ALGEBRA QUALIFYING EXAM PROBLEMS
FIELD THEORY

Kent State University
Department of Mathematical Sciences

Compiled and Maintained
by
Donald L. White

Version: September 7, 2023

CONTENTS

FIELD THEORY

General Field Theory

1. Prove or disprove each of the following statements.
   (a) If K is a subfield of F and F is isomorphic to K, then $F = K$.
   (b) The field $\mathbb{C}$ of complex numbers is an algebraic closure of the field $\mathbb{Q}$ of rational numbers.
   (c) If K is a finitely generated extension of F, then $[K : F]$ is finite.
   (d) If K is a finitely generated algebraic extension of F, then $[K : F]$ is finite.
   (e) If $F \subseteq E \subseteq K$ is a tower of fields and K is normal over F, then E is normal over F.
   (f) If $F \subseteq E \subseteq K$ is a tower of fields and K is normal over F, then K is normal over E.
   (g) If $F \subseteq E \subseteq K$ is a tower of fields, E is normal over F and K is normal over E, then K is normal over F.
   (h) If $F \subseteq E \subseteq K$ is a tower of fields and K is separable over F, then E is separable over F.
   (i) If $F \subseteq E \subseteq K$ is a tower of fields and K is separable over F, then K is separable over E.
   (j) If $F \subseteq E \subseteq K$ is a tower of fields, E is separable over F and K is separable over E, then K is separable over F.

2. Give an example of an infinite chain $\Omega_1 \subset \Omega_2 \subset \Omega_3 \subset \cdots$ of algebraically closed fields.

3. Let E be an extension field of a field F and $f(x), g(x) \in F[x]$. Prove that a greatest common divisor of f and g in $F[x]$ is also a greatest common divisor of f and g in $E[x]$.

4. Let F be a field and F^* its multiplicative group. Show that the abelian groups $(F, +)$ and $(F^*, \cdot)$ are not isomorphic.

5. Prove that a finite subgroup of the multiplicative group of a field must be cyclic.

6. (a) Prove that a finite integral domain is a field.
   (b) Prove that if R is an integral domain that is finite dimensional over a subfield $F \subseteq R$, then R is a field.

7. Show that if F is a finite extension of $\mathbb{Q}$, then the torsion subgroup of F^* is finite. [Hint: The torsion subgroup consists of roots of unity.]

8. Suppose $F \subset E \subset K$ is any tower of fields and $[K : F]$ is finite.
   Show that $[K : F] = [K : E][E : F]$.

9. Let K be a field extension of F of degree n and let $f(x) \in F[x]$ be an irreducible polynomial of degree $m > 1$. Show that if m is relatively prime to n, then f has no root in K.

10. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be an irreducible polynomial of degree greater than 1 in which all roots lie on the unit circle of $\mathbb{C}$. Prove that $a_i = a_{n-i}$ for all i.

11. Let F be a field extension of the rational numbers.
    (a) Show that $\{a + b\sqrt{2} \mid a, b \in F\}$ is a field.
    (b) Give necessary and sufficient conditions for $\{a + b\sqrt[3]{2} \mid a, b \in F\}$ to be a field.

12. Let K be a field extension of a field F and let α be an element of K. Give necessary and sufficient conditions for $\{a + b\alpha \mid a, b \in F\}$ to be a field.

13. Let K be an extension field of F with $a, b \in K$. Let $[F(a) : F] = m$ and $[F(b) : F] = n$ and assume $(m, n) = 1$. Show that $F(a) \cap F(b) = F$ and $[F(a, b) : F] = mn$.

14. Let F, L, and K be subfields of a field M, with $F \subseteq K$ and $F \subseteq L$. Let $[K : F] = k$ and $[L : F] = \ell$.
    (a) Show that $[KL : F] \leqslant k\ell$.
    (b) Show that if $(k, \ell) = 1$ then $[KL : F] = k\ell$.
    (c) Give an example where $[KL : F] < k\ell$.

15. Let K be a finite dimensional extension field of a field F and let G be a group of F-automorphisms of K. Prove that $|G| \leqslant [K : F]$.

16. Let E be a finite dimensional extension of a field F and let G be a group of F-automorphisms of E such that $[E : F] = |G|$. Show that F is the fixed field of G.

17. Let E be a finite dimensional extension of a field F and let G be a group of F-automorphisms of E. Show that if F is the fixed field of G, then $[E : F] = |G|$.

18. Let F be a field with the property

    (*) If $a, b \in F$ and $a^2 + b^2 = 0$, then $a = 0$ and $b = 0$.

    (a) Show that $x^2 + 1$ is irreducible in $F[x]$.
    (b) Which of the fields $\mathbb{Z}_3$, $\mathbb{Z}_5$ satisfy (*)?

19. Show that $p(x) = x^3 + x - 6$ is irreducible over $\mathbb{Q}[i]$.

20. In each case below a field F and a polynomial $f(x) \in F[x]$ are given. Either prove that f is irreducible over f or factor $f(x)$ into irreducible polynomials in $F[x]$. Find $[K : F]$, where K is a splitting field for f over F.
    (a) $F = \mathbb{Q}$, $f(x) = x^4 - 5$.
    (b) $F = \mathbb{Q}(\sqrt{-3})$, $f(x) = x^3 - 3$.
    (c) $F = \mathbb{Q}$, $f(x) = x^3 - x^2 - 5x + 5$.

21. Let $\mathbb{Q}$ be the field of rational numbers. Show that the group of automorphisms of $\mathbb{Q}$ is trivial.

22. Let $\mathbb{R}$ be the field of real numbers. Show that the group of automorphisms of $\mathbb{R}$ is trivial.

23. Let $\mathbb{R}$ be the field of real numbers. Show that if $f(x)$ is an irreducible polynomial over $\mathbb{R}$, then f is of degree 1 or 2.

