Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 649 - Abstract Algebra
Instructor: Professor Sasha Polishchuk

Homework - Week 3
ID: 952091294
Term: Spring 2025
Due Date: 23^{th} April, 2025

Problem 11.5.5
Let $\mathbb{K}/\mathbb{k}$ be a Galois extension, and $\mathbb{L}$, $\mathbb{M}$ be intermediate fields. Denote by $\mathbb{L} \vee \mathbb{M}$ the minimal subfield of $\mathbb{K}$ containing $\mathbb{L}$ and $\mathbb{M}$.

(a) $(\mathbb{L} \cap \mathbb{M})^* = \langle \mathbb{L}^*, \mathbb{M}^* \rangle$.

(b) $(\mathbb{L} \vee \mathbb{M})^* = \mathbb{L}^* \cap \mathbb{M}^*$.

(c) Assume that $\mathbb{L}/\mathbb{k}$ is normal. Then $\mathrm{Gal}(\mathbb{L} \vee \mathbb{M}/\mathbb{M}) \cong \mathrm{Gal}(\mathbb{L}/(\mathbb{L} \cap \mathbb{M}))$.

Solution:

(a) We know that $L \cap M \subseteq L$, by the Galois correspondence, we have $L^* \subseteq (L \cap M)^*$. Similarly, we can see that $M^* \subseteq (L \cap M)^*$. Note that $\langle L^*, M^* \rangle$ is the smallest subgroup containing L^* and M^*. This implies $(L \cap M)^*$ contains $\langle L^*, M^* \rangle$. On the other hand, suppose $a \in \mathbb{K}$ is fixed by every element in the group $\langle L^*, M^* \rangle$, so a is invariant under every element in L^* and M^*. This is the same as $a \in L$ and $a \in M$, so $a \in L \cap M$. This proves $\langle L^*, M^* \rangle^* \subseteq L \cap M$, by Galois correspondence, we have $(L \cap M)^* \subseteq \langle L^*, M^* \rangle$. Thus, we can conclude that $(L \cap M)^* = \langle L^*, M^* \rangle$.

(b) By definition, we know that $L \vee M \supseteq L$ and $L \vee M \supseteq M$, by Galois correspondence, we have $(L \vee M)^* \subseteq L^*$ and $(L \vee M)^* \subseteq M^*$, so $(L \vee M)^* \subseteq L^* \cap M^*$. On the other hand, $L^* \cap M^* \subseteq L^*$ and $L^* \cap M^* \subseteq M^*$, by Galois correspondence, we have $(L^* \cap M^*)^* \supseteq L$ and $(L^* \cap M^*)^* \supseteq M$. Note that $L \vee M$ is the smallest subfield containing L and M, so $(L^* \cap M^*)^* \supseteq L \vee M$, by Galois correspondence, we have $L^* \cap M^* \subseteq (L \vee M)^*$. Thus, we can conclude that $(L \vee M)^* = L^* \cap M^*$.

(c) Consider the field extension $\mathbb{L}/(\mathbb{L} \cap \mathbb{M})/\mathbb{k}$. We know $\mathbb{L}/\mathbb{k}$ is normal, so $\mathbb{L}/\mathbb{L} \cap \mathbb{M}$ is also normal. The Galois correspondence and the isomorphisms in (a) and (b) give us two graphs as follows

$$
\begin{tikzcd}[column sep=small]
 & \mathbb{k} \arrow[d, dash] & \\
 & \mathbb{L} \cap \mathbb{M} \arrow[dl, dash, "\text{normal}"'] \arrow[dr, dash] & \\
\mathbb{L} \arrow[dr, dash] & & \mathbb{M} \arrow[dl, dash] \\
 & \mathbb{L} \vee \mathbb{M} \arrow[d, dash] & \\
 & \mathbb{K} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathrm{Gal}(\mathbb{K}/\mathbb{k}) \arrow[d, dash] & \\
 & \langle \mathbb{L}^*, \mathbb{M}^* \rangle \arrow[dl, dash, "\text{normal}"'] \arrow[dr, dash] & \\
\mathbb{L}^* \arrow[dr, dash] & & \mathbb{M}^* \arrow[dl, dash] \\
 & \mathbb{L}^* \cap \mathbb{M}^* \arrow[d, dash] & \\
 & \{e\} &
\end{tikzcd}
$$

