Honors Algebra **Spring 2025**
HW 10: Galois Theory, Automorphisms of Fields, Splitting Fields **4/22/2025**

Abstract Algebra: An Integrated Approach by J.H. Silverman.
Page 285-294: 9.22, 9.23, 9.25, 9.26, 9.29, 9.32, 9.32, 9.39, 9.40, 9.41, 9.44, 9.48, 9.53

Problem 1 (9.22)**.** Let F be a field, let $f(x) \in F[x]$ be a seperable polynomial of degree $n \geq 1$, and let K/F be a splitting field for $f(x)$ over F. Prove the following implications:

$$\#G(K/F) = n! \iff G(K/F) \cong \mathcal{S}_n \implies f(x) \text{ is irreducible in } F[x]$$

Note that the first implication is an "if and only if," but the second only goes in one direction. Show that the second implication cannot be reversed, by writing down an example for which it is false.

We are given a separable polynomial $f(x) \in F[x]$ of degree $n \geq 1$, and its splitting field K over F. Let us prove each of the implications:

($\Rightarrow$) Suppose $\#G(K/F) = n!$. Since the Galois group $G(K/F)$ is a subgroup of the symmetric group $\mathcal{S}_n$ (as it permutes the n distinct roots of the separable polynomial $f(x)$), and its order is $n!$, we must have $G(K/F) \cong \mathcal{S}_n$ because $\mathcal{S}_n$ is the only subgroup of itself of order $n!$.

($\Leftarrow$) Conversely, if $G(K/F) \cong \mathcal{S}_n$, then clearly $\#G(K/F) = \#\mathcal{S}_n = n!$.

($\Rightarrow$) Now suppose $G(K/F) \cong \mathcal{S}_n$. Then $G(K/F)$ acts transitively on the set of roots of $f(x)$, and the full symmetry of $\mathcal{S}_n$ implies that there are no nontrivial intermediate fields fixed by proper subgroups of $G(K/F)$. If $f(x)$ were reducible, say $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ and both of lower degree, then the roots of $g(x)$ and $h(x)$ would be in disjoint orbits under the action of $G(K/F)$, contradicting the transitivity of $\mathcal{S}_n$. Therefore, $f(x)$ must be irreducible.

Counterexample to the converse of the second implication:

Consider $f(x) = x^4 + 2x^2 + 4 \in \mathbb{Q}[x]$. This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (after substituting $x \mapsto x+1$). Let K be its splitting field over $\mathbb{Q}$. The roots are complex and come in conjugate pairs, and the Galois group $G(K/\mathbb{Q})$ has order 8, which is strictly less than $4! = 24$, the order of $\mathcal{S}_4$. Therefore, $f(x)$ is irreducible, but $G(K/\mathbb{Q}) \ncong \mathcal{S}_4$, disproving the converse.

Problem 2 (9.23)**.** Let K/F be a Galois extension, let $\alpha \in K$, and let

$$f(X) = \prod_{\sigma \in G(K/F)} (X - \sigma(\alpha))$$

(a) Prove that $f(x) \in F[x]$; i.e., prove that the coefficients of $f(x)$ are in F.

We are given a Galois extension K/F and an element $\alpha \in K$. Define

$$f(X) = \prod_{\sigma \in G(K/F)} (X - \sigma(\alpha)).$$

Since $G(K/F)$ is a group of automorphisms fixing F, the action of each $\sigma \in G(K/F)$ sends α to another conjugate of α in K, and permutes the set of conjugates. Therefore, the coefficients of $f(X)$, which are elementary symmetric polynomials in the $\sigma(\alpha)$, are fixed by every $\tau \in G(K/F)$. That is, for any $\tau \in G(K/F)$:

$$\tau(f(X)) = \prod_{\sigma \in G(K/F)} (X - \tau(\sigma(\alpha))) = \prod_{\sigma \in G(K/F)} (X - \sigma(\alpha)) = f(X),$$

since $\tau \circ \sigma$ runs over the same set as σ. Thus, $f(X)$ is fixed by all automorphisms in $G(K/F)$, meaning its coefficients lie in F, so $f(X) \in F[X]$.

(b) Let $\Phi_{\alpha,F} \in F[x]$ be the minimal polynomial of $f(X)$ over F. Prove that

$$f(X) = \Phi_{\alpha,F}(X) \iff K = F(\alpha)$$

Let $\Phi_{\alpha,F}(X)$ be the minimal polynomial of α over F. Then $\Phi_{\alpha,F}(X)$ divides any polynomial in $F[X]$ that vanishes at α, and in particular it divides $f(X)$.

Now suppose $f(X) = \Phi_{\alpha,F}(X)$. Since $\Phi_{\alpha,F}$ is irreducible and has degree equal to the number of distinct conjugates $\sigma(\alpha)$ as σ ranges over $G(K/F)$, this implies that the F-orbit of α under the Galois group accounts for all roots of the minimal polynomial. Thus, the degree of $\Phi_{\alpha,F}$ is equal to $[F(\alpha) : F]$.

Also, since $f(X)$ has as many distinct roots as elements of $G(K/F)$, this implies that $[F(\alpha) : F] = [K : F]$, so $F(\alpha) = K$.

Conversely, if $K = F(\alpha)$, then α generates K over F, and all automorphisms $\sigma \in G(K/F)$ are determined by the image of α. Hence, the orbit $\{\sigma(\alpha)\}$ has size equal to $\#G(K/F) = [K : F] = [F(\alpha) : F] = \deg \Phi_{\alpha,F}$, and since $f(X)$ is a product of the conjugates of α, it must be equal to $\Phi_{\alpha,F}(X)$.

(c) In general, even if $K \neq F(\alpha)$, prove that there is an integer $d \geq 1$ such that

$$f(X) = \Phi_{\alpha,F}(X)^d$$

(*Hint.* Use the $G(K/F)$-orbit of α to split the factors of $f(X)$ into subsets, and relate them to the $G(K/F)$-stabilizer subgroup of α.)

