Feb 16

Fix a ground field F.
Every finite seperable extension is $F(u)$ for some u. In particular every Galois extension is the splitting field of some irreducible polynomial.

Given $f(x) \in F[x]$ seperable irreducible polynomial of degree n.

$$G = Gal(f) = Gal(\text{any splitting field of } f)$$

General Comments

f has exactly n roots, G permutes them transitively and faithfully.

$$G \hookrightarrow S_n$$

Orbit - Stabilizer Theorem

$$\#G = \#(\text{stabilizer of any root})\, n$$

Proposition

Let $F \subset \mathbb{R}$ e.g $F \subset \mathbb{Q}$
Suppose degree $f = p$ prime.
Suppose f has exactly $p-2$ real roots
Then $G = S_p$.

proof

complex conjugaison obviously $\in G$.

$\curvearrowright$ a 2-cycle in S_p.

p divides $\#G$, $\exists$ an element of order p.
The only elements of S_p of order p are p-cycles.

$$\langle \text{any 2-cycle} + \text{any } p\text{-cycle} \rangle = S_p$$

What are possible Galois groups by $\deg f$?

$\deg f = 2$ $\quad G = \mathbb{Z}/2 = S_2$

$\deg f = 3$ $\quad G = S_3$ or A_3

Pick ordering of roots of f $\quad \alpha_1, \alpha_2 \dots, \alpha_n$

$$\Delta_f := \prod_{i<j} (\alpha_i - \alpha_j)$$

(remark: $f(x) \longmapsto f(x-a)$ doesn't change Δ)

If $g \in G$, $g\Delta = \pm \Delta$ $\quad \begin{cases} +\Delta & G \text{ alternating subgroup} \\ -\Delta & G \text{ not alternating subgroup} \end{cases}$

We learn:
discriminant $\mathcal{D} = \Delta^2$ is G-invariant
Δ is G-invariant iff $G \subseteq A_n$

$F \hookrightarrow E$ Galois so G-invariant $\longleftrightarrow$ in F

Why? $\mathcal{D} \in F$, $\sqrt{\mathcal{D}} \in F$ iff $G \subseteq A_n$

Example $\quad f(x) = x^2 + bx + c \qquad \Delta = \sqrt{b^2 - 4c}$

Suppose char $F \neq 2$
$f(x) \rightsquigarrow f(x - \frac{b}{2})$

$$f = x^2 - \cancel{xb} + \frac{b^2}{4} + \cancel{bx} - \frac{b^2}{2} + c = x^2 - \frac{b^2}{4} + c$$

$$x = \pm \sqrt{\frac{b^2}{4} - c}$$

Cubic $\quad f(x) = x^3 + ax^2 + bx + c \qquad$ char $\neq 2, 3$
$f(x) \rightsquigarrow f(x - \frac{a}{3}) = x^3 + px + q$

$$\Delta^2 = -4p^3 - 27q^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = \mathcal{D}$$

$x^3 + px + q = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$= x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)x - \alpha_1\alpha_2\alpha_3$

Example $x^3 - 3x + 1$

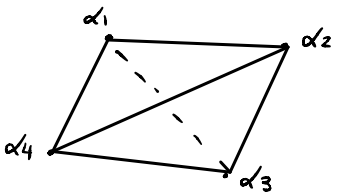
$D = -4(-3)^3 - 27(1)^2 = 81 \qquad \Delta = \sqrt{D} \in \mathbb{Q}$

G in this case is A_3

$\mathbb{Q}(\alpha)$ is splitting field

Quartics

$\deg f = 4$



← has S_4 as rotations
also A_4

There is a group homomorphism

$$(\mathbb{Z}/2)^2 = \left\{ \begin{matrix} 1 \\ (12)(34) \\ (13)(24) \\ (14)(23) \end{matrix} \right\} \longrightarrow S_4 \twoheadrightarrow S_3$$

ker

$S_4 \cong (\mathbb{Z}/2)^2 \times S_3$

$A_4 \cong (\mathbb{Z}/2)^2 \times A_3$

$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$

$\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$

$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$

$G \subseteq S_4$ permutes the β_i's via this homomorphism

$g(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3) \in F[x]$ (called <u>resolving cubic</u> of f)

What are the possible Galois groups?

$G \subset S_4$ acting transitively

So, G is

- A_4
- S_4
- $(\mathbb{Z}/2)^2$

} normal transitive subgroups ($(\mathbb{Z}/2)^2 \subseteq A_4, S_4, D_8$)

- $C_4 = \mathbb{Z}_4$ (three of these all conjugate)
- D_8 (dihedral group of order 8, also three of these all conjugate)

} non-normal

$F \subset K$ = splitting field of g $\subset E$ = splitting field of f
$= F(\beta_1, \beta_2, \beta_3)$ $= F(\alpha_1, \dots, \alpha_4)$

$G = Gal(E/F) \subseteq S_4$
image of G under $S_3 \longrightarrow S_4 = Gal(K/F) \subset S_3$
$G \cap (\mathbb{Z}/2)^2 = Gal(E/K)$

$G = S_4$ iff $Gal(K/F) = S_3 \longleftrightarrow \sqrt{\text{disc of } g} \notin F$
$G = A_4$ iff $Gal(K/F) = A_3 \longleftrightarrow [K:F] = 3$
$G = (\mathbb{Z}/2)^2$ iff $Gal(K/F) = 1 \longleftrightarrow \beta_1, \beta_2, \beta_3 \in F$
$G = C_4$ or D_8 iff $Gal(K/F) = 2\text{-cycles}$ $\beta_1 \in 1$

