# WS #2 – MATH 6320
# SPRING 2015

DUE: THURSDAY FEBRUARY 5TH

You are encouraged to work in groups on this. Only one writeup needs to be turned in per group. I'll also give you some time to work on this on Tuesday.

Let us recall first what we know.

**Theorem.** *Let $G \subseteq \mathrm{Aut}(K)$ be a group with $n$ elements acting on a field $K$. Let $F = K^G$ be the fixed field. Then $[K : F] = n = |G|$.*

**Corollary.** *Let $K/F$ be a finite extension then $|\mathrm{Aut}(K/F)| \leq [K : F]$.*

**Corollary.** *Let $F = K^G$ as above. Then every element $\sigma \in \mathrm{Aut}(K)$ that fixes $F$ is contained in $G$.*

**Theorem.** *Let $K/F$ be a finite extension of fields. The following are equivalent:*

1. *$K$ is the splitting field of a separable polynomial defined over $F$.*
2. *$[K : F] = |\mathrm{Aut}(K/F)|$*
3. *$F = K^G$ where $G = \mathrm{Aut}(K/F)$.*
4. *$K/F$ is Galois (you can take Galois to mean any of the above).*

Our goal is to prove the fundamental theorem of Galois Theory. We begin with the statement.

**Theorem.** (Fundamental theorem of Galois theory) *Let $K/F$ be Galois and let $G = \mathrm{Gal}(K/F)$. Then there is a bijection between subfields $F \subseteq E \subseteq K$ and subgroups $\{1\} \leq H \leq G$. This is obtained by $H \mapsto K^H$ and $E \mapsto \{g \in G \mid$ which fix $E\ \}$. Furthermore:*

1. *This bijection is inclusion reversing ($H_1 \subseteq H_2$ if and only if $E_2 \subseteq E_1$).*
2. *$[K : E] = |H|$ and $[E : F] = |G : H|$.*
3. *$K/E$ is always Galois with $\mathrm{Gal}(K/E) = H$.*
4. *$E$ is Galois over $F$ if and only if $H$ is a normal subgroup in $G$. In this case $\mathrm{Gal}(E/F) \cong G/H$.*
5. *If $E_1, E_2$ correspond to $H_1, H_2$ then $E_1 \cap E_2$ corresponds to the group generated by $H_1$ and $H_2$. Likewise $E_1E_2$ corresponds to $H_1 \cap H_2$. In particular, the lattice of subfields is the same as the lattice of subgroups (upside down).*

Ok, your job is to prove it.

**1.** Given a subgroup $H \leq G$ we obtain a fixed field $E = K^H$. Show that the field obtained is unique. In other words if $K^{H_1} = K^{H_2}$ then show $H_1 = H_2$. This shows that the bijection from subgroups to subfields is injective.

*Hint:* Note that if $K^{H_1} \subseteq K^{H_2}$ then every element of $H_2$ fixes $K^{H_1}$. Use the second corollary.

**2.** Show that every extension $K/E$ is Galois (where $F \subseteq E \subseteq K$) and hence that $E$ is the fixed field of $\text{Aut}(K/E) \leq G$. Show that this finishes the proof that the correspondence is a bijection.

**3.** Verify (again) the the correspondence is order reversing.

**4.** Next prove (2).

*Hint:* You already know that $\text{Aut}(K/E)$ has $[K : E]$ elements, the rest should be integer division.

**5.** Next prove (3) simply by citing your previous work.

We'll prove (4) and (5) in class.