Galois groups of Polynomials

Def: $f(x) \in F[x]$ the Galois gp. of $f(x)$ is $Gal(K/F)$ for K the s.f. of $f(x)$.

$f(x)$ has roots $r_1, -, r_n$.

$K = F(r_1, \dots, r_n)$. Any element of $Gal(K/F)$ is determined by action on r_i's.

You get an injection

$$Gal(K/F) \hookrightarrow S_n$$

by viewing $\sigma \in Gal(K/F)$ as a permutation of the roots.

Def: $H \leq S_n$ is called transitive if for all $i \neq j$ there is $\sigma \in H$ w/

$\sigma(i) = j$.

<u>Thm:</u> $f(x) \in F[x]$ sep. of degree n,

f irred. $\iff$ $\mathrm{Gal}(f)$ is a transitive subgroup of S_n.

<u>Proof:</u>

$\Rightarrow$) follows from what we know about splitting fields: there is $\sigma \in \mathrm{Gal}(K/F)$ w/ $\sigma(r_i) = r_j$ for any $i \neq j$.

$\Leftarrow$) $f(x)$ reducible, it factors into a product of (distinct) irreducibles

let r_i be a root of one, r_j a root of the other. There is no σ s.t.

$\sigma(r_i) = r_j$ $\Rightarrow$ not transitive.

Note: every Galois ext^n is s.f. of some irred.

Possible Galois groups:

n	Transitive Subgps of S_n
2	$\mathbb{Z}/2\mathbb{Z}$
3	A_3, S_3
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, A_4, S_4, D_8
5	$\mathbb{Z}/5\mathbb{Z}$, D_{10}, A_5, S_5, $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$

<u>Def:</u> $f(x) \in F[x]$ Suppose f factors in a s.f. as

$$c(x-r_1)\cdots(x-r_n).$$ The

discriminant of f is defined as

$$\operatorname{disc}(f) = \prod_{i<j} (r_j - r_i)^2$$

Note: $\operatorname{disc}(f) \neq 0 \iff f$ separable

<u>Ex:</u> $f(x) = ax^2 + bx + c$

$$= a(x-r_1)(x-r_2)$$

$$\operatorname{disc}(f) = (r_2 - r_1)^2 = (r_1 + r_2)^2 - 4r_1 r_2$$

$$= \frac{b^2 - 4ac}{a^2}$$

So if $f(x)$ is monic, this agrees w/ usual notion of discriminant.

By general nonsense, disc(f) is a symmetric poly. in roots of $f(x)$

Since symm. poly are fixed by action of S_n $\Rightarrow$ disc$(f) \in F$.

<u>Prop</u>: Char$(F) \neq 2$

Gal$(f) \leq A_n \iff$ disc$(f) = \square$ in F.

<u>Cor</u>: $f(x) \in F[x]$ sep. irred cubic

Char$(F) \neq 2$

- $\mathrm{disc}(f) = \square \iff \mathrm{Gal}(f) = A_3$
- $\mathrm{disc}(f) \neq \square \iff \mathrm{Gal}(f) = S_3$

Ex: $f(x) = x^3 + ax + b$

$\mathrm{disc}(f) = -4a^3 - 27b^2$

$f(x) = x^3 - x - 1$ $\quad \mathrm{disc}(f) = -23$

$\Rightarrow \mathrm{Gal}(f) \cong S_3.$

Cor: f irred., sep quartic $\mathrm{Char}(F) \neq 2$

- $\mathrm{disc}(f) = \square \iff \mathrm{Gal}(f) = A_4$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathrm{disc}(f) \neq \square \iff \mathrm{Gal}(f) = S_4, D_8, \mathbb{Z}/4\mathbb{Z}$

Note: can narrow down further using "resolvent cubic" but it's mostly useless.

Actually useful results:

Prop. $f(x) \in \mathbb{Q}[x]$ irred. of degree p, p prime. If f has exactly two complex roots, then $Gal(f) \cong S_p$

Proof: $[\mathbb{Q}(\alpha):\mathbb{Q}] = p \Rightarrow p \mid |Gal(f)|$

$\Rightarrow$ $Gal(f)$ has an element of order p.

