Lecture 1: What is Galois Theory?

A Galois theory is the study of field extensions using symmetry i.e. group theory.

Original Motivating Question

Eg. Let F = field char $\neq 2$ or 3

Recall quadratic eq^n

$F[x] \ni x^2 + bx + c = 0$

has sol^n $x = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$

while Cubic eq^n

$x^3 + px + q = 0$ has sol^n

$$x = \gamma - \frac{p}{3\gamma}, \quad \gamma = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Note: * sol^n in terms of co-eff. of poly & uses $+, -, \times, \div$ & $\sqrt[n]{}$.

* Sim. formula for quartics

Major Q of 18th century algebra:
Is there a similar formula for the quintic?

A Abel, Ruffini, Galois: NO! (c. 1820)

We reformulate Q after some

Revision Let K/F = field ext.

Recall

(a) $\alpha \in K$ is algebraic over F if $f(\alpha)=0$ for some poly. $f(x) \in F[x]$ with $\deg f > 0$

(b) In this case, "the" minimal polynomial of α (over F) is any such poly(s) of minimal degree. It's unique up to constant in F.

(c) It's also called the irreducible polynomial of α, since it's any irred. $p(x) \in F[x]$ with $p(\alpha)=0$.

(d) $F(\alpha)$ is the simple field ext^{n} of F gen. by α.

Thm: (a) If α is alg /F say with min. poly $p(x)$ then there's a well-defined field isom.

$$\frac{F[x]}{\langle p(x) \rangle} \xrightarrow{\sim} F(\alpha)$$

N.B. $\frac{F[x]}{\langle p(x) \rangle}$ is a field

$$g(x) + \langle p(x) \rangle \longmapsto g(\alpha)$$

so $x \longmapsto \alpha$

Hence $[F(\alpha):F] = \deg p(x)$

(b) otherwise we say α is transcendental /F &

field of rational functions $F(x) \simeq F(\alpha)$

$x \longleftrightarrow \alpha$

Eg. 2 $\sqrt[3]{2} \in \mathbb{C}$ is alg. / $\mathbb{Q}$ with min. poly $p(x) = x^3 - 2$. Thm @ $\Rightarrow$ every elt of $\mathbb{Q}(\sqrt[3]{2})$ can be written uniquely in the form

$\alpha + \beta \sqrt[3]{2} + \gamma \sqrt[3]{2^2}$ for $\alpha, \beta, \gamma \in \mathbb{Q}$

Modern Reformulation of Classical Q

Eg. 1 again $f(x) = x^2 + bx + c \in F[x]$ has roots in $F(\underbrace{\sqrt{b^2 - 4ac}}_{\in F})$ ext^n of F obtained by adjoining a square root.

$f(x) = x^3 + px + q$ has roots in $F(\delta, \gamma)$ where

$\delta = \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, $\gamma = \sqrt[3]{-\frac{q}{2} + \delta}$

Have tower of field ext^{n}s

$F \subset F(\delta) \subset F(\gamma, \delta) = F(Y)$

adjoin $\sqrt{}$ adjoin $\sqrt[3]{}$

Suggests

Def^{n} A field ext^{n} K/F is **radical** if there's a tower of field ext^{n}s

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$$

s.t. $F_{i+1} = F_i(\sqrt[m_i]{\alpha_i})$ for some $\alpha_i \in F_i$, $m_i \in \mathbb{N}$ i.e. K is obtained from F by successively adjoining m-th roots.

Point: α is expressible in terms of elts of F using $+, -, \times, \div, \sqrt[m]{}$ iff

(*) α lies in a radical ext^{n} of F.

Modern Q Given $f(x) \in F[x]$, how can you tell if its roots lie in a radical ext^{n} of F?

Key to Galois's Approach

"Symmetry" in the roots completely determines all the possible "intermediate" fields (i.e. between K & F). This reduces analysing towers of field ext^{n}s to problems in finite group theory.