24. Let F be a field and p a prime. Let $G = \{c \in F \mid c^{p^n} = 1 \text{ for some positive integer } n\}$.
    (a) Show that G is a subgroup of the multiplicative group of F.
    (b) Prove that either G is a cyclic group or G is isomorphic to $\mathbb{Z}(p^\infty)$, the Prüfer group for the prime p.

25. Let E be a finite dimensional extension of a field F and let G be a group of F-automorphisms of E. Show the following.
   (a) If $e \in E$ then $G_e = \{\sigma \in G \mid \sigma(e) = e\}$ is a subgroup of G.
   (b) $[G : G_e] \leqslant [F(e) : F]$.
   (c) If F is the fixed field of G and $e_1, e_2, \ldots, e_n$ are the distinct images of e under G, then $f(x) = (x - e_1)(x - e_2) \cdots (x - e_n)$ is the minimal polynomial of e over F.

26. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension of $\mathbb{Q}$.

27. Find the minimal polynomial of $\alpha = \sqrt{3 + \sqrt{7}}$ over the field $\mathbb{Q}$ of rational numbers, and *prove* it is the minimal polynomial.

28. Find the minimal polynomial of $\alpha = \sqrt{5 + \sqrt{3}}$ over the field $\mathbb{Q}$ of rational numbers, and *prove* it is the minimal polynomial.

29. Find the minimal polynomial of $\alpha = \sqrt{11 + \sqrt{3}}$ over the field $\mathbb{Q}$ of rational numbers, and *prove* it is the minimal polynomial.

30. Find the minimal polynomial of $\alpha = \sqrt{3 + 2\sqrt{2}}$ over the field $\mathbb{Q}$ of rational numbers, and *prove* it is the minimal polynomial.

31. Find the minimal polynomial of $\alpha = \sqrt[3]{2 + \sqrt{2}}$ over the field $\mathbb{Q}$ of rational numbers, and *prove* it is the minimal polynomial.

32. Let F be a field. Show that F is algebraically closed if and only if every maximal ideal of $F[x]$ has codimension 1.

Algebraic Extensions

33. Let α belong to some field extension of the field F. Prove that $F(\alpha) = F[\alpha]$ if and only if α is algebraic over F.

34. Show that $p(x) = x^3 + 2x + 1$ is irreducible over $\mathbb{Q}$. Let θ be a root of $p(x)$ in an extension field and find the mutiplicative inverse of $1 + \theta$ in $\mathbb{Q}[\theta]$.

35. Let $F \subseteq K$ be fields and let $\alpha \in K$ be algebraic over F with minimal polynomial $f(x) \in F[x]$ of degree n. Show that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F.

36. Show that if K is finite dimensional field extension of F, then K is algebraic over F.

37. Let F be a field, let $E = F(\alpha)$ be a simple extension field of F, and let $\beta \in E - F$. Prove that α is algebraic over $F(\beta)$.

38. Show that if $|F : \mathbb{Q}| = 2$, then there exists a square free integer m different from 1 so that $F = \mathbb{Q}(\sqrt{m})$.

39. Let K be an extension field of the field F such that $[K : F]$ is odd. Show that if $u \in K$ then $F(u) = F(u^2)$.

40. (a) Let α be algebraic over a field F and set $E = F(\alpha)$. Prove that if $|E : F|$ is odd, then $E = F(\alpha^2)$.
   (b) Give an example of a simple algebraic extension $E = F(\alpha)$ where $|E : F|$ is not divisible by 3 but $F(\alpha^3)$ is strictly contained in E.

41. Let K be a finite degree extension of the field F such that $[K : F]$ is relatively prime to 6. Show that if $u \in K$ then $F(u) = F(u^3)$.

42. Let F be a field, $f(x)$ an irreducible polynomial in $F[x]$, and α a root of f in some extension of F. Show that if some odd degree term of $f(x)$ has a non-zero coefficient, then $F(\alpha) = F(\alpha^2)$.

43. Let $f(x)$ and $g(x)$ be irreducible polynomials in $F[x]$ of degrees m and n, respectively, where $(m, n) = 1$. Show that if α is a root of $f(x)$ in some field extension of F, then $g(x)$ is irreducible in $F(\alpha)[x]$.

44. Let K be an extension field of F and let α be an element of K. Show that if $F(\alpha) = F(\alpha^2)$, then α is algebraic over F.

45. Let K be an extension field of F and let α be an element of K. Show that the following are equivalent:
    (i) α is algebraic over F,
    (ii) $F(\alpha)$ is a finite dimensional extension of F,
    (iii) α is contained in a finite dimensional extension of F.

46. Let α be algebraic over $\mathbb{Q}$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and set $F = \mathbb{Q}(\alpha)$. Prove that if $f(x) \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$, then one of the following occurs:
    (i) $f(x)$ remains irreducible in $F[x]$;
    (ii) $f(x)$ is a product of two irreducible polynomials in $F[x]$ of equal degree.

47. Let $F \subset E \subset K$ be a tower of fields such that $K = F(\alpha)$ with α algebraic over F. Prove that if $f(x) \in F[x]$ is the minimal polynomial of α over F and $F \neq E$, then $f(x)$ is not irreducible in $E[x]$.

48. Let E be an extension field of F and $A = \{e \in E \mid e \text{ is algebraic over } F\}$.
    (a) Show that A is a subfield of E containing F.
    (b) Show that if $\sigma : E \to E$ is a one-to-one F-homomorphism, then $\sigma(A) = A$.

