§16.2, 16.8, 16.9 Galois groups and the discriminant

How to describe the Galois group $G(\mathbb{K}/\mathbb{F})$ for $\mathbb{K}/\mathbb{F}$ Galois??
It's a bit tricky in general, but there are some things we can say easily.

THEOREM (16.6.6): If $\mathrm{char}(\mathbb{F})=0$ and $\mathbb{K}/\mathbb{F}$ is Galois with $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))$ having roots $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $\alpha_i\in\mathbb{K}$
then $G=G(\mathbb{K}/\mathbb{F})$ permutes $\{\alpha_1,\dots,\alpha_n\}$
giving an injective homomorphism $G\longrightarrow S_n$, i.e. $G\subset S_n$
Furthermore, if $f(x)$ is irreducible, then G is a transitive subgroup of S_n, i.e. G has only one orbit on $\{\alpha_1,\dots,\alpha_n\}$.

proof: We know G must permute $\{\alpha_1,\dots,\alpha_n\}$ since $f(x)\in\mathbb{F}[x]$ so $\sigma(f)=f$ $\forall\sigma\in G=G(\mathbb{K}/\mathbb{F})$.
We also know $\mathbb{K}=\mathbb{F}(\alpha_1,\dots,\alpha_n)$ so every $\sigma\in G$ is determined by how it permutes the $\{\alpha_1,\dots,\alpha_n\}$, giving injectivity. We also know when $f(x)$ is irreducible, so $f(x)=m_{\mathbb{F},\alpha_i}(x)$ for $i=1,\dots,n$, we can find $\sigma_i\in G$ sending $\alpha_1\xmapsto{\sigma_i}\alpha_i$ $\forall i=1,\dots,n$, so there is only one G-orbit. ∎

4/17/2019>

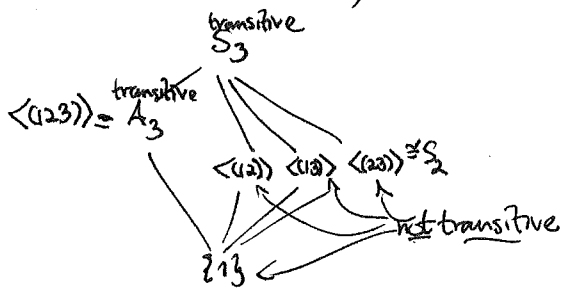
EXAMPLES:

① If $[\mathbb{K}:\mathbb{F}]=2$ then $\mathbb{K}=\mathbb{F}[\sqrt{a}]$ for some $a\in\mathbb{F}$ that is not a square
(since any $\gamma\in\mathbb{K}-\mathbb{F}$ has $m_{\mathbb{F},\gamma}(x)=x^2+bx+c$, so $\gamma=\frac{-b\pm\sqrt{b^2-4c}}{2}$ and $D=b^2-4c$ works)

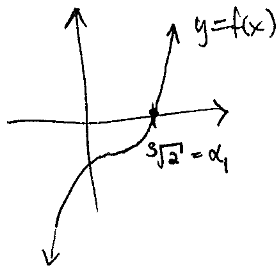
Here $G=\underset{\langle\sigma\rangle}{S_2}$ where $\sigma:\sqrt{D}\mapsto-\sqrt{D}$

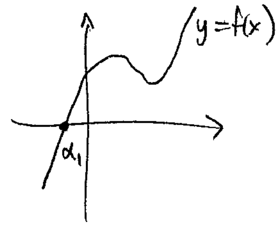
② If $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))$ for some irreducible cubic $f(x)=x^3+bx^2+cx+d\in\mathbb{F}[x]$
$=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\in\mathbb{K}[x]$

then $G=G(\mathbb{K}/\mathbb{F})$ is a transitive subgroup of S_3, so either $A_3=\langle(123)\rangle$ and $[\mathbb{K}:\mathbb{F}]=3$
or S_3 itself and $[\mathbb{K}:\mathbb{F}]=6$



e.g. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, or any $f(x)$ with only one real root,



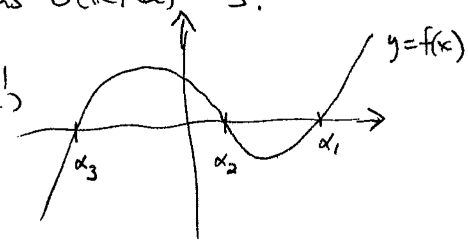


will have $G = S_3$
$\quad\;\, \| $
$G(\mathbb{K}/\mathbb{Q})$ for $\mathbb{K} = \text{split}_{\mathbb{Q}}(f(x))$

since

$\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$
$2 \,|\!\cup\!|$ ← because $\alpha_2, \alpha_3 \notin \mathbb{R} \supset \mathbb{Q}(\alpha_1)$
$\mathbb{Q}(\alpha_1)$
$|3$
$\mathbb{Q}$

<u>And in fact</u>, for <u>most</u> cubics having 3 real roots, one still has $G(\mathbb{K}/\mathbb{Q}) = S_3$.
But, for example, $f(x) = x^3 - 3x + 1$ is <u>very special</u>
(16.8.3) (we'll see <u>how special</u> later...)

