Galois groups of polys.

Recall: Gal(irred. poly. of deg n) is a transitive subgp of S_n (can get from any root to another).

Q: How many #fields, ordered by discriminant have different Galois groups?

E.g. "Country" D_ℓ Galois groups, ℓ = prime $\Leftrightarrow$ Cohen-Lenstra (Athens-Atlanta recently); will see "why" most #'ed polys have deg Gal. gp. $= S_n$.

Def: $x_1, \dots, x_n$ are indeterminants (I have a record on A_n-gps).

elementary symmetric fns:

$$S_1 = x_1 + \dots + x_n$$
$$S_2 = x_1x_2 + x_1x_3 + \dots + x_2x_3 + x_2x_4 + \dots + x_{n-1}x_n$$
$$\vdots$$
$$S_n = x_1 \cdots x_n$$

i.e., S_i = sum of all prods of i many x_j's.

Note they are S_n-invariants

Def: General polynomial of degree n:

$$(x_1, \dots, x_n) = \prod_{i=1}^{n} (x - x_i)$$

, i.e. monic with roots $x_1, \dots, x_n$

(i.e., how polys look over splitting fields)

Connection: coeffs of gen. poly. are elem. symm. fns:

$$G(x_1, \dots, x_n) = x^n - S_1 x^{n-1} + S_2 x^{n-2} + \dots + (-1)^n S_n$$

(prove by induction).

E.g.: (1) $\sum$ roots $\simeq$ second highest term (trace)
$\prod$ roots $\simeq$ constant term (norm).

∴, for any poly field F,

$F(x_1,\dots,x_n)/F(s_1,\dots,s_n)$ is Galois, as it's the splitting field of G.

S_n acts on by permuting roots, i.e., the subscripts of $x_1,\dots,x_n$. We get an automorphism by each permutation on the x_i's which gives a map: $S_n \hookrightarrow \mathrm{Aut}(F(x_1,\dots,x_n))$

So $S_n \equiv$ subgp. of $\mathrm{Aut}(F(x_1,\dots,x_n))$ of rational fns.

The elem. symm. fns $s_1,\dots,s_n$ are fixed by the S_n-action by choice.

Thus, the subfield $F(s_1,\dots,s_n) \subseteq$ fixed field of S_n

Fundamental Theorem of Galois Theory $\Rightarrow [F(x_1,\dots,x_n) : \text{fixed field of } S_n] = n!$

Now, as $F(x_1,\dots,x_n)$ is the splitting field of $G(x_1,\dots,x_n)$ over $F(s_1,\dots,s_n)$,

$$[F(x_1,\dots,x_n) : F(s_1,\dots,s_n)] \leq n!$$

Thus, this is an equality, and fixed field $F(s_1,\dots,s_n)$ is the splitting field!

So the rational fns in $x_1,\dots,x_n$ invariant under S_n are just the rational fns in the elem. symm. fns.

a p^n is called symmetric.

This was the fund. Th^m on symmetric p^ns.

N.B: S_n-invariant p^ns are actually polynomials (not just rat'l p^ns) in $s_1, \dots, s_n$.

Ex: 1). $(x_1 - x_2)^2$ is symmetric

So it must be a p^n in s_1, s_2.

$s_1 = x_1 + x_2$
$s_2 = x_1 \cdot x_2$

$f = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2$

leading terms: $x_1^2 + x_2^2$. Start @ $s_1^2 = (x_1 + x_2)^2 = x_1^2 + x_2^2 + 2x_1x_2$

$f - s_1^2 = -2x_1x_2 - 2x_1x_2 = -4x_1x_2 = -4s_2$

$\Rightarrow$ $f = s_1^2 - 4s_2$.

[redacted]

2). $f = x_1^2 + x_2^2 + x_3^2$ is symmetric

match squares:

$s_1 = (x_1 + x_2 + x_3)$
$s_2 = x_1x_2 + x_1x_3 + x_2x_3$
$s_3 = x_1x_2x_3$

$f - s_1^2 = -2x_1x_2 - 2x_1x_3 - 2x_2x_3 = -2s_2$

$\Rightarrow f = s_1^2 - 2s_2$.

