

ANNUAL FOUNDATION SCHOOL (AFS-I)

5 - 31, DEC., 2005.

(BHASKARACHARYA PRATISHTHANA, & DEPT. OF MATH., UNIV. OF PUNE)

EXERCISES IN FIELD THEORY AND GALOIS THEORY

1. Algebraic extensions

- (1) Let F be a finite field with characteristic p . Prove that $|F| = p^n$ for some n .
- (2) Using $f(x) = x^2 + x - 1$ and $g(x) = x^3 - x + 1$, construct finite fields containing 4, 8, 9, 27 elements. Write down multiplication tables for the fields with 4 and 9 elements and verify that the multiplicative groups of these fields are cyclic.
- (3) Determine irreducible monic polynomials over \mathbb{Q} for $1 + i$, $2 + \sqrt{3}$, and $1 + \sqrt[3]{2} + \sqrt[3]{4}$.
- (4) Prove that $x^3 - 2$ and $x^3 - 3$ are irreducible over $\mathbb{Q}(i)$.
- (5) Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find an irreducible polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} .
- (6) Determine the degree $[\mathbb{Q}(\sqrt{3 + 2\sqrt{2}}) : \mathbb{Q}]$.
- (7) Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.
- (8) Let K/F be an algebraic field extension and R be a ring such that $F \subset R \subset K$. Show that R is a field.
- (9) Let K/F be an extension of degree n .
 - (a) For any $a \in K$, prove that the map $\mu_a : K \rightarrow K$ defined by $\mu_a(x) = ax$ for all $x \in K$, is a linear transformation of the F -vector space K . Show that K is isomorphic to a subfield of the ring $F^{n \times n}$ of $n \times n$ matrices with entries in F .
 - (b) Prove that a is a root of the characteristic polynomial of μ_a . Use this procedure to find monic polynomials satisfied by $\sqrt[3]{2}$ and $1 + \sqrt[3]{2} + \sqrt[3]{4}$.
- (10) Let $K = \mathbb{Q}(\sqrt{d})$ for some squarefree integer d . Let $\alpha = a + b\sqrt{d} \in K$. Use the basis $B = \{1, \sqrt{d}\}$ of K over F and find the matrix $M_B^B(\mu_\alpha)$ of $\mu_\alpha : K \rightarrow K$ with respect to B . Prove directly that the map $a + b\sqrt{d} \mapsto M_B^B(\mu_\alpha)$, is an isomorphism of fields.
- (11) Prove that -1 is not a sum of squares in the field $\mathbb{Q}(\beta)$ where $\beta = \sqrt[3]{2} e^{2\pi i/3}$.
- (12) Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$. Suppose that $f(0)$ and $f(1)$ are odd integers. Show that $f(x)$ has no integer roots.
- (13) Let R be an integral domain containing \mathbb{C} . Suppose that R is a finite dimensional \mathbb{C} -vector space. Show that $R = \mathbb{C}$.
- (14) Let k be a field and x be an indeterminate. Let $y = x^3/(x + 1)$. Find the minimal polynomial of x over $k(y)$.

- (15) Find an algebraic extension K of $\mathbb{Q}(x)$ such that the polynomial $f(y) = y^2 - x^3/(x^2 + 1) \in \mathbb{Q}(x)[y]$ has a root in K .

2. Ruler and compass constructions

- (1) The construction of a regular 7-gon amounts to the construction of the real number $\alpha = \cos(2\pi/7)$. Show that α is a root of $f(x) = x^3 + x^2 - 2x - 1$. Hence conclude that a regular 7-gon is not constructible by ruler and compass.
- (2) Show that $\alpha = 2\cos(2\pi/5)$ satisfies the equation $x^2 + x - 1 = 0$. Conclude that a regular 5-gon is constructible by ruler and compass. Describe a ruler and compass construction of the regular pentagon.
- (3) Show that it is impossible to construct a regular 9-gon by ruler and compass.
- (4) Show that an angle of n degrees, $n \in \mathbb{N}$, is constructible if and only if $3 \mid n$.
- (5) Prove that it is impossible, in general, to quintsect an arbitrary angle by ruler and compass. Is it possible to divide the angle 60 degrees into five equal parts by ruler and compass?
- (6) Without using Gauss's theorem show that if m and n are coprime natural numbers and regular m -gon and n -gon are constructible, then we can construct a regular mn -gon by ruler and compass.
- (7) Let p/q be a rational number written in lowest terms. Show that for an angle of p/q degrees to be constructible, it is necessary and sufficient that 3 divides p and $q = 2^k p_1 p_2 \dots p_t$ where p_1, p_2, \dots, p_t are distinct Fermat primes other than 3 or 5.