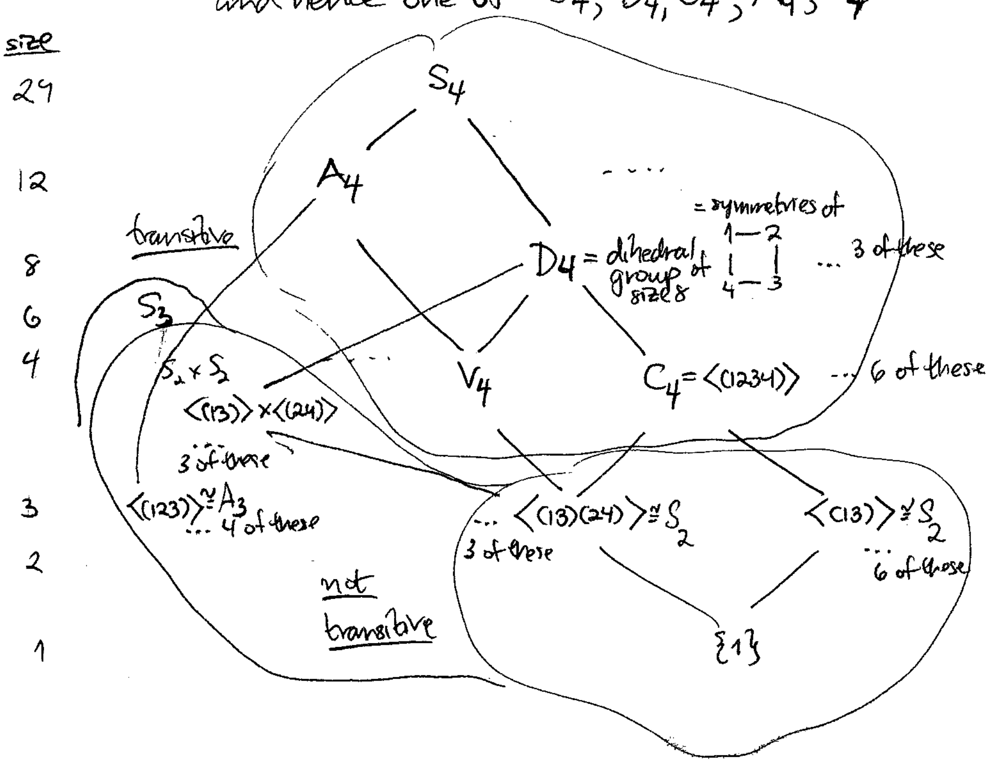


and if α_1 is one of its roots (so $\alpha_1^3 - 3\alpha_1 + 1 = 0$)

then $\left.\begin{array}{l} \alpha_2 = \alpha_1^2 - 2 \\ \alpha_3 = -\alpha_1^2 - \alpha_1 + 2 \end{array}\right\}$ happen to be the other two roots (all real)

and so $\mathbb{K} = \text{split}_{\mathbb{Q}}(f(x)) = \mathbb{Q}(\alpha_1)$, and $[\mathbb{K}:\mathbb{Q}] = 3$, so $G = A_3$.

③ When $\mathbb{K} = \text{split}_{\mathbb{F}}(f(x))$ for an irreducible quartic $f(x) = x^4 + bx^3 + cx^2 + dx + e$,
$G = G(\mathbb{K}/\mathbb{F})$ is a transitive subgroup of S_4,
and hence one of S_4, D_4, C_4, A_4, V_4:



↙ a picture of <u>part of</u> the subgroup poset of S_4

G (= $G(\mathbb{K}/\mathbb{F})$)

There is a convenient test for whether $G \leq A_n$ or not,

and hence whether $G = A_3$ or S_3 for $\deg(f(x)) = 3$

whether $G \in \{A_4, V_4\}$ or $G \in \{C_4, D_4, S_4\}$ for $\deg(f(x)) = 4$.

DEF'N: (16.2.1) Given $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots \pm (-1)^n s_n \in \mathbb{F}[x]$

$= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in \mathbb{K}[x]$ where $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ (= $\text{split}_{\mathbb{F}}(f(x))$)

so that $s_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}$ = k^{th} elementary symmetric function of $\alpha_1, \dots, \alpha_n$

define the discriminant of f

$$D := D(f) := D(\alpha_1, \dots, \alpha_n) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

EXAMPLE: $n=2$, $f(x) = x^2 - s_1 x + s_2 = x^2 + bx + c$

$= (x-\alpha_1)(x-\alpha_2) = x^2 - \underbrace{(\alpha_1+\alpha_2)}_{s_1} x + \underbrace{\alpha_1\alpha_2}_{s_2}$

$D = D(f) = D(\alpha_1, \alpha_2) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2$

$= (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2$ ← as in $x = \frac{-b \pm \sqrt{b^2-4c}}{2}$

$= s_1^2 - 4s_2 = b^2 - 4c$

PROP: $D(f) \in \mathbb{Q}(s_1, \dots, s_n)$, **i.e.** $\exists$ a rational function $\Delta(s_1, \dots, s_n)$ in $s_1, \dots, s_n$ that equals $D(f)$.

