It's been a fun year for me, but it's winding down now! Let us do one problem per day for the next four days. First, we review where we are with field extensions.

Let E/F be field extension.

The *degree* of E/F, denoted $[E : F]$, is the dimension of E as a vector space over F.

Let $\alpha \in E$. We say that α is *algebraic* over F if α is a root of a polynomial over f. In this case, there is a unique monic irreducible polynomial $f \in F[x]$ such that $f(\alpha) = 0$. We call f the *minimum polynomial* of α over F.

The smallest subfield of E which contains F and α is denoted $F[\alpha]$. Evaluation of polynomials by plugging α into every one of them creates a homomorphism $F[X] \to F[\alpha]$ whose kernel is generated by f. By the Isomorphism Theorem, $F[X]/\langle f\rangle \cong F[\alpha]$.

If $\alpha_1, \alpha_2 \in E$ are roots of an irreducible polynomial f over F, there exists a unique isomorphism $F[\alpha_1] \to F[\alpha_2]$ which fixes F and sends α_1 to α_2. Its just $\phi_2 \circ \phi_1^{-1}$, where $\phi_i : F[X]/\langle f\rangle \to F[\alpha_i]$ is the isomorphism referred to in the Isomorphism Theorem.

What does the above paragraph say about the case where $E = F[\alpha_1] = F[\alpha_2]$?

Recall the following terminology regarding a field extension.

- E/F is *finite* if $[E : F]$ is finite.
- E/F is *primitive* if $E = F[\alpha]$ for some α, in which case $[E : F]$ is the degree of the minimum polynomial of α.
- E/F is *algebraic* if every element in E is algebraic over F; that is, for every $\alpha \in E$ there exists $f \in F[X]$ such that $f(\alpha) = 0$. Every finite extension is algebraic.
- E/F is *normal* if every polynomial over F which has a root in E splits in E. It can be shown that E/F is finite and normal if and only if E is a splitting field for a polynomial over F.
- E/F is *separable* if no irreducible polynomial over F has multiple roots in E. It can be shown that finite separable extensions are primitive.
- E/F is *Galois* if it is normal and separable.

Okay that's a lot of setup, but if we believe all that, interesting things start to happen.

Let $\mathrm{Aut}(E)$ denote the set of all automorphisms of E. Let $\mathrm{Aut}(E/F)$ denote the subgroup of $\mathrm{Aut}(E)$ consisting of those automorphisms we fix F pointwise:

$$\mathrm{Aut}(E/F) = \{\phi \in \mathrm{Aut}(E) \mid \phi(x) = x \text{ for all } x \in F\}.$$

If E/F is a normal extension, we may write $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$. In this case, we call $\mathrm{Gal}(E/F)$ the *Galois group* of E/F.

Your challenge for today is to write these proof and submit it in Microsoft Classroom Assignment H0427.

Problem 1. Let E/F be a finite separable extension.

(a) Show that $|\mathrm{Aut}(E/F)| \leq [E : F]$.

(b) Show that if E/F is Galois, then $|\mathrm{Aut}(E/F)| = [E : F]$.