3. Symmetric polynomials

- (1) Write the symmetric polynomials $f(x, y, z) = x^2y^2 + y^2z^2 + z^2x^2$ and $g(x, y, z) = x^3y + xy^3 + x^3z + xz^3 + y^3z + yz^3$ in terms of elementary symmetric polynomials.
- (2) Let $\text{dis}(f(x))$ denote the discriminant of a polynomial $f(x)$. Show that
 - (a) $\text{dis}(x^3 + px + q) = -(4p^3 + 27q^2)$.
 - (b) $\text{dis}(x^4 + px^2 + r) = 16r(p^2 - 4r)^2$.
 - (c) $\text{dis}(x^4 + qx + r) = -27q^4 + 256r^3$.
- (3) Find the sum of 7th powers of the roots of $x^3 + px + q$.
- (4) Let $g(x) = x^3 + px + q$ where $q \neq 0$. Determine the monic polynomial whose roots are inverses of the squares of the roots of $g(x)$.
- (5) (a) Show that $\text{dis}(x^n - 1) = (-1)^{\binom{n}{2} + n - 1} n^n$.
 (b) Let $g(x)$ and $h(x)$ be monic polynomials and $g(x) = (x - a)h(x)$. Show that $\text{dis}(g(x)) = h(a)^2 \text{dis}(h(x))$.
 (c) Show that $\text{dis}(x^{n-1} + x^{n-2} + \dots + 1) = (-1)^{(n-1)(n+2)/2} n^{n-2}$.

- (6) Show that a polynomial $f \in S := R[x_1, x_2, \dots, x_n]$ where R is a commutative ring is fixed under all the automorphisms of S induced by even permutations in S_n if and only if $f = g + \delta h$ where g and h are symmetric polynomials and $\delta = \prod_{i < j} (x_i - x_j)$.
- (7) Let $f(x) = \prod_{i=1}^n (x - r_i)$. Show that $\text{dis}(f(x)) = (-1)^{\binom{n}{2}} \prod_{i=1}^n f'(r_i)$. Use this formula to show that $\text{dis}(\Phi_p(x)) = (-1)^{\binom{p}{2}} p^{p-2}$. Here $\Phi_p(x) = \text{irr}(\zeta_p, \mathbb{Q})$ for a prime number p .

4. Splitting fields of polynomials

- (1) Let F be a field and let K be a splitting field of a polynomial $f(x) \in F[x]$. Show that $[K : F] \leq n!$.
- (2) Find degrees of splitting fields over \mathbb{Q} of each of the following polynomials: (a) $x^3 - 2$ (b) $x^4 - 1$ (c) $x^4 + 1$ (d) $x^6 + 1$ (e) $(x^2 + 1)(x^3 - 1)$ and (f) $x^6 + x^3 + 1$.
- (3) Find a splitting field K of $x^3 - 10$ over $\mathbb{Q}(\sqrt{2})$. Find $[K : \mathbb{Q}]$.
- (4) Let p be a prime number. Show that the degree of a splitting field of $x^p - 2$ over \mathbb{Q} is $p(p - 1)$.
- (5) Let $f(x) \in \mathbb{Q}[x]$ be a cubic polynomial and K be a splitting field of $f(x)$ over \mathbb{Q} . Show that $[K : \mathbb{Q}]$ is either 1, 2, 3 or 6. Provide examples in each case.
- (6) Let \mathbb{F}_q denote a finite field with q elements. Show that for a prime number p , the finite field \mathbb{F}_{p^n} is a splitting field over \mathbb{F}_p of the polynomial $f(x) = x^{p^n} - x$. [Hint: Show that \mathbb{F}_{p^n} is precisely the set of roots of $f(x)$.]
- (7) Let $K \subset \mathbb{C}$ be a splitting field of $f(x) = x^3 - 2$ over \mathbb{Q} . Find a complex number z such that $K = \mathbb{Q}(z)$.
- (8) Let F be a field of characteristic p . Let $f(x) = x^p - x - c \in F[x]$. Show that either all roots of $f(x)$ lie in F or $f(x)$ is irreducible in $F[x]$. [Hint: show that if a is a root of $f(x)$ then so is $a + 1$.]
- (9) Let F be a field of characteristic zero and let p be an odd prime. Let $a \in F^\times$ such that a is not a p^{th} power of any element in F . Show that $f(x) = x^p - a$ is irreducible in $F[x]$. What can you say about the degree of a splitting field of $f(x)$ over F ?
- (10) Let E be a splitting field over a field F of $f(x)$. Let K be a subfield of the field extension E/F . Let $\sigma : K \rightarrow E$ be a monomorphism such that $\sigma(a) = a$ for all $a \in F$. Such a map is called an F -embedding of K into E . Show that σ can be extended to an automorphism of E .