In general, even if $K \neq F(\alpha)$, the Galois group $G(K/F)$ acts on the set $\{\sigma(\alpha) \mid \sigma \in G(K/F)\}$, partitioning it into orbits under the action of the stabilizer subgroup of α. The stabilizer subgroup $G(K/F)_\alpha = \{\sigma \in G(K/F) \mid \sigma(\alpha) = \alpha\}$ is a subgroup of $G(K/F)$, and the orbit-stabilizer theorem gives:

$$\#\text{orbit of } \alpha = [G(K/F) : G(K/F)_\alpha].$$

Thus, the set of conjugates of α under $G(K/F)$ is of this cardinality, and the number of distinct such conjugates is equal to $\deg \Phi_{\alpha,F}$. Since $f(X)$ includes all of these roots, and the other conjugates repeat in a way determined by how many distinct cosets of the stabilizer exist, $f(X)$ must be a power of $\Phi_{\alpha,F}$:

$$f(X) = \Phi_{\alpha,F}(X)^d,$$

for some integer $d \geq 1$. This d is the number of distinct conjugates of α in K under $G(K/F)$ divided by the number of distinct roots of $\Phi_{\alpha,F}$ (which are the same), so this simply counts multiplicities arising from repeated factors in $f(X)$ due to repeated $\sigma(\alpha)$ values.

Problem 3 (9.25).

(a) Let $f(x) = x^4 - 6x^2 + 2$, and let K be the splitting field of $f(x)$ over $\mathbb{Q}$.

(1) Compute the Galois group $G(K/\mathbb{Q})$.

(2) Make a list of the subgroups H of $G(K/\mathbb{Q})$ and the corresponding intermediate fields K^H; cf. Figure 29 on page 249.

(3) Make a field diagram and a group diagram illustrating the Galois correspondence that you found in (2); cf Figure 30 on page 251.

(b) Same as (a) for the polynomial $f(x) = x^4 - 10x^2 + 20$.

(c) Same as (a) for the polynomial $f(x) = x^4 - 5x^2 + 6$

(1)
Let $f(x) = x^4 - 6x^2 + 2 \in \mathbb{Q}[x]$. First, we find its roots. Let $y = x^2$, then

$$f(x) = x^4 - 6x^2 + 2 = y^2 - 6y + 2.$$

The quadratic in y has roots:

$$y = \frac{6 \pm \sqrt{36-8}}{2} = \frac{6 \pm \sqrt{28}}{2} = \frac{6 \pm 2\sqrt{7}}{2} = 3 \pm \sqrt{7}.$$

Thus, the values of x^2 are $3 + \sqrt{7}$ and $3 - \sqrt{7}$. Taking square roots, the roots of $f(x)$ are:

$$\pm\sqrt{3+\sqrt{7}}, \quad \pm\sqrt{3-\sqrt{7}}.$$

So the splitting field K is:

$$K = \mathbb{Q}(\sqrt{3+\sqrt{7}}, \sqrt{3-\sqrt{7}}).$$

Let us understand the structure of this field. Let $a = \sqrt{3+\sqrt{7}}$ and $b = \sqrt{3-\sqrt{7}}$. Then $a^2 = 3 + \sqrt{7}$ and $b^2 = 3 - \sqrt{7}$, so $a^2 + b^2 = 6$ and $a^2 - b^2 = 2\sqrt{7}$, which implies:

$$\sqrt{7} = \frac{a^2 - b^2}{2} \in \mathbb{Q}(a, b).$$

So $\sqrt{7} \in K$, and then $a^2 = 3 + \sqrt{7}$ implies $a \in \mathbb{Q}(\sqrt{7}, a)$. Hence, $K = \mathbb{Q}(\sqrt{7}, \sqrt{3+\sqrt{7}})$.

We claim that $[K : \mathbb{Q}] = 8$. To see this: - $\sqrt{7} \notin \mathbb{Q}$, so $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$. - In $\mathbb{Q}(\sqrt{7})$, the element $3 + \sqrt{7}$ is not a square. So $\sqrt{3+\sqrt{7}}$ has degree 2 over $\mathbb{Q}(\sqrt{7})$. - Therefore, $[K : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$.

Since $f(x)$ is separable and we have found all 4 roots in K, and the degree of the splitting field is 8, the Galois group $G(K/\mathbb{Q})$ has order 8.

Now we identify the group. This Galois group permutes 4 roots and has order 8. The group is not $\mathbb{Z}_8$ (not cyclic), and it's not D_8 (doesn't fit a geometric symmetry model), but is instead the dihedral group D_4 acting on the square formed by the roots. Alternatively, it is isomorphic to the *quartic* Galois group often denoted by D_4 or $G_{8,3}$ in the small groups library.

Therefore, $G(K/\mathbb{Q}) \cong D_4$, the dihedral group of order 8.

(2)
Let $f(x) = x^4 - 10x^2 + 20$. Substitute $y = x^2$ to get $y^2 - 10y + 20$. Solving yields $y = 5 \pm \sqrt{5}$, so roots of f are $\pm\sqrt{5+\sqrt{5}}, \pm\sqrt{5-\sqrt{5}}$.

Let $a = \sqrt{5+\sqrt{5}}, b = \sqrt{5-\sqrt{5}}$. Then $K = \mathbb{Q}(a,b)$ and $\sqrt{5} = \frac{a^2-b^2}{2} \in K$. So $K = \mathbb{Q}(\sqrt{5}, a)$.

Each square root extension is quadratic, and both are needed for full splitting, so $[K : \mathbb{Q}] = 4$. The Galois group is the Klein four-group V_4.

Intermediate fields: $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(a), \mathbb{Q}(b)$.

Field diagram and group diagram similar to above, with V_4 replacing D_4.

(3)
Same as (a) for the polynomial $f(x) = x^4 - 5x^2 + 6$.

Factor $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$. Roots are $\pm\sqrt{2}, \pm\sqrt{3}$. The splitting field is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, the Galois group is V_4, and the intermediate fields are $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$.

Problem 4 (9.26)**.** Let K/F be a Galois extension.