49. Let p and q be distinct primes. Show that $\sqrt{q}$ is not an element of $\mathbb{Q}(\sqrt{p})$.

50. Show that if $p_1, \ldots, p_n, p_{n+1}$ are distinct prime numbers, then $\sqrt{p_{n+1}}$ is not an element of the field $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.

51. Let α_1, α_2, and α_3 be real numbers such that $(\alpha_i)^2 \in \mathbb{Q}$ for each i, and let $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Show that $\sqrt[3]{2}$ is not in K.

52. (a) Prove that if E is a finite dimensional field extension of F that is generated over F by a subset S of E satisfying $a^2 \in F$ for all $a \in S$, then $|E : F|$ is a power of 2.
    (b) Give an example that shows 2 cannot be replaced by 3 in part (a).

53. Let $F \subseteq L \subseteq K$ with $[L : F]$ finite, and let α be an element of K. Show that α is algebraic over L if and only if α is algebraic over F.

54. Show that if K is algebraic over F and $\sigma : K \to K$ is an F-monomorphism, then σ is onto.

55. Suppose K is an algebraic extension field of a field F such that there are only finitely many intermediate fields between F and K. Show that K is a simple extension of F.

56. Let K be a simple algebraic extension of a field F. Show that there are only finitely many intermediate fields between F and K.

57. Suppose E is an algebraic extension of F and $\bar{E}$ is an algebraic closure of E. Show that $\bar{E}$ is an algebraic closure of F.

58. Let α be algebraic over the field F with minimal polynomial $f(x) \in F[x]$ and let $K = F[\alpha]$. Show that if $\sigma : F \to L$ is a field monomorphism and $\beta \in L$ is a root of $f^{\sigma}(x) \in L[x]$, then σ has a unique extension $\hat{\sigma} : K \to L$ satisfying $\hat{\sigma}(\alpha) = \beta$.

59. Suppose E_1 and E_2 are algebraic closures of a field F. Show that there is an F-isomorphism $\sigma : E_1 \to E_2$.

60. (a) Show that for every prime p and every positive integer n there is an irreducible polynomial of degree n over the field $\mathbb{F}_p$ of p elements.
    (b) Show that for every positive integer n there is an irreducible polynomial of degree n over the field $\mathbb{Q}$ of rational numbers.

Normality and Splitting Fields

61. Let K be an extension field of F. Show that the following are equivalent.
    (i) Each irreducible polynomial in $F[x]$ with one root in K has all its roots in K.
    (ii) K is obtained from F by adjoining all roots of a set of polynomials in $F[x]$.
    (iii) Every F-isomorphism of K in a fixed algebraic closure is an F-automorphism.

62. Let K be the splitting field of $x^2 + 2$ over $\mathbb{Q}$. Prove or disprove that $i = \sqrt{-1}$ is an element of K.

63. Let K be the splitting field of $x^3 - 5$ over $\mathbb{Q}$. Prove or disprove that $i = \sqrt{-1}$ is an element of K.

64. Let Ω be a fixed algebraic closure of F and $K \subseteq \Omega$ an algebraic extension of F. Show that K is a normal extension of F if and only if every F-isomorphism $\varphi : K \to K' \subseteq \Omega$ is an F-automorphism.

65. Let F be a field and E a splitting field of the irreducible polynomial $f(x) \in F[x]$. Show that if $c, d \in F$ and $c \neq 0$, then the polynomial $f(cx + d)$ splits in $E[x]$.

Separability

66. Show that if K is a separable extension of F and L is a field with $F \subseteq L \subseteq K$, then L is a separable extension of F and K is a separable extension of L.

67. Let $f(x) \in F[x]$ be a polynomial, and let $f'(x)$ denote its formal derivative in $F[x]$. Prove that $f(x)$ has distinct roots in any extension field of F if and only if $\gcd(f(x), f'(x)) = 1$.

68. Show that if K is a finite dimensional separable extension of F, then $K = F(u)$ for some u in K.

69. Let F be a field and let $f(x) = x^n - x \in F[x]$. Show that if $\operatorname{char} F = 0$ or if $\operatorname{char} F = p$ and $p \nmid n-1$, then f has no multiple root in any extension of F.

70. Show that if F is a field of characteristic 0 then every algebraic extension of F is separable. (Provide an argument; do not just state that every field of characteristic 0 is perfect and every algebraic extension of a perfect field is separable.)

71. Show that if F is a finite field then every algebraic extension of F is separable.

72. Let F be a field of characteristic p and let x be an indeterminate over F.
    (a) Show that $F(x^p)$ is a proper subfield of $F(x)$.
    (b) Show that $F(x)$ is a splitting field for some polynomial over $F(x^p)$.
    (c) Show that the only automorphism of $F(x)$ fixing $F(x^p)$ is the identity automorphism.

73. Let F be a field and $f(x) \in F[x]$ an irreducible polynomial. Prove that there is a prime p, an integer $a \geqslant 0$ and a separable polynomial $g(x) \in F[x]$ such that $f(x) = g(x^{p^a})$.

74. Let K be an arbitrary separable extension of F. Show that if every element of K is a root of a polynomial in $F[x]$ of degree less than or equal to n, then K is a simple extension of F of degree less than or equal to n.

75. Let F be a field and let $f(x) \in F[x]$ have splitting field K. Show that if the degree of f is a prime p and $[K : F] = tp$ for some integer t, then
    (a) $f(x)$ is irreducible over F and
    (b) if $t > 1$ then K is a separable extension of F.

76. Let x and y be independent indeterminates over $\mathbb{Z}_p$, $K = \mathbb{Z}_p(x, y)$, and $F = \mathbb{Z}_p(x^p, y^p)$.
    (a) Show that $[K : F] = p^2$
    (b) Show that K is not a simple extension of F.

