

ALGEBRA QUALIFYING EXAM PROBLEMS  
FIELD THEORY

Kent State University  
Department of Mathematical Sciences

Compiled and Maintained  
by  
Donald L. White

Version: May 27, 2009



## CONTENTS

### FIELD THEORY

|  |    |
|--|----|
| General Field Theory .....                           | 1  |
| Algebraic Extensions .....                           | 3  |
| Normality and Splitting Fields .....                 | 4  |
| Separability .....                                   | 5  |
| Galois Theory .....                                  | 7  |
| Cyclotomic Extensions .....                          | 10 |
| Finite Fields .....                                  | 10 |
| Cyclic Extensions .....                              | 12 |
| Radical Extensions and Solvability by Radicals ..... | 12 |
| Transcendental Extensions .....                      | 12 |



# 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. 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.]
7. Suppose  $F \subset E \subset K$  is any tower of fields and  $[K : F]$  is finite. Show that  $[K : F] = [K : E][E : F]$ .
8. 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  $K$ .
9. **[CORRECTED]**  
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  $i$ .
10. 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.
11. 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  $[F(a, b) : F] = mn$ .

12. Let  $F$ ,  $L$ , and  $K$  be subfields of a field  $M$ , with  $F \subseteq K$  and  $F \subseteq L$ . Let  $[K : F] = k$  and  $[L : F] = \ell$ .
- Show that  $[KL : F] \leq k\ell$ .
  - Show that if  $(k, \ell) = 1$  then  $[KL : F] = k\ell$ .
  - Give an example where  $[KL : F] < k\ell$ .
13. 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  $|G| \leq [K : F]$ .
14. 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  $G$ .
15. 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  $[E : F] = |G|$ .
16. Let  $F$  be a field with the property
- (\*) If  $a, b \in F$  and  $a^2 + b^2 = 0$ , then  $a = 0$  and  $b = 0$ .
- Show that  $x^2 + 1$  is irreducible in  $F[x]$ .
  - Which of the fields  $\mathbb{Z}_3, \mathbb{Z}_5$  satisfy (\*)?
17. 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  $F$ .
- $F = \mathbb{Q}, f(x) = x^4 - 5$ .
  - $F = \mathbb{Q}(\sqrt{-3}), f(x) = x^3 - 3$ .
  - $F = \mathbb{Q}, f(x) = x^3 - x^2 - 5x + 5$ .
18. Let  $\mathbb{Q}$  be the field of rational numbers. Show that the group of automorphisms of  $\mathbb{Q}$  is trivial.
19. Let  $\mathbb{R}$  be the field of real numbers. Show that the group of automorphisms of  $\mathbb{R}$  is trivial.
20. 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.
21. Let  $F$  be a field and  $p$  a prime. Let  $G = \{c \in F \mid c^{p^n} = 1 \text{ for some positive integer } n\}$ .
- Show that  $G$  is a subgroup of the multiplicative group of  $F$ .
  - Prove that either  $G$  is a cyclic group or  $G$  is isomorphic to  $\mathbb{Z}(p^\infty)$ , the Prüfer group for the prime  $p$ .
22. 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.
- If  $e \in E$  then  $G_e = \{\sigma \in G \mid \sigma(e) = e\}$  is a subgroup of  $G$ .
  - $[G : G_e] \leq [F(e) : F]$ .
  - If  $F$  is the fixed field of  $G$  and  $e_1, e_2, \dots, e_n$  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  $F$ .
23. 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.

24. 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.
25. 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.
26. 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.
27. 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

28. 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  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is a basis for  $F(\alpha)$  over  $F$ .
29. Show that if  $K$  is finite dimensional field extension of  $F$ , then  $K$  is algebraic over  $F$ .
30. Let  $F$  be a field, let  $E = F(a)$  be a simple extension field of  $F$ , and let  $b \in E - F$ . Prove that  $a$  is algebraic over  $F(b)$ .
31. Let  $K$  be an extension field of the field  $F$  such that  $[K : F]$  is odd. Show that if  $u \in K$  then  $F(u) = F(u^2)$ .
32. 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  $F(u) = F(u^3)$ .
33. Let  $F$  be a field,  $f(x)$  an irreducible polynomial in  $F[x]$ , and  $\alpha$  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  $F(\alpha) = F(\alpha^2)$ .
34. 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  $\alpha$  is a root of  $f(x)$  in some field extension of  $F$ , then  $g(x)$  is irreducible in  $F(\alpha)[x]$ .
35. Let  $K$  be an extension field of  $F$  and let  $\alpha$  be an element of  $K$ . Show that if  $F(\alpha) = F(\alpha^2)$ , then  $\alpha$  is algebraic over  $F$ .
36. Let  $K$  be an extension field of  $F$  and let  $\alpha$  be an element of  $K$ . Show that the following are equivalent:
  - (i)  $\alpha$  is algebraic over  $F$ ,
  - (ii)  $F(\alpha)$  is a finite dimensional extension of  $F$ ,
  - (iii)  $\alpha$  is contained in a finite dimensional extension of  $F$ .
37. Let  $\alpha$  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.

