Galois ~~theory~~ group Galois-style

Galois' original definition of his group.

Ⓓ K a field, $f \in K[x]$ a separable polynomial

$\alpha = (\alpha_1, \dots, \alpha_n) \in \overline{K}^n$ w/ $\{\alpha_1, \dots, \alpha_n\} = f^{-1}(0)$

$K(\alpha) = K(\alpha_1, \dots, \alpha_n)$, $G_f = Aut(K(\alpha)/K)$ Galois gr of f (Artin's def)

$Q_f := Ker(K[x_1, \dots, x_n] \to K(\alpha),\ x_i \mapsto \alpha_i)$ ideal of relations among roots

Ⓟ G_f nat iso to $\Gamma_f = \{\sigma \in S_n \mid \sigma Q_f = Q_f\} = \left\{\sigma \in S_n \,\middle|\, \begin{array}{l} F \in K[x_1, \dots, x_n] \ \&\ F(\alpha_1, \dots, \alpha_n) = 0 \\ \Rightarrow F(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) = 0 \end{array}\right\}$

decomposition group

Pf. $\Gamma_f \xrightarrow{nat} G_f$ iso (EX)

$A = K[s_1, \dots, s_n]$ $\cup$

Ⓓ $s_1, \dots, s_n \in K[x_1, \dots, x_n]$ fund sym polyns, $f = \sum c_{n-i} x^i$ monic, $\underline{P}_f = (s_1 + c_1, s_2 - c_2, \dots)A$

Ⓡ $A = K[s_1, \dots, s_n] \subset K[x_1, \dots, x_n] = B$ is flat (b/c $K[s_1, \dots, s_n]$ is regular) so loc free of rk $n!$ (b/c by Gal th $K(s_1, \dots, s_n) \subset K(x_1, \dots, x_n)$ has deg $n!$) Hence $A/\underline{P}_f \to B/\underline{P}_f B$ loc free of rk $n!$

So $\dim K[x_1, \dots, x_n]/(s_1 + c_1, s_2 - c_2, \dots) = n!$ if $f = x^n + c_1 x^{n-1} + \dots + c_n$.

Ⓡ f sep $\Leftrightarrow$ $Disc^K := \prod (x_i - x_j)^2 \notin \underline{P}_f$.

Ⓡ Have surj

$$\begin{tikzcd} B = K[x_1, \dots, x_n] \arrow[r] \arrow[d] & K(\alpha) \\ \dfrac{B}{\underline{P}_f B} = \dfrac{K[x_1, \dots, x_n]}{(s_1 + c_1, s_2 - c_2, \dots)} \arrow[ur, "\pi"] & \end{tikzcd}$$

Hence π iso $\Longleftrightarrow$ $Q_f = (s_1 + c_1, s_2 - c_2, \dots)B \overset{triv}{=} \underline{P}_f B$

$\Updownarrow$

$[K(\alpha) : K] = n!$

$\Updownarrow$

$G_f \simeq S_n$

Hence $G_f = S_n \Leftrightarrow$ the id Q_f of rel's among roots is gen by the "Viette" rels $s_1 + c_1, s_2 - c_2, \dots$

Ⓡ $B \to \dfrac{B}{Q_f} = K(\alpha)$ induces Kpt $B^{\Gamma_f} \to K(\alpha)^{G_f} = K$ which induces $c: A \to A/\underline{P}_f = K$, So the latter is in the image $(X/\Gamma_f)(K) \to Y(K)$ So the set of all c's w/ Gal gr $\Gamma \subsetneq S_n$ is "thin" (à la Serre)

Ⓡ Q_f lies over $\underline{P}_f$. If Q'_f is another max of B lying over $\underline{P}_f$ then the dec group $\Gamma'_f = \{\sigma \in S_n \mid \sigma Q'_f = Q'_f\}$ is conj to Γ_f in S_n (b/c S_n acts transitively on fibers of $X = \mathrm{Spec}\, B \to \mathrm{Spec}\, A = Y$). So one can define (up to conj in S_n) the Gal gr of f as the dec group of ANY maximal of B lying over $\underline{P}_f$. This is a def that does not involve the roots!!!