14.6 Galois groups of polynomials.

Recall. For separable $f(x) \in F[x]$ with splitting field K and $f(x) = (x - \alpha_1)\dots(x - \alpha_n)$ over K,

$$\mathrm{Gal}(K/F) \hookrightarrow S_n.$$

Symmetric functions.

S_n acts on the rational function field $F(x_1, \dots, x_n)$ for indeterminates $x_1, \dots, x_n$ via

$$\pi(x_i) = x_{\pi(i)} \quad \text{for } \pi \in S_n, 1 \le i \le n.$$

Ex $\pi\left(\frac{2x_1^3 + 3x_2x_3}{4x_1}\right)$

Definition. $\mathrm{Fix}(S_n) := \{a \in F(x_1, \dots, x_n) : \pi(a) = a \text{ for all } \pi \in S_n\}$ is the set of all *symmetric* rational functions (invariant under permutations of $x_1, \dots, x_n$).

For $1 \le k \le n$ the *k-th elementary symmetric function* of $x_1, \dots, x_n$ is

$$s_k := \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} x_{i_1} \dots x_{i_k} \in \mathrm{Fix}(S_n).$$

Example. $\underbrace{x_1^2 + x_2^2 + \dots + x_n^2}_{s_1^2 - 2s_2} \in \mathrm{Fix}(S_n)$

$s_1 = x_1 + x_2 + \dots + x_n$

$s_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n$

$\vdots$

$s_n = x_1 \cdots x_n$

Theorem. *$F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ is Galois with Galois group S_n, and $F(s_1, \dots, s_n) = \mathrm{Fix}(S_n)$* inside $F(x_1, \dots, x_n)$.

Proof. $F(x_1, \dots, x_n)$ is the splitting field of

$(y - x_1) \cdots (y - x_n) = y^n - s_1 y^{n-1} + s_2 y^{n-2} - \dots + (-1)^n s_n \in F(s_1, \dots, s_n)[y]$

Hence $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ is Galois.

$F(s_1, \dots, s_n) \subseteq \mathrm{Fix}(S_n)$

$|F(x_1, \dots, x_n) : F(s_1, \dots, s_n)| \le n!$

$|F(x_1, \dots, x_n) : \mathrm{Fix}(S_n)| = n!$

yield $\mathrm{Fix}(S_n) = F(s_1, \dots, s_n)$. $\square$

Corollary (Fundamental Theorem of Symmetric Functions)**.** *Every symmetric function in $x_1, \dots, x_n$ is a rational function in $s_1, \dots, s_n$.*

Alternating groups.

$$\begin{array}{ccc} | & & F(x_1,\dots,x_n) \\ | & & | \\ A_n & & \mathrm{Fix}(A_n) \\ | & & | \\ S_n & & F(s_1,\dots,s_n) \end{array} \Big\}\ \text{degree } 2$$

Recall. $\sigma \in A_n$ iff $\operatorname{sign} \sigma = 1$ iff

$$\sigma\Big(\prod_{1\le i<j\le n} (x_i - x_j)\Big) = \prod_{1\le i<j\le n} (x_i - x_j).$$

Thus, if $\mathrm{ch} F \neq 2$, then

$$F(s_1,\dots,s_n) \neq F(s_1,\dots,s_n, \underbrace{\prod_{1\le i<j\le n} (x_i - x_j)}_{\text{not symmetric}}) = \mathrm{Fix}(A_n)$$

Discriminant.

Definition. For $f(x) \in F[x]$ of degree n with roots $\alpha_1,\dots,\alpha_n$ in some splitting field, the *discriminant* is

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

Note.

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in F[x]$$
$$= x^n - \underbrace{s_1(\alpha_1,\dots,\alpha_n)}_{\in F} x^{n-1} + \underbrace{s_2(\alpha_1,\dots,\alpha_n)}_{\in F} x^{n-2} - \dots$$

(1) $D(f) \neq 0$ iff f is separable.
(2) $D(f) \in F$.

Since $D(f)$ is invariant under S_n, it is a rational function of the $s_i(\alpha_1,\dots,\alpha_n)$, hence in F.