38. Let  $F \subset E \subset K$  be a tower of fields such that  $K = F(\alpha)$  with  $\alpha$  algebraic over  $F$ . Prove that if  $f(x) \in F[x]$  is the minimal polynomial of  $\alpha$  over  $F$  and  $F \neq E$ , then  $f(x)$  is not irreducible in  $E[x]$ .
39. Let  $E$  be an extension field of  $F$  and  $A = \{e \in E \mid e \text{ is algebraic over } F\}$ .
- Show that  $A$  is a subfield of  $E$  containing  $F$ .
  - Show that if  $\sigma : E \rightarrow E$  is a one-to-one  $F$ -homomorphism, then  $\sigma(A) = A$ .
40. Show that if  $p_1, \dots, p_n, p_{n+1}$  are distinct prime numbers, then  $\sqrt{p_{n+1}}$  is not an element of the field  $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ .
41. Let  $\alpha_1, \alpha_2$ , and  $\alpha_3$  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  $K$ .
42. Let  $F \subseteq L \subseteq K$  with  $[L : F]$  finite, and let  $\alpha$  be an element of  $K$ . Show that  $\alpha$  is algebraic over  $L$  if and only if  $\alpha$  is algebraic over  $F$ .
43. Show that if  $K$  is algebraic over  $F$  and  $\sigma : K \rightarrow K$  is an  $F$ -monomorphism, then  $\sigma$  is onto.
44. 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  $F$ .
45. Let  $K$  be a simple algebraic extension of a field  $F$ . Show that there are only finitely many intermediate fields between  $F$  and  $K$ .
46. 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  $F$ .
47. Let  $\alpha$  be algebraic over the field  $F$  with minimal polynomial  $f(x) \in F[x]$  and let  $K = F[\alpha]$ . Show that if  $\sigma : F \rightarrow L$  is a field monomorphism and  $\beta \in L$  is a root of  $f^\sigma(x) \in L[x]$ , then  $\sigma$  has a unique extension  $\hat{\sigma} : K \rightarrow L$  satisfying  $\hat{\sigma}(\alpha) = \beta$ .
48. Suppose  $E_1$  and  $E_2$  are algebraic closures of a field  $F$ . Show that there is an  $F$ -isomorphism  $\sigma : E_1 \rightarrow E_2$ .
49. (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

50. Let  $K$  be an extension field of  $F$ . Show that the following are equivalent.
- Each irreducible polynomial in  $F[x]$  with one root in  $K$  has all its roots in  $K$ .
  - $K$  is obtained from  $F$  by adjoining all roots of a set of polynomials in  $F[x]$ .
  - Every  $F$ -isomorphism of  $K$  in a fixed algebraic closure is an  $F$ -automorphism.
51. Let  $K$  be the splitting field of  $x^2 + 2$  over  $\mathbb{Q}$ . Prove or disprove that  $i = \sqrt{-1}$  is an element of  $K$ .

52. Let  $K$  be the splitting field of  $x^3 - 5$  over  $\mathbb{Q}$ . Prove or disprove that  $i = \sqrt{-1}$  is an element of  $K$ .
53. Let  $\Omega$  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  $\varphi : K \rightarrow K' \subseteq \Omega$  is an  $F$ -automorphism.
54. 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