5. Separable extensions

Notation: Throughout these exercises, $F \subset K \subset L$ is a tower of fields. Assume that $\text{char } F = p > 0$ in the problems 4-10.

- (1) Let $\text{char } F = 0$ and $f(x) \in F[x]$ be a monic polynomial of positive degree. Let $d(x) = (f(x), f'(x))$. Show that $g(x) = f(x)/d(x)$ has same roots as $f(x)$ and $g(x)$ is separable.
- (2) Let $a \in L$ be separable over F . Show that a is separable over K .
- (3) Show that an algebraic extension of a perfect field is perfect.
- (4) Let $f(x) = x^{p^n} - a \in F[x]$ where n is a positive integer. Show that $f(x)$ is irreducible over F if and only if $a \notin F^p$.
- (5) Let $([K : F], p) = 1$. Show that K is a separable algebraic extension of F .
- (6) Show that $\bigcap_{i=0}^{\infty} F^{p^i}$ is the largest perfect subfield of F .
- (7) Let $f(x) \in F[x]$ be irreducible. Show that there exists an irreducible separable polynomial $g(x) \in F[x]$ and a positive integer e such that $f(x) = g(x^{p^e})$. Show that all roots of $f(x)$ have same multiplicity p^e .
- (8) A polynomial $f(x) \in F[x]$ is called a p -polynomial if it is of the form $x^{p^m} + a_1 x^{p^{m-1}} + \cdots + a_m x$. Show that a monic polynomial of positive degree is a p -polynomial if and only if its roots form a finite subgroup of the additive group of a splitting field of $f(x)$ over F and every root has same multiplicity p^e .
- (9) Let t be an indeterminate. Show that the field extension $F(t)/F(t^p)$ is not separable.
- (10) Let $K = \mathbb{F}_p(t, w)$ be the rational function field in two indeterminates t, w over \mathbb{F}_p . Let L be the splitting field over K of the polynomial $h(x) = f(x)g(x)$ where $f(x) = x^p - t$ and $g(x) = x^p - w$. Prove the following:
 - (a) f and g are irreducible over K .
 - (b) $[L : K] = p^2$.
 - (c) L/K is not separable.
 - (d) $a^p \in K$ for all $a \in L$.

6. Finite fields

- (1) Identify the finite fields $\mathbb{Z}[i]/(1+i)$ and $\mathbb{Z}[i]/(2+i)$.
- (2) Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree m . Let $f(x)$ have a root $r \in \mathbb{F}_{p^m}$. Show that the roots of $f(x)$ are precisely $r^p, r^{p^2}, \dots, r^{p^{m-1}}$.
- (3) Find a necessary and sufficient condition on n and m so that \mathbb{F}_{p^n} is a subfield of \mathbb{F}_{p^m} .
- (4) Show that $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$ if $m \mid n$.
- (5) Factorize $x^8 - x$ into irreducible polynomials over \mathbb{F}_2 .
- (6) Let I denote the ideal $(X^3 + 2X + 1)\mathbb{F}_3[X]$ and let x denote the residue class $X + I$ in the field $K = \mathbb{F}_3[X]/I$. Show that x