Recall the discriminant of a (monic) polynomial f

w/ roots $\alpha_1, \ldots, \alpha_n$ is $\prod_{i<j} (\alpha_i - \alpha_j)^2 = \Delta(\alpha_1, \ldots, \alpha_n)$

Our goal is to compute this in terms of the coefficients

of f.

Thm. (Vieta's formulas)

$$f(t) = \prod_{i=1}^{n} (t-\alpha_i) = \sum (-1)^j s_j(\alpha_1, \ldots, \alpha_n) t^{n-j}$$

where $s_j(t_1, \ldots, t_n) = \sum_{1 \le i_1 < \ldots < i_j \le n} t_{i_1} \cdots t_{i_n}$

e.g. $s_1 = t_1 + \ldots + t_n$

$$\begin{aligned} s_2 = \; & t_1 t_2 + \ldots + t_1 t_n \\ & + \ldots + t_2 t_n \\ & + \ldots + t_3 t_n \\ & \ldots t_{n-1} t_n \end{aligned}$$

$\vdots$

$s_n = t_1 \cdots t_n$

e.g. $(t-\alpha_1)(t-\alpha_2) = t^2 - (\alpha_1 + \alpha_2) t + \alpha_1 \alpha_2$

Thus, we may write the coefficients as elementary symmetric polynomials (up to a sign) in the roots. We seek to reverse this.

Thm (Fundamental theorem of elementary symmetric polynomials)

Let $p \in R[t_1, -, t_n]$ be a symmetric polynomial,

i.e. $\forall \sigma \in S_n$, $p(t_{\sigma(1)}, \dots, t_{\sigma(n)}) = p(t_1, \dots, t_n)$.

Then $\exists! \, q \in R[t_1, -, t_n]$ s.t. $p = q(s_1, -, s_n)$ the elementary symmetric polynomials.

Abstractly, S_n acts on $R[t_1, -, t_n]$, so this says that $R[t_1, -, t_n]^{S_n} = R[s_1, -, s_n]$, a free polynomial ring in n generators ($t_i \mapsto s_i$ is an iso).

e.g. $t_1^3 + t_2^3 = (t_1 + t_2)^3 - 3 t_1 t_2 (t_1 + t_2)$

$= s_1(t_1, t_2)^3 - 3 s_2(t_1, t_2) s_1(t_1, t_2)$

$p = t_1^3 + t_2^3 \longleftrightarrow q = t_1^3 - 3 t_2 t_1$

So any symmetric polynomial in the roots of f will be a polynomial in the coefficients of f

$\Delta(\alpha_1, -, \alpha_n)$ is a symmetric polynomial in the α_i,

so there must be some way to write Δ as a polynomial in the coefficients of f.

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

Then $\det(A) = \prod_{i<j} (\alpha_j - \alpha_i)$

So $\det(A)^2 = \Delta$,

Then $\det(AA^t) = \Delta$,

We compute $(AA^t)_{ij} = (\alpha_1^{i-1} \cdots \alpha_n^{i-1}) \begin{pmatrix} \alpha_1^{j-1} \\ \vdots \\ \alpha_n^{j-1} \end{pmatrix}$

$$= \alpha_1^{i+j-2} + \alpha_2^{i+j-2} + \cdots + \alpha_n^{i+j-2}$$

Let $e_i(t_1, \ldots, t_n) = \sum_{j=1}^{n} t_j^i$

Then $(AA^t)_{ij} = e_{i+j-2}(\alpha_1, \ldots, \alpha_n)$

$$AA^t = \begin{pmatrix} e_0^{(=n)} & e_1 & \cdots & e_{n-1} \\ e_1 & e_2 & \cdots & e_n \\ \vdots & \vdots & \ddots & \vdots \\ e_{n-1} & e_n & \cdots & e_{2n-2} \end{pmatrix}$$

Critically, the e_i are symmetric polynomials, so they must be polynomials in the s_i.