77. A field F is called *perfect* if every element of an algebraic closure of F is separable over F. Let F be a field of characteristic p. Show that the following are equivalent.
    (i) The field F is perfect.
    (ii) For every $\epsilon \in F$ there exists a $\delta \in F$ such that $\delta^p = \epsilon$.
    (iii) The map $a \mapsto a^p$ is an automorphism of F.

78. Show that every field of characteristic 0 is perfect.

79. Show that every finite field is perfect.

80. Let $F \subseteq K$ be fields having characteristic p and assume that K is a normal algebraic extension of F. Prove that there exists a field E with $F \subseteq E \subseteq K$, E/F purely inseparable, and K/E separable.

81. Let E be a field and let G be a finite group of automorphisms of E. Let F be the fixed field of G. Prove that E is a separable algebraic extension of F.

82. Let G be a finite group of automorphisms of the field K and set

$$F = \{\alpha \in K \mid \alpha^\sigma = \alpha \text{ for all } \sigma \in G\}.$$

Show that every element of K is separably algebraic over F of degree at most $|G|$.

83. Let p be a prime and let $F = \mathbb{Z}_p(x)$ be the field of fractions of $\mathbb{Z}_p[x]$. Let E be the splitting field of $f(y) = y^p - x$ over F.
    (a) Show that $[E : F] = p$.
    (b) Show that $|\mathrm{Aut}_F(E)| = 1$.
    (c) What conclusion can you draw from (a) and (b)?

84. Let $K = F(u)$ be a separable extension of F with $u^m \in F$ for some positive integer m. Show that if the characteristic of F is p and $m = p^t r$, then $u^r \in F$.

85. If K is an extension of a field F of characteristic $p \neq 0$, then an element u of K is called *purely inseparable* over F if $u^{p^t} \in F$ for some t. Show that the following are equivalent.
    (i) u is purely inseparable over F.
    (ii) u is algebraic over F with minimal polynomial $x^{p^n} - a$ for some $a \in F$ and integer n.
    (iii) u is algebraic over F and its minimal polynomial factors as $(x - u)^m$.

86. Show that every purely inseparable field extension is a normal extension.

87. Let K be an extension of a field F of characteristic $p \neq 0$. Show that an element u of K is both separable and purely inseparable if and only if $u \in F$.

88. Let $\mathbb{Z}_2(x)$ be the field of fractions of the polynomial ring $\mathbb{Z}_2[x]$. Construct an extension of $\mathbb{Z}_2(x)$ that is neither separable nor purely inseparable.

Galois Theory

89. State the Fundamental Theorem of Galois Theory.

90. Let K be a finite Galois extension of F with Galois group G. Suppose that E_1 and E_2 are intermediate extensions satisfying $E_1 \subset E_2$, and let $H_1 \supset H_2$ be the corresponding subgroups of G. Prove that E_2 is a normal extension of E_1 if and only if H_2 is a normal subgroup of H_1, and when this happens, the Galois group of E_2 over E_1 is isomorphic to H_1/H_2.

91. Let K be a finite Galois extension of F with Galois group $G = \mathrm{Gal}(K/F)$. Let E be an intermediate field that is normal over F. Prove that $\mathrm{Gal}(K/E) \trianglelefteq G$ and $G/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F)$.

92. Let K be a finite algebraic extension of F and let G be the group of all F-automorphisms of K. Let $\mathcal{F}(G) = \{u \in K \mid \sigma(u) = u \text{ for all } \sigma \in G\}$. Show that K is both separable and normal (i.e. Galois) over F if and only if $\mathcal{F}(G) = F$.

93. Let K be a Galois extension of the field F with Galois group G. Let $g(x)$ be a monic polynomial over F that splits over K (that is, K contains a splitting field for $g(x)$ over F) and let $\Delta \subseteq K$ be the set of roots of $g(x)$. Prove that $g(x)$ is a power of a polynomial that is irreducible over F if and only if G is transitive on Δ.

94. Let K be a finite dimensional extension field of L and let $\sigma : L \to F$ be an embedding of L into a field F. Prove that there are at most $[K : L]$ extensions of σ to embeddings of K into F.

95. If S is any semi-group (written multiplicatively) and F any field, a homomorphism from S into the multiplicative group of nonzero elements of F is called an F-character of S.

    Prove that any set $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ of F-characters of S is linearly independent in the vector space over F of functions $S \to F$.

96. Let K be an extension field of F and let F' be the fixed field of the group of F-automorphisms of K. Show that K is a Galois extension of F'.

97. Let K be a finite normal extension of F and let E be the fixed field of the group of all F-automorphisms of K. Show that the minimal polynomial over F of each element of E has only one distinct root.

98. Let E be a splitting field over F of a separable polynomial $f(x)$ in $F[x]$ and $G = \mathrm{Gal}(E/F)$. Show that $\{e \in E \mid \sigma(e) = e \text{ for all } \sigma \in G\} = F$.

99. **[NEW]**
    Let F be a field, $f(x) \in F[x]$ irreducible and separable over F, and K the splitting field of $f(x)$ over F. Prove that if the Galois group of K over F is abelian, then $K = F(\alpha)$, where α is a root of $f(x)$.

100. Let K be a Galois extension of F with $|\mathrm{Gal}(K/F)| = 12$. Prove that there exists a subfield E of K containing F with $[E : F] = 3$. Does a subextension L necessarily exist satisfying $[L : F] = 2$? Explain.

101. Suppose $K = F(\alpha)$ is a proper Galois extension of F and assume there exists an element σ of $\mathrm{Gal}(K/F)$ satisfying $\sigma(\alpha) = \alpha^{-1}$. Show that $[K : F]$ is even and that $[F(\alpha + \alpha^{-1}) : F] = \frac{1}{2}[K : F]$.

