Debra Griffin
Galois Theory III
Worksheet #1 – 5

---

1. *Let F, K, E be fields. Prove that if $F \subseteq K \subseteq E$ and $F \lhd E$, then $K \lhd E$.*

Proof:
Assume $F \lhd E$, then E is a splitting field for some $f(x) \in F[x]$ such that f is separable (Lecture Notes 4/21/10).

Since $F \subseteq K \subseteq E$, then E is a splitting field for $f(x) \in K[x]$; hence $K \lhd E$.

---

2. *Let E be an extension of F. Prove that E is a splitting field of a separable polynomial in F[x] if and only if E is a splitting field of a polynomial in F[x] with no repeated roots.*

Proof:
Assume E is a splitting field of a separable polynomial $f(x)$ in $F[x]$.

Since F is a field, then $F[x]$ is a UFD, hence $f(x) = up_1(x)^{e_1}p_2(x)^{e_2}\cdots p_n(x)^{e_n}$ where the p_i's are distinct monic irreducible polynomials.

Since f is separable, then each p_i has no repeated roots.

Let $g(x) = p_1(x)p_2(x)\cdots p_n(x)$. Then $g(x) \in F[x]$ and has no repeated roots.

Conversely, assume E is a splitting field of a polynomial $h(x)$ in $F[x]$ with no repeated roots. Then $h(x)$ is separable. Thus E is a splitting field of a separable polynomial $h(x)$ in $F[x]$.

---

3. *Let E be an extension of F. Prove that if [E:F] = 2, then F ◁ E.*

Proof:

Assume [E:F] = 2. Then {1, v} is a basis for E over F.

(∗) We know $v \notin F$. For if $v \in F$, then $\forall\ w \in E$, $w = a \bullet 1 + b \bullet v$ where $a, b \in F$ and we would have $w \in F$. But [E:F] = 2 $\Rightarrow E \neq F$.

Claim: $E = F(v)$.

$F(v) \subseteq E$. So 2 = [E:F] = [E:$F(v)$][$F(v)$:F].

Since $v \notin F$, then [$F(v)$:F] > 1, hence [$F(v)$:F] = 2.

Thus [E:$F(v)$] = 1. Consequently, $E = F(v)$.

So 2 = [E:F] = [$F(v)$:F]. Since [$F(v)$:F] is finite, then by

Theorem 37, Field Extensions, Part I and LN 3/15/10, (If E/F is an extension of fields and $a \in E$, then [$F(a)$:F] is finite iff a is algebraic over F.)

v is algebraic over F.

By Theorem 34, Field Extensions, Part I and LN 3/15/10,(If E/F is an extension of fields and α is algebraic over F, then ∃! monic irreducible polynomial in $F[x]$ for which α is a root...)

∃! monic irreducible polynomial $f \in F[x]$ such that v is a root.

By Corollary 28, Field Extensions, Part I and LN 3/10/10,
(If E/F is an extension of fields, α is algebraic over F and $p \in F[x]$ is a irreducible polynomial which has α as a zero, then [$F(\alpha)$:F] = deg $p(x)$.)

[$F(v)$:F] = deg($f(x)$).

Thus $f(x) = x^2 + bx + c$ for some $b, c \in F$ and $f(v) = 0$.

Applying the quadratic formula, the roots of f are $\dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$.

If f has a repeated root then $b^2 - 4c = 0$.

Since $v^2 + bv + c = 0$, then $v = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2} = \dfrac{-b}{2}$.

This would force $v \in F$, a contradiction to (∗).

Thus f has no repeated roots.

Suppose $v = \dfrac{-b + \sqrt{b^2 - 4c}}{2}$ where $b^2 - 4c \neq 0$. Then the other root is

$\dfrac{-b - \sqrt{b^2 - 4c}}{2} = -b - \dfrac{-b + \sqrt{b^2 - 4c}}{2} = -b - v \in F(v)$.

Thus, E is a splitting field of a polynomial with no repeated roots.

$\therefore\ F \lhd E$.

---

4. *Let α and β be algebraic elements over $\mathbb{Q}$. Prove $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + r\beta)$ for some $r \in \mathbb{Q}$.*

Proof:
Let $p(x) = \text{irr}(\alpha,\mathbb{Q})$, and $q(x) = \text{irr}(\beta,\mathbb{Q})$.
Let L be a splitting field of $p(x)q(x)$ over $\mathbb{Q}$.
Let $\alpha = v_1, \ldots, v_m$ be roots of p in L.
Let $\beta = w_1, .., w_n$ be roots of q in L.
Since $\mathbb{Q}$ is infinite, $\exists\, r \in \mathbb{Q}$ such that $r \neq \frac{v_i - \alpha}{\beta - w_j}$ $\forall\ 1 \le i \le m, 1 < j \le n$.

