Debra Griffin
Galois Theory I
Worksheet #1 - 4

---

1. *Let $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$, and let α be a root of $p(x)$. Prove that the splitting field for $p(x)$ is $\mathbb{Q}(\alpha)$.*

Proof:

$p(x) = (x - e^{\frac{2\pi i}{5}})(x - e^{\frac{4\pi i}{5}})(x - e^{\frac{6\pi i}{5}})(x - e^{\frac{8\pi i}{5}})$.

So $\mathbb{Q}(e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}})$ is a splitting field for $p(x)$.

Claim: The 5th roots of unity, form a multiplicative group of order 5.

Let T be the set containing the 5th roots of unity.
Then the elements of T are roots of $f(x) = x^5 - 1$.
Note that $T \subseteq \mathbb{C}$, so multiplication is associative and commutative in T.
$1 \in T$ as $1^5 = 1$. Let $a, b \in T$. Then $a^5 = 1 = b^5$ as $f(a) = f(b) = 0$.
And we have $(ab)^5 = a^5 \bullet b^5 = 1 \bullet 1 = 1$. So T is closed under multiplication.
Since $(a^4)^5 = (a^5)^4 = 1^4 = 1$, then $\forall\, a \in T$, $a^4 \in T$. And $a \bullet a^4 = a^5 = 1$. Thus each element of T has an inverse. $\therefore$ T is a multiplicative group.
Since the elements of T are roots of $f(x)$, then $|T| \leq 5$.
Since $f'(x) = 5x^4$, then f and f' are relatively prime.
Hence f has no repeated roots, which gives us that $|T| = 5$.

Since 5 is prime, then the group is cyclic, and each nonidentity element generates the whole group.

$\therefore$ If $\alpha \in \{e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\}$, then $\mathbb{Q}(e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}) = \mathbb{Q}(\alpha)$.

---

2. *Let E be a field extension of F.*

(a) *Prove that Gal(E/F) is a subgroup of Aut(E).*

Proof:

Clearly $\text{Gal}(E/F) \subseteq \text{Aut}(E)$.

$i : E \to E$, the identity map, is an automorphism that fixes F, hence $\text{Gal}(E/F) \neq \emptyset$.

If $\sigma, \tau \in \text{Gal}(E/F)$, then since $\text{Aut}(E)$ is a group under composition (by Lecture Notes 4/5/10), we know $\sigma \circ \tau \in \text{Aut}(E)$.
Since $\sigma, \tau \in \text{Gal}(E/F)$, then $\forall\, c \in F$, $(\sigma \circ \tau)(c) = \sigma(\tau(c)) = \sigma(c) = c$.
So $\sigma \circ \tau \in \text{Gal}(E/F)$. Hence $\text{Gal}(E/F)$ is closed under composition.

Since $\text{Gal}(E/F) \subseteq \text{Aut}(E)$, i is the identity of $\text{Aut}(E)$, and i fixes F, then i is the identity of $\text{Gal}(E/F)$.

Since every element σ of $\text{Aut}(E)$ has an inverse, σ^{-1}, then if
$\sigma \in \text{Gal}(E/F)$, we have
$\forall\, c \in F$, $\sigma(c) = c$, and $\sigma^{-1}(c) = \sigma^{-1}(\sigma(c)) = c$, hence $\sigma^{-1} \in \text{Gal}(E/F)$.
$\therefore$ $\text{Gal}(E/F)$ satisfies all the axioms of a subgroup.

---

2. (b) *Prove that if E is an extension of $\mathbb{Q}$, then Gal(E/$\mathbb{Q}$) = Aut(E).*
(In other words, any automorphism of E will fix $\mathbb{Q}$.)

Proof:
By definition $\text{Gal}(E/\mathbb{Q}) \subseteq \text{Aut}(E)$.
Let $\sigma \in \text{Aut}(E)$.
Since $\sigma(1_{\mathbb{Q}}) = 1_E$, then $\forall\, n \in \mathbb{N}$, $\sigma(n) = \sigma(n \bullet 1_{\mathbb{Q}}) =$
$= \sigma(\, 1_{\mathbb{Q}} + 1_{\mathbb{Q}} + \cdots + 1_{\mathbb{Q}}\,)$ (for n summands)
$= \sigma(1_{\mathbb{Q}}) + \sigma(1_{\mathbb{Q}}) + \cdots + \sigma(1_{\mathbb{Q}})$
$= 1_E + 1_E + \cdots + 1_E$ (for n summands)
$= n \bullet 1_E$
$= n$.
And by hmo properties, we have
$\forall\, n \in \mathbb{N}$ $\sigma(-n) = -\sigma(n) = -n$ and $\sigma(n^{-1}) = \sigma(n)^{-1} = n^{-1}$.
Let $c \in \mathbb{Q}$, then $c = ab^{-1}$ where $a, b \in \mathbb{Z}$, $b \neq 0$.
Thus we have $\sigma(c) = \sigma(ab^{-1}) = \sigma(a)\varphi(b^{-1}) = \sigma(a)\, \sigma(b)^{-1} = ab^{-1} = c$.
$\therefore$ σ fixes $\mathbb{Q}$.

