Following Friedman, Notes Galois Theory IV

E/F splitting field of $f(x) \in F[x]$, roots $\alpha_1 \dots \alpha_n$ in E

$f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) =$

$= x^n - \underbrace{(\alpha_1+\alpha_2+\dots+\alpha_n)}_{= s_1 \text{ (or } e_1)} x^{n-1} + \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n)}_{= s_2} x^{n-2} - \dots + (-1)^n \alpha_1 \dots \alpha_n$.

$s_1 = \alpha_1 + \alpha_2 + \dots + \alpha_n = \sum_{i=1}^{n} \alpha_i$ n terms

$s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n = \sum_{1 \le i < j \le n} \alpha_i\alpha_j$ $\binom{n}{2}$ terms

s_k - k-th elementary symmetric function.

$s_k = \alpha_1\alpha_2\dots\alpha_k + \dots = \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k}$ $\binom{n}{k}$ terms

$s_n = \alpha_1 \dots \alpha_n$ $\pm s_k$ are coefficients of $f(x)$

$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - s_3 x^{n-3} + \dots + (-1)^n s_n = 0$

$G = Gal(E/F)$ acts on α_i's by permutations. preserves s_k.

2 ways to think about this:

I) $\alpha_i \in E$, $s_k \in F$

II) α_i's are formal variables $R = F[\alpha_1 \dots \alpha_n]$

S_n acts on R by permuting α_i

$Sym \subset R$ - ring of symmetric functions $h \in Sym$ iff $\sigma(h) = h$ $\forall \sigma \in S_n$

$s_1 \dots s_n \in R$

<u>Thm</u> $Sym \simeq F[s_1 \dots s_n]$ $s_1 \dots s_n$ are polynomial generators of R.

Example $n=2$ $F[\alpha_1, \alpha_2]$ $s_1 = \alpha_1 + \alpha_2$, $s_2 = \alpha_1 \alpha_2$

$\alpha_1^2 + \alpha_2^2 \in Sym$ $\alpha_1^2 + \alpha_2^2 = (\alpha_1+\alpha_2)^2 - 2\alpha_1\alpha_2 = s_1^2 - 2s_2$ $\Rightarrow$

$(\alpha_1^2+\alpha_2^2)(\alpha_1+\alpha_2) = \underbrace{\alpha_1^3+\alpha_2^3}_{\text{use induction}} + \alpha_1\alpha_2(\alpha_1+\alpha_2)$

$\alpha_1^3 + \alpha_2^3 = (\alpha_1+\alpha_2)^3 - 3\alpha_1\alpha_2(\alpha_1+\alpha_2) = s_1^3 - 3s_1s_2$

Exercise: Prove by induction that $\alpha_1^m + \alpha_2^m \in F[s_1, s_2]$, for all m.

Exercise: Prove the Theorem for $n=2$; for all n.

Ways to get symmetric f's.

Example: start with monomial $\alpha_1^2\alpha_2$, symmetrize $\alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_1^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_3\alpha_2^2$

get a basis in Sym

Back to I). $\alpha_i \in E$. roots of F.

$x^2 + bx + c$ $\alpha_1 + \alpha_2 = -b$, $\alpha_1\alpha_2 = c$ $D = b^2 - 4c = (\alpha_1-\alpha_2)^2$

$\quad ||$ $\sqrt{D} = \pm(\alpha_1 - \alpha_2)$

$(x-\alpha_1)(x-\alpha_2)$ $\uparrow$ depends on labeling $\alpha_1 \leftrightarrow \alpha_2$

$\begin{cases} \alpha_1 - \alpha_2 = \sqrt{D} \\ \alpha_1 + \alpha_2 = -b \end{cases}$

solve for α_1, α_2

$2\alpha_1 = -b + \sqrt{D}$ $\alpha_1 = \frac{-b+\sqrt{D}}{2}$ works unless char $F = 2$