Theorem. *Let $f(x) \in F[x]$ be separable of degree n. Then the Galois group of $f(x)$ embeds into A_n iff $x^2 - D(f)$ splits over F.*

Proof. $\sqrt{D(f)} = \prod_{i<j} (\alpha_i - \alpha_j) \in \mathrm{Fix}(A_n)$ □

Galois groups by polynomial degree.

Degree 2. $f(x) = x^2 + bx + c$
$= (x-\alpha)(x-\beta)$
$= x^2 - s_1(\alpha,\beta)\, x + s_2(\alpha,\beta)$

$s_1(\alpha,\beta) = \alpha + \beta$
$s_2(\alpha,\beta) = \alpha\beta$

$$D(f) = (\alpha-\beta)^2 = s_1(\alpha,\beta)^2 - 4 s_2(\alpha,\beta) = b^2 - 4c$$

$f(x)$ is separable iff $D(f) \neq 0$

$$\mathrm{Gal}(F(\alpha,\beta)/F) \cong \begin{cases} 1 & \text{if } \alpha,\beta \in F \\ S_2 & \text{else} \end{cases}$$

$s_1(\alpha,\beta,\gamma) = \alpha+\beta+\gamma$
$s_2(\alpha,\beta,\gamma) = \alpha\beta+\alpha\gamma+\beta\gamma$
$s_3(\alpha,\beta,\gamma) = \alpha\beta\gamma$

Degree 3. $f(x) = x^3 + ax^2 + bx + c$
$\quad = (x-\alpha)(x-\beta)(x-\gamma)$
$\quad = x^3 - s_1x^2 + s_2x - s_3$

$D(f) = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$
$\quad = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$

symmetric, hence polynomial in s_1, s_2, s_3

1) $\alpha,\beta,\gamma \in F$: $\qquad G = 1$

2) $f(x) = (x-\alpha)\,g(x)$ for $\alpha \in F$, $g(x)$ irreducible in $F[x]$: $\qquad G \cong S_2$

3) $f(x)$ irreducible over F:

a) $F(\alpha) = F(\alpha,\beta,\gamma)$: $\qquad G \cong A_3$.
(all roots real, $D(f) > 0$, in $\mathbb{R}$)

b) $F(\alpha) \neq F(\alpha,\beta,\gamma)$: $\qquad G \cong S_3$
(α real, β,γ complex conjugates, $D(f) < 0$ in $\mathbb{R}$)

$$\begin{tikzcd} F(\alpha,\beta,\gamma) \arrow[d, dash, "\le 2"] \\ F(\alpha) \arrow[d, dash, "3"] \\ F \end{tikzcd}$$

Degree 4. see book

The Fundamental Theorem of Algebra.

Recall.

(1) If $f(x) \in \mathbb{R}[x]$ has odd degree, then $f(x)$ has a root in $\mathbb{R}$ (Intermediate Value Theorem).
(2) If $f(x) \in \mathbb{C}[x]$ has degree 2, then $f(x)$ splits (Quadratic Formula).

Fundamental Theorem of Algebra. $\mathbb{C}$ is algebraically closed.

Proof. To show $\overline{\mathbb{R}} = \mathbb{C}$, let $f(x) \in \mathbb{R}[x]$ with splitting field K (may assume that $f(x)$ is squarefree, hence separable).

$$\begin{tikzcd} & K(i) \arrow[d, dash] \\ \mathbb{C} \arrow[ur, dash] \arrow[d, dash] & K \\ \mathbb{R} \arrow[ur, dash] & \end{tikzcd}$$

$K(i)$ is Galois over $\mathbb{R}$.

Let P be the Sylow 2-subgroup of $\mathrm{Gal}(K(i)/\mathbb{R}) =: G$.

Then $|\mathrm{Fix}(P) : \mathbb{R}|$ is odd and $\mathrm{Fix}(P) = \mathbb{R}$ by (1) above.

$$\begin{tikzcd} 1 \arrow[d, dash] & K(i) \arrow[d, dash] \\ P \arrow[d, dash] & \mathrm{Fix}(P) \arrow[d, dash] \\ G & \mathbb{R} \end{tikzcd}$$

Hence G is a 2-group.

Since $\mathbb{C}$ has no quadratic extensions by (2), $K(i) = \mathbb{C}$ and $K \subseteq \mathbb{C}$. $\square$