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 $f(x) \in \mathbb{F}[x]$. This means that $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ for some distinct elements $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ satisfying

$$f(x) = \prod_i (x - \alpha_i)^{k_i}$$

for some integers $k_i \geq 1$. 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.]

(a): Consider any $\sigma \in G$. Since $f(x)$ has coefficients in $\mathbb{F}$ and since G fixes $\mathbb{F}$ we have

$$0 = \sigma(0) = \sigma(f(\alpha_i)) = f^\sigma(\sigma(\alpha_i)) = f(\sigma(\alpha_i)).$$

Hence $\sigma(\alpha_i) = \alpha_j$ for some j. We define the function $\pi_\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ so that $\sigma(\alpha_i) = \alpha_{\pi_\sigma(i)}$. In other words, we have $\pi_\sigma(i) = j$ if and only if $\sigma(\alpha_i) = \alpha_j$.

(b): If $\pi_\sigma(i) = \pi_\sigma(j)$ then $\sigma(\alpha_i) = \sigma(\alpha_j)$. Since σ is injective this implies that $\alpha_i = \alpha_j$, and since the roots are distinct this implies $i = j$.

(c): Define the function $\Pi : G \to S_n$ by $\Pi(\sigma) := \pi_\sigma$. (This notation is really piling up!) I claim that Π is a group homomorphism. To see this, consider any $\sigma, \mu \in G$. We wish to show that $\Pi(\sigma \circ \mu) = \Pi(\sigma) \circ \Pi(\mu)$, i.e., $\pi_{\sigma\circ\mu} = \pi_\sigma \circ \pi_\mu$ as permutations. That is, for any $i \in \{1, \ldots, n\}$ we wish to show that

$$\pi_{\sigma\circ\mu}(i) = [\pi_\sigma \circ \pi_\mu](i).$$

This is a lot easier than it looks. Suppose that $\mu(\alpha_i) = \alpha_j$ and $\sigma(\alpha_j) = \alpha_k$, hence $(\sigma\circ\mu)(i) = k$. This implies that $\pi_\mu(i) = j$ and $\pi_\sigma(j) = k$, hence $[\pi_\sigma \circ \pi_\mu](i) = k$. And it also implies that $\pi_{\sigma\circ\mu}(i) = k$. Done.

Remark: The difficulty here is that the function Π sends functions σ to functions π_σ. But in order to check that functions are equal we need to apply them to all possible inputs. There's a lot going on. It's really an exercise in notational hygiene.

(d): To show that the group homomorphism Π is injective it is sufficient to show that $\ker \Pi = \{\mathrm{id}\}$, where id is the identity automorphism $\mathbb{E} \to \mathbb{E}$. So consider any $\sigma \in \ker \Pi$, i.e., such that π_σ is the identity permutation. Since $\pi_\sigma(i) = i$ for all i we have $\sigma(\alpha_i) = \alpha_i$ for all i. Since $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$, a general element of $\mathbb{E}$ has the form $f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n)$ for polynomials $f(\mathbf{x}), g(\mathbf{x})$ with coefficients in $\mathbb{F}$. Since σ preserves field operations and fixes the coefficients of f and g, we have

$$\sigma\left(\frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\ldots,\alpha_n)}\right) = \frac{f(\sigma(\alpha_1),\ldots,(\alpha_n))}{g(\sigma(\alpha_1),\ldots,\sigma(\alpha_n))} = \frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\ldots,\alpha_n)}.$$

Since σ fixes every element of $\mathbb{E}$ we conclude that $\sigma = \mathrm{id}$ as desired.

Remark: In general, an automorphism of a field extension $\mathbb{F}(\alpha_1,\ldots,\alpha_n)$ is determined by its values on $\mathbb{F}$ and $\alpha_1,\ldots,\alpha_n$.

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]

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

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**:

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

(a): For any $p \in P$ we have $(p^*) \leq (p)^*$ by reflexivity of $\leq$. Then from $(*)$ we get $(p) \leq (p^*)^*$.

(b): Consider $p_1, p_2 \in P$ with $p_1 \leq p_2$. From (a) we have $p_1 \leq p_2 \leq p_2^{**}$, which implies $p_1 \leq p_2^{**}$ by transitivity of $\leq$. Then $(*)$ says that $(p_1) \leq (p_2^*)^*$ implies $(p_2^*) \leq (p_1)^*$.