$(\alpha_1 - \alpha_2) = \sqrt{D}$ not in Sym $\sigma = (12)$ $\sigma(\alpha_1-\alpha_2) = \alpha_2 - \alpha_1 = -(\alpha_1 - \alpha_2)$

sign appears

n=3 case

$\alpha_i - \alpha_j$ $i<j$

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

$\sigma = (12)$

$(12).\delta = -\delta$ $\sigma\delta = \mathrm{sgn}(\sigma)\delta$ $\mathrm{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$

Thm let $\delta = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)$. $\delta \in R = F[\alpha_1 \ldots \alpha_n]$.

Then $\sigma\delta = \ldots \operatorname{sgn}(\sigma)\delta$.

Proof: Apply $\tau_i = (i, i+1)$ elementary transposition.

Check that $\alpha_i - \alpha_{i+1}$ changes sign, other terms are permuted.

$\Rightarrow$ $\delta \notin Sym$, $\delta^2 \in Sym$.

$\deg \delta = \binom{n}{2}$ polynomial in $\alpha_1 \ldots \alpha_n$

Let $\Delta = \delta^2 = \left(\prod_{i<j} (\alpha_i - \alpha_j)\right)^2$ discriminant Δ

$\deg \Delta = n(n-1)$

2 ways to think of Δ

I) symmetric function, $\Delta \in Sym$

II) $\Delta \in F$ if $\alpha_1 \ldots \alpha_n \in E$ splitting field as before.

We can write Δ as a polynomial in s_i's (coeff of f), but it's a complicated f'la.

$n=2$ case $\Delta = D = b^2 - 4c = s_1^2 - 4s_2$

different notations $x^2 + bx + c$, $x^2 - s_1 x + s_2$

Want a formula for $\alpha_1 \ldots \alpha_n$.

know symmetric f's $s_1 \ldots s_n$

First step: take $\sqrt{\Delta}$ $F \subset F(\sqrt{\Delta}) \subset E$.

may be $\sqrt{\Delta}$ already in F (usually it's not).

Thm For F, E, α's as above, (& no multiple roots, $\alpha_i \neq \alpha_j$). $\delta = \sqrt{\Delta}$

$G = \mathrm{Gal}(E/F) \subset S_n$. Then $G \subset A_n$ (alternating group) iff $\sqrt{\Delta} \in F$.

$\sigma(\sqrt{\Delta}) = \mathrm{sgn}(\sigma)\sqrt{\Delta}$. if $\sqrt{\Delta} \in F$ $\mathrm{sgn}(\sigma) = 1$ $\forall \sigma \in \mathrm{Gal}(E/F)$

& vice versa.

(This is Prop 10.2 in Friedman NGT IV)

Let's compute discriminant for $n = 3$. Make our life easier by assuming coeff of x^2 is 0.

$f(x) = x^3 + ax^2 + bx + c$ $\quad y = x + \frac{a}{3}$ $\quad$ char $F \neq 3$. relabel y into x

$f(x) = x^3 + px + q$ $\quad p, q \in F$.

$x^3 - \overset{0}{\overset{\shortparallel}{(\alpha_1 + \alpha_2 + \alpha_3)}} x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3$

$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ in splitting field

$\alpha_1 + \alpha_2 + \alpha_3 = 0$ $\leftarrow$ our simplification

$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$

$\alpha_1\alpha_2\alpha_3 = -q$.

