Math 562/662 **Spring 2024**
Homework 6 **Drew Armstrong**

---

1. The Galois Group Permutes the Roots. Let $\mathbb{E} \supseteq \mathbb{F}$ be a splitting field for a specific polynomial $f(x) \in \mathbb{F}[x]$ of degree n. This means that $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ for some elements $\alpha_1, \ldots, \alpha_n$ satisfying

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Let $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ be the group of automorphisms $\sigma : \mathbb{E} \to \mathbb{E}$ satisfying $\sigma(a) = a$ for all $a \in \mathbb{F}$.

(a) For each $\sigma \in G$ and each root α_i of $f(x)$, show that $\sigma(\alpha_i)$ is also a root of $f(x)$. Hence for each $\sigma \in G$ and $i \in \{1, \ldots, n\}$ there exists a unique $\pi_\sigma(i) \in \{1, \ldots, n\}$ satisfying

$$\sigma(\alpha_i) = \alpha_{\pi_\sigma(i)}.$$

Let $\pi_\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ denote the corresponding function.

(b) Show that the function π_σ is a permutation. [Hint: It suffices to show that π_σ is injective. Recall that σ is injective by assumption.]

(c) Show that the function $\Pi : G \to S_n$ defined by $\sigma \mapsto \pi_\sigma$ is a group homomorphism.

(d) Finally, show that Π is injective. [Hint: A group homomorphism is injective if and only if its kernel is trivial. If $\pi_\sigma \in S_n$ is the identity permutation, show that $\sigma \in G$ must be the identity automorphism.]

2. Abstract Galois Connections. Let $(P, \leq)$ and $(Q, \leq)$ be posets. Let $* : P \leftrightarrows Q : *$ be a pair of functions satisfying the following property:[1]

$$\text{for all } p \in P \text{ and } q \in Q \text{ we have } p \leq q^* \iff q \leq p^*.$$

Such a pair is called an *abstract Galois connection*. Since the following results are symmetric in P and Q you only need to prove half of them.

(a) For all $p \in P$ and $q \in Q$ show that $p \leq p^{**}$ and $q \leq q^{**}$.

(b) For all $p_1, p_2 \in P$ and $q_1, q_2 \in Q$ show that $p_1 \leq p_2 \Rightarrow p_2^* \leq p_1^*$ and $q_1 \leq q_2 \Rightarrow q_2^* \leq q_1^*$.

(c) For all $p \in P$ and $q \in Q$ show that $p^{***} = p^*$ and $q^{***} = q^*$.

(d) Let $P' = \{p \in P : p^{**} = p\}$ and $Q' = \{q \in Q : q^{**} = q\}$. Show that the maps $* : P \leftrightarrows Q : *$ restrict to a **bijection**:

$$* : P' \leftrightarrow Q' : *.$$

3. The Galois Group of a Cyclotomic Extension. Let $\omega = \exp(2\pi i/n)$. The splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$ is

$$\mathbb{Q}(1, \omega, \ldots, \omega^{n-1}) = \mathbb{Q}(\omega).$$

In this problem you will prove that $G := \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, assuming that the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.[2]

(a) For any $\sigma \in G$ show that we must have $\sigma(\omega) = \omega^k$ for some $\gcd(k, n) = 1$. [Hint: Show that $\Phi_n(\omega) = 0$ implies $\Phi_n(\sigma(\omega)) = 0$.]

---

[1]We write p^* instead of $*(p)$. Because of the symmetry we don't need to give the functions different names.

[2]This is fairly difficult to prove in general. On the previous homework you (almost) proved that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ when p is prime.

(b) For any $0 \leq k < n$ with $\gcd(k,n) = 1$ show that there exists a (unique) element $\sigma \in G$ satisfying $\sigma(\omega) = \omega^k$. [Hint: Since ω and ω^k are both roots of the irreducible polynomial $\Phi_n(x) \in \mathbb{Q}[x]$, the minimal polynomial theorem implies that

$$\mathbb{Q}(\omega) \cong \frac{\mathbb{Q}[x]}{\Phi_n(x)\mathbb{Q}[x]} \cong \mathbb{Q}(\omega^k).]$$

(c) For any $0 \leq k < n$ with $\gcd(k,n) = 1$ let $\sigma_k \in G$ we the unique element satisfying $\sigma_k(\omega) = \omega^k$. Show that the map $(\mathbb{Z}/n\mathbb{Z})^\times \to G$ defined by $k \mapsto \sigma_k$ is a group isomorphism. [Hint: First show that $(\sigma_k \circ \sigma_\ell)(\omega) = \sigma_{k\ell}(\omega)$. Then use the fact that every element of $\mathbb{Q}(\omega)$ has the form $f(\omega)/g(\omega)$ for some $f(x), g(x) \in \mathbb{Q}[x]$ with $g(\omega) \neq 0$.]

4. Finite Dimensional Field Extensions. Consider a field extension $\mathbb{E} \supseteq \mathbb{F}$ where $\mathbb{E}$ is finite-dimensional as a vector space over $\mathbb{F}$, i.e., $[\mathbb{E}/\mathbb{F}] < \infty$.

