MATH 123 FACTSHEET

MD

1. Automorphisms and Embeddings

Consider $F \subset E \subset A$. E is an algebraic extension of F, A some algebraically closed field containing the two.

An *embedding* of F into A is an injective homomorphism $\sigma : F \to A$. Each embedding of the base field "lifts" to a number of embeddings of the extension into A, namely $[E : F]$ of them. (We say $\sigma : F \to A$ lifts to $\sigma' : E \to A$ if $\sigma'|_F = \sigma$.) Note that, **a priori**, a lifted embedding does not have to pointwise fix the base field (it does whatever σ did to the base field); however, when we talk of an embedding of E into A *over* F, we want $\sigma|_F = e$.

Since an automorphism is just a bijective self-homomorphism, it is equivalent to an embedding from E into itself over F.

Take some polynomial $f \in F[x]$ and let E be its splitting field. Then $E = F(\gamma)$ for some primitive element γ. Then we have the following information:

$$\operatorname{split}(f) = E = \operatorname{split}(\operatorname{irr}(\gamma, F))$$

but it *does not follow* that the polynomials have the same degree. In fact,

$$\deg(\operatorname{irr}(\gamma, F)) = [E : F] = |G_{E/F}| \quad \text{and} \quad \deg(\operatorname{irr}(\gamma, F)) \mid (\deg f)!$$

What's going on is that $\deg(\operatorname{irr}(\gamma, F))$ is the degree of the full extension of the splitting field, while $\deg f$ is only the degree of the extension attained by adjoining a single root of f; in an extreme case, you would have linearly independent roots, so you would next have to adjoin a root of the remaining polynomial of degree $(\deg f) - 1$, and then the next would have degree $(\deg f) - 2$, and so on... by multiplicativity of extensions and since the number of automorphisms for a splitting field is the degree of the extension, this is the scenario which gives a group of order $(\deg f)!$ (the full symmetric group $S_{\deg f}$) as the automorphism group of E/F.

2. Normal and Separable Extensions

The following are equivalent definitions of what it means for E to be *normal* over F

1. Every embedding of E in A over F is an automorphism.
2. E is the splitting field of a family of polynomials in $F[x]$.
3. Every irreducible polynomial of $F[x]$ which has a root in F splits into linear factors in F.

Now for an irreducible polynomial to be *separable* is to have distinct roots. We call a field *perfect* if all irreducible polynomials are separable. Note that all fields of characteristic 0 are perfect. Why? If a polynomial f had some root α with multiplicity > 1, then α would satisfy the derivative f' as well, which has smaller degree, which contradicts irreducibility. (verify this)

Remark. In fact, it turns out that all finite fields are perfect... so to get something non-separable, you have to look at a field like $\mathbb{F}_p[t]$, where $x^p - t = (x - \alpha)^p$ in some algebraic closure.

Separability is what we need for the maxims of Galois theory to extend to characteristic p. A Galois extension, then, is a separable normal extension, and it is (only) on these items that Galois groups are defined.

Date: February 26, 1997.