55. 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  $L$ .
56. 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  $\gcd(f(x), f'(x)) = 1$ .
57. Show that if  $K$  is a finite dimensional separable extension of  $F$ , then  $K = F(u)$  for some  $u$  in  $K$ .
58. Let  $F$  be a field and let  $f(x) = x^n - x \in F[x]$ . Show that if  $\text{char } F = 0$  or if  $\text{char } F = p$  and  $p \nmid n - 1$ , then  $f$  has no multiple root in any extension of  $F$ .
59. Show that if  $F$  is a field of characteristic 0 then every algebraic extension of  $F$  is separable.
60. Show that if  $F$  is a finite field then every algebraic extension of  $F$  is separable.
61. Let  $F$  be a field of characteristic  $p$  and let  $x$  be an indeterminate over  $F$ .
- Show that  $F(x^p)$  is a proper subfield of  $F(x)$ .
  - Show that  $F(x)$  is a splitting field for some polynomial over  $F(x^p)$ .
  - Show that the only automorphism of  $F(x)$  fixing  $F(x^p)$  is the identity automorphism.
62. Let  $F$  be a field and  $f(x) \in F[x]$  an irreducible polynomial. Prove that there is a prime  $p$ , an integer  $a \geq 0$  and a separable polynomial  $g(x) \in F[x]$  such that  $f(x) = g(x^{p^a})$ .
63. 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  $n$ .
64. 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
- $f(x)$  is irreducible over  $F$  and
  - if  $t > 1$  then  $K$  is a separable extension of  $F$ .
65. Let  $x$  and  $y$  be independent indeterminates over  $\mathbb{Z}_p$ ,  $K = \mathbb{Z}_p(x, y)$ , and  $F = \mathbb{Z}_p(x^p, y^p)$ .
- Show that  $[K : F] = p^2$
  - Show that  $K$  is not a simple extension of  $F$ .

66. 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  $F$ .

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

68. Show that every finite field is perfect.

69. 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.

70. 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  $F$ .

71. 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  $|G|$ .

72. 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  $|\text{Aut}_F(E)| = 1$ .
  - (c) What conclusion can you draw from (a) and (b)?

73. 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  $u^r \in F$ .

74. 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  $(x - u)^m$ .

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

76. 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  $u \in F$ .

77. 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

78. State the Fundamental Theorem of Galois Theory.
79. 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  $H_1/H_2$ .
80. Let  $K$  be a finite Galois extension of  $F$  with Galois group  $G = \text{Gal}(K/F)$ . Let  $E$  be an intermediate field that is normal over  $F$ . Prove that  $\text{Gal}(K/E) \trianglelefteq G$  and  $G/\text{Gal}(K/E) \cong \text{Gal}(E/F)$ .
81. 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  $\mathcal{F}(G) = F$ .
82. Let  $K$  be a finite dimensional extension field of  $L$  and let  $\sigma : L \rightarrow F$  be an embedding of  $L$  into a field  $F$ . Prove that there are at most  $[K : L]$  extensions of  $\sigma$  to embeddings of  $K$  into  $F$ .
83. 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  $F'$ .
84. 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.
85. Let  $E$  be a splitting field over  $F$  of a separable polynomial  $f(x)$  in  $F[x]$  and  $G = \text{Gal}(E/F)$ . Show that  $\{e \in E \mid \sigma(e) = e \text{ for all } \sigma \in G\} = F$ .
86. Let  $K$  be a Galois extension of  $F$  with  $|\text{Gal}(K/F)| = 12$ . Prove that there exists a subfield  $E$  of  $K$  containing  $F$  with  $[E : F] = 3$ . Does a subextension necessarily exist satisfying  $[E : F] = 2$ ? Explain.
87. Suppose  $K = F(\alpha)$  is a proper Galois extension of  $F$  and assume there exists an element  $\sigma$  of  $\text{Gal}(K/F)$  satisfying  $\sigma(\alpha) = \alpha^{-1}$ . Show that  $[K : F]$  is even and that  $[F(\alpha + \alpha^{-1}) : F] = \frac{1}{2}[K : F]$ .
88. Let  $K$  be a finite Galois extension of  $F$  of characteristic 0. Show that if  $\text{Gal}(K/F)$  is a non-trivial 2-group, then there is a quadratic extension of  $F$  contained in  $K$ .
89. 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  $G \cong \text{Gal}(K/F)$ .
90. (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.
91. 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  $\text{Gal}(K/F)$  is abelian.