(a) Prove that every element $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, i.e., is the root of some polynomial $f(x) \in \mathbb{F}[x]$. [Hint: Since $\mathbb{E}$ is finite-dimensional over $\mathbb{F}$, the infinite list of elements $1, \alpha, \alpha^2, \ldots$ must be linearly dependent over $\mathbb{F}$.]

(b) Prove that $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ for some finite list of elements $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$. [Hint: Use induction on dimension. If $[\mathbb{E}/\mathbb{F}] = 1$ then $\mathbb{E} = \mathbb{F}$ and there is nothing to show so suppose that $[\mathbb{E}/\mathbb{F}] \geq 2$, i.e., $\mathbb{E} \neq \mathbb{F}$. Choose any element $\alpha_1 \in \mathbb{E} \setminus \mathbb{F}$ and consider the fields $\mathbb{E} \supseteq \mathbb{F}(\alpha_1) \supseteq \mathbb{F}$. Dedekind's Tower Law says

$$[\mathbb{E}/\mathbb{F}] = [\mathbb{E}/\mathbb{F}(\alpha_1)] \cdot [\mathbb{F}(\alpha_1)/\mathbb{F}].$$

Since $\mathbb{F}(\alpha_1) \neq \mathbb{F}$ we have $[\mathbb{F}(\alpha_1)/\mathbb{F}] \geq 2$, hence $[\mathbb{E}/\mathbb{F}(\alpha_1)]$ is strictly less than $[\mathbb{E}/\mathbb{F}]$.]

5. Characteristic Zero Fields are Perfect. A field $\mathbb{F}$ is called *perfect* if irreducible polynomials $f(x) \in \mathbb{F}[x]$ have *no repeated roots* in any field extension $\mathbb{E} \supseteq \mathbb{F}$. Prove that fields of characteristic zero are perfect. [Hint: Since $\mathbb{F}$ has characteristic zero we know that $\deg(Df) = \deg(f) - 1$. In particular, $Df(x) \neq 0$. Use the fact that $f(x)$ is irreducible to show that $\gcd(f, Df) = 1$ in $\mathbb{F}[x]$. On the other hand, if $f(x)$ has a repeated root $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ in some field extension show that we must have $\deg(f, Df) \neq 1$ in $\mathbb{E}[x]$.]

6. The Primitive Element Theorem. Let $\mathbb{F}$ be any subfield of $\mathbb{C}$, so $\mathbb{F}$ has characteristic zero.[3] Given any two numbers $\alpha, \beta \in \mathbb{C}$ that are algebraic over $\mathbb{F}$, we will prove that there exists a number $\gamma \in \mathbb{C}$ (also algebraic over $\mathbb{F}$) satisfying

$$\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma).$$

More precisely, we will show that there exists a scalar $c \in \mathbb{F}$ such that $\gamma := \alpha + c\beta$ satisfies the desired property.

(a) Show that every field of characteristic zero is infinite.

(b) Let $f(x), g(x) \in \mathbb{F}[x]$ be the minimal polynomials of α, β. Since $\mathbb{F}$ is infinite we may choose an element $c \in \mathbb{F}$ such that $c \neq (\alpha' - \alpha)/(\beta - \beta')$ for all roots $\alpha', \beta' \in \mathbb{E}$ of $f(x), g(x)$, respectively. Define $\gamma := \alpha + c\beta$ and consider the polynomial

$$h(x) := f(\gamma - cx) \in \mathbb{F}(\gamma)[x].$$

Show that the greatest common divisor of $g(x)$ and $h(x)$ in $\mathbb{F}(\gamma)[x]$ has degree ≤ 1. [Hint: Note that β is a common root of $g(x)$ and $h(x)$. If the gcd of $g(x)$ and $h(x)$ in $\mathbb{F}(\gamma)[x]$ has degree ≥ 2, use Problem 5 to show that $g(x)$ and $h(x)$ have another common root $\beta' \neq \beta$, which contradicts the definition of c.]

[3] This proof works more generally for any perfect field $\mathbb{F}$; e.g., for any finite field. Then we replace $\mathbb{C}$ with any field large enough to contain all the roots of the minimal polynomials of α and β.

(c) Let $p(x) \in \mathbb{F}(\gamma)[x]$ be the minimal polynomial of β over $\mathbb{F}(\gamma)$. Prove that $p(x) = x - \beta$, and hence $\beta \in \mathbb{F}(\gamma)$. [Hint: Since $g(x), h(x) \in \mathbb{F}(\gamma)[x]$ have β as a common root, show that $p(x)$ divides the gcd of $g(x)$ and $h(x)$ in $\mathbb{F}(\gamma)[x]$. Then use part (b).]

(d) Finally, use (c) to show that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$.

(e) **Corollary.** Let $\mathbb{E} \supseteq \mathbb{F}$ be any finite-dimensional extension of characteristic zero fields. Use Problem 4 to show that $\mathbb{E} = \mathbb{F}(\gamma)$ for some $\gamma \in \mathbb{E}$.

Remark: This result is the **first step** in the proof of the Fundamental Theorem of Galois Theory. I will provide a note that sketches out the rest of the proof.