Final Exam:

Time: Tuesday 5PM – 7PM.

Exam has two parts
- in-class component
- take-home component
- practice exam coming soon!

Today: Using Galois Theory to solve cubic equations

Ex: What are the roots of $\boxed{f(x) = x^3 - 4x + 7}$
or more generally the roots of

$$f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$$

E = splitting field of $f(x)$
$G = G(E/\mathbb{Q})$ = Galois group of $f(x)$

If $\lambda_1, \lambda_2, \lambda_3$ are the roots of $f(x)$, then

$$E = \mathbb{Q}[\lambda_1, \lambda_2, \lambda_3]$$

Moreover, we know that G permutes the roots: if $\sigma \in G$, then $\sigma(\lambda_i) \in \{\lambda_1, \lambda_2, \lambda_3\}$ $\forall\, i = 1,2,3$.
$G \longrightarrow S_3$ Generically, this is an isomorphism!

For all but very special combos of a, b, c,

$$G \cong S_3 \quad \text{and} \quad [E:\mathbb{Q}] = |S_3| = 6$$

$$
\begin{array}{c}
G \cong S_3 \\
| \\
\langle \sigma \rangle \cong A_3 \\
| \\
\{e\}
\end{array}
\qquad\qquad
\begin{array}{rl}
\left.\begin{array}{l} E = K[y] \\ \mid \leftarrow \text{deg } 3 \text{ ext} \\ K = E^{\sigma} \end{array}\right\} A_3 & y \in E,\ y^3 \in K \\
& K = \mathbb{Q}[y^3] \\
\left.\begin{array}{l} \mid \leftarrow \text{deg } 2 \text{ ext} \\ \mathbb{Q} \end{array}\right\} S_3/A_3 &
\end{array}
$$

$$S_3 = \langle (123), (12) \rangle \qquad \sigma : \begin{array}{l} \lambda_1 \mapsto \lambda_2 \\ \lambda_2 \mapsto \lambda_3 \\ \lambda_3 \mapsto \lambda_1 \end{array}$$

$$G = \langle \sigma, \tau \rangle$$

$$\tau : \begin{array}{l} \lambda_1 \mapsto \lambda_2 \\ \lambda_2 \mapsto \lambda_1 \\ \lambda_3 \mapsto \lambda_3 \end{array}$$

$$y \in E, \quad y^3 \in K, \quad E = K[y]$$

$$K = E^{\sigma} \qquad \sigma(y^3) = y^3$$

$$\sigma(y)^3 = y^3 \qquad (\sigma(y)/y)^3 = 1$$

- $\sigma(y)/y = 1$ or $\sigma(y)/y = e^{2\pi i/3}$ or $\sigma(y)/y = e^{4\pi i/3}$

$$\zeta_3 := e^{2\pi i/3} \qquad \sigma(y) = \zeta_3^m y \text{ for } m = 0, 1, 2$$

Looking for some $y \in E = \mathbb{Q}[\lambda_1, \lambda_2, \lambda_3]$ satisfying

$$\sigma(y) = \zeta_3^m y \quad \text{for some } m$$

Remember $\sigma : \{\lambda_1, \lambda_2, \lambda_3\} \to \{\lambda_1, \lambda_2, \lambda_3\}$

$$\operatorname{span}_{\mathbb{Q}}\{\lambda_1, \lambda_2, \lambda_3\} \longrightarrow \operatorname{span}_{\mathbb{Q}}\{\lambda_1, \lambda_2, \lambda_3\}$$

$$\operatorname{span}_{\mathbb{Q}}\{\lambda_1,\lambda_2,\lambda_3\} \cong \mathbb{Q}^3$$

$$a\lambda_1 + b\lambda_2 + c\lambda_3 \longmapsto \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

$$\sigma(\lambda_1) = \lambda_2$$
$$\sigma(\lambda_2) = \lambda_3$$
$$\sigma(\lambda_3) = \lambda_1$$

$$\rightsquigarrow \boxed{\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}$$

$$\begin{bmatrix} a \\ d \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Eigenvectors + eigenvalues?

$$p(x) = \det\left(\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} - x\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right)$$

$$= \det\begin{bmatrix} -x & 0 & 1 \\ 1 & -x & 0 \\ 0 & 1 & -x \end{bmatrix} = -x((-x)^2) + 1$$

$$= -x^3 + 1 = 0$$

Roots are $x = 1$, $x = \zeta_3$, $x = \zeta_3^2$

$$\mathcal{E}_1 = \operatorname{span}\left\{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}\right\} \longleftrightarrow \underline{\lambda_1 + \lambda_2 + \lambda_3} = y_0$$

$$\mathcal{E}_{\zeta_3} = \operatorname{span}\left\{\begin{bmatrix} 1 \\ \zeta_3^2 \\ \zeta_3^1 \end{bmatrix}\right\} \longleftrightarrow \underline{\lambda_1 + \zeta_3^2\lambda_2 + \zeta_3^1\lambda_3} = y_2$$

$$\zeta_3 = e^{2\pi i/3}$$

$$\mathcal{E}_{\zeta_3^2} = \operatorname{span}\left\{\begin{bmatrix} 1 \\ \zeta_3^1 \\ \zeta_3^2 \end{bmatrix}\right\} \longleftrightarrow \lambda_1 + \zeta_3^1\lambda_2 + \zeta_3^2\lambda_3 = y_1$$