(a) Let $\sigma \in G(K/F)$, and let E be an intermediate field of K/F. Prove that

$$G(K/\sigma(E)) = \sigma G(K/E)\sigma^{-1}$$

Since $\sigma \in G(K/F)$ is an automorphism of K fixing F, and E is an intermediate field of K/F, consider the subgroup $G(K/E) = \{\tau \in G(K/F) \mid \tau(x) = x \text{ for all } x \in E\}$.

Now let us conjugate $G(K/E)$ by σ. Define:

$$\sigma G(K/E)\sigma^{-1} = \{\sigma\tau\sigma^{-1} \mid \tau \in G(K/E)\}$$

Let $x \in \sigma(E)$. Then $x = \sigma(y)$ for some $y \in E$. For any $\tau \in G(K/E)$ and $\rho = \sigma\tau\sigma^{-1}$, we compute:

$$\rho(x) = \sigma\tau\sigma^{-1}(\sigma(y)) = \sigma\tau(y) = \sigma(y) = x$$

so ρ fixes every element of $\sigma(E)$. Hence, $\sigma G(K/E)\sigma^{-1} \subseteq G(K/\sigma(E))$.

Conversely, suppose $\rho \in G(K/\sigma(E))$, and define $\tau = \sigma^{-1}\rho\sigma$. Then for $y \in E$, we have:

$$\tau(y) = \sigma^{-1}\rho\sigma(y)$$

Since $\sigma(y) \in \sigma(E)$ and ρ fixes $\sigma(E)$, $\rho(\sigma(y)) = \sigma(y)$, so:

$$\tau(y) = \sigma^{-1}(\sigma(y)) = y$$

Hence $\tau \in G(K/E)$, so $\rho = \sigma\tau\sigma^{-1} \in \sigma G(K/E)\sigma^{-1}$.

Therefore, $G(K/\sigma(E)) = \sigma G(K/E)\sigma^{-1}$.

(b) Let $\sigma \in G(K/F)$, and let $H \subseteq G(K/F)$ be a subgroup. Prove that

$$\sigma(K^H) = K^{\sigma H\sigma^{-1}}$$

Let $L = K^H = \{x \in K \mid \tau(x) = x \text{ for all } \tau \in H\}$. We want to show that $\sigma(L) = K^{\sigma H\sigma^{-1}}$.

Take $x \in L$, so $\tau(x) = x$ for all $\tau \in H$. Let $y = \sigma(x)$. Then for any $\rho \in \sigma H\sigma^{-1}$, there exists $\tau \in H$ such that $\rho = \sigma\tau\sigma^{-1}$. Then:

$$\rho(y) = \rho(\sigma(x)) = \sigma\tau\sigma^{-1}\sigma(x) = \sigma\tau(x) = \sigma(x) = y$$

So $y \in K^{\sigma H\sigma^{-1}}$, which shows $\sigma(L) \subseteq K^{\sigma H\sigma^{-1}}$.

Conversely, let $y \in K^{\sigma H\sigma^{-1}}$, and let $x = \sigma^{-1}(y)$. For all $\tau \in H$, let $\rho = \sigma\tau\sigma^{-1} \in \sigma H\sigma^{-1}$. Then:

$$\rho(y) = y \Rightarrow \sigma\tau\sigma^{-1}(y) = y \Rightarrow \tau(\sigma^{-1}(y)) = \sigma^{-1}(y)$$

So $x = \sigma^{-1}(y) \in K^H = L$, which implies $y = \sigma(x) \in \sigma(L)$.

Hence, $\sigma(K^H) = K^{\sigma H\sigma^{-1}}$.

(c) We say that intermediate fields E_1 and E_2 are conjugate subfields of K/F if

$$\sigma(E_1) = E_2 \quad \text{for some} \quad \sigma \in G(K/F)$$

Prove that E_1 and E_2 are conjugate subfields of K/F if and only if the groups $G(K/E_1)$ and $G(K/E_2)$ are conjugate subgroups of $G(K/F)$.

($\Rightarrow$) Suppose $\sigma(E_1) = E_2$ for some $\sigma \in G(K/F)$. By part (a),

$$G(K/E_2) = G(K/\sigma(E_1)) = \sigma G(K/E_1)\sigma^{-1}$$

so $G(K/E_2)$ and $G(K/E_1)$ are conjugate subgroups.

($\Leftarrow$) Suppose $G(K/E_2) = \sigma G(K/E_1)\sigma^{-1}$ for some $\sigma \in G(K/F)$. Then again by part (a),

$$G(K/\sigma(E_1)) = \sigma G(K/E_1)\sigma^{-1} = G(K/E_2)$$

and by the Galois correspondence (which is bijective and order-reversing), the fixed fields of these groups must be equal:

$$\sigma(E_1) = E_2$$

So E_1 and E_2 are conjugate subfields.

(d) Let $H_1, H_2 \subseteq G(K/F)$ be subgroups. Prove that their fixed fields K^{H_1} and K^{H_2} are conjugate subfields of K/F if and only if H_1 and H_2 are conjugate subgroups of $G(K/F)$. ($\Rightarrow$) Suppose $\sigma(K^{H_1}) = K^{H_2}$ for some $\sigma \in G(K/F)$. Then by part (b),

$$K^{\sigma H_1 \sigma^{-1}} = \sigma(K^{H_1}) = K^{H_2}$$

and since the Galois correspondence is a bijection, we must have:

$$\sigma H_1 \sigma^{-1} = H_2$$

So H_1 and H_2 are conjugate subgroups.

($\Leftarrow$) Suppose $H_2 = \sigma H_1 \sigma^{-1}$ for some $\sigma \in G(K/F)$. Then by part (b),

$$\sigma(K^{H_1}) = K^{\sigma H_1 \sigma^{-1}} = K^{H_2}$$

so the fixed fields K^{H_1} and K^{H_2} are conjugate subfields.

Problem 5 (9.29)**.** Let $f(X) = X^5 - iX^2 + 1 - i \in \mathbb{C}[X]$. Find a polynomial $g(X) \in \mathbb{R}[X]$ of degree 10 with the property that every complex root of $f(X)$ is also a root of $g(X)$.

To solve this problem, we need to find a real polynomial $g(X)$ of degree 10 that has the same roots as $f(X)$, but in a way that $g(X)$ is a polynomial with real coefficients.