By the second isomorphism theorems in groups, we know that $\mathbb{L}^* \cap \mathbb{M}^*$ is normal in $\mathbb{M}^*$ and we have an isomorphism

$$\langle \mathbb{L}^*, \mathbb{M}^* \rangle / \mathbb{L}^* \cong \mathbb{M}^* / \mathbb{L}^* \cap \mathbb{M}^*.$$

Apply the Galois correspondence again, and we have

$$(\mathbb{L} \cap \mathbb{M})^* / \mathbb{L}^* \cong \mathrm{Gal}(\mathbb{L}/\mathbb{L} \cap \mathbb{M}) \cong (\mathbb{L} \vee \mathbb{M})^* / \mathbb{M}^* \cong \mathrm{Gal}(\mathbb{L} \vee \mathbb{M}/\mathbb{M}).$$

Problem 11.5.6
Let $\mathbb{K}/\mathbb{k}$ be a finite Galois extension and p be a prime number.

(a) $\mathbb{K}$ has an intermediate subfield $\mathbb{L}$ such that $[\mathbb{K} : \mathbb{L}]$ is a prime power.

(b) If $\mathbb{L}_1$ and $\mathbb{L}_{\not\models}$ are intermediate subfields with $[\mathbb{K} : \mathbb{L}_1]$, $[\mathbb{K} : \mathbb{L}_2]$ both p-powers, and $[\mathbb{L}_1 : \mathbb{k}]$, $[\mathbb{L}_2 : \mathbb{k}]$ both prime to p, then $\mathbb{L}_1$ is $\mathbb{L}_1$ is $\mathbb{k}$-isomorphic to $\mathbb{L}_2$.

Solution:

(a) Suppose $[\mathbb{K} : \mathbb{k}] = n$ is finite. We know n can be written as product of prime powers and suppose $n = p^k m$ for some prime number p and $(p, m) = 1$. The Galois group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{k})$ has order n and by Sylow's theorem, the Sylow p-subgroup of G exists and has order p^k. By Galois correspondence, there exists a subfield $\mathbb{K}/\mathbb{L}/\mathbb{k}$ such that $[\mathbb{K} : \mathbb{L}] = p^k$.

(b) Under the same assumption of (a), suppose $[\mathbb{K} : \mathbb{L}_1] = [\mathbb{K} : \mathbb{L}_2] = p^k$ and since $[\mathbb{L}_1 : \mathbb{k}]$, $[\mathbb{L}_2] : \mathbb{k}$ are prime to p, the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{L}_1)$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{L}_2)$ are Sylow p-subgroups in G, and by Sylow theory, they are conjugate. There exists $g \in G$ such that $g\mathbb{L}_1^* g^{-1} = \mathbb{L}_2^*$. By Galois correspondence and the proof of Theorem 11.5.4 (iv), we know that

$$g\mathbb{L}_1^* g^{-1} = g(\mathbb{L}_1)^* = \mathbb{L}_2^*.$$

So $g : \mathbb{K} \to \mathbb{K}$ restricting to $\mathbb{L}_1$ defines an isomorphism $\mathbb{L}_1 \to \mathbb{L}_2$ fixing the base field $\mathbb{k}$.

Problem 11.5.7
Let $f \in \mathbb{k}[x]$, $\mathbb{K}/\mathbb{k}$ be a splitting field for f over $\mathbb{k}$, and $G := \mathrm{Gal}(\mathbb{K}/\mathbb{k})$.

1. G acts on the set of the roots of f.
2. G acts transitively if f is irreducible.
3. If f has no multiple roots and G acts transitively then f is irreducible.

Solution:

(a) We need to show that for any $g \in G$ and any $\alpha \in \mathbb{K}$ is a root of f, $g(\alpha)$ is also a root of f. Indeed, we know that $g(\alpha)$ is a root of $g(f)$ and since $f \in \mathbb{k}[x]$ and g fixes every element in $\mathbb{k}$, g fixes the polynomial f, so $g(f) = f$. Thus, we can conclude that G acts on the set of roots of f.

(b) By Theorem 11.3.3, $\mathbb{K}/\mathbb{k}$ is a normal extension and by Proposition 11.3.9, G acts transitively if f is irreducible.