92. Let  $\eta_7$  be a complex primitive 7th root of unity and let  $K = \mathbb{Q}(\eta_7)$ . Find  $\text{Gal}(K/\mathbb{Q})$  and express each intermediate field  $F$  between  $\mathbb{Q}$  and  $K$  as  $F = \mathbb{Q}(\beta)$  for some  $\beta \in K$ .
93. Let  $\eta$  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  $F = \mathbb{Q}(\sqrt{q})$ .
94. Let  $\mathbb{Q}$  be the field of rational numbers and  $\eta$  a complex primitive 8th root of unity. Determine  $\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$  and all the intermediate fields between  $\mathbb{Q}$  and  $\mathbb{Q}(\eta)$ .
95. (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  $x^4 - 4$ ?
96. **[NEW]**  
 Determine the Galois group of  $x^4 - 3$  over the field  $\mathbb{Q}$  of rational numbers.
97. Determine the Galois group of  $x^4 + 2$  over the field  $\mathbb{Q}$  of rational numbers.
98. Determine the Galois group of  $x^3 + 3x^2 - 1$  over  $\mathbb{Q}$ .
99. 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  $\mathbb{Q}$ ?
100. Let  $K$  be a splitting field for  $x^5 - 2$  over  $\mathbb{Q}$ .  
 (a) Determine  $[K : \mathbb{Q}]$ .  
 (b) Show that  $\text{Gal}(K/\mathbb{Q})$  is non-abelian.  
 (c) Find all normal intermediate extensions  $F$  and express as  $F = \mathbb{Q}(\alpha)$  for appropriate  $\alpha$ .
101. 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  $|\text{Gal}(E/\mathbb{Q})|$ .  
 (b) Let  $\sigma \in \text{Gal}(E/\mathbb{Q})$  be such that  $\sigma(\alpha) = \bar{\alpha}$  for all  $\alpha \in E$  (where  $\bar{\alpha}$  is the complex conjugate of  $\alpha$ ). Find  $\text{Inv}(\langle \sigma \rangle) = \{\alpha \in E \mid \sigma(\alpha) = \alpha\}$ .  
 (c) Is  $\langle \sigma \rangle$  a normal subgroup of  $\text{Gal}(E/\mathbb{Q})$ ?
102. 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.
103. 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  $\text{Gal}(K/F)$  and express each intermediate field between  $F$  and  $K$  as  $F(b)$  for appropriate  $b$  in  $K$ .
104. 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  $\mathbb{Q}$ .
105. Let  $f(x) \in \mathbb{Q}[x]$  be an irreducible polynomial of degree  $n$  with roots  $\alpha_1, \dots, \alpha_n$ . Show that  $\sum_{i=1}^n \frac{1}{\alpha_i}$  is a rational number.

106. Let  $\alpha = \sqrt{2} + \sqrt{3}$  and let  $E = \mathbb{Q}(\alpha)$ .
- Find the minimal polynomial  $m(x)$  of  $\alpha$  over  $\mathbb{Q}$  and  $|E : \mathbb{Q}|$ .
  - 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.
107. 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.
- Find the minimal polynomial  $f(x)$  of  $u$  over  $\mathbb{Q}$ .
  - Show  $v \in E$ . Hence conclude that  $E$  is a splitting field of  $f(x)$  over  $\mathbb{Q}$ .
  - Determine the Galois group of  $E$  over  $\mathbb{Q}$ .
108. 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  $\alpha$  over  $\mathbb{Q}$  and that the roots of  $f$  are  $\pm\alpha, \pm\frac{\sqrt{5}}{\alpha}$ .]
109. 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  $\alpha$  over  $\mathbb{Q}$  and that the roots of  $f$  are  $\pm\alpha, \pm\frac{\sqrt{p}}{\alpha}$ .]
110. 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  $f$  is either  $S_4$  or the dihedral group of order 8.
111. 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  $\alpha$  is a root of  $f$  then  $1/\alpha$  is also a root, and  $|\text{Gal}(F/\mathbb{Q})| \leq 8$ .
112. Let  $F$  be a field and let  $f(x) \in F[x]$  be an irreducible polynomial of degree 4 with distinct roots  $\alpha_1, \alpha_2, \alpha_3$ , and  $\alpha_4$ . Let  $K$  be a splitting field for  $f$  over  $F$  and assume  $\text{Gal}(K/F) \cong S_4$ . Find  $\text{Gal}(K/F(\beta))$ , where  $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$ .
113. Let  $E$  be a finite dimensional Galois extension of a field  $F$  and let  $G = \text{Gal}(E/F)$ . 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  $F$ .
114. Let  $K$  be a finite Galois extension of  $F$  and let  $E$  be an intermediate field which is normal over  $F$ . For an element  $\sigma$  of  $\text{Gal}(K/F)$  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  $\alpha$  of  $K$ , let  $f(x) \in E[x]$  be the minimal polynomial of  $\alpha$  over  $E$ . Show the following.
- $\sigma(\alpha)$  is a root of  $\sigma f(x)$ .
  - If  $f_1(x), f_2(x), \dots, f_n(x)$  are all the distinct elements of  $\{\sigma f(x) \mid \sigma \in \text{Gal}(K/F)\}$ , then  $h(x) = f_1(x)f_2(x)\cdots f_n(x)$  is in  $F[x]$ .
  - $h(x)$  is the minimal polynomial of  $\alpha$  over  $F$ .
115. Let  $K$  be a Galois extension of  $k$  and let  $k \subseteq F \subseteq K$  and  $k \subseteq L \subseteq K$ .
- Show that  $\text{Gal}(K/LF) = \text{Gal}(K/L) \cap \text{Gal}(K/F)$ .
  - Show that  $\text{Gal}(K/L \cap F) = \langle \text{Gal}(K/L), \text{Gal}(K/F) \rangle$ .