(c): Consider any $p \in P$. By reflexivity of $\leq$ we have $(p^{**}) \leq (p^*)^*$ and then $(*)$ implies $(p^*) \leq (p^{**})^*$. On the other hand, from (a) we have $p \leq p^{**}$, then from (b) we have $(p^{**})^* \leq (p)^*$. Since $p^* \leq p^{***}$ and $p^{***} \leq p^*$ we conclude from antisymmetry of $\leq$ that $p^{***} = p^*$.

(d): First note that $*$ sends elements of P' to elements of Q'. Indeed, consider any $p \in P'$ so that $p^{**} = p$ and let $q = p^*$. Then from (c) we have $q^{**} = p^{***} = p^* = q$, hence $q \in Q'$. To show that $* : P' \to Q'$ is injective, suppose that $p_1^* = p_2^*$ for some $p_1, p_2 \in P'$. Then applying $*$ to both sides gives $p_1 = p_1^{**} = p_2^{**} = p_2$. To show that $* : P' \to Q'$ is surjective, consider any $q \in Q'$ and define $p := q^*$. This p is in P' because $p^{**} = q^{***} = q^* = p$ by (c). We also have $p^* = q^{**} = q$, so q is the image of $p \in P'$ under $*$.

Remark: Abstract Galois connections between posets are a simple example of *adjoint functors between categories.*[2] I say that category theory is "empty" because it doesn't care what kind of objects you're working with; only the abstract relations between them. In the sketch of Galois theory linked below, when I say that something is true for "empty reasons", I am referring to Problem 2.

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

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

[1] We write p^* instead of $*(p)$. Because of the symmetry we don't need to give the functions different names.
[2] A poset is a simple example of a category.

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 $\mathbb{Q}$.[3]

(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 $\Phi_n(\sigma(\omega)) = 0$.]

(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 $g(\omega) \neq 0$.]

(a): Consider any $\sigma \in G$. Since $\Phi_n(\omega) = 0$ and since σ fixes the coefficients of $\Phi_n(x)$ (because they are in $\mathbb{Q}$) we have

$$0 = \sigma(0) = \sigma(\Phi_n(\omega)) = \Phi_n(\sigma(\omega)).$$

This implies that $\sigma(\omega)$ is also a root of $\Phi_n(x)$, which implies that $\sigma(\omega) = \omega^k$ for some integer $1 \leq k \leq n$ with $\gcd(k,n) = 1$.[4]

(b): For any integer k we have $\omega^k \in \mathbb{Q}(\omega)$ and hence $\mathbb{Q}(\omega^k) \subseteq \mathbb{Q}(\omega)$. If $\gcd(k,n) = 1$ then I claim that we also have $\omega \in \mathbb{Q}(\omega^k)$, and hence $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\omega^k)$. Indeed, since $\gcd(k,n) = 1$ we can write $ka + nb = 1$ for some $a, b \in \mathbb{Z}$. Then we have

$$\omega = \omega^{ka+nb} = (\omega^k)^a(\omega^n)^b = (\omega^k)^a(1)^b = (\omega^k)^a \in \mathbb{Q}(\omega^k).$$

We have shown that $\Omega(\omega) = \Omega(\omega^k)$ when $\gcd(k,n) = 1$. In this case we also know that ω and ω^k are both roots of $\Phi_n(x)$. Assuming that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ (which it is), we obtain ring isomorphisms $\varphi : \mathbb{Q}(\omega) \cong \mathbb{Q}[x]/\Phi_n(x)\mathbb{Q}[x]$ and $\psi : \mathbb{Q}(\omega^k) \cong \mathbb{Q}[x]/\Phi_n(x)\mathbb{Q}[x]$ with $\varphi(\omega) = [x]$ and $\psi(\omega^k) = [x]$. Hence $\sigma_k := \psi^{-1} \circ \varphi$ is a ring isomorphism of $\mathbb{Q}(\omega) \to \mathbb{Q}(\omega^k)$ sending ω to ω^k. But $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$, so σ_k is an automorphism of $\mathbb{Q}(\omega)$ as desired.

(c): Note that an element of G is uniquely determined by its action on ω. This implies that

$$\sigma_k = \sigma_\ell \iff \omega^k = \omega^\ell \iff k \equiv \ell \bmod n.$$

Combining this with (a) and (b) gives us a bijection $(\mathbb{Z}/n\mathbb{Z})^\times \to G$ defined by $\sigma \mapsto \sigma_k$. I claim that this map is also a group homomorphism. To see this we must show that $\sigma_k \circ \sigma_\ell = \sigma_{k\ell}$ and for this it suffices to show that the two maps do the same thing to ω.[5] Indeed, we have

$$\sigma_{k\ell}(\omega) = \omega^{k\ell} = (\omega^k)^\ell = \sigma_k(\omega)^\ell = \sigma_k(\omega^\ell) = \sigma_k(\sigma_\ell(\omega)) = [\sigma_k \circ \sigma_\ell](\omega).$$

[3] 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.

