Graduate Algebra II: Lecture 2: Galois theory.

Recall: Fundamental object of study:

Field auto~~iso~~morphisms: isomorphisms from $K \to K$.

For field ext^{ns}, study

$$Aut(K/F) := \{\text{aut. } \sigma : K \to K \mid \sigma(x) = x \ \forall x \in F\}.$$

Special case) $Aut(K/\mathbb{Q})$ or $Aut(K/\mathbb{F}_p)$ (depending on $char(K)$) ~~doesn't~~ is just $Aut(K)$, since automorphisms send $1 \mapsto 1$ and 1 generates $\mathbb{Q}/\mathbb{F}_p$.

First main observation: $(Aut(K), \circ)$ is a gp.

$Aut(K/F)$ is a subgp.

Why: We've already seen $Aut(K)$ is a gp;

for subgp. criterion, ~~$\emptyset$~~ $id_K \in Aut(K/F)$,

and if $\sigma(x) = \tau(x) = x \ \forall x \in F$, then $\sigma\tau(x) = \sigma(x) = x$

and $\sigma^{-1}(x) = x \ \forall x \in F \Rightarrow \sigma\circ\tau, \sigma^{-1} \in Aut(K/F)$.

Origins of Galois theory: ~~$\emptyset$~~ Action of automorphisms on roots of Polys.

Th^{m}: If $\alpha \in K$ is algebraic over F, and $\sigma \in Aut(K/F)$, then $\sigma(\alpha)$ is a root of $\text{minpoly}_F(\alpha)$.

(1)

Cor: Elts of $\mathrm{Aut}(K/F)$ permute roots of irred. poly

If a poly over F has a root α, then $\sigma(\alpha)$ is a root too.

Pf: If α is algebraic, say $\min\text{poly}_F(\alpha) = \sum_{n=0}^{k} a_n x^n$.

Then $\sum a_n \alpha^n = 0 \Rightarrow \sum a_n (\sigma(\alpha))^n = 0$

$\sum \sigma(a_n)\sigma(\alpha)^n = 0$

$\sum a_n \sigma(\alpha)^n$ (as $a_n \in F$, σ fixes F)

$\Rightarrow \min\text{poly}_F(\alpha)(\sigma(\alpha)) = 0$, ☑ E-Z!

Ex: 1). $\mathrm{Aut}(\mathbb{R}(i)/\mathbb{R}) = \{\mathrm{id}, \text{conjugation}\}$.
permutes $i, -i$, roots of x^2+1.

2). $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F = \mathbb{Q}$.

Get $\sigma \in \mathrm{Aut}(K/F)$ given by $\sigma: \sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$.

The root of $x^2 - 2$ must go to $\pm\sqrt{2}$, similarly for 3.

So these must be all the auts.

Getting to the Galois correspondence

Def: The roots of a common irred. poly in K are called K-conjugates.

Thm: If $H \leq \mathrm{Aut}(K$

Cor: For a finite ext^n K/F, $\mathrm{Aut}(K/F)$ is finite.

Pf: If $K = F(\alpha_1, \ldots, \alpha_n)$, then $\sigma \in \mathrm{Aut}(K/F)$ determined by $\{\sigma(\alpha_i)\}$. But $\sigma(\alpha_i)$ must be in the

finitely many) K-conjugates of α_i in L. ☐

Getting to the Galois correspondence...

Prop: 1) If $H \leq \mathrm{Aut}(K)$, then the fixed set of elts of K fixed by H is a subfield of K. Call this $\mathrm{Fix}(H)$, the fixed field

2) If $F \subseteq K \subseteq L$, then $\mathrm{Aut}(L/K) \leq \mathrm{Aut}(L/F)$.

3) If $H \leq H' \leq \mathrm{Aut}(K)$, then $\mathrm{Fix}(H') \leq \mathrm{Fix}(H)$. (reverses order).

Pf: 1) Just check the def^n: If $h \in H$, $a, b \in F$, then $h(a \pm b) = h(a) \pm h(b) = a \pm b$, $h(ab^{-1}) = h(a)h(b)^{-1} = ab^{-1}$.

2) If $\sigma \in \mathrm{Aut}(L/K)$, then σ is an aut. of L fixing all elts in K, in particular those in F.

3) If α is fixed by every $\sigma \in H'$, then in particular it is by those in H.

Ex: In $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, there is always the automorphism $\cdot^c$ of complex conjugation.

This obviously has order 2 in $\mathrm{Aut}(\mathbb{Q}(\zeta_n))$.

By Galois theory, we'll see the fixed field should be contained in $\mathbb{Q}(\zeta_n)$ with degree 2.

It turns out $\mathrm{Fix}(\cdot^c)$, the maximal real subfield

is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

We'll check this is real and contained @ degree 2:

Real: $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n) \in \mathbb{R}$

(also: fixed by conjugation as $\overline{\zeta} = \zeta^{-1}$ $\Leftrightarrow |\zeta| = 1$!)

Thus, $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{R}$

Thus, $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \neq \mathbb{Q}(\zeta_n)$, and so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})]$

Now consider $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$ ≥ 2.

$f(x)$ factors as $f(x) = (x - \zeta_n)(x - \zeta_n^{-1})$

and so has ζ_n as a root

As $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \geq 2$,

$f(x)$ is the min. poly. of ζ_n over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$

$\Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$.

This is a super important example: CM field: totally real (all embeddings into $\mathbb{C}$ are real) but with a totally imaginary quad. extension.

How many auts. of K/F can there be? Say $K = \text{split}(f(x))$ over F.

Claim: $|\text{Aut}(K/F)| \leq [K:F]$, equality if $f(x)$ separable.

Induction: Clear if $[K:F] = 1 \Rightarrow K = F$. If $[K:F] > 1$ ~~$f(x)$ has~~ an irred factor $p(x)$ of $f(x)$ of deg. > 1, Proof: NEXT TIME...

New def^{n}: K/F Galois if $[K:F] = |\text{Aut}(K/F)|$.

In this case, $\text{Aut}(K/F)$ is called $\text{Gal}(K/F)$