The first step is to recognize that if $f(X)$ has complex roots, they must appear in conjugate pairs because the coefficients of $f(X)$ are complex, but $g(X)$ must have real coefficients. This means that if z is a root of $f(X)$, then its conjugate $\overline{z}$ must also be a root of $f(X)$.

The polynomial $f(X)$ has degree 5, and since complex roots come in conjugate pairs, it must have an odd number of complex roots. Therefore, one of the roots must be real, while the other four roots must come in two conjugate pairs.

To find $g(X)$, we start by writing down the fact that $g(X)$ must have the same roots as $f(X)$, but with real coefficients. If z is a complex root of $f(X)$, then $\overline{z}$ must also be a root of $g(X)$. So, we construct a quadratic factor for each conjugate pair of complex roots of $f(X)$.

Since $f(X)$ is a degree 5 polynomial, it has 5 roots, and one of these roots is real. The real root of $f(X)$ will appear as a linear factor in $g(X)$, while each conjugate pair of complex roots will give a quadratic factor.

In summary, the polynomial $g(X)$ must be the product of the following factors:

$$g(X) = (X - r) \cdot (X^2 - 2\Re(z)X + |z|^2) \cdot (X^2 - 2\Re(\overline{z})X + |\overline{z}|^2)$$

where r is the real root of $f(X)$ and z is a complex root of $f(X)$.

By finding the exact roots of $f(X)$ and constructing these factors, we can then express $g(X)$ explicitly as a degree 10 polynomial with real coefficients.

Problem 6 (9.32)**.** Let q be a prime power, let $N \in \mathbb{Z}$ be a prime satisfying $\gcd(q, N) = 1$, and let ζ be a primitive Nth-root of unity in some extension field of $\mathbb{F}_q$.

(a) Prove that $\mathbb{F}_q(\zeta)/\mathbb{F}_q$ is a separable extension.

To prove that the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$ is separable, we first observe that since q and N are coprime, the characteristic of the finite field $\mathbb{F}_q$ does not divide N. In characteristic zero, every finite extension of a field is separable. In positive characteristic, separability of the extension depends on the polynomial having distinct roots in its splitting field.

The minimal polynomial of ζ, the primitive Nth root of unity, over $\mathbb{F}_q$ is:

$$f(X) = X^N - 1$$

This polynomial splits completely in $\mathbb{F}_q(\zeta)$, and since the characteristic of $\mathbb{F}_q$ does not divide N, $f(X)$ has distinct roots (the Nth roots of unity), so the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$ is separable.

Therefore, the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$ is separable.

(b) Let e be the order of q in the group $(\mathbb{Z}/N\mathbb{Z})^*$; i.e.,

$$q^e \equiv 1 (\operatorname{mod} N) \quad \text{and} \quad q^i \not\equiv 1 (\operatorname{mod} N) \quad \text{for } 1 \leq i < e$$

Prove that

$$[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = e$$

The order of q in the group $(\mathbb{Z}/N\mathbb{Z})^*$ is the smallest integer e such that:

$$q^e \equiv 1 \pmod{N}$$

This means that the powers of q modulo N form a periodic sequence with period e. The extension degree $[\mathbb{F}_q(\zeta) : \mathbb{F}_q]$ corresponds to the smallest degree of the extension of $\mathbb{F}_q$ required to contain a primitive Nth root of unity ζ.

Since ζ is a primitive Nth root of unity, the minimal polynomial of ζ over $\mathbb{F}_q$ is the polynomial:

$$f(X) = X^N - 1 = (X - 1)(X - \zeta)(X - \zeta^2) \cdots (X - \zeta^{N-1})$$

The degree of this polynomial over $\mathbb{F}_q$ is N, but we need to determine the degree of the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$.

The key observation is that the multiplicative group of non-zero elements of $\mathbb{F}_q$ is cyclic, and the order of q modulo N gives the smallest e such that $q^e \equiv 1 \pmod{N}$. This is exactly the degree of the extension, because the order of q modulo N tells us how the powers of q generate the roots of unity in the field extension.

Therefore, the extension degree is:

$$[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = e$$

(c) Prove that the polynomial

$$X^{N-1} + X^{N-2} + \cdots + X + 1$$

is irreducible in $\mathbb{F}_q[X]$ if and only if q generates the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$.

The polynomial we are considering is:

$$f(X) = X^{N-1} + X^{N-2} + \cdots + X + 1 = \frac{X^N - 1}{X - 1}$$

This is the Nth cyclotomic polynomial, which has the Nth roots of unity as its roots, excluding $X = 1$. We want to prove that this polynomial is irreducible in $\mathbb{F}_q[X]$ if and only if q generates the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$.

($\Rightarrow$) Suppose q generates $(\mathbb{Z}/N\mathbb{Z})^*$. This means that the order of q modulo N is exactly $N - 1$. In this case, the powers of q modulo N are distinct, and the Nth roots of unity in $\mathbb{F}_q$ are all distinct, implying that the Nth cyclotomic polynomial is irreducible in $\mathbb{F}_q[X]$.

($\Leftarrow$) Suppose the polynomial $f(X) = X^{N-1} + X^{N-2} + \cdots + X + 1$ is irreducible in $\mathbb{F}_q[X]$. This implies that the roots of this polynomial (the primitive Nth roots of unity) must all lie in the field $\mathbb{F}_q(\zeta)$, where ζ is a primitive Nth root of unity. For this to happen, the powers of q modulo N must generate all the Nth roots of unity. Hence, q must generate the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$, meaning the order of q modulo N is exactly $N - 1$.

Therefore, the polynomial $f(X)$ is irreducible in $\mathbb{F}_q[X]$ if and only if q generates the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$.