(c) The condition is equivalent to $\mathbb{K}/\mathbb{k}$ is a finite Galois extension. Assume f is not irreducible over $\mathbb{k}$ and $h|f$ for some irreducible polynomial $h \in \mathbb{k}[x]$. Suppose $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ are roots of f and $\alpha_1, \ldots, \alpha_k$ are roots of h for $1 \le k < n$. Note that for any $g \in G$, g fixes $h \in \mathbb{k}[x]$ so g must send a root of h to another root of h. This means there does not exists $g \in G$ such that $g(\alpha_1) = \alpha_n$. This contradicts the assumption that G acts transitively, so f is irreducible.

Problem 11.6.2

Let $\mathbb{k}$ be a field, $p(x)$ be an irreducible polynomial in $\mathbb{k}[x]$ of degree n, and let $\mathbb{K}$ be a Galois extension of $\mathbb{k}$ containing a root α of $p(x)$. Let $G = \mathrm{Gal}(\mathbb{K}/\mathbb{k})$, and G_α be the set of all $\sigma \in G$ with $\sigma(\alpha) = \alpha$. Then:

(a) $[G : G_\alpha] = n$;

(b) $G_\alpha^* = \mathbb{k}(\alpha)$;

(c) If G_α is normal in G then $p(x)$ splits in the fixed field of G_α.

Solution:

(a) Suppose $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ are roots of $p(x)$. For all $1 \le i \le n$, choose $\sigma_i \in G$ satisfying $\sigma_i(\alpha_1) = \alpha_i$.

Claim: $G = \sigma_1 G_\alpha \sqcup \cdots \sqcup \sigma_n G_\alpha$ is a coset decomposition of G with respect to the subgroup G_α.

Proof: We first prove the cosets are disjoint. Suppose there exists $g \in \sigma_i G_\alpha \cap \sigma_j G_\alpha$ for some $1 \le i, j \le n$, then $g = \sigma_i g_1 = \sigma_j g_2$ for some $g_1, g_2 \in G_\alpha$. Then

$$\alpha_i = \sigma_i g_1(\alpha_1) = \sigma_j g_2(\alpha_1) = \alpha_j.$$

This implies $i = j$. Next, we are going to show that for every $g \in G$, g must be in one of the coset. Suppose $g(\alpha_1) = \alpha_k$ for some $1 \le k \le n$. Note that $\sigma_k^{-1} g(\alpha_1) = \alpha_1$, so $\sigma_k^{-1} g \in G_\alpha$. There exists $g' \in G_\alpha$ such that $\sigma_k^{-1} g = g'$, namely $g = \sigma_k g'$, so $g \in \sigma_k G_\alpha$. ■

From the claim, we know that G_α has n cosets in G, so by definition $[G : G_\alpha] = n$.

(b) By definition, G_α fixes every element in $\mathbb{k}(\alpha)$, so $G_\alpha \subseteq \mathrm{Gal}(\mathbb{k}(\alpha)/\mathbb{k})$. By Galois correspondence, this means $G_\alpha^* \supseteq \mathbb{k}(\alpha)$. Moreover, by Galois correspondence and (a), we have

$$[\mathbb{k}(\alpha) : \mathbb{k}] = |\mathrm{Gal}(\mathbb{k}(\alpha)/\mathbb{k})| = n = [G : G_\alpha] = [G_\alpha^* : \mathbb{k}].$$

This tells us that $G_\alpha^* = \mathbb{k}(\alpha)$.

(c) If G_α is normal in G, by Galois correspondence, $G_\alpha^*/\mathbb{k}$ is a normal extension. We know the polynomial $p(x)$ already has one root α in $G_\alpha^* = \mathbb{k}(\alpha)$, by definition of normal extension, $p(x)$ splits in G_α^*.

Problem 11.6.3

Let $\Bbbk(\alpha)/\Bbbk$ be a field extension obtained by adjoining a root α of an irreducible separable polynomial $f \in \Bbbk[x]$. Then there exists an intermediate field $\Bbbk \subsetneq \mathbb{F} \subsetneq \Bbbk(\alpha)$ if and only if $\mathrm{Gal}(f; \Bbbk)$ is imprimitive (as a permutation group on the roots), in which case $\mathbb{F}$ can be chosen so that $[\mathbb{F} : \Bbbk]$ is equal to the number of imprimitive blocks.