This is a simple instance of a very useful result the Newton-Girard identities.

kth power sum: $p_k(x_1,\dots,x_n) := \sum_{i=1}^{n} x_i^k$.

These are symmetric, so they must be expressible in elem. symm. fns.

$p_1 = e_1$

$p_2 = e_1 p_1 - 2e_2 = e_1^2 - 2e_2$ ← saw for $n=3$...

$p_3 = e_1 p_2 - e_2 p_1 + 3e_3 = e_1(e_1 p_1 - 2e_2) - e_2 p_1 + 3e_3$

$= e_1^2 p_1 - 2e_1 e_2 - e_2 p_1 + 3e_3$

$= e_1^3 - 2e_1 e_2 - e_1 e_2 + 3e_3$

⋮ general.

$p_k(x_1,\dots,x_n)$

$$p_k = (-1)^{k-1} k e_k(x_1,\dots,x_n) + \sum_{i=1}^{k-1} (-1)^{k-1+i} e_{k-i} p_i.$$

Can also go backwards:

$$k e_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i$$

Thus, the ring of symmetric fns is also gen. by the p_i's.

Faster way to realize this: generating fns!

$$E(t) = \sum_{k\ge 0} e_k t^k = \prod_{i=1}^{\infty} (1 + x_i t)$$ work in vars $x_1,\dots,x_n,\dots$ to ∞

$$P(t) = \sum_{k\ge 0} p_k t^k = \sum_{i\ge 1} \frac{x_i t}{1 - x_i t} = t\,\frac{E'(t)}{E(t)}$$

$$= -t \frac{d}{dt} \log(E(-t)).$$

All this is useful in locating roots of (u) & other fns

wring to Galois theory,

starting with poly. $x^n - s_1 x^{n-1} + s_2 x^{n-2} + \dots + (-1)^n s_n$ over $F(s_1, \dots, s_n)$, and defining the roots to be $x_1, \dots, x_n$, then the s_i are the elementary symmetric f$^{\text{ns}}$ in the roots x_i. These x_i are also indeterminants, i.e., there are no poly rel$^{\text{n}}$ over F in a among them.

To see this, suppose $p(t_1, \dots, t_n)$ is a non-zero poly. $/F$ s.t. $p(x_1, \dots, x_n) = 0$. Take the product, call it $\tilde{p}$, of $p(t_{\sigma(1)}, \dots, t_{\sigma(n)})$ over all $\sigma \in S_n$. This is a non-zero symmetric poly. @ $\tilde{p}(x_1, \dots, x_n) = 0$.

This gives a non-zero poly. rel$^{\text{n}}$ among the $s_1, \dots, s_n$, a contradiction. Conversely, if the roots of a poly f are independent indeterminants $/F$, so are the coeffs of f (cf. § 9 of book). That is, defining $G(x_1, \dots, x_n)$ as having indeterminant roots a coefficients is equivalent.

$\Rightarrow$ The general poly $x_n^n - s_1 x^{n-1} + \dots + (-1)^n s_n$ over $F(s_1, \dots, s_n)$ is separable w Galois group S_n.

Thus if there are no rel$^{\text{n}}$ among the coeffs of

a poly, then the Galois group over the field gen. by the coeffs. is the full symmetric gp.

Thus, "most" polys should have S_n Galois gp.

(Not always: e.g. over finite fields, as all extns are cyclic; so all poly coeffs have relns but does give a good heuristic for # fields.)

Classification of Galois for small deg. polys.

$n \geq 5$ different as only normal subgp. of S_n is A_n.

Whether you live in A_n or not:

Discriminants: $D = \prod_{i<j} (x_i - x_j)^2$. $x_1, \dots, x_n$ roots of poly = product of roots.

D is symmetric, so in $K = F(s_1, \dots, s_n)$.