Problem 7 (9.39)**.** Let K/F be a Galois extension of fields. For subgroups $H_1, H_2 \subset G(K/F)$, we define

$$H_1 \star H_2 = \bigcap_{\substack{\text{subgroups } H \subset G(K/F) \\ \text{with } H_1, H_2 \subseteq H}} H$$

to be the smallest subgroup of $G(K/F)$ that contains both H_1 and H_2. Similarly, for intermediate fields E_1, E_2 of K/F, we define

$$E_1 \star E_2 = \bigcap_{\substack{\text{subgroups } E \subseteq K \\ \text{with } E_1, E_2 \subseteq E}} E$$

to be the smallest intermediate field containing both E_1 and E_2. Prove that

$$K^{H_1 \star H_2} = K^{H_1} \cap K^{H_2} \quad \text{and} \quad K^{H_1 \cap H_2} = K^{H_1} \star K^{H_2}$$

We are given that K/F is a Galois extension, and that $G = \text{Gal}(K/F)$. For subgroups $H_1, H_2 \subseteq G$, define

$$H_1 \star H_2 = \bigcap_{\substack{H \subseteq G \\ H_1, H_2 \subseteq H}} H,$$

which is the smallest subgroup of G containing both H_1 and H_2, i.e., the subgroup generated by $H_1 \cup H_2$. Similarly, for intermediate fields E_1, E_2, define

$$E_1 \star E_2 = \bigcap_{\substack{E \subseteq K \\ E_1, E_2 \subseteq E}} E,$$

which is the smallest intermediate field of K/F containing both E_1 and E_2, i.e., their compositum.

Claim 1: $K^{H_1 \star H_2} = K^{H_1} \cap K^{H_2}$

Proof: The fixed field $K^{H_1} = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in H_1\}$, and similarly for K^{H_2}. So

$$K^{H_1} \cap K^{H_2} = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in H_1 \cup H_2\}.$$

This is precisely the fixed field of the subgroup generated by $H_1 \cup H_2$, i.e., of $H_1 \star H_2$. Therefore,

$$K^{H_1 \star H_2} = K^{H_1} \cap K^{H_2}.$$

Claim 2: $K^{H_1 \cap H_2} = K^{H_1} \star K^{H_2}$

Proof: Since the Galois correspondence is inclusion-reversing and bijective, we have:

$$H_1 \cap H_2 \longleftrightarrow K^{H_1 \cap H_2} \supseteq K^{H_1}, K^{H_2}.$$

Therefore, $K^{H_1 \cap H_2}$ is the smallest intermediate field containing both K^{H_1} and K^{H_2}, i.e.,

$$K^{H_1 \cap H_2} = K^{H_1} \star K^{H_2}.$$

Thus,

$$\boxed{K^{H_1 \star H_2} = K^{H_1} \cap K^{H_2} \quad \text{and} \quad K^{H_1 \cap H_2} = K^{H_1} \star K^{H_2}}$$

Problem 8 (9.40)**.** Let K/F be a Galois extension, and let E_1 and E_2 be intermediate fields such that E_1/F and E_2/F are Galois extensions. Let $E_1 \star E_2$ be the compositum of E_1 and E_2 as defined in Exercise 9.39.

(a) Prove that $E_1 \star E_2$ is a Galois extension of F.

Since K/F is Galois, it is normal and separable. E_1 and E_2 are intermediate fields such that both E_1/F and E_2/F are Galois. That means E_1/F and E_2/F are also normal and separable.

Let $E = E_1 \star E_2$ denote the compositum of E_1 and E_2 in K, which is the smallest subfield of K containing both E_1 and E_2.

Separable: Since both E_1 and E_2 are separable over F, and separability is preserved under field extensions, $E = E_1E_2$ is also separable over F.

Normal: Since E_1 and E_2 are normal over F, any embedding of E into an algebraic closure of F that fixes F will permute the roots of the minimal polynomials of elements of E_1 and E_2. Since K/F is normal and contains both E_1 and E_2, the compositum E is the splitting field of the union of splitting fields of the minimal polynomials of elements in E_1 and E_2, hence E/F is also normal.

Therefore, $E_1 \star E_2/F$ is Galois.

(b) What is the kernel of the homomorphism

$$G(K/F) \longrightarrow G(E_1/F) \times G(E_2/F)$$

Describe the kernel explicitly as a subgroup of $G(K/F)$.

Let us define the homomorphism φ as

$$\varphi : G(K/F) \to G(E_1/F) \times G(E_2/F), \quad \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2}).$$

The kernel of this map consists of those automorphisms $\sigma \in G(K/F)$ that restrict to the identity on both E_1 and E_2. That is,

$$\ker(\varphi) = \{\sigma \in G(K/F) \mid \sigma|_{E_1} = \mathrm{id},\ \sigma|_{E_2} = \mathrm{id}\}.$$

So these are automorphisms that fix pointwise both E_1 and E_2.

Hence, the kernel is the subgroup of $G(K/F)$ that fixes the compositum $E = E_1 \star E_2$ pointwise. This subgroup is

$$\ker(\varphi) = \mathrm{Gal}(K/E_1 \star E_2).$$

(c) Prove that

$$\gcd([E_1 : F], [E_2 : F]) = 1 \quad \Longrightarrow \quad \text{the map (9.44) in (b) is surjective.}$$

Assume that $\gcd([E_1 : F], [E_2 : F]) = 1$.

From part (b), we have the map

$$\varphi : \mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F).$$

Since E_1 and E_2 are Galois over F, we know:

$$\mathrm{Gal}(E_1/F) \cong \mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E_1), \quad \mathrm{Gal}(E_2/F) \cong \mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E_2).$$

Consider the map induced by restriction:

$$\mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(K/E_1) \cap \mathrm{Gal}(K/E_2).$$

The First Isomorphism Theorem tells us that the image of φ is isomorphic to the quotient group

$$\mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E_1 \star E_2).$$

But by the fundamental theorem of Galois theory, the group $\mathrm{Gal}(E_1 \star E_2/F)$ is isomorphic to the image of φ.

Now consider the degrees:

$$[E_1 \star E_2 : F] \leq [E_1 : F] \cdot [E_2 : F].$$

If $\gcd([E_1 : F], [E_2 : F]) = 1$, then in fact $[E_1 \star E_2 : F] = [E_1 : F] \cdot [E_2 : F]$.

Therefore, $\mathrm{Gal}(E_1 \star E_2/F) \cong \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

This implies that the map

$$\varphi : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

is surjective, because both sides have the same cardinality and φ is a homomorphism of finite groups with kernel $\mathrm{Gal}(K/E_1 \star E_2)$.