Thus, $e_i(\alpha_1, \dots, \alpha_n)$ is a polynomial in $s_i(\alpha_1, \dots, \alpha_n)$, the coefficients of f.

This affords a method to compute Δ in terms of the coefficients of f.

Newton identities

$$e_1 = s_1$$

$$e_2 = \sum t_i^2 = \Big(\sum t_i\Big)^2 - 2\sum_{i<j} t_i t_j$$

$$= s_1^2 - 2 s_2$$

$$= s_1 e_1 - 2 s_2$$

$$e_3 = \sum t_i^3 = \Big(\sum t_a^2\Big)\Big(\sum t_b\Big) - \Big(\sum t_c\Big)\Big(\sum_{d<e} t_d t_e\Big) + 3\sum_{f<g<h} t_f t_g t_h$$

$$= e_2 \cdot s_1 - e_1 \cdot s_2 + 3 s_3$$

From there, we can compute some small degree discriminants.

$n=2$, $f = t^2 + a_1 t + a_0 = (t-\alpha_1)(t-\alpha_2)$

$$= t^2 - (\alpha_1 + \alpha_2) t + \alpha_1 \alpha_2$$

$$= t^2 - s_1(\alpha_1, \alpha_2) t + s_2(\alpha_1, \alpha_2)$$

$$\Delta(\alpha_1, \alpha_2) = \det \begin{pmatrix} 2 & e_1(\alpha_1, \alpha_2) \\ e_1(\alpha_1, \alpha_2) & e_2(\alpha_1, \alpha_2) \end{pmatrix}$$

$$e_1(\alpha_1,\alpha_2) = s_1(\alpha_1,\alpha_2) = -a_1$$

$$e_2(\alpha_1,\alpha_2) = s_1(\alpha_1,\alpha_2)^2 - 2s_2(\alpha_1,\alpha_2)$$

$$= a_1^2 - 2a_0$$

so $$\Delta(\alpha_1,\alpha_2) = \det\begin{pmatrix} 2 & e_1 \\ e_1 & e_2 \end{pmatrix}$$

$$= \det\begin{pmatrix} 2 & -a_1 \\ -a_1 & a_1^2 - 2a_0 \end{pmatrix}$$

$$= 2a_1^2 - 4a_0 - a_1^2$$

$$= a_1^2 - 4a_0$$

Thm (Newton identities).

$$\forall j \quad \sum_{i=0}^{j} (-1)^i s_i e_{j-i} + (-1)^j s_j \cdot j = 0$$

So we can recursively determine a formula for the e's in terms of the s's.

pf. Use the formal identity $p(x) = \prod_{i=1}^{n} (x - t_i) = \sum_j (-1)^j s_j x^{n-j}$.

Then $p'(x) = \sum_j (-1)^j (n-j) s_j x^{n-j-1}$

and $$\frac{p'(x)}{p(x)} = \sum_i \frac{1}{x - t_i} = \sum_{i=1}^{n} \sum_{k \geq 0} \frac{t_i^k}{x^{k+1}}$$

Then we also have

$$p'(x) = p(x)\frac{p'(x)}{p(x)} = p(x)\sum_{i=1}^{n}\sum_{k\geq 0}\frac{t_i^k}{x^{k+1}}$$

$$= p(x)\sum_k \frac{e_k}{x^{k+1}}$$

$$= \left(\sum_i (-1)^i s_i x^{n-i}\right)\left(\sum_k \frac{e_k}{x^{k+1}}\right)$$

$$= \sum_{k,i} (-1)^i s_i e_k x^{n-i-k-1}$$

$$(j = k+i) \qquad = \sum_j \left(\sum_i (-1)^i s_i e_{j-i}\right) x^{n-j-1}$$

So $$\sum_j \left(\sum_i (-1)^i s_i e_{j-i}\right) x^{n-j-1} = \sum_j (-1)^j (n-j) s_j x^{n-j-1}$$