$$f'(x) = (x - \alpha_2)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_2)$$

$$f'(\alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$$

$$f'(\alpha_2) = (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)$$

$$f'(\alpha_3) = (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$$

$$f'(\alpha_1) f'(\alpha_2) f'(\alpha_3) = (-1)^3 \Delta(f) = -\Delta(f).$$

$$f'(x) = 3x^2 + p.$$

$$-\Delta(f) = f'(\alpha_1) f'(\alpha_2) f'(\alpha_3) = (3\alpha_1^2 + p)(3\alpha_2^2 + p)(3\alpha_3^2 + p)$$

$$-\Delta(f) = 27\underline{\alpha_1^2\alpha_2^2\alpha_3^2} + 9p\,\underline{(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2)} + 3p^2\,\underline{(\alpha_1^2+\alpha_2^2+\alpha_3^2)} + p^3$$

$$\underline{\alpha_1^2\alpha_2^2\alpha_3^2} = q^2$$

$$0 = (\alpha_1+\alpha_2+\alpha_3)^2 = \alpha_1^2+\alpha_2^2+\alpha_3^2 + 2\underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)}_{=p}$$

$$\underline{\alpha_1^2+\alpha_2^2+\alpha_3^2 = -2p}$$

$$p^2 = (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 = \underline{\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2} + 2(\alpha_1\alpha_2\alpha_3)\underbrace{(\alpha_1+\alpha_2+\alpha_3)}_{=0}$$

$$= \underline{\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2}$$

$$-\Delta(f) = 27q^2 + 9p\,p^2 + 3p^2(-2p) + p^3 = 27q^2 + 4p^3$$

$$\boxed{\Delta = \Delta(f) = -4p^3 - 27q^2}$$

Δ - degree 6 in $\alpha_1, \alpha_2, \alpha_3$

p - degree 2

q - degree 3.

(and $\alpha_1+\alpha_2+\alpha_3 = 0$)

only way to get to deg 6 is via p^3 or q^2.

$4 = 2^2$, $27 = 3^3$

<u>Example</u> 1) $f = x^3 - 2$ $\quad G = S_3$ $\quad \Delta = -27(-2)^2 = -27\cdot 4 = -3(6^2)$.

$p = 0,\ q = -2$ $\quad \leftrightarrow \quad \underline{\sqrt{\Delta} \notin \mathbb{Q}}$

2) $f = x^3 - 3x + 1$ $\quad$ irreducible$/\mathbb{Q}$ by rat. roots test

$p = -3,\ q = -1$ $\quad \Delta = +4\cdot 27 - 27 = 3\cdot 27 = 9^2$ $\quad \Rightarrow \sqrt{\Delta} = 9 \in F = \mathbb{Q}$

$\Rightarrow G = C_3$ cyclic ($C_3 \cong A_3$).

Most of the time $\sqrt{\Delta} \notin \mathbb{Q}$ & $G = S_3$.

Vandermonde determinant

$$\begin{pmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{pmatrix} = \alpha_2 - \alpha_1$$

$$A = \begin{pmatrix} 1 & \cdots & & 1 \\ \alpha_1 & \alpha_2 & & \alpha_n \\ \alpha_1^2 & & & \\ \vdots & & & \\ \alpha_1^{n-1} & & & \alpha_n^{n-1} \end{pmatrix}$$

det A - polyn in $\alpha_1 \ldots \alpha_n$ of deg $0+1+\cdots+n-1 = \frac{n(n-1)}{2} = \binom{n}{2}$.

$\alpha_i - \alpha_j \mid \det A$ since $\det(A_{\alpha_i = \alpha_j}) = 0$.

$\Rightarrow \prod_{i<j} (\alpha_i - \alpha_j) \mid \det A \Rightarrow \det A = \lambda \cdot \prod_{i<j} (\alpha_i - \alpha_j)$

same deg

$\alpha_1^{n-1} \alpha_2^{n-2} \cdots \alpha_{n-1}$ enters $\prod_{i<j} (\alpha_i - \alpha_j)$ coeff 1

$\lambda = (-1)^{\binom{n}{2}}$

coeff in det A is $\binom{n}{2}$

$$\begin{pmatrix} & & \cdot \\ & \cdot & \\ \cdot & & \end{pmatrix}$$

Thm $\det A = (-1)^{\binom{n}{2}} \prod_{i<j} (\alpha_i - \alpha_j) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$