Recall: $\sigma \in S_n$ is an even perm. iff it fixes $\sqrt{D} = \prod_{i<j} (x_i - x_j)$.

Thus as long as $\operatorname{char} F \neq 2$, $\sqrt{D}$ generates the fixed field of A_n and generates a quadratic extn of K.

~~$\Rightarrow$? if $\operatorname{char} F \neq 2$,~~

Classification: ~~spe~~ Separable polys of deg ≤ 4 (start).

$\operatorname{char} F \neq 2, 3$. ($f$ ix over $\mathbb{Q}$ or $\mathbb{F}_{p^n}$; take each irred. factor in a product)

f a monic poly. / F

Note: $D = 0 \iff f$ isn't separable (repeated roots), over perfect field $\Rightarrow$ f is reducible.

Disc. D is symm. in roots $\Rightarrow$ fixed by all of Galois group.

$\Rightarrow D \in F$. Roots By the def $\sqrt{D} = \prod_{\alpha_i} \alpha_\ell - \alpha_j$, $\sqrt{D}$ is the splitting field of f.

Fund. Prop: Galois gp of f is a subgp of $A_n \iff$ f acts

$\iff D$ is a square in F (if $\operatorname{char} F \neq 2$)

[redacted]

Pf:

$Gal(K/F) \leq A_n \Leftrightarrow$ all elts. fix $\sqrt{D}$

$\Leftrightarrow \sqrt{D} \in F$.

Cases of small degree. Throughout: char$(F) \neq 2, 3$.

deg 2: ~~ax^2~~ $\underline{x^2 + ax + b}$.

$D = a^2 - 4b$.

$D = 0 \to$ roots $\in F \Rightarrow$ deg. 1 ext^n no. ~~sep~~ sep.

$D \neq 0 \to$ separable

[redacted]

if $D = \square$ in F, then deg. 1 ext^n

if $D \neq \square$ in F, then Galois of deg. 2 with gp. $\mathbb{Z}_2$.

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

$x = y - a/3 \rightsquigarrow g(y) = y^3 + py + q$. $p = \frac{3b - a^2}{3}$

$q = \frac{2a^3 - 9ab + 27c}{27}$ ← elliptic curves.

Disc: $g(y) = (y - \alpha)(y - \beta)(y - \gamma)$

$\rightsquigarrow$ ~~$g'(y) =$~~ $g'(\alpha) = (\alpha - \beta)(\alpha - \gamma)$ ...

$\to D = (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2 = -g'(\alpha) g'(\beta) g'(\gamma)$

And $g'(y) = 3y^2 + p$ ...

$D = -4p^3 - 27q^2$

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

$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$

Cases:

1). Reducible. $f(x) = (\text{linear})(\text{irr})$ $(\text{lin})(\text{lin})(\text{lin}) \to Gal = 1$

or $(\text{lin})(\text{quad}) \to Gal = \mathbb{Z}_2$

2). irred.

$Gal(F(\text{Root of } f(x))/F) \leq S_3$, order at least 3 $\to$ is A_3 or S_3.

Its $A_3 \iff D = \square$ in F.

Read about quartics, quintics in book...

Ex: $\forall n \in \mathbb{Z}$, if $a = n^2 + n + 7$, then $f(x) = x^3 - ax + a$ is irred. w/ Galois gp. A_3.

Pf: a odd $\Rightarrow x^3 - ax + a \equiv x^3 + x + 1 \pmod 2$ irred. $\Rightarrow$ irred. / $\mathbb{Q}$

$D = -4(-a)^3 - 27a^2 = a^2(4a - 27)$

$4a - 27 = c^2 \to a = \frac{1}{4}(c^2 + 27)$. $\mathbb{Z}$ & odd

$c = 2k+1 \to a = \frac{1}{4}(4k^2 + 4k + 28) = k^2 + k + 7$.

Now $\forall n \in \mathbb{Z}$, $k^2 + n + 7$ good, D is $\square \Rightarrow A_3$.