Claim: $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + r\beta)$.
Since $\alpha + r\beta \in \mathbb{Q}(\alpha, \beta)$ by closure, then $\mathbb{Q}(\alpha + r\beta) \subseteq \mathbb{Q}(\alpha, \beta)$.
To show $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha + r\beta)$, we only need to show $\beta \in \mathbb{Q}(\alpha + r\beta)$.
For if $\beta \in \mathbb{Q}(\alpha + r\beta)$, then $\alpha = \alpha + r\beta - r\beta \in \mathbb{Q}(\alpha + r\beta)$.

Let $h(x) = p(\alpha + r\beta - rx) \in \mathbb{Q}(\alpha + r\beta)[x]$. Note that $h(\beta) = p(\alpha + r\beta - r\beta) = p(\alpha) = 0$.
Let $s(x) = \text{irr}(\beta,\mathbb{Q}(\alpha + r\beta))$. Since $h(\beta) = q(\beta) = 0$, and $q(x) \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\alpha + r\beta)[x]$, then they are both divisible by $s(x)$ by Lecture Notes 3/15/10 (If E/F is an extension, $a \in E$, a is algebraic over F, then (1) $\exists!$ monic irreducible polynomial $p(x)$ such that a is a root; (2) $p(x)$ is of minimal degree among all polynomials that have a as a root; and (3) If $f(x) \in F[x]$ such that $f(a) = 0$, then $p(x)|f(x)$.)
So all the roots of $s(x)$ are roots of $h(x)$ and all the roots of $s(x)$ are roots of $q(x)$.
We would like to show $s(x) = x - \beta$, for this would imply $\beta \in \mathbb{Q}(\alpha + r\beta)$ and our proof would be complete.
To this end, we return to consider the roots of $h(x) = p(\alpha + r\beta - rx)$ that are common to $q(x)$.
Suppose $h(w_j) = p(\alpha + r\beta - rw_j) = 0$ for some $j \neq 1$.
So $\alpha + r\beta - rw_j = v_i$ for some i.
So then $r\beta - cw_j = v_i - \alpha$
$r(\beta - w_j) = v_i - \alpha$
$r = \frac{v_i - \alpha}{\beta - w_j}$, a contradiction to how r was chosen.
$\therefore\ \beta$ is the only common root of $q(x)$ and $h(x)$.
Thus $s(x)$ has the single root, β, in L, hence $s(x) = (x - \beta)^u$ for some $u \in \mathbb{N}$.
Since char $\mathbb{Q} = 0$, then by Lecture Notes 4/19/10 (If F is a field and char $(F) = 0$, then every polynomial over $F[x]$ is separable.) we have that $u = 1$.
Thus, $s(x) = x - \beta$ as desired.

$\therefore\ \mathbb{Q}(\alpha + r\beta) = \mathbb{Q}(\alpha, \beta)$.

---

5. (a) *Prove* $\mathbb{F}_p \lhd \mathbb{F}_{p^n}$.

Proof:
$\mathbb{F}_p \lhd \mathbb{F}_{p^n}$ if and only if $\mathbb{F}_{p^n}$ is the splitting field of a separable polynomial $f(x) \in \mathbb{F}_p[x]$
(Lecture Notes 4/21/10 F ◁ E iff E is a splitting field for a separable polynomial over F.)

We have shown previously that $\mathbb{F}_{p^n}$ is a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p \cong \mathbb{F}_p$
(Lecture Notes 3/24/10 If E is a field with p^n elements, then E is a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$.)
Since $\mathbb{F}_p$ is finite, every polynomial over $\mathbb{F}_p$ is separable. (Lecture Notes 4/19/10).
Thus, $f(x) = x^{p^n} - x$ is separable.
$\therefore \mathbb{F}_p \lhd \mathbb{F}_{p^n}$.

(b) *Prove* $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$.

Proof:
By Galois Theory I, HW, #4, we have shown the Frobenius map $\sigma_p: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $\sigma_p(a) = a^p$ is an element of $\mathrm{Aut}(\mathbb{F}_{p^n})$ and $\circ(\sigma_p) = n$.
Thus $\langle \sigma_p \rangle \leq \mathrm{Aut}(\mathbb{F}_{p^n})$ and $|\langle \sigma_p \rangle| = n$. And as $\langle \sigma_p \rangle$ is cyclic, then $\langle \sigma_p \rangle \cong \mathbb{Z}_n$.
Since $\mathbb{F}_p \lhd \mathbb{F}_{p^n}$, by part (a), then $\mathbb{F}_{p^n}{}^{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)} = \mathbb{F}_p$.
So $n = [\mathbb{F}_{p^n}: \mathbb{F}_p] = [\mathbb{F}_{p^n}: \mathbb{F}_{p^n}{}^{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}] = |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$.
Note that by Galois Theory HW, # 2c, (If E is an extension of $\mathbb{F}_p$, then $\mathrm{Gal}(E/\mathbb{F}_p) = \mathrm{Aut}(E)$.)
we have that $\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.
Thus $\langle \sigma_p \rangle \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. And since $|\langle \sigma_p \rangle| = |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$, then $\langle \sigma_p \rangle = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.
Thus, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$.