(c) *Prove that if E is an extension of $\mathbb{F}_p$, then Gal(E/$\mathbb{F}_p$) = Aut(E).*
(In other words, any automorphism of E will fix $\mathbb{F}_p$.)

Proof:
By definition $\text{Gal}(E/\mathbb{Q}) \subseteq \text{Aut}(E)$.
Let $\sigma \in \text{Aut}(E)$.
Since $\mathbb{F}_p \cong \mathbb{Z}_p$ and $\sigma(1_{\mathbb{Z}_p}) = 1_E$, then $\forall\, a \in \mathbb{Z}_p$, $\sigma(a) = \sigma(a \bullet 1_{\mathbb{Q}}) =$
$= \sigma(\, 1_{\mathbb{Z}_p} + 1_{\mathbb{Z}_p} + \cdots + 1_{\mathbb{Z}_p}\,)$ (for a summands)
$= \sigma(1_{\mathbb{Z}_p}) + \sigma(1_{\mathbb{Z}_p}) + \cdots + \sigma(1_{\mathbb{Z}_p})$
$= 1_E + 1_E + \cdots + 1_E$ (for a summands)
$= a \bullet 1_E$
$= a$.
$\therefore$ σ fixes $\mathbb{F}_p$.

---

3. *Determine Gal($\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$).*

Proof:

Let $f(x) = x^2 - \sqrt{2} = (x + \sqrt[4]{2})(x - \sqrt[4]{2})$.

Note that $\sqrt[4]{2}, -\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$, for if $\sqrt[4]{2} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$, then squaring both sides and collecting like terms would give us

$0 = a^2 + 2b^2 + (2ab - 1)\sqrt{2}$.

And linear independence of the basis elements of $\{1, \sqrt{2}\}$ determines that $a^2 + 2b^2 = 0$. This would imply that $a^2 = -2b^2$, a contradiction as $a, b \in \mathbb{Q}$.

Thus f is irreducible over $\mathbb{Q}(\sqrt{2})$.

And clearly, $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field for f.

Since f is irreducible over $\mathbb{Q}(\sqrt{2})$, we have

$\mathbb{Q}(\sqrt{2})(\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt{2})[x]/(f) \cong \mathbb{Q}(\sqrt{2})(-\sqrt[4]{2})$. Thus, $\forall\ \sigma \in \text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$, $\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}$.

And by definition of $\text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$, σ fixes $\mathbb{Q}(\sqrt{2})$. So then if $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$, then $\sigma = \text{Id}$.

If $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$, then $\sigma \neq \text{Id}$.

$\therefore\ \text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}_2$.

---

4. *Let $\sigma_p: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be given by $\sigma_p(a) = a^p$. This map is called the Frobenius map.*

(a) *Prove $\sigma_p \in Aut(\mathbb{F}_{p^n})$.*

Proof:

Let $a, b \in \mathbb{F}_{p^n}$. By commutative properties of a field and char $\mathbb{F}_{p^n} = p$, we have $\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a)\sigma_p(b)$ and $\sigma_p(a + b) = (a + b)^p = a^p + b^p = \sigma_p(a) + \sigma_p(b)$.

Thus, σ_p is a homomorphism.

Since $\mathbb{F}_{p^n}$ is a field, and ker σ_p is an ideal, then ker $\sigma_p = \{0\}$ or $\mathbb{F}_{p^n}$.

Homomorphism properties $\sigma_p(0) = 0$ and $\sigma_p(1) = 1$ give us that ker $\sigma_p \neq \mathbb{F}_{p^n}$.

Thus, ker $\sigma_p = \{0\}$, hence σ_p is injective.

And since $\mathbb{F}_{p^n}$ is finite and σ_p is injective, then σ_p is surjective by basic set theory.

$\therefore\ \sigma_p \in \text{Aut}(\mathbb{F}_{p^n})$.

---

4. (b) *Determine the order of σ_p in Aut($\mathbb{F}_{p^n}$).*

ord $(\sigma_p) = n$.

Proof:
Since $|\mathbb{F}_{p^n}| = p^n$ and $\mathbb{F}_{p^n}{}^*$ is a multiplicative group,

then $\forall\ a \in \mathbb{F}_{p^n}$ such that $a \neq 0$, $a^{p^n-1} = 1$. Hence $a^{p^n} = a$.

Since $(\sigma_p)^n(a) = (((a^p)^p)^p \cdots)^p = a^{p^n} = a$, then ord $(\sigma_p) \leq n$.

Suppose ord $(\sigma_p) = d < n$. Then $p^d < p^n$. Let $f(x) = x^{p^d} - x$.

We know f has at most p^d roots, but if we have $a = (\sigma_p)^d(a) = a^{p^d}$ for any $a \in \mathbb{F}_{p^n}$, then

then all p^n elements of $\mathbb{F}_{p^n}$ are roots of f, a contradiction.

$\therefore$ ord $(\sigma_p) = n$.