Hence, the condition $\gcd([E_1 : F], [E_2 : F]) = 1$ implies the surjectivity of the map.

Problem 9 (9.41)**.** Let K/F be a finite extension of fields. For each $\alpha \in K$, we define a multiplication by α map by

$$\mu_\alpha : K \longrightarrow K, \quad \mu_\alpha(\beta) = \alpha\beta$$

(a) If we view K as an F-vector space, prove that μ_α is an F-linear transformation of K to itself. Let $\alpha \in K$. We define the map $\mu_\alpha : K \to K$ by $\mu_\alpha(\beta) = \alpha\beta$. To prove μ_α is F-linear, we must show that for all $\beta_1, \beta_2 \in K$ and $c \in F$, we have:

$$\mu_\alpha(\beta_1 + \beta_2) = \mu_\alpha(\beta_1) + \mu_\alpha(\beta_2), \quad \mu_\alpha(c\beta_1) = c\mu_\alpha(\beta_1)$$

These follow from associativity and distributivity in the field K:

$$\mu_\alpha(\beta_1 + \beta_2) = \alpha(\beta_1 + \beta_2) = \alpha\beta_1 + \alpha\beta_2 = \mu_\alpha(\beta_1) + \mu_\alpha(\beta_2)$$
$$\mu_\alpha(c\beta_1) = \alpha(c\beta_1) = c(\alpha\beta_1) = c\mu_\alpha(\beta_1)$$

Therefore, μ_α is F-linear.

(b) We recall that any F-linear operator on a finite-dimensional F-vector space has a well-defined trace and determinant; see Section 10.6 and Exercise 10.23. For $\alpha \in K$, we define the K/F-trace and the K/F-norm of α by

$$\mathrm{tr}_{K/F}(\alpha) = \mathrm{tr}(\mu_\alpha) \quad \text{and} \quad N_{K/F}(\alpha) = \det(\mu_\alpha)$$

Prove that for all $\alpha_1, \alpha_2 \in K$ we have

$$\mathrm{tr}_{K/F}(\alpha_1 + \alpha_2) = \mathrm{tr}_{K/F}(\alpha_1) + \mathrm{tr}_{K/F}(\alpha_2)$$
$$N_{K/F}(\alpha_1 \cdot \alpha_2) = N_{K/F}(\alpha_1) \cdot N_{K/F}(\alpha_2)$$

Since $\mu_{\alpha_1+\alpha_2} = \mu_{\alpha_1} + \mu_{\alpha_2}$ and the trace is a linear function on endomorphisms, we have:

$$\mathrm{tr}_{K/F}(\alpha_1+\alpha_2) = \mathrm{tr}(\mu_{\alpha_1+\alpha_2}) = \mathrm{tr}(\mu_{\alpha_1}+\mu_{\alpha_2}) = \mathrm{tr}(\mu_{\alpha_1})+\mathrm{tr}(\mu_{\alpha_2}) = \mathrm{tr}_{K/F}(\alpha_1)+\mathrm{tr}_{K/F}(\alpha_2)$$

Similarly, since $\mu_{\alpha_1\alpha_2} = \mu_{\alpha_1} \circ \mu_{\alpha_2}$ and the determinant is multiplicative over compositions, we have:

$$N_{K/F}(\alpha_1\alpha_2) = \det(\mu_{\alpha_1\alpha_2}) = \det(\mu_{\alpha_1} \circ \mu_{\alpha_2}) = \det(\mu_{\alpha_1}) \cdot \det(\mu_{\alpha_2}) = N_{K/F}(\alpha_1) \cdot N_{K/F}(\alpha_2)$$

(c) For each of the following K/F and $\alpha \in K$, compute $\operatorname{tr}_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ directly from the definition (9.45) by choosing a basis for K/F and writing down the matrix associated to μ_α:

(1) $F = \mathbb{R}, \quad K = \mathbb{C}, \quad \alpha = a + bi$ with $a, b \in \mathbb{R}$

Basis: $\{1, i\}$ over $\mathbb{R}$. Then μ_α acts as:

$$\mu_\alpha(1) = a + bi, \quad \mu_\alpha(i) = ai + bi^2 = ai - b$$

$$M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

$$\operatorname{tr}_{K/F}(\alpha) = \operatorname{tr}(M) = 2a, \quad N_{K/F}(\alpha) = \det(M) = a^2 + b^2$$

(2) $F = \mathbb{Q}, \quad K = \mathbb{Q}(\sqrt{3}), \quad \alpha = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$

Basis: $\{1, \sqrt{3}\}$ over $\mathbb{Q}$. Then:

$$\mu_\alpha(1) = a + b\sqrt{3}, \quad \mu_\alpha(\sqrt{3}) = a\sqrt{3} + b \cdot 3 = 3b + a\sqrt{3}$$

$$M = \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

$$\operatorname{tr}_{K/F}(\alpha) = 2a, \quad N_{K/F}(\alpha) = a^2 - 3b^2$$

(3) $F = \mathbb{Q}, \quad K = \mathbb{Q}(\sqrt[3]{2}), \quad \alpha = 2 - 3\sqrt[3]{2} + \sqrt[3]{4}$

Let $\theta = \sqrt[3]{2}$ so that $K = \mathbb{Q}(\theta)$ has basis $\{1, \theta, \theta^2\}$.