$\Rightarrow$ $Gal(f) \leq S_p$ contains a p-cycle. Having exactly two complex roots means $Gal(f)$ contains a transposition (complex conjugation)

$\Rightarrow$ $Gal(f)$ contains S_p $\square$

Ex: $x^5 - 4x + 2 \in \mathbb{Q}[x]$.

Irred. by Eisenstein.

Can use basic Calculus to show

has 3 real roots. $\Longrightarrow$ $Gal(f) \cong S_5$.

Thm: (Dedekind)

$f(x) \in \mathbb{Z}[x]$ be monic, irred of

degree n. For any prime p w/

$p \nmid disc(f)$ suppose $f(x)$

factors as

$$f(x) \equiv f_1(x) \cdots f_k(x) \mod p$$

$d_i = \deg(f_i)$ $\quad$ $Gal(f)$ contains

a permutation of type

$(d_1, \dots, d_k)$.

Proof: Too hard for course.

Ex: $x^5 - 100x - 400$ irred. b/c it's irred mod 3.

$$\operatorname{disc}(f) = 8800000^2$$

$$\operatorname{Gal}(f) \leq A_5.$$

$$x^5 - 100x - 400 \equiv x^5 + 2x + 2 \mod 3$$

$$x^5 - 100x - 400 \equiv (x+1)(x+3)(x^3+3x^2+6x+2) \mod 7$$

$\Longrightarrow$ Gal(f) contains a 5-cycle and a 3-cycle

$\Rightarrow \quad 15 \mid |Gal(f)|$

$\Rightarrow \quad Gal(f) = A_5.$

LMFDB

Ask for number field assoc. to a polynomial.

Operations on extensions:

Def: $F_1, F_2 \subseteq F$ the <u>composite</u> of F_1, F_2 is denoted F_1F_2 is the smallest subfield of F containing F_1 and F_2.

Thm: K/F Galois L/F is any ext^n

Then KL/L is Galois and

$$\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K\cap L)$$

$$\begin{tikzcd}
 & KL & \\
K \arrow[ur, dash] & & L \arrow[ul, "\text{Galois}"'] \\
 & K\cap L \arrow[ul, dash, "\text{Galois}"] \arrow[ur, dash] &
\end{tikzcd}$$

Galois

$$\begin{tikzcd} \arrow[d, dash] \\ F \end{tikzcd}$$

Proof: Techne.

Thm: K/F, L/F Galois

$$\begin{tikzcd}[column sep=small]
 & KL \arrow[dl, dash, "\text{Galois}"'] \arrow[dr, dash, "\text{Galois}"] \arrow[ddd, dash, bend left=60, "\text{Galois}"] & \\
K \arrow[dr, dash, "\text{Galois}"'] & & L \arrow[dl, dash, "\text{Galois}"] \\
 & K \cap L \arrow[d, dash, "\text{Galois}"] & \\
 & F &
\end{tikzcd}$$

- $K \cap L | F$ is Galois
- $KL|F$ is Galois
- $\mathrm{Gal}(KL|F) = \{ (\sigma, \tau) \in \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F) : \sigma|_{K\cap L} = \tau|_{K \cap L} \}$

Proof:

1.) $K \cap L$ is sep. b/c $K|F$ is sep.

$f(x) \in F[x]$ is irred w/ a root in $K \cap L$. $\Rightarrow$ root in K, L

$\Rightarrow$ splits in K, L b/c both ~~...~~ normal $\Rightarrow$ split in $K \cap L$

$\Rightarrow$ normal.

2.) K is s.f. of $f(x)$ over F

L is s.f. of $g(x)$ over F

KL is s.f. of squarefree part of $f(x)g(x)$ over F $\Longrightarrow$

Galois.

3.) $\varphi: Gal(KL/F) \longrightarrow Gal(K/F) \times Gal(L/F)$

$\sigma \longrightarrow (\sigma|_K, \sigma|_L)$

Let H = subgp in the statement.