[4] Indeed, we **defined** $\Phi_n(x)$ as the product of $(x - \omega^k)$ over integers $1 \leq k \leq n$ with $\gcd(k,n) = 1$. Then from this we had to prove that the coefficients are in $\mathbb{Q}$ (in fact, in $\mathbb{Z}$).

[5] For any two $\varphi, \psi \in G$ with $\varphi(\omega) = \psi(\omega)$ we must have $\varphi = \psi$, since for any element $\alpha = f(\omega)/g(\omega) \in \mathbb{Q}(\omega)$ with $f(x), g(x) \in \mathbb{Q}[x]$ we must have

$$\varphi(\alpha) = \frac{f(\varphi(\omega))}{g(\varphi(\omega))} = \frac{f(\psi(\omega))}{g(\psi(\omega))} = \psi(\alpha).$$

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 $[\mathbb{E}/\mathbb{F}]$.]

(a): Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension with $[\mathbb{E}/\mathbb{F}] = n < \infty$. Then for any $\alpha \in \mathbb{E}$ the set $1, \alpha, \ldots, \alpha^n$ of $n+1$ elements must be linearly dependent over $\mathbb{F}$. That is, we can find some $a_0, \ldots, a_n \in \mathbb{F}$, not all zero, such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Then α is algebraic over $\mathbb{F}$ because it is a root of the nonzero polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$.

(b): Let $[\mathbb{E}/\mathbb{F}] < \infty$. If $[\mathbb{E}/\mathbb{F}] = 1$ then we have $\mathbb{E} = \mathbb{F}$. So let $[\mathbb{E}/\mathbb{F}] \geq 2$ and pick any $\alpha_1 \in \mathbb{E} \setminus \mathbb{F}$. Since $\mathbb{F}(\alpha_1) \neq \mathbb{F}$ we have $[\mathbb{F}(\alpha_1)/\mathbb{F}] \geq 2$. Combining this with the Tower Law $[\mathbb{E}/\mathbb{F}] = [\mathbb{E}/\mathbb{F}(\alpha_1)][\mathbb{F}(\alpha_1)/\mathbb{F}]$ shows that $[\mathbb{E}/\mathbb{F}(\alpha_1)] < [\mathbb{E}/\mathbb{F}]$. By induction on dimension, we may assume that there exist $\alpha_2, \ldots, \alpha_n \in \mathbb{E}$ such that

$$\mathbb{E} = \mathbb{F}(\alpha_1)(\alpha_2, \ldots, \alpha_n).$$

But $\mathbb{F}(\alpha_1)(\alpha_2, \ldots, \alpha_n) = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

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 $\mathbb{E}[x]$.]

Let $\mathbb{F}$ have characteristic zero and let $f(x) \in \mathbb{F}[x]$ be any irreducible polynomial. If $f(x)$ has a repeated root $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ then we can write $f(x) = (x - \alpha)^2 g(x)$ with $g(x) \in \mathbb{E}[x]$ and then taking the derivative shows that $x - \alpha$ divides $\gcd(f, Df)$ in $\mathbb{E}[x]$. But you showed on the last homework that $\gcd(f, Df) \neq 1$ in $\mathbb{E}[x]$ implies $\gcd(f, Df) \neq 1$ in $\mathbb{F}[x]$. Since $f(x)$ is irreducible in $f(x)$ this is only possible if $f(x)$ divides $Df(x)$. But this is impossible because $\deg(Df) < \deg(f)$.

6. The Primitive Element Theorem. Let $\mathbb{F}$ be any subfield of $\mathbb{C}$, so $\mathbb{F}$ has characteristic zero.[6] 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

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

[6] 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.

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.]

(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 $\gamma \in \mathbb{E}$.