Thus $\forall j$ $$\sum_i (-1)^i s_i e_{j-i} = (-1)^j (n-j) s_j \qquad \square$$

Rmk. For a matrix A with eigenvalues $\lambda_1, \dots, \lambda_n$, we have that $tr(A^k) = e_k(\lambda_1, \dots, \lambda_n)$. Thus, the Newton identities relate $tr(A^k)$ to the coefficients of the characteristic polynomial of A.

$$\left(\chi_A(t) = \sum_i (-1)^i tr(\underbrace{\Lambda^k A}_{\text{exterior product}}) t^{n-i}, \text{ where } tr(\Lambda^k A) = s_k(\lambda_1, \dots, \lambda_n)\right)$$

Application to Galois theory

Let $\mathrm{char}(F) \neq 2$, K/F the splitting field of f, suppose K/F is also separable.

Then $G(K/F) \hookrightarrow \Sigma(\{\alpha_1, \ldots, \alpha_n\})$

$$\begin{array}{c} \Sigma(\{\alpha_1, \ldots, \alpha_n\}) \\ \| ? \\ S_n \end{array}$$

$G(K/F) \hookrightarrow S_n$

Let $d(\alpha_1, \ldots, \alpha_n) = \prod_{i<j} (\alpha_i - \alpha_j)$

Then $\sigma(d(\alpha_1, \ldots, \alpha_n)) = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$

$= \mathrm{sgn}(\sigma)\, d(\alpha_1, \ldots, \alpha_n)$

Thus, $\sigma(d(\alpha_1, \ldots, \alpha_n)) = \begin{cases} d(\alpha_1, \ldots, \alpha_n) & \sigma \mapsto A_n \\ -d(\alpha_1, \ldots, \alpha_n) & \sigma \not\mapsto A_n \end{cases}$

And $\sigma(\Delta(\alpha_1, \ldots, \alpha_n)) = \Delta(\alpha_1, \ldots, \alpha_n)$.

Hence i) $\Delta \in K^{G(K/F)} = F$

ii) $d \in F \iff \sigma(d) = \sigma \ \forall \sigma \in G(K/F)$

$\iff G(K/F) \hookrightarrow A_n$

e.g. Let f be irreducible and separable of degree 3,

Then let K/F its splitting field.

$G(K/F) \hookrightarrow S_3$, an order 3 (transitive) subgroup,

so $G(K/F)$ has image A_3 or S_3

$G(K/F) \xrightarrow{\sim} A_3 \iff \Delta(f)$ is a square in F

$G(K/F) \xrightarrow{\sim} S_3 \iff \Delta(f)$ is not a square in F

For instance, take $F = \mathbb{Q}$, $f = t^3 - a$ for $a \in \mathbb{Z}$ not a cube. Then f is irred and sep$/\mathbb{Q}$ and it has splitting field $K = \mathbb{Q}(\sqrt[3]{a}, \zeta_3)$

Fact, $\Delta(f) = -27a^2$.

This is never a square

$$G(K/\mathbb{Q}) \xrightarrow{\sim} S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$$

$$\sigma(\sqrt[3]{a}) = \zeta_3 \sqrt[3]{a}$$
$$\sigma(\zeta_3) = \zeta_3$$
$$\tau(\sqrt[3]{a}) = \sqrt[3]{a}$$
$$\tau(\zeta_3) = \zeta_3^{-1}$$

e.g. $F = \mathbb{R}$, $f(t) = t^2 + a_1 t + a_0$. As a Gal, $\Delta(f) = a_1^2 - 4a_0$,

so $\Delta \in \mathbb{R}^2 \iff \Delta \geq 0 \iff a_1^2 - 4a_0 \geq 0$.

Let K be the splitting field $G(K/\mathbb{R}) \cong \begin{cases} S_2 & a_1^2 - 4a_0 < 0 \rightarrow K = \mathbb{C} \\ \{1\} & a_1^2 - 4a_0 \geq 0 \rightarrow K = \mathbb{R} \end{cases}$