Write $\alpha = 2 - 3\theta + \theta^2$.

$$\mu_\alpha(1) = \alpha = 2 - 3\theta + \theta^2$$
$$\mu_\alpha(\theta) = \alpha \cdot \theta = 2\theta - 3\theta^2 + \theta^3 = 2\theta - 3\theta^2 + 2 \quad (\text{since } \theta^3 = 2)$$
$$\mu_\alpha(\theta^2) = \alpha \cdot \theta^2 = 2\theta^2 - 3\theta^3 + \theta^4 = 2\theta^2 - 6 + 2\theta \quad (\theta^4 = \theta \cdot \theta^3 = 2\theta)$$

So the matrix of μ_α is:

$$M = \begin{pmatrix} 2 & 2 & -6 \\ -3 & 2 & 2 \\ 1 & -3 & 2 \end{pmatrix}$$

$$\operatorname{tr}_{K/F}(\alpha) = 2 + 2 + 2 = 6$$

Compute determinant (or use a computer or cofactor expansion):

$$N_{K/F}(\alpha) = \det(M) = 16$$

(d) Let K/F be a Galois extension, and let $\alpha \in K$. Prove that

$$\operatorname{tr}_{K/F}(\alpha) = \sum_{\sigma \in G(K/F)} \sigma(\alpha) \quad \text{and} \quad N_{K/F}(\alpha) = \prod_{\sigma \in G(K/F)} \sigma(\alpha)$$

(*Hint.* First do the case that $\#\{\sigma(\alpha) : \sigma \in G(K/F)\} = [K : F]$ and use the Cayley-Hamilton theorem from linear algebra. See Exercise 11.47 on page 368 for a statement of the Cayley-Hamilton theorem.)

Since K/F is Galois, it is a normal and separable extension. Then $[K : F] = \#G(K/F)$. Let $\sigma_1, \dots, \sigma_n$ be the elements of $G(K/F)$. The action of each σ_i gives a distinct conjugate of α.

Consider the F-linear map μ_α with characteristic polynomial

$$f(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$$

This is the minimal polynomial of μ_α, and by the Cayley-Hamilton theorem, μ_α satisfies this polynomial.

Therefore,

$$\operatorname{tr}_{K/F}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \quad N_{K/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

Even if the set of conjugates $\{\sigma(\alpha)\}$ is smaller than $[K : F]$, the trace and norm formulas still hold because the trace and norm are defined via the action of μ_α, which depends on the full set of Galois automorphisms.

Problem 10 (9.44)**.** For this problem, we write ζ_n for a primitive nth-root of unity. Kronecker's Theorem (Theorem 9.66) implies in particular that every square root lies in a cyclotomic extension of $\mathbb{Q}$. This problem asks you to verify this special case.

(a) Prove that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.

The 8th roots of unity are given by $\zeta_8 = e^{2\pi i/8}$, so:

$$\zeta_8 = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

Then:

$$\zeta_8 + \zeta_8^{-1} = 2\cos\left(\frac{\pi}{4}\right) = \sqrt{2}$$

Since $\zeta_8 \in \mathbb{Q}(\zeta_8)$, it follows that $\zeta_8^{-1} \in \mathbb{Q}(\zeta_8)$ and thus their sum is also in $\mathbb{Q}(\zeta_8)$.

Therefore:

$$\sqrt{2} \in \mathbb{Q}(\zeta_8)$$

(b) Prove that $\sqrt{3} \in \mathbb{Q}(\zeta_{12})$

Consider $\zeta_{12} = e^{2\pi i/12} = \cos\left(\frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{6}\right)$.

Then:

$$\zeta_{12} - \zeta_{12}^{-1} = 2i \sin\left(\frac{\pi}{6}\right) = 2i \cdot \frac{1}{2} = i$$

and:

$$\zeta_{12} + \zeta_{12}^{-1} = 2 \cos\left(\frac{\pi}{6}\right) = 2 \cdot \frac{\sqrt{3}}{2} = \sqrt{3}$$

Hence, since both ζ_{12} and ζ_{12}^{-1} lie in $\mathbb{Q}(\zeta_{12})$, so does their sum.

Therefore:

$$\sqrt{3} \in \mathbb{Q}(\zeta_{12})$$

(c) More generally, prove that if p is an odd prime, then $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$. (*Hint.* We haven't really developed the tools yet to prove (c), but it's fun to think about. One way to prove is to show that $p = \Phi_{\zeta_p,\mathbb{Q}}(1)$ is (almost) a square in $\mathbb{Q}(\zeta_{4p})$ by using the factorization of $\Phi_{\zeta_p,\mathbb{Q}}(x)$ into linear factors in $\mathbb{Q}(\zeta_p)[x]$.)

Let p be an odd prime, and consider the field $\mathbb{Q}(\zeta_{4p})$. Since ζ_{4p} is a primitive $4p$th root of unity, we have:

$$\mathbb{Q}(\zeta_{4p}) \supseteq \mathbb{Q}(\zeta_p)$$

and it is known that $\mathbb{Q}(\zeta_p)$ contains all the conjugates of ζ_p, hence splitting the pth cyclotomic polynomial:

$$\Phi_p(x) = \prod_{1 \le k < p, \gcd(k,p)=1} (x - \zeta_p^k)$$

The key fact is that the Gaussian periods (i.e., certain symmetric sums of the ζ_p^k) generate $\sqrt{p}$ over $\mathbb{Q}$ in $\mathbb{Q}(\zeta_{4p})$.

In more advanced theory (e.g., via quadratic Gauss sums), one can show that:

$$\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$$

as a sum or difference of roots of unity, sometimes up to a scalar factor.

Hence, although we haven't proven it directly via explicit computation, this inclusion is consistent with deeper results from cyclotomic fields and Gauss sums, validating that:

$$\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$$

Problem 11 (9.48)**.** Consider the cyclotomic polynomial

$$\Phi_{17}(x) = \frac{x^{17} - 1}{x - 1} = x^{16} + x^{15} + \cdots + x + 1$$

which we know is irreducible from Example 8.36.

(a) Prove that $f(x)$ is solvable in radicals over $\mathbb{Q}$.

The roots of $\Phi_{17}(x)$ are the primitive 17th roots of unity:

$$\zeta_{17}, \zeta_{17}^2, \ldots, \zeta_{17}^{16}$$

where ζ_{17} is a primitive 17th root of unity. The splitting field of $\Phi_{17}(x)$ is $\mathbb{Q}(\zeta_{17})$.

The Galois group of $\mathbb{Q}(\zeta_{17})/\mathbb{Q}$ is isomorphic to the multiplicative group $(\mathbb{Z}/17\mathbb{Z})^\times$, which is cyclic of order 16:

$$G = \text{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \cong \mathbb{Z}_{16}$$

Since this Galois group is abelian and its order is a power of 2, the extension is solvable. Hence, the polynomial $\Phi_{17}(x)$ is solvable in radicals over $\mathbb{Q}$.

