Debra Griffin
Galois Theory II
Worksheet #1, 2

---

**1.** *Let $E$ be a field and $S$ and $T$ be subsets of Aut(E).*
**(a)** *Prove that $E^S$ is a subfield of $E$.*

**Proof**:

Clearly $E^S \subseteq E$.

Let $\varphi \in S$.

$0 \in E^S$ and $1 \in E^S$ as $\varphi(0) = 0$ and $\varphi(1) = 1$ by homomorphism properties, so $E^S \neq \emptyset$.

Let $a, b \in E^S$. Then by homomorphism properties we have

$\varphi(a - b) = \varphi(a) - \varphi(b) = a - b$, $\varphi(ab) = \varphi(a)\varphi(b) = ab$, and $\varphi(a^{-1}) = \varphi(a)^{-1} = a^{-1}$.

Since $\varphi$ was arbitrary, then $a - b$, $ab$, and $a^{-1} \in E^S$.

Hence $E^S$ is a subfield of $E$.

---

**(b)** *Prove that if $S \subseteq T$, then $E^T \subseteq E^S$.*

**Proof**:
Let $a \in E^T$. Let $\sigma \in S$. Since $S \subseteq T$, then $\sigma \in T$. Thus $\sigma(a) = a$. Hence $a \in E^S$.

---

**(c)** *If $S$ is an infinite set, then $[E:E^S] = \infty$.*
*(Hint: Prove $[E:E^S] \geq n$, for all $n \in \mathbb{N}$.)*

**Proof**:

Let $n \in \mathbb{N}$. Let $T = \{\sigma_1, \ldots, \sigma_n\} \subseteq S$. By part (b), $E^S \subseteq E^T$.

By part (a) $E^T$ and $E^S$ are subfields of $E$, hence $E^S$ is a subfield of $E^T$.

If $[E:E^T]$ or $[E^T:E^S]$ is infinite, then $[E:E^S]$ is infinite by Theorem 39 of Extension Fields Part I. Assume both are finite.

Then $[E:E^S] = [E:E^T][E^T:E^S]$

by Lecture Notes 3/15/10 (Let $K/E$ be an extension and $E/F$ be an extension. If $[K:E]$ and $[E:F]$ are both finite, then $[K:F] = [K:E][E:F]$.)

Since $|T| = n$, then by Lecture Notes 4/7/10 (If $S \subseteq \text{Aut}(E)$ and $|S| = n$, then $[E:E^S] \geq n$),

we have $[E:E^T] \geq n$. And $[E^T:E^S] \geq 1$ as extension field degrees are always $\geq 1$.

Thus $[E:E^S] \geq n$, $\forall\, n \in \mathbb{N}$.

$\therefore$ $[E:E^S] = \infty$.

---

**2.** *Let K be the splitting field of some polynomial over F, and let u, v ∈ K. Prove that if u and v have the same minimal polynomial in F[x], then there exists σ ∈ Gal(K/F) such that σ(u) = v. (**Hint**: You may want to look back at the work we did to show splitting fields are unique.)*

**Proof**:

If $u$ and $v$ have the same minimal polynomial $p(x)$ in $F[x]$, then

$\overline{\varphi}_u: F[x]/(p(x)) \to F(u)$ defined by $f(x) + (p(x)) \mapsto f(u)$ and

$\overline{\varphi}_v: F[x]/(p(x)) \to F(u)$ defined by $f(x) + (p(x)) \mapsto f(v)$ are isomorphisms

by Lecture Notes 3/10/10 (If $E/F$ is an extension, $a \in E$, and $a$ is algebraic over $F$, then $F(a) \cong F[x](p(x))$ where $p(x)$ is an irreducible polynomial in $F[x]$ such that $a$ is a root.)

Thus $\psi: F(u) \to F(v)$ defined by $\psi(a) = \overline{\varphi}_v\,(\overline{\varphi}_u^{-1}(a))$ is an isomorphism.

Note that $\forall\ c \in F$, $\psi(c) = \overline{\varphi}_v\,(\overline{\varphi}_u^{-1}(c)) = \overline{\varphi}_v\,(c + (p(x))) = c$, and

$\psi(u) = \overline{\varphi}_v\,(\overline{\varphi}_u^{-1}(u)) = \overline{\varphi}_v\,(x + (p(x))) = v$. That is, $\psi$ fixes $F$ and sends $u$ to $v$.

Since $K$ is a splitting field of some polynomial $f(x)$ over $F$, it is a splitting field of

$f(x)$over both $F(u)$ and $F(v)$.

So we have

(1) $f(x) \in F[x] \subseteq F(u)[x]$ and $F[x] \subseteq F(v)[x]$ where $F$ is a field,

(2) $K$ is a splitting field for $f(x)$ over $F(u)$,

(3) $\psi: F(u) \to F(v)$ is an isomorphism,

(4) $K$ is a splitting field for $f(x)$ over $F(v)$.

Then by Lecture Notes 3/24/10 (If $f(x) \in F[x]$ where $F$ is a field, $E$ is a splitting field for $f(x)$ over $F$, $\varphi: F \to F'$ is an isomorphism, $\varphi^*: F[x] \to F'[x]$ is an isomorphism induced by $\varphi$, $E'$ is a splitting field for $f^*(x)$ over $F'$, then $\exists$ isomorphism $\Phi: E \to E'$ such that $\Phi$ extends $\varphi$ and $\varphi^*$.)

there is an isomorphism $\Phi: K \to K$ that extends $\psi$.

Thus, $\Phi$ is an automorphism of $K$ that fixes $F$. Thus $\Phi \in \text{Gal}(K/F)$ and $\Phi(u) = v$.

---