Feb 18

Char = 0 (automatically seperable)

Let $K \subset L$ be any finite field extension. Pick an algebraic closure $\bar{K}$.
I can look at $\hom_K(L, \bar{K})$ $\circlearrowleft$ $Gal(\bar{K}/K)$
$\cong$
$Gal(\bar{K}/K) / Gal(\bar{K}/L) = X$

Given $u \in L$,
$Tr_K^L(u) = \sum_{\varphi: L \to \bar{K}} \varphi(u)$
$N_K^L(u) = \prod_{\varphi: L \to \bar{K}} \varphi(u)$
} obviously both Galois and invariant so $\in K$

L = $\bar{K}$-valued functions on X equiv for $Gal(\bar{K}/K)$

$K = \mathbb{R}$ $L \cong \mathbb{C}$ $\bar{K} = \mathbb{C}$ $X =$ . . $u \longmapsto (u, \bar{u})$ as fct
$Tr(u) = 2Re(u)$ $N(u) = \|u\|^2$

Study <u>cyclic extensions</u> : Galois extensions $K \subset L$ such that $Gal(L/K) \cong \mathbb{Z}/n$

<u>Remark</u> If $K \subset L$ Galois, then Tr and N are Σ and Π indexed by $Gal(L/K)$.
$N(u) = \prod_{\sigma \in Gal(L/K)} \sigma(u)$

In general, if $K \subset L$ separable, $\#\hom(L, \overline{K}) = [L:K]$

$\|$

$\mathrm{Gal}(\overline{K}/K) / \mathrm{Gal}(\overline{K}/L)$

Let $K \subset L$ cyclic, $\mathrm{Gal} = \langle \sigma \rangle$ $\quad \sigma^m = id$

Pick $v \in L^\times$, $\dfrac{\sigma(v)}{v} = \begin{cases} 1 & \text{iff } v \in K \\ \text{some element of } L^\times \end{cases}$

$$1 \longrightarrow K^\times \longrightarrow L^\times \xrightarrow{\;v \mapsto \frac{\sigma(v)}{v}\;} L^\times \longrightarrow K^\times$$

($\sigma \mapsto id$)

$$N\left(\frac{\sigma(v)}{v}\right) = \frac{\sigma(v)}{v}\,\sigma\left(\frac{\sigma(v)}{v}\right)\,\sigma^2\left(\frac{\sigma(v)}{v}\right) \cdots \sigma^{n-1}\left(\frac{\sigma(v)}{v}\right) = 1$$

Theorem (Hilbert 90)

If $u \in L^\times$ such that $N(u) = 1$, then $\exists v$ such that $u = \dfrac{\sigma(v)}{v}$

$$\longrightarrow \frac{\ker(N)}{\mathrm{Im}\left(v \mapsto \frac{\sigma(v)}{v}\right)} = \{1\} \quad \text{trivial}$$

$\|$

$H^1(\;)$

Special Case of Theorem of Noether:

For any finite Galois extension, $H^1(K, L^\times) = \{1\}$

proof

Fix $K \subset L$ Galois with $\mathrm{Gal}(L/K) = \langle \sigma \rangle = G$

Fix $u \in L$ such that $N(u) = 1$

Want to solve $\dfrac{v}{\sigma(v)} = u$.

In other words, we want to show that the K-linear map $T : V \longrightarrow V$ given $u \cdot \sigma(-)$ has 1 as an eigenvalue. where $V = L$

$\hookrightarrow$ this happens iff $\underbrace{V \otimes L \longrightarrow V \otimes L : T \otimes id_L}_{\text{map of } L\text{-vector spaces}}$ has 1 as an eigenvalue.

$G \curvearrowright V \otimes L$ as an L-vectorspace $\cong$ L-valued fcts on G

G-module

$\cong \bigoplus_{g \in G} Lg$

Under this isomorphism,

mult by u $\longmapsto$ $\begin{pmatrix} u & & & & \\ & \sigma_1(u) & & & \\ & & \sigma^2(u) & & \\ & & & \ddots & \\ & & & & \sigma^{n-1}(u) \end{pmatrix}$

$\sigma(-)$ $\longmapsto$ $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$

To prove the Theorem is to show that the product of these operators has 1 as an eigenvalue.

$(u, \sigma(u), \sigma(u)\sigma^2(u), \sigma(u)\sigma^2(u)\sigma^3(u), \dots, \sigma(u)\dots\sigma^{n-1}(u))$ is an eigenvector with eigenvalue 1.

Theorem

Suppose F is a field which contains the primitive m'th roots of unity ξ. $(x^m - 1)$ completely splits over F.

Then $F \subset E = F[\sqrt[m]{a}]$ where $a \in F^\times$ is cyclic with Galois group $\leq \mathbb{Z}/m$

Converse if $F \subset E$ is Galois with Galois group $\leq \mathbb{Z}/m$ then $E = F[\sqrt[m]{a}]$ for some $a \in F^\times$

Note $x^m - a$ splits completely over E

$\mathbb{Z}/m \cong \mu_m$ = group of m'th roots of unity $\subseteq F^\times$

proof

$$\begin{array}{ccc} \mathrm{Gal}(E/F) & \longrightarrow & \mu_m \\ \| & & \\ G & & \\ g & \longmapsto & \dfrac{g(\alpha)}{\alpha} \end{array}$$

} is a homomorphism