(b) Let K be the splitting field over $\mathbb{Q}$ of $\Phi_{17}(x)$. Prove that there is a sequence of fields

$$\mathbb{Q} = E_0 \subset E_1 \subset E_2 \subset E_3 \subset E_4 = K$$

with each $[E_{i+1} : E_i] = 2$. Conclude that the roots of $f(x)$ require taking only square roots.

As shown in part (a), $K = \mathbb{Q}(\zeta_{17})$ is a Galois extension of degree $16 = 2^4$. So:

$$[K : \mathbb{Q}] = 16$$

Because the Galois group is cyclic of order 16, we can construct a tower of subfields corresponding to the unique subgroup chain of the cyclic group:

$$\mathbb{Q} = E_0 \subset E_1 \subset E_2 \subset E_3 \subset E_4 = \mathbb{Q}(\zeta_{17})$$

where each extension has degree 2:

$$[E_{i+1} : E_i] = 2$$

Since each step in the field tower is a quadratic extension, each step involves adjoining a square root. Therefore, adjoining the roots of $\Phi_{17}(x)$ requires only taking square roots.

(c) Recall that we proved that a number is constructible if and only if it lives in a field obtained by taking successive square roots. Use (b) to prove that it is possible to draw a regular 17-gon using ruler and compass.

A point in the complex plane is constructible by straightedge and compass if and only if its coordinates lie in a field obtained from $\mathbb{Q}$ by a sequence of quadratic extensions, i.e., degrees of 2.

From (b), the coordinates of ζ_{17} lie in $\mathbb{Q}(\zeta_{17})$, which is obtained from $\mathbb{Q}$ by four successive quadratic extensions. Hence, ζ_{17} is constructible.

The vertices of the regular 17-gon are the powers of ζ_{17} on the unit circle:

$$\zeta_{17}^k \text{ for } k = 0, 1, \ldots, 16$$

Thus, all the vertices are constructible, and the regular 17-gon is constructible by ruler and compass.

Therefore, it is possible to draw a regular 17-gon using only a straightedge and compass.

Problem 12 (9.53)**.** Let K be a field, let $\sigma_1 : K \longrightarrow K$ and $\sigma_2 : K \longrightarrow K$ be field automorphisms, let $c_1, c_2 \in K$, and define a function

$$\phi : K \longrightarrow K, \quad \phi(\alpha) = c_1\sigma_1(\alpha) + c_2\sigma_2(\alpha)$$

(a) Give an example of a field K, distinct field automorphisms σ_1, σ_2 of K, and non-zero field elements $c_1, c_2 \in K$, so that the map $\phi = c_1\sigma_1 + c_2\sigma_2$ is neither injective nor surjective.

Let $K = \mathbb{C}$, the field of complex numbers. Consider the identity automorphism $\sigma_1 = \mathrm{id}$ and complex conjugation $\sigma_2 = \mathrm{conj}$.

Let $c_1 = 1$ and $c_2 = 1$, so the map is:

$$\phi(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = \alpha + \overline{\alpha} = 2\Re(\alpha)$$

This map sends every complex number to twice its real part. So:

- It is not injective, since all purely imaginary numbers $\alpha = bi$ (with $b \neq 0$) get mapped to 0. - It is not surjective, since its image is the set of real numbers (a proper subfield of $\mathbb{C}$).

Therefore, ϕ is neither injective nor surjective.

(b) Let $\alpha, \beta \in K$. Expand and simplify the difference

$$\phi(\alpha) \cdot \phi(\beta) - \phi(\alpha \cdot \beta)$$

to find an expression that makes it clear that the difference is unlikely to be 0.

First, write out both terms:

$$\phi(\alpha) = c_1\sigma_1(\alpha) + c_2\sigma_2(\alpha), \quad \phi(\beta) = c_1\sigma_1(\beta) + c_2\sigma_2(\beta)$$

So their product is:

$$\begin{aligned}\phi(\alpha) \cdot \phi(\beta) &= (c_1\sigma_1(\alpha) + c_2\sigma_2(\alpha))(c_1\sigma_1(\beta) + c_2\sigma_2(\beta)) \\ &= c_1^2\sigma_1(\alpha)\sigma_1(\beta) + c_1c_2\sigma_1(\alpha)\sigma_2(\beta) + c_2c_1\sigma_2(\alpha)\sigma_1(\beta) + c_2^2\sigma_2(\alpha)\sigma_2(\beta)\end{aligned}$$

Now compute $\phi(\alpha\beta)$:

$$\phi(\alpha\beta) = c_1\sigma_1(\alpha\beta) + c_2\sigma_2(\alpha\beta) = c_1\sigma_1(\alpha)\sigma_1(\beta) + c_2\sigma_2(\alpha)\sigma_2(\beta)$$

Taking the difference:

$$\begin{aligned}\phi(\alpha)\phi(\beta) - \phi(\alpha\beta) = &\left(c_1^2\sigma_1(\alpha)\sigma_1(\beta) + c_2^2\sigma_2(\alpha)\sigma_2(\beta)\right) + (c_1c_2\sigma_1(\alpha)\sigma_2(\beta) + c_2c_1\sigma_2(\alpha)\sigma_1(\beta)) \\ &- (c_1\sigma_1(\alpha)\sigma_1(\beta) + c_2\sigma_2(\alpha)\sigma_2(\beta)) \\ = &(c_1^2 - c_1)\sigma_1(\alpha)\sigma_1(\beta) + (c_2^2 - c_2)\sigma_2(\alpha)\sigma_2(\beta) \\ &+ c_1c_2\sigma_1(\alpha)\sigma_2(\beta) + c_1c_2\sigma_2(\alpha)\sigma_1(\beta)\end{aligned}$$

This expression is typically non-zero unless $\sigma_1 = \sigma_2$, or $c_1 = 0$ or 1, or special cancellation occurs. The presence of cross terms like $\sigma_1(\alpha)\sigma_2(\beta)$ shows that ϕ is very unlikely to preserve multiplication, and thus is generally not a ring homomorphism.