Algebra II Lecture 3:

Recall: we saw: $|\mathrm{Aut}(K/F)| < \infty$.

Lets look at the size in more detail.

Say $K = \mathrm{Spl}_F(f(x))$; K is a splitting field.

Recall: Isomorphisms $\varphi: F \xrightarrow{\sim} F'$ can be lifted to $\Phi: K \to K'$; $K' = \mathrm{Spl}_{K'}(f^{\varphi}(x))$; $f^{\varphi}(x) := \varphi(f(x))$ (coefficients acted on by φ).

Prop: [The # of such extensions, Φ of φ ($F \xrightarrow{\varphi} F'$, $K \xrightarrow{\Phi} K'$) is $\le [K:F]$.] Equality is obtained if $f(x)$ is separable/F.

pf: By induction on $[K:F]$.

Base case: $[K:F] = 1 \Rightarrow K = F \Rightarrow K' = F'$, $\varphi = \Phi$ and the # of ext$^{\text{ns}}$ is 1.

Induction step: If $[K:F] > 1$, then f has some irred. factor $g(x)$ of degree > 1. This corresponds to an irred. factor $g'(x)$ of $f^{\varphi}(x)$. Pick a root α of $g(x)$.

If Φ is an ext$^{\text{n}}$ of φ, then $\Phi|_{F(\alpha)} =: \tau$ is an isomorphism from $F(\alpha)$ to a subfield of K'. (restriction)

As α generates the ext$^{\text{n}}$ $F(\alpha)/F$, τ is determined by $\tau(\alpha)$.

As before, we find $\tau(\alpha)$ is a root, say β, of $g'(x)$.

Picture:

$$\begin{array}{ccc} K & \xrightarrow{\Phi} & K' \\ \cup & & \cup \\ F(\alpha) & \xrightarrow{\tau} & F'(\beta) \\ \cup & & \cup \\ F & \xrightarrow{\varphi} & F' \end{array}$$

Conversely, given a root β of $g'(x)$, we get the ext$^{\text{ns}}$ τ, Φ.

Thus, counting ext^ms is equivalent to such ϕ's

The # of extensions of ϕ to an isomorphism τ equals the # of distinct roots β of g'(α).

Since deg(g) = deg(g') = [F(α):F], the # of extensions ϕ → τ is at most [F(α):F], with equality iff the roots are distinct.

Now K is also the splitting field of g(x) over F(α), K' = Spl_{F'(β)}(g'(x)), and [K:F(α)] < [K:F].

Thus, by induction, # extensions of τ to Φ is ≤ [K:F(α)] with = if g(x) has distinct roots.

As [K:F] = [K:F(α)] · [F(α):F]

# of ext^ms of ϕ to Φ is ≤ [K:F], with = if φ(x) and f(x) have distinct roots (⇔ f(x) does) (see notation above).

Cor: |Aut(K/F)| ≤ [K:F] with = iff f(x) is F-separable.

Pf: Take F = F', ϕ = id_F ⇒ K = K'

Rmk: |Aut(K/F)| ≤ [K:F] even in the case when it is not a splitting field.

Def^n 2: K/F finite. Then it's Galois if |Aut(K/F)| = [K:F]. In this case, the Galois group is Gal(K/F) := Aut(K/F).

Normal + sep. (Defn 1) $\Rightarrow$ Defn 2

- $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is the splitting field of $\Phi_n(x)$
$\mathbb{Q}$ is perfect, so $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.

2). Another way to see $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ not Galois!
Only 1 automorphism of $\mathbb{Q}(\sqrt[3]{2})$!

3). $\mathbb{F}_{p^n}$ was constructed as a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, $\mathbb{F}_p$ is perfect,
So $\mathbb{F}_{p^n}$ is Galois. Ifs E-Z to find $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$:
$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
The Frobenius Frob_p is an elt. of the Galois gp.
Pows: $\mathrm{Frob}_p^i(\alpha) = \alpha^{p^i}$. If $\mathrm{Frob}_p^i = id_{\mathbb{F}_{p^n}}$
then $\alpha^{p^i} = \alpha \ \forall \alpha$. If $i < n$, this
can't be true as $x^{p^i} - x$ has at most p^i roots
in $\mathbb{F}_{p^n}$. Thus, $|\mathrm{Frob}_p| \geq n \Rightarrow |\mathrm{Frob}_p| = n$
$\Rightarrow \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

* For infinite extensions, have to say Galois & normal + seperable.
We'll maybe see how Galois correspondence (3) works then need a topology on Gal.

Fundamental Thm of Galois theory.

Correspondence b/w subgps. of Galois & intermediate fields.

We saw some examples before. Here's a new one:

$\mathbb{Q}(\zeta_5)/\mathbb{Q}$. Min poly: $x^4+x^3+x^2+x+1$.

So deg is $\varphi(5)=4$.

The automorphisms of $\mathbb{Q}(\zeta_5)$ are $\sigma_i: \zeta \mapsto \zeta^i$. $i=1,2,3,4$

Claim: This is cyclic.

Indeed, $\sigma_2(\zeta_5) = \zeta_5^2$

$\sigma_2^2(\zeta_5) = \sigma_2(\zeta_5^2) = \zeta_5^4 = \zeta_5^{-1}$

$\sigma_2^3(\zeta_5) = \sigma_2(\zeta_5^4) = \zeta_5^8 = \zeta_5^3$

$\sigma_2^4(\zeta_5) = \zeta_5^{16} = \zeta_5$

note: $\sigma_2^2: x \mapsto x^{-1} = x$

$\Rightarrow$ order of σ_2 is 4 $\Rightarrow$ $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \langle \sigma_2 \rangle \cong \mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^\times$.

lattice of subgps of $\mathbb{Z}/4\mathbb{Z}$: $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z}$ generated by σ_2^2 = complex conjugation.

1

lattice of intermediate fields: $\mathbb{Q}(\zeta_5)$

$\mathbb{Q}(\zeta_5+\zeta_5^{-1}) = \mathbb{Q}(\cos(2\pi/5))$

$\mathbb{Q}$. field

Need first: some character theory.

Def^n. A character χ of a group G in L is a hom $\chi: G \to L^\times$.

Def^n: If $\chi_1, \dots, \chi_n$ are characters, they are linearly independent if $a_1\chi_1 + \dots + a_n\chi_n = 0 \Rightarrow a_1 = \dots = a_n = 0$.