102. Let K be a finite Galois extension of F of characteristic 0. Show that if $\mathrm{Gal}(K/F)$ is a non-trivial 2-group, then there is a quadratic extension of F contained in K.

103. Let G be a finite group. Show that there is an algebraic extension F of the field $\mathbb{Q}$ of rational numbers and a Galois extension K of F such that $G \cong \mathrm{Gal}(K/F)$.

104. (a) Find the Galois group of $x^3 - 2$ over $\mathbb{Q}$ and demonstrate the Galois correspondence between the subgroups of the Galois group and the subfields of the splitting field.

     (b) Find all automorphisms of $\mathbb{Q}(\sqrt[3]{2})$. Is there an $f(x) \in \mathbb{Q}[x]$ with splitting field $\mathbb{Q}(\sqrt[3]{2})$? Explain.

105. Let F be any field and let $f(x) = x^n - 1 \in F[x]$. Show that if K is the splitting field of $f(x)$ over F, then K is separable over F (hence Galois) and that $\mathrm{Gal}(K/F)$ is abelian.

106. Let η_7 be a complex primitive 7th root of unity and let $K = \mathbb{Q}(\eta_7)$. Find $\mathrm{Gal}(K/\mathbb{Q})$ and express each intermediate field F between $\mathbb{Q}$ and K as $F = \mathbb{Q}(\beta)$ for some $\beta \in K$.

107. Let η be a complex primitive 7th root of unity and let $K = \mathbb{Q}(\eta)$, where $\mathbb{Q}$ is the field of rational numbers. Show that there is a unique extension F of degree 2 of $\mathbb{Q}$ contained in K and find $q \in \mathbb{Q}$ such that $F = \mathbb{Q}(\sqrt{q})$.

108. Let $\mathbb{Q}$ be the field of rational numbers and η a complex primitive 8th root of unity. Determine $\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$ and all the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\eta)$.

109. (a) Determine the Galois group of $x^4 - 4$ over the field $\mathbb{Q}$ of rational numbers.
   (b) How many intermediate fields are there between $\mathbb{Q}$ and the splitting field of $x^4 - 4$?

110. Let $f(x) = (x^2 - 2)(x^2 - 3)$ and let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Find, with proof, all elements of $\mathrm{Gal}(K/\mathbb{Q})$ and all intermediate subfields of K.

111. Determine the Galois group of $x^4 - 4$ over the field $\mathbb{Q}$ of rational numbers and identify all of the intermediate fields between $\mathbb{Q}$ and the splitting field of $x^4 - 4$. Use the Fundamental Theorem.

112. Determine the Galois group of $x^4 - 3$ over the field $\mathbb{Q}$ of rational numbers.

113. Determine the Galois group of $x^4 + 2$ over the field $\mathbb{Q}$ of rational numbers.

114. Determine the Galois group of $x^3 + 3x^2 - 1$ over $\mathbb{Q}$.

115. Show that the Galois group of $x^3 - 5$ over $\mathbb{Q}$ is S_3 and demonstrate the Galois correspondence between the subgroups of S_3 and the subfields of the splitting field. Which subfields are normal over $\mathbb{Q}$?

116. Let K be the splitting field of $x^3 - 3$ over $\mathbb{Q}$. Use Galois Theory to identify $\mathrm{Gal}(K/\mathbb{Q})$ and find explicitly all of the intermediate subfields.

117. Let K be a splitting field for $x^5 - 2$ over $\mathbb{Q}$.
   (a) Determine $[K : \mathbb{Q}]$.
   (b) Show that $\mathrm{Gal}(K/\mathbb{Q})$ is non-abelian.
   (c) Find all normal intermediate extensions F and express as $F = \mathbb{Q}(\alpha)$ for appropriate α.

118. Let $\mathbb{Q}$ be the field of rational numbers and E the splitting field (in the field of complex numbers) of $x^4 - 2$.
   (a) Find $|\mathrm{Gal}(E/\mathbb{Q})|$.
   (b) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ be such that $\sigma(\alpha) = \bar{\alpha}$ for all $\alpha \in E$ (where $\bar{\alpha}$ is the complex conjugate of α). Find $\mathrm{Inv}(\langle\sigma\rangle) = \{\alpha \in E \mid \sigma(\alpha) = \alpha\}$.
   (c) Is $\langle\sigma\rangle$ a normal subgroup of $\mathrm{Gal}(E/\mathbb{Q})$?

119. Let $f(x) = x^4 + 4x^2 + 2$ and let K be the splitting field of f over $\mathbb{Q}$. Show that the Galois group of K over $\mathbb{Q}$ is cyclic of order 4.

120. **[NEW]**
   Find, with proof, the Galois group of the splitting field over the rational numbers of the polynomial $f(x)$ where
   (a) $f(x) = x^6 + 3$,
   (b) $f(x) = x^6 - 3$,
   (c) $f(x) = x^8 + 2$,
   (d) $f(x) = x^8 - 2$.

121. Let p be a prime number, and let K be the splitting field of $f(x) = x^6 - p$ over $\mathbb{Q}$, the field of rational numbers. Determine the Galois group of K over $\mathbb{Q}$ as well as all of the intermediate fields E satisfying $|E : \mathbb{Q}| = 2$.

122. Let F be the field of 2 elements and K a splitting field of $f(x) = x^6 + x^3 + 1$ over F.
   (a) Show that if r is a root of f, then $r^9 = 1$ but $r^3 \neq 1$.
   (b) Show that f is irreducible over F.
   (c) Find $\mathrm{Gal}(K/F)$ and express each intermediate field between F and K as $F(b)$ for appropriate b in K.