116. Let  $\overline{\mathbb{Q}}$  be the algebraic closure of  $\mathbb{Q}$  and let  $\alpha$  be an element of  $\overline{\mathbb{Q}}$  not in  $\mathbb{Q}$ .
- Show that there is a field  $M \subseteq \overline{\mathbb{Q}}$  that is maximal with respect to the property that  $\alpha \notin M$ .
  - Show that any finite Galois extension of  $M$  has cyclic Galois group.
  - Show that any finite extension of  $M$  is a Galois extension.
117. Let  $E$  be a finite dimensional Galois extension of a field  $F$  and let  $G = \text{Gal}(E/F)$ . For  $e \in E$  let  $G(e) = \{\sigma(e) \mid \sigma \in G\}$ . Let  $e_1, e_2, \dots, e_n$  be all the distinct elements of  $G(e)$ .
- Prove that  $f(x) = (x - e_1)(x - e_2) \cdots (x - e_n)$  is in  $F[x]$ .
  - Prove that  $f(x)$  is irreducible in  $F[x]$ .
118. Let  $E$  be a finite dimensional Galois extension of  $F$  of characteristic different from 2. Suppose  $\text{Gal}(E/F)$  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  $\beta^2 \in F$ .

### Cyclotomic Extensions

119. Find the 6th, 8th, and 12th cyclotomic polynomials over  $\mathbb{Q}$ .
120. Let  $\alpha$  be a complex primitive 43rd root of 1. Prove that there is an extension field  $F$  of the rational numbers such that  $[F(\alpha) : F] = 14$ .
121. Let  $m$  be an odd integer and let  $\eta_m, \eta_{2m}$  be a complex primitive  $m$ -th,  $2m$ -th root of unity, respectively. Show that  $\mathbb{Q}(\eta_m) = \mathbb{Q}(\eta_{2m})$ .
122. Let  $(m, n) = 1$ , and if  $i$  is any positive integer let  $\eta_i$  denote a complex primitive  $i$ -th root of unity. Show that  $\mathbb{Q}(\eta_{mn}) = \mathbb{Q}(\eta_m)\mathbb{Q}(\eta_n)$  and  $\mathbb{Q}(\eta_m) \cap \mathbb{Q}(\eta_n) = \mathbb{Q}$ .
123. Let  $\epsilon$  be the complex number  $\cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$ , where  $n$  is a positive integer. Show
- $\epsilon$  is algebraic over the field  $\mathbb{Q}$  of rational numbers,
  - if  $\Phi_n(x)$  is the minimal polynomial of  $\epsilon$  over  $\mathbb{Q}$ , then  $\mathbb{Q}(\epsilon)$  is a splitting field of  $\Phi_n(x)$  over  $\mathbb{Q}$ ,
  - the Galois group of  $\mathbb{Q}(\epsilon)$  over  $\mathbb{Q}$  is isomorphic to the group of units of  $\mathbb{Z}_n$ .
124. Let  $\epsilon$  be a primitive  $n$ -th root of unity over  $\mathbb{Q}$ , where  $n > 2$ , and let  $\alpha = \epsilon + \epsilon^{-1}$ . Prove that  $\alpha$  is algebraic over  $\mathbb{Q}$  of degree  $\varphi(n)/2$ .