Define: $y_m := \lambda_1 + \zeta_3^m \lambda_2 + \zeta_3^{2m} \lambda_3$

$$\sigma(y_m) = \sigma(\lambda_1 + \zeta_3^m \lambda_2 + \zeta_3^{2m}\lambda_3)$$

$$= \sigma(\lambda_1) + \sigma(\zeta_3^m)\sigma(\lambda_2) + \sigma(\zeta_3^{2m})\sigma(\lambda_3)$$

$$= \lambda_2 + \zeta_3^m \lambda_3 + \zeta_3^{2m} \lambda_1$$

$$= \zeta_3^{2m}(\lambda_1 + \zeta_3^m \lambda_2 + \zeta_3^{2m}\lambda_3)$$

$$\boxed{\sigma(y_m) = \zeta_3^{2m} y_m}$$

$$\begin{array}{ll} & E = K[y_1] \\ \deg 3 & \quad | \\ & K = E^{\sigma} = \mathbb{Q}[y_1^3] \\ \deg 2 & \quad | \\ & \mathbb{Q} = K^{\tau} \end{array}$$

Notice: y_m^3 is a root of

$$x^2 - \underbrace{(y_m^3 + \tau(y_m^3))}_{\tilde{b}} x + \underbrace{y_m^3 \tau(y_m)^3}_{\tilde{c}}$$

Also since $\sigma(y_m^3) = y_m^3$, and $\langle\sigma\rangle \trianglelefteq G$

$$\sigma(\tau(y_m^3) + y_m^3) = \tau(y_m^3) + y_m^3$$

$$\sigma(y_m^3 \tau(y_m)^3) = y_m^3 \tau(y_m^3)$$

$$\tau(\tau(y_m^3) + y_m^3) = \tau(y_m^3) + y_m^3$$

$$\tau(\tau(y_m^3)\,y_m^3) = \tau(y_m^3)\,y_m^3$$

So both $\tilde{b}$ and $\tilde{c}$ are fixed by σ, τ and $\langle \tau, \sigma \rangle = G$ so

$$\tilde{b}, \tilde{c} \in E^G = \mathbb{Q}$$

$\therefore$ $\tilde{b}, \tilde{c}$ rational!

y_m^3 is a root of $x^2 - \tilde{b}x + \tilde{c} = 0$

$$y_m^3 = \frac{\tilde{b} \pm \sqrt{\tilde{b}^2 - 4\tilde{c}}}{2} \Rightarrow y_m = \sqrt[3]{\frac{\tilde{b} \pm \sqrt{\tilde{b}^2 - 4\tilde{c}}}{2}}$$

$$\begin{cases} y_0 = \lambda_1 + \lambda_2 + \lambda_3 \\ y_1 = \lambda_1 + \zeta_3 \lambda_2 + \zeta_3^2 \lambda_3 \\ y_3 = \lambda_1 + \zeta_3^2 \lambda_2 + \zeta_3 \lambda_3 \end{cases} \qquad \zeta_3 + \zeta_3^2 + 1 = 0$$

$$y_0 + y_1 + y_2 = 3\lambda_1$$

Root: $\dfrac{y_0 + y_1 + y_2}{3}$

Method for finding a root of

$$f(x) = x^3 + ax^2 + bx + c$$

(1) For each $m = 0, 1, 2$ calculate

$$y_m = \lambda_1 + \zeta_3^m \lambda_2 + \zeta_3^{2m} \lambda_3$$

by finding $\tilde{b}$ and $\tilde{c}$ and getting the root of $x^2 - \tilde{b}x + \tilde{c}$

and taking its cube root!

(2) $$\lambda_1 = \frac{y_1 + y_2 + y_3}{3}.$$

In practice, the values of $\tilde{b}, \tilde{c}$ (and therefore y_k's) can be written in terms of the coefficients of $f(x) = x^3 + ax^2 + bx + c$

$$f(x) = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

$$= x^3 - (\lambda_1+\lambda_2+\lambda_3)x^2 + (\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3)x - \lambda_1\lambda_2\lambda_3$$

$$\Rightarrow y_1 = \lambda_1 + \lambda_2 + \lambda_3 = -a.$$

y_1 is a root of

$x^2 - \tilde{b}x + \tilde{c}$

$$\tilde{b} = y_1^3 + \tau(y_1^3) \in \mathbb{Q}$$
$$\tilde{c} = y_1^3 \tau(y_1^3) \in \mathbb{Q}$$

$$G = \langle \sigma, \tau \rangle$$

$$y_1 = \lambda_1 + \xi_3\lambda_2 + \xi_3^2\lambda_3$$

$$y_1^3 = (\lambda_1 + \xi_3\lambda_2 + \xi_3^2\lambda_3)^3 + \tau(\lambda_1 + \xi_3\lambda_2 + \xi_3^2\lambda_3)^3$$

$$(\lambda_1 + \xi_3\lambda_2 + \xi_3^2\lambda_3)^3 + (\lambda_2 + \xi_3^2\lambda_1 + \xi_3\lambda_3)^3$$