123. Let K be a Galois extension of $\mathbb{Q}$ whose Galois group is isomorphic to S_5. Prove that K is the splitting field of some polynomial of degree 5 over $\mathbb{Q}$.

124. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Show that $\displaystyle\sum_{i=1}^{n} \frac{1}{\alpha_i}$ is a rational number.

125. Let $\alpha = \sqrt{2} + \sqrt{3}$ and let $E = \mathbb{Q}(\alpha)$.
   (a) Find the minimal polynomial $m(x)$ of α over $\mathbb{Q}$ and $|E : \mathbb{Q}|$.
   (b) Find the splitting field of $m(x)$ over $\mathbb{Q}$ and all intermediate fields, and find its Galois group over $\mathbb{Q}$ and all its subgroups.

126. Let $\alpha = \sqrt{3 + \sqrt{5}}$.
   (a) Find the minimal polynomial $m(x)$ of α over $\mathbb{Q}$.
   (b) Find, with proof, the Galois group of the splitting field of $m(x)$ over $\mathbb{Q}$.

127. (a) Find the minimal polynomial $f(x)$ of $\alpha = \sqrt{8 + \sqrt{15}}$ over $\mathbb{Q}$ and prove that your answer is correct.
   (b) Find the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$.

128. Let $u = \sqrt{2 + \sqrt{2}}$, $v = \sqrt{2 - \sqrt{2}}$, and $E = \mathbb{Q}(u)$, where $\mathbb{Q}$ is the field of rational numbers.
   (a) Find the minimal polynomial $f(x)$ of u over $\mathbb{Q}$.
   (b) Show $v \in E$. Hence conclude that E is a splitting field of $f(x)$ over $\mathbb{Q}$.
   (c) Determine the Galois group of E over $\mathbb{Q}$.

129. Let F be a field of characteristic 0 and let $a \in F$. Prove that if $f(x) = x^4 + ax^2 + 1$ is irreducible over F and K is a splitting field for $f(x)$ over F, then $\mathrm{Gal}(K/F)$ has order 4 and is not cyclic. [Hint: If α is a root of $f(x)$, then so are $-\alpha$ and $1/\alpha$.]

130. Let $\alpha = \sqrt{5 + 2\sqrt{5}}$. Show that $\mathbb{Q}(\alpha)$ is a cyclic Galois extension of $\mathbb{Q}$ of degree 4. Find all fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\alpha)$.
[Hint: Show that $f(x) = x^4 - 10x^2 + 5$ is the minimal polynomial of α over $\mathbb{Q}$ and that the roots of f are $\pm\alpha$, $\pm\frac{\sqrt{5}}{\alpha}$.]

131. Let p be a prime such that there is a positive integer d with $p = 1 + d^2$ and let $\alpha = \sqrt{p + d\sqrt{p}}$. Show that $\mathbb{Q}(\alpha)$ is a cyclic Galois extension of $\mathbb{Q}$ of degree 4. Find all fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\alpha)$.
[Hint: Show that $f(x) = x^4 - 2px^2 + p$ is the minimal polynomial of α over $\mathbb{Q}$ and that the roots of f are $\pm\alpha$, $\pm\frac{\sqrt{p}}{\alpha}$.]

132. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with exactly two real roots. Show that the Galois group of f over $\mathbb{Q}$ has order either 8 or 24.

133. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with exactly 2 real roots. Show that the Galois group of f over $\mathbb{Q}$ is either S_4 or the dihedral group of order 8.

134. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. Assume $f(x)$ has exactly 3 distinct real roots and one complex conjugate pair of roots. Prove that if K is the splitting field of $f(x)$ over $\mathbb{Q}$, then $\mathrm{Gal}(K/\mathbb{Q})$ is S_5.

135. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $n > 2$ that has $n-2$ real roots and exactly one pair of complex conjugate roots. Prove that the Galois group of $f(x)$ over $\mathbb{Q}$ is not a simple group.

136. Let $f(x) = x^4 + ax^3 + bx^2 + ax + 1 \in \mathbb{Q}[x]$ and let F be a splitting field over $\mathbb{Q}$. Show that if α is a root of f then $1/\alpha$ is also a root, and $|\mathrm{Gal}(F/\mathbb{Q})| \leqslant 8$.

137. Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial of degree 4 with distinct roots α_1, α_2, α_3, and α_4. Let K be a splitting field for f over F and assume $\mathrm{Gal}(K/F) \cong S_4$. Find $\mathrm{Gal}(K/F(\beta))$, where $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$.

138. Let E be a finite dimensional Galois extension of a field F and let $G = \mathrm{Gal}(E/F)$. Suppose that G is an abelian group. Prove that if K is any field between E and F, then K is a Galois extension of F.

139. Let K be a finite Galois extension of F and let E be an intermediate field which is normal over F. For an element σ of $\mathrm{Gal}(K/F)$ and $g(x) = e_0 + e_1x + \cdots + e_mx^m$ in $E[x]$, denote $\sigma g(x) = \sigma(e_0) + \sigma(e_1)x + \cdots + \sigma(e_m)x^m$. For a fixed element α of K, let $f(x) \in E[x]$ be the minimal polynomial of α over E. Show the following.
    (a) $\sigma(\alpha)$ is a root of $\sigma f(x)$.
    (b) If $f_1(x)$, $f_2(x)$, $\ldots$, $f_n(x)$ are all the distinct elements of $\{\sigma f(x) \mid \sigma \in \mathrm{Gal}(K/F)\}$, then $h(x) = f_1(x)f_2(x)\cdots f_n(x)$ is in $F[x]$.
    (c) $h(x)$ is the minimal polynomial of α over F.

