \quad [\mathbf{K}_f : K] = 2$ if and only if K_f is a quadratic extension of $\mathbf{K}$ if and only if f is irreducible over $\mathbf{K}$.

Example 3. (degree 3 case). $f \in \mathbf{K}[x]$ separable of degree 3; $G_f \subset S_3 = \{id, (12), (13, (23), (123), (132)\}$; possible subgroups (up to conjugation): id, S_3, $\{id, (12)\}$, $\{id, (123), (132)\}$.
(a) $G_f = id \quad \Leftrightarrow \quad [\mathbf{K}_f : K] = 1$ if and only if f factors in $\mathbf{K}$.
(b) $G_f = S_3 \quad \Rightarrow f$ is irreducible.
(c) G_f has order 2 $\Rightarrow f$ is a product of a linear and a quadratic polynomial in $K[X]$.
(d) G_f has order 3 and hence $G_f = A_3 \quad \Rightarrow f$ is irreducible.

If $char(K) \neq 2$, we can distinguish between cases (b) and (d) using the discriminant. The Galois group G_f is contained in A_3 if and only if $Disc(f)$ is a square in K.

Excercises from the file Excercises 1.

Let Tr and N denote the trace and norm maps from $\mathbf{F}_{p^m}$ to $\mathbf{F}_p$.
By definition $Tr(x) = \sum_{i=0}^{m-1} \phi^i(x)$ and $N(x) = \prod_{i=0}^{m-1} \phi^i(x)$, where $\phi : \mathbf{F}_{p^m} \longrightarrow \mathbf{F}_{p^m}$ denotes the Frobenius automorphism.

8. (a) Show that for every $a \in \mathbf{F}_{p^m}$ we have $Tr(a) = a + a^p + \ldots + a^{p^{m-1}}$ and $N(a) = a^{1+p+\ldots+p^{m-1}}$.
   (b) Show that the trace is a surjective homomorphism of additive groups. (Hint: estimate the size of the kernel).

(c) Show that the Norm map is a surjective homomorphism $\mathbf{F}_{p^m}^*$ to $\mathbf{F}_p^*$. (Hint: estimate the size of the kernel).

6. Let p and r be distinct primes. Show that p is a primitive root modulo $r \Leftrightarrow \Phi_r(x) := \frac{x^r-1}{x-1}$ is irreducible in $\mathbf{F}_p[X]$.

7. (a) Factor $x^7 - 1$ and $x^{11} - 1$ in $\mathbf{F}_2[x]$.
   (b) Factor $x^{16} - 1$ and $x^{16} - x$ in $\mathbf{F}_2[x]$.