(a): For any field $\mathbb{F}$ and for any integer $n \geq 1$ we recall that $n \cdot 1 := 1 + \cdots + 1$ (n times). If $\mathbb{F}$ has characteristic zero then $n \cdot 1 \neq 0$ for all $n \geq 1$. Furthermore, if $m \cdot 1 = n \cdot 1$ with $m < n$, then subtracting $m \cdot 1$ from both sides gives $(n - m) \cdot 1 = 0$, which is a contradiction. Hence $\mathbb{F}$ contains the infinitely many distinct elements $n \cdot 1$ with $n \in \mathbb{N}$.[7]

(b): **This is the hard part.** Let $\mathbb{F}$ have characteristic zero and let $f(x), g(x) \in \mathbb{F}[x]$ be the minimal polynomials of $\alpha, \beta \in \mathbb{E} \supseteq \mathbb{F}$, respectively. Let's say

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots \quad \text{and} \quad g(x) = (x - \beta_1)(x - \beta_2)\cdots$$

in $\mathbb{C}[x]$,[8] with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. Since $f(x)$ and $g(x)$ are irreducible over $\mathbb{F}$, it follows from Problem 5 that $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for $i \neq j$. Since $f(x)$ and $g(x)$ have finitely many roots and since $\mathbb{F}$ is infinite from part (a), we may choose $c \in \mathbb{F}$ such that $c \neq (\alpha_i - \alpha)/(\beta - \beta_j)$ for all i, j. Define $\gamma := \alpha + c\beta$ and $h(x) := f(\gamma - cx) \in \mathbb{F}(\gamma)[x]$. Let $d(x) = \gcd(g, h)$ in the ring $\mathbb{F}(\gamma)[x]$. I claim that $\deg(d) \leq 1$. Indeed, since $g(\beta) = 0$ and $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$ we know that $x - \beta$ divides $d(x)$ in $\mathbb{C}[x]$. Furthermore, since $d(x)$ divides $g(x)$ we know that $d(x) = \prod_{j \in J}(x - \beta_j) \in \mathbb{C}[x]$ for some set J containing 1. If $\deg(d) \geq 2$ this implies that $d(x)$ has another root $d(\beta_j) = 0$ with $j \neq 1$. Since $d(x)$ divides $h(x)$ we would have $0 = h(\beta_j) = f(\gamma - c\beta_j)$, which implies that $\gamma - c\beta_j = \alpha_i$ for some i. But this contradicts the definition of c because

$$\gamma - c\beta_j = \alpha_i \quad \Longrightarrow \quad c = (\alpha_i - \alpha)/(\beta - \beta_j).$$

We conclude that $\deg(d) \leq 1$.

(c): Let $p(x)$ be the minimal polynomial over β over $\mathbb{F}(\gamma)[x]$. Since $g(x), h(x) \in \mathbb{F}(\gamma)[x]$ both have β as a root we see that $p(x)|g(x)$ and $p(x)|h(x)$, hence $p(x)|\gcd(g, h)$, in $\mathbb{F}(\gamma)[x]$. From part (b) this implies that $\deg(p) = 1$, say $p(x) = a + bx$ with $a, b \in \mathbb{F}(\gamma)$. But then since $p(\beta) = 0$ we have $\beta = -a/b \in \mathbb{F}(\gamma)$.

---

[7] Or you can just quote the fact, proved on a previous homework, that every field of characteristic zero contains $\mathbb{Q}$ as as its smallest subfield.

[8] Here we use the fact that $\mathbb{C}$ is algebraically closed. In the general case we would take a field extension $\mathbb{E} \supseteq \mathbb{F}$ that contains all the roots of $f(x)$ and $g(x)$.

(d): Since $c \in \mathbb{F}$ and $\gamma = \alpha + c\beta \in \mathbb{F}(\alpha, \beta)$ we have $\mathbb{F}(\gamma) \subseteq \mathbb{F}(\alpha, \beta)$. On the other hand, we showed in (c) that $\beta \in \mathbb{F}(\gamma)$. Then we also have $\alpha = \gamma - c\beta \in \mathbb{F}(\gamma)$, hence $\mathbb{F}(\alpha, \beta) \subseteq \mathbb{F}(\gamma)$.

(e): For any $\alpha, \beta \in \mathbb{C}$ algebraic over a subfield $\mathbb{F}$, we have shown that there exists $\gamma \in \mathbb{C}$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. For any $\mathbb{C} \supseteq \mathbb{E} \supseteq \mathbb{F}$ with $[\mathbb{E}/\mathbb{F}] < \infty$ we proved in Problem 4 that $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ are algebraic over $\mathbb{F}$. Since α_{n-1}, α_n are also algebraic over $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})$ there exists some γ such that

$$\begin{aligned} \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) &= \mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})(\alpha_{n-1}, \alpha_n) \\ &= \mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})(\gamma) \\ &= \mathbb{F}(\alpha_1, \ldots, \alpha_{n-2}, \gamma). \end{aligned}$$

Now the result follows by induction.

Remark: The Primitive Element Theorem is the **first step** in the proof of the Fundamental Theorem of Galois Theory. Here is a note that sketches the rest of the proof: `http://math.miami.edu/~armstrong/562sp24/562sp24galois_sketch.pdf`