140. Let K be a Galois extension of k and let $k \subseteq F \subseteq K$ and $k \subseteq L \subseteq K$.
    (a) Show that $\mathrm{Gal}(K/LF) = \mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/F)$.
    (b) Show that $\mathrm{Gal}(K/L \cap F) = \langle \mathrm{Gal}(K/L), \mathrm{Gal}(K/F) \rangle$.

141. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and let α be an element of $\overline{\mathbb{Q}}$ not in $\mathbb{Q}$.
    (a) Show that there is a field $M \subseteq \overline{\mathbb{Q}}$ that is maximal with respect to the property that $\alpha \notin M$.
    (b) Show that any finite Galois extension of M has cyclic Galois group.
    (c) Show that any finite extension of M is a Galois extension.

142. Let E be a finite dimensional Galois extension of a field F and let $G = \mathrm{Gal}(E/F)$. For $e \in E$ let $G(e) = \{\sigma(e) \mid \sigma \in G\}$. Let e_1, e_2, $\ldots$, e_n be all the distinct elements of $G(e)$.
    (a) Prove that $f(x) = (x - e_1)(x - e_2)\cdots(x - e_n)$ is in $F[x]$.
    (b) Prove that $f(x)$ is irreducible in $F[x]$.

143. Let E be a finite dimensional Galois extension of F of characteristic different from 2. Suppose $\mathrm{Gal}(E/F)$ is a non-cyclic group of order 4. Show that $E = F(\alpha, \beta)$ for some $\alpha, \beta \in E$ with $\alpha^2 \in F$ and $\beta^2 \in F$.

144. Let $E = \mathbb{Q}[\alpha, \beta]$, where $\alpha^2, \beta^2 \in \mathbb{Q}$ and $|E : \mathbb{Q}| = 4$. Prove that if $\gamma \in E - \mathbb{Q}$ and $\gamma^2 \in \mathbb{Q}$, then γ is a rational multiple of one of α, β, or $\alpha\beta$.

Cyclotomic Extensions

145. Find the 6th, 8th, and 12th cyclotomic polynomials over $\mathbb{Q}$.

146. Let α be a complex primitive 43rd root of 1. Prove that there is an extension field F of the rational numbers such that $[F(\alpha) : F] = 14$.

147. Let m be an odd integer and let η_m, η_{2m} be a complex primitive m-th, $2m$-th root of unity, respectively. Show that $\mathbb{Q}(\eta_m) = \mathbb{Q}(\eta_{2m})$.

148. Let $(m, n) = 1$, and if i is any positive integer let η_i denote a complex primitive i-th root of unity. Show that $\mathbb{Q}(\eta_{mn}) = \mathbb{Q}(\eta_m)\mathbb{Q}(\eta_n)$ and $\mathbb{Q}(\eta_m) \cap \mathbb{Q}(\eta_n) = \mathbb{Q}$.

149. Let ϵ be the complex number $\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, where n is a positive integer. Show
   (a) ϵ is algebraic over the field $\mathbb{Q}$ of rational numbers,
   (b) if $\Phi_n(x)$ is the minimal polynomial of ϵ over $\mathbb{Q}$, then $\mathbb{Q}(\epsilon)$ is a splitting field of $\Phi_n(x)$ over $\mathbb{Q}$,
   (c) the Galois group of $\mathbb{Q}(\epsilon)$ over $\mathbb{Q}$ is isomorphic to the group of units of $\mathbb{Z}_n$.

150. Let ϵ be a primitive n-th root of unity over $\mathbb{Q}$, where $n > 2$, and let $\alpha = \epsilon + \epsilon^{-1}$. Prove that α is algebraic over $\mathbb{Q}$ of degree $\varphi(n)/2$.

Finite Fields

151. Prove that the multiplicative group of a finite field must be cyclic.

152. Prove that any finite extension of a finite field must be a simple extension.

153. Show that any two finite fields of the same order are isomorphic.

154. Let F be an extension of $\mathbb{Z}_p$ of degree n. Show that F is a Galois extension and $\text{Gal}(F/\mathbb{Z}_p)$ is cyclic of order n.

155. Show that every finite extension of a finite field is a Galois extension.

156. Show that every algebraic extension of a finite field is separable.

157. Show that every finite field is perfect. (Recall that a field F of characteristic p is called *perfect* if the map $\alpha \mapsto \alpha^p$ is a surjection on F.)

158. Let $f(x) \in \mathbb{Z}_p[x]$ be irreducible of degree m. Show that $f(x) \mid (x^{p^n} - x)$ if and only if $m \mid n$.

159. Let p be a prime. Show that the field of p^a elements is a subfield of the field of p^b elements if and only if $a \mid b$.

160. Let p be a prime and $\mathbb{F}_p$ the field of p elements. Show that for every positive integer n, there is an irreducible polynomial of degree n over $\mathbb{F}_p$.

161. Let F be a finite field. Prove that the polynomial ring $F[x]$ contains irreducible polynomials of arbitrarily large degree.

162. Let F be a finite field. Show that the product of all the non-zero elements of F is -1.

163. Let $\mathbb{F}_q$ be the field of q elements and let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$. Show that if α is a root of $f(x)$, then α^q is also a root of $f(x)$.

164. Let E and F be subfields of a finite field K. Show that if E is isomorphic to F then $E = F$.

165. Let E and F be finite subfields of a field K. Show that if E and F have the same number of elements, then $E = F$.

166. Let $\mathbb{F}_p$ be the field of p elements and let K be an extension of $\mathbb{F}_p$ of degree n. Show that the set of subfields of K is linearly ordered (i.e., for every pair of subfields L_1, L_2, either $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$) if and only if n is a prime power.