$Im(\varphi) \leq H$ is clear.

$L/K \cap L$ is Galois, for any

autc. of $K \cap L$, there are

$[L : K \cap L]$ number of ways

to extend it to an automorphism

of L.

For any $\sigma \in Gal(K|F) \Rightarrow$

there are $[L : K \cap L]$ ways to

pick τ so that $(\sigma, \tau) \in H$.

$$|H| = |Gal(K|F)| \cdot |Gal(L|K \cap L)|$$

$$= |Gal(KL|F)|$$

(check: follows from previous thm)

$\square$

Cor: K/F, L/F Galois, $K \cap L = F$

then

$$\mathrm{Gal}(KL/F) \cong \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F).$$

Ex:

$\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ has degree 8

and Galois group D_8

$\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ has degree 6

and Galois gp S_3

Composite is $\mathbb{Q}(\sqrt[4]{2}, i, \sqrt[3]{2}, \sqrt{3}) =$

$\mathbb{Q}(\sqrt[12]{2}, i, \sqrt{3}) := K.$

this ext^n has degree 48.

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt[12]{2}, \sqrt{3}, i) \arrow[dl, dash, "\leq 3"'] \arrow[ddr, dash, "\leq 16"] & \\
\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}, i) \arrow[d, dash, "2"'] & & \\
\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}) \arrow[d, dash, "4"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[ddl, dash, "3"] \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & & \\
 & \mathbb{Q} &
\end{tikzcd}
$$

$[\mathbb{Q}(\sqrt[4]{2}, i) \cap \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}]$

divides 6 and 8 $\Rightarrow$

divids 2.

$\Rightarrow$ equals 1 or 2.

if degree is 2, then

Intersection is a quadratic

ext^n in $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. By

Galois corr. the only quadratic

Subfield is $\mathbb{Q}(i\sqrt{3})$.

$$\Rightarrow \quad \mathbb{Q}(\sqrt[4]{2}, i) \cap \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$$

$= \mathbb{Q}(i\sqrt{3})$

Can check that $\mathbb{Q}(i\sqrt{3}) \not\subset \mathbb{Q}(\sqrt[4]{2}, i)$ so this means that degree is 1, so

$\mathbb{Q}(\sqrt[4]{2}, i) \cap \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = \mathbb{Q}.$

By the corollary,

$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt[12]{2}, i, \sqrt{3})/\mathbb{Q})$

$\cong S_3 \times D_8$ $\square$

Closures:

Often times want ext^n, with certain properties: separable, normal, Galois, etc.

Def: K/F then $F_{sep} = \{ x \in K : x \text{ sep. over } F \}$ is a field by HW and we call F_{sep} the separable closure of F in K. If $K = \bar{F}$ we just call it separable closure.

We've seen

$$
\begin{tikzcd}
K \arrow[d, dash, "\text{purely insep.}"] \\
F_{sep} \arrow[d, dash, "\text{sep}"] \\
F
\end{tikzcd}
$$

Prop: if K/F finite, there is L/K s.t. L/F is normal and $[L:K]$ is minimal w.r.t. this property.

Proof: $K = F(\alpha_1, \dots, \alpha_n)$ $\quad f(x) = \prod m_{\alpha_i}(x) \in F[x]$. Take L = s.f. of $f(x)$. $\square$

Def: The extension L above is called the normal closure of K/F.

Note: For general K/F algebraic, need to use def. of normality in terms of field embeddings.

separable

Prop: K/F finite, there is L/K s.t. L/F is Galois and $[L:K]$ minimal w.r.t. this property.

Proof: $K = F(\alpha_1, \dots, \alpha_n)$. $L =$ composite of s.f. of $m_{\alpha_i}(x)$ for all i

$\Rightarrow$ L/F Galois by earlier thm and L is minimal by def^n.

Def: L above is called the __Galois closure__ of K/F.

Often times want to pass extension to it's Galois closure so you can use Galois theory to do computations, etc.