### Finite Fields

125. Prove that the multiplicative group of a finite field must be cyclic.
126. Prove that any finite extension of a finite field must be a simple extension.
127. Show that any two finite fields of the same order are isomorphic.
128. 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  $n$ .
129. Show that every finite extension of a finite field is a Galois extension.

130. Show that every algebraic extension of a finite field is separable.
131. 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  $F$ .)
132. Let  $f(x) \in \mathbb{Z}_p[x]$  be irreducible of degree  $m$ . Show that  $f|(x^{p^n} - x)$  if and only if  $m|n$ .
133. 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  $a|b$ .
134. 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  $\mathbb{F}_p$ .
135. Let  $F$  be a finite field. Show that the product of all the non-zero elements of  $F$  is  $-1$ .
136. 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  $\alpha$  is a root of  $f(x)$ , then  $\alpha^q$  is also a root of  $f(x)$ .
137. Let  $E$  and  $F$  be subfields of a finite field  $K$ . Show that if  $E$  is isomorphic to  $F$  then  $E = F$ .
138. Let  $E$  and  $F$  be finite subfields of a field  $K$ . Show that if  $E$  and  $F$  have the same number of elements, then  $E = F$ .
139. 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.
140. Let  $\alpha$  be a root of  $x^2 + 1$  in an extension of  $\mathbb{Z}_3$ ,  $K = \mathbb{Z}_3(\alpha)$ , and let  $f(x) = x^4 + 1 \in \mathbb{Z}_3[x]$ .
- Show that  $f$  splits over  $K$ .
  - Find a generator  $\beta$  of the multiplicative group  $K^*$  of  $K$ .
  - Express the roots of  $f$  in terms of  $\beta$ .
141. Let  $K = \mathbb{Z}_3(\sqrt{2})$  and let  $f(x) = x^4 + x^3 + x + 2 \in \mathbb{Z}_3[x]$ .
- Show that  $f$  splits over  $K$ .
  - Find a generator  $\alpha$  of the multiplicative group  $K^*$  of  $K$ .
  - Express the roots of  $f$  in terms of  $\alpha$ .
142. Let  $\mathbb{F} = \mathbb{F}_{81}$  be the field of 81 elements.
- Find all subfields of  $\mathbb{F}$ .
  - Determine the number of primitive elements for  $\mathbb{F}$  over the field  $\mathbb{F}_3$  of 3 elements (i.e., elements  $\alpha$  of  $\mathbb{F}$  such that  $\mathbb{F} = \mathbb{F}_3(\alpha)$ ).
  - Find the number of generators for the multiplicative group  $\mathbb{F}^*$  of  $\mathbb{F}$  (i.e., elements  $\beta$  of  $\mathbb{F}$  such that  $\langle \beta \rangle = \mathbb{F}^*$ ).
143. 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

144. 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  $K \neq K_p$ .
145. 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  $F$ .
146. 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  $1 \neq m|n$ . Show that if  $\alpha$  is any root of  $x^n - a$ , then  $F(\alpha)$  is a cyclic extension of  $F$  of degree  $n$ .
147. Let  $F$  be a field that contains a primitive  $n$ th 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  $n$ .
148. 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  $\alpha$  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

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

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

such that for  $i = 1, \dots, n$ ,  $u_i^{m_i} \in F(u_1, \dots, u_{i-1})$  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.
150. 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  $K$ .
151. 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.
152. Let  $x_1, \dots, x_n$  be indeterminates over a field  $F$  and let  $s_1, \dots, s_n$  be the elementary symmetric functions of the  $x_i$ . Show that  $[F(x_1, \dots, x_n) : F(s_1, \dots, s_n)] = n!$ .

## Transcendental Extensions

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

155. 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  $\sigma$  is an automorphism of  $E$  such that  $\sigma(u) = u$  for all  $u \in F$ , then  $\sigma(x) = \frac{ax + b}{cx + d}$  for some  $a, b, c, d \in F$  with  $ad - bc \neq 0$ .
- (b) Determine the group  $\text{Aut}_F(E)$  of  $F$ -automorphisms of  $E$ .
156. 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  $P(\alpha, \beta) = 0$ .