167. Let $f(x) = x^2 - 2 \in \mathbb{F}_p[x]$, where $p > 2$ is prime and $\mathbb{F}_p$ is the field of p elements. Give an example of a prime p for which f is irreducible and another example where f reduces.

168. Let α be a root of x^2+1 in an extension of $\mathbb{Z}_3$, $K = \mathbb{Z}_3(\alpha)$, and let $f(x) = x^4+x^3+x+2 \in \mathbb{Z}_3[x]$.

    (a) Show that f splits over K.

    (b) Find a generator α of the multiplicative group of K and express the roots of f in terms of α.

169. Let α be a root of $x^2 + 1$ in an extension of $\mathbb{Z}_3$, $K = \mathbb{Z}_3(\alpha)$, and let $f(x) = x^4 + 1 \in \mathbb{Z}_3[x]$.

    (a) Show that f splits over K.

    (b) Find a generator β of the multiplicative group K^* of K.

    (c) Express the roots of f in terms of β.

170. Let $K = \mathbb{Z}_3(\sqrt{2})$ and let $f(x) = x^4 + x^3 + x + 2 \in \mathbb{Z}_3[x]$.

    (a) Show that f splits over K.

    (b) Find a generator α of the multiplicative group K^* of K.

    (c) Express the roots of f in terms of α.

171. Let $\mathbb{F} = \mathbb{F}_{81}$ be the field of 81 elements.

    (a) Find all subfields of $\mathbb{F}$.

    (b) Determine the number of primitive elements for $\mathbb{F}$ over the field $\mathbb{F}_3$ of 3 elements (i.e., elements α of $\mathbb{F}$ such that $\mathbb{F} = \mathbb{F}_3(\alpha)$).

    (c) Find the number of generators for the multiplicative group $\mathbb{F}^*$ of $\mathbb{F}$ (i.e., elements β of $\mathbb{F}$ such that $\langle\beta\rangle = \mathbb{F}^*$).

172. Let $f(x) = x^4 + x^3 + 4x - 1 \in \mathbb{Z}_5[x]$.
    Find the Galois group of the splitting field of f over $\mathbb{Z}_5$.

Cyclic Extensions

173. Let K be a field of characteristic $p \neq 0$ and let $K_p = \{u^p - u : u \in K\}$. Show that K has a cyclic extension of degree p if and only if $K \neq K_p$.

174. Let p be a prime and F the field of fractions of $\mathbb{Z}_p[x]$. If E is the splitting field of $y^p - y - x$ over F, determine the Galois group of E over F.

175. Let n be a positive integer and let F be a field of characteristic 0 containing a primitive n-th root of unity. Let a be an element of F such that a is not an m-th power of an element of F for any $1 \neq m \mid n$. Show that if α is any root of $x^n - a$, then $F(\alpha)$ is a cyclic extension of F of degree n.

176. Let F be a field that contains a primitive nth root of unity and let $K = F(t)$, the field of fractions of the polynomial ring $F[t]$. Let $L = F(t^n) \subseteq K$. Prove that K is a Galois extension of L and that the Galois group is cyclic of order n.

177. Let F be a field of characteristic p. Fix $c \in F$ and let $f(x) = x^p - x + c \in F[x]$. Prove that if α is a root of $f(x)$ in some extension field, then so is $\alpha + 1$. Use this to prove that if K is the splitting field of $f(x)$ over F, then either $K = F$ and $f(x)$ splits completely over F, or $[K : F] = p$ and $f(x)$ is irreducible over F. (Use Galois groups.)

Radical Extensions and Solvability By Radicals

178. An extension K of F is called a *radical extension* if there is a tower of fields

$$F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \cdots \subseteq F(u_1, \ldots, u_n) = K$$

such that for $i = 1, \ldots, n$, $u_i^{m_i} \in F(u_1, \ldots, u_{i-1})$ for some positive integer m_i.
   (a) Give an example of a radical extension that is not separable.
   (b) Give an example of a radical extension that is not normal.

179. Let F be a radical extension of K. Show that there is a radical extension N of K with $N \supseteq F \supseteq K$ and N normal over K.

180. Let F be a finite field of characteristic p. Show that if $f \in F[x]$ is an irreducible polynomial and the degree of f is less than p, then $f(x) = 0$ is solvable by radicals.

181. Let $x_1, \ldots, x_n$ be indeterminates over a field F and let $s_1, \ldots, s_n$ be the elementary symmetric functions of the x_i. Show that $[F(x_1, \ldots, x_n) : F(s_1, \ldots, s_n)] = n!$.

Transcendental Extensions

182. Let x be an indeterminate over the field F. Show that an element of $F(x)$ is algebraic over F if and only if it is an element of F.

183. Let $F \subseteq E$ be fields with $E = F(\alpha)$, where α is transcendental over F. Show that if $\beta \in E - F$, then $[E : F(\beta)]$ is finite.

184. Let F be a field, $F[x]$ the ring of polynomials over F in the indeterminate x, and $E = F(x)$ the field of fractions of $F[x]$.

(a) Show that if σ is an automorphism of E such that $\sigma(u) = u$ for all $u \in F$, then $\sigma(x) = \dfrac{ax+b}{cx+d}$ for some $a, b, c, d \in F$ with $ad - bc \neq 0$.

(b) Determine the group $\mathrm{Aut}_F(E)$ of F-automorphisms of E.

185. Let K be an extension field of F and let $\alpha \in K$ be transcendental over F. Show that if $\beta \in K$ is algebraic over $F(\alpha)$, then there is a nonzero polynomial $p(x, y) \in F[x, y]$ such that $P(\alpha, \beta) = 0$.