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.

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.

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

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

(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.)

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 $f(x) = x^4 - 5x^2 + 6$

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

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

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

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

(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 $G(K/F)$.

(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 $G(K/F)$.

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 $g(X)$.

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 seperable extension.

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

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

Prove that

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

(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 $(\mathbb{Z}/N\mathbb{Z})^*$.

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

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

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.

(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 $G(K/F)$.

(c) Prove that

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

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.

(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

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

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

(c) For each of the following K/F and $\alpha \in K$, compute $\mathrm{tr}_{K/F}(\alpha)$ 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) $F = \mathbb{R}$, $K = \mathbb{C}$, $\alpha = a + bi$ with $a, b \in \mathbb{R}$

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

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

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

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

(*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.)

Problem 10 (9.44)**.** For this problem, we write ζ_n for a primite 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 $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.

(b) Prove that $\sqrt{3} \in \mathbb{Q}(\zeta_1 2)$

(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 $\mathbb{Q}(\zeta_p)[x]$.)

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

$$\Phi_1 7(x) = \frac{x^1 7 - 1}{x - 1} = x^1 6 + x^1 5 + \cdots + x + 1$$

which we know is irreducible from Example 8.36.

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

(b) Let K be the splitting field over $\mathbb{Q}$ of $\Phi_1 7(x)$. 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.

(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.

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 sujective.

(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.