($s_1 = \alpha_1 + \dots + \alpha_n$, $s_n = \alpha_1 \cdots \alpha_n$)

(**REMARK:** Actually, $\Delta(s_1, \dots, s_n) \in \mathbb{Z}[s_1, \dots, s_n]$, i.e. it is a polynomial in $s_1, \dots, s_n$, but that is slightly trickier to prove – see Artin Thm 16.A.6)

EXAMPLE: $n=3$, $f(x) = x^3 - s_1 x^2 + s_2 x - s_3 = x^3 + bx^2 + cx + d$

$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

has $D = D(f) = D(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 = \alpha_1^4\alpha_2^2 + \alpha_1^2\alpha_2^4 + \alpha_1^4\alpha_3^2 + \alpha_1^2\alpha_3^4 + \dots$

$= s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 + 18 s_1 s_2 s_3 - 27 s_3^2$ (some brute force algebraic manipulation!)

$= b^2c^2 - 4c^3 - 4b^3 d + 18bcd - 27d^2$

e.g. $f_1(x) = x^3 - 2$ ($b=0, c=0, d=-2$) has $D(f_1) = -27(-2)^2 = -108$, while $f_2(x) = x^3 - 3x + 1$ ($b=0, c=-3, d=1$) has $D(f_2) = -4(-3)^3 - 27(1)^2 = (4-1)3^3 = 3^4$

proof of PROP: Consider the field $\hat{K} = \mathbb{Q}(u_1, \dots, u_n)$ of rational functions in variables $u_1, \dots, u_n$

$\cup$

$\hat{F} = \mathbb{Q}(s_1(\underline{u}), s_2(\underline{u}), \dots, s_n(\underline{u}))$

$s_1(\underline{u}) = u_1 + u_2 + \dots + u_n$

$s_2(\underline{u}) = u_1u_2 + u_1u_3 + \dots + u_{n-1}u_n$

$s_n(\underline{u}) = u_1u_2 \cdots u_n$

and $f(x) = x^n - s_1(\underline{u})x^{n-1} + s_2(\underline{u})x^{n-2} - \dots + (-1)^n s_n(\underline{u}) \in \hat{F}[x]$

$= \mathbb{Q}(s_1(\underline{u}), \dots, s_n(\underline{u}))[x]$

$= (x-u_1)(x-u_2)\cdots(x-u_n)$ in $\hat{K}[x]$, so $\hat{K} = \text{split}_{\hat{F}}(f(x))$

4/19/2019 > Our strategy will be to show two things about the action of S_n on $\hat{K} = \mathbb{Q}(u_1, \dots, u_n)$ by permuting variables: $\sigma(u_i) = u_{\sigma(i)}$ for $\sigma \in S_n$

(i) $\sigma\left(\prod_{1 \le i < j \le n} (u_i - u_j)\right) = \underbrace{\text{sgn}(\sigma)}_{\pm 1} \cdot \prod_{1 \le i < j \le n} (u_i - u_j)$

and hence $\prod_{1 \le i < j \le n} (u_i - u_j)^2 \in \hat{K}^{S_n}$, i.e. it is fixed by all $\sigma \in S_n$

(ii) $\hat{K}^{S_n} = \hat{F}$, so $\prod_{1 \le i < j \le n} (u_i - u_j)^2 \in \mathbb{Q}(s_1(\underline{u}), \dots, s_n(\underline{u}))$ i.e. it is a rational function of $s_1(\underline{u}), \dots, s_n(\underline{u})$.

Checking (i) is easy because each adjacent transposition $(k, k+1)$ will send most factors $u_i - u_j$ ($i<j$) to other factors $u_{i'} - u_{j'}$ ($i'<j'$) with same sign, and it negates one factor: $(k,k+1)(u_k - u_{k+1}) = u_{k+1} - u_k = -(u_k - u_{k+1})$.

Thus $(k,k+1)$ scales $\prod_{i<j} (u_i - u_j)$ by $-1 = \text{sgn}((k,k+1))$, so every $\sigma \in S_n$ scales it by $\text{sgn}(\sigma)$ since $S_n = \langle (1,2), (2,3), \dots, (n-1,n) \rangle$

For (ii), note that

$\hat{K}$

$\cup$ ← degree $n!$ by Fixed Field Thm

$\hat{K}^{S_n}$

$\cup$

$\hat{F}$

(degree $\le n!$ since $\hat{K} = \text{split}_{\hat{F}}(f(x))$)

$\Rightarrow \hat{F} = \hat{K}^{S_n}$ ∎