Solution: By Theorem 7.1.11 (Primitivity Criterion), $G = \mathrm{Gal}(f; \Bbbk)$ is primitive if and only if the stabilizer G_β is a maximal subgroup for any root β of the polynomial f. Write $\mathbb{N}$ as the splitting field of f. Suppose there exists an intermediate field $\Bbbk \subsetneq \mathbb{F} \subsetneq \Bbbk(\alpha)$, by Galois correspondence, there exists a proper subgroup $\mathbb{F}^* \subsetneq G$ containing the stabilizer $\Bbbk(\alpha)^* = G_\alpha$. This implies G is not primitive. Conversely, suppose G is not primitive. Then there exists a proper subgroup H satisfying $G_\alpha \subsetneq H \subsetneq G$. By Galois correspondence, the fixed field H^* is an intermediate field and $[H^* : \Bbbk] = [G : H] = n$. Write

$$G = g_1 H \sqcup \cdots \sqcup g_n H$$

and define $X_i := \{g_i h \cdot \alpha \mid h \in H\}$ for $1 \le i \le n$. We have proved in the proof of Theorem 7.1.11, $X_1, \ldots, X_n$ are imprimitivity blocks, so this implies that $\mathbb{F} = H^*$ can be chosen so that $[\mathbb{F} : \Bbbk]$ is equal to the number of imprimitive blocks.

Problem 11.6.6

Find all subfields of the splitting field of $x^3 - 7$ over $\mathbb{Q}$. Which of the subfields are normal over $\mathbb{Q}$?

Solution: Write

$$x^3 - 7 = (x - \sqrt[3]{7})(x - \sqrt[3]{7}\omega)(x - \sqrt[3]{7}\omega^2)$$

where ω is the 3rd primitive root of unit satisfying $\omega^2 + \omega + 1 = 0$. The splitting field of $x^3 - 7$ is $\mathbb{K} = \mathbb{Q}(\sqrt[3]{7}, \omega)$. We know that

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt[3]{7})][\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

So the Galois group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is a group of order 6. Consider the following two field automorphisms $\sigma, \tau : \mathbb{K} \to \mathbb{K}$ where σ fixes $\sqrt[3]{7}$ and permutes ω and ω^2 in $\mathbb{K}$, τ sends $\sqrt[3]{7}$ to $\sqrt[3]{7}\omega$, $\sqrt[3]{7}\omega$ to $\sqrt[3]{7}\omega^2$ and $\sqrt[3]{7}\omega^2$ to $\sqrt[3]{7}$. $\sigma \in G$ is an element of order 2 and $\tau \in G$ is an element of order 3. Note that

$$\sigma\tau(\sqrt[3]{7}) = \sigma(\sqrt[3]{7}\omega) = \sqrt[3]{7}\omega^2 \neq \sqrt[3]{7}\omega = \tau\sigma(\sqrt[3]{7}).$$

So G is not commutative and has to be S_3. The subgroup generated by σ is a subgroup of index 2 in G, thus it is the normal subgroup $\langle(123)\rangle$, corresponding to the normal extension $\mathbb{Q}(\omega)/\mathbb{Q}$. The subgroups $\langle(12)\rangle$, $\langle(23)\rangle$ and $\langle(13)\rangle$ are conjugate Sylow 2-group in G of index 3, corresponding to the degree 3 subextension $\mathbb{Q}(\sqrt[3]{7})$, $\mathbb{Q}(\sqrt[3]{7}\omega)$ and $\mathbb{Q}(\sqrt[3]{7}\omega^2)$. None of them are normal. These are all the subfields of $\mathbb{K}$.

Problem 11.6.7
Let $\mathbb{K}$ be a splitting field for $x^4 + 6x^2 + 5$ over $\mathbb{Q}$. Find subfields of $\mathbb{K}$.

Solution: Write

$$x^4 + 6x^2 + 5 = (x + i)(x - i)(x + \sqrt{5}i)(x - \sqrt{5}i).$$

We know that

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

So the Galois group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is either the cyclic group C_4 or the direct sum of two cyclic groups $C_2 \oplus C_2$. Note that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ are two different subfields of $\mathbb{K}$, but C_4 only has one nontrivial proper subgroup, so $G = C_2 \oplus C_2$. G has three subgroups of index 2, corresponding to the subfields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{5}i)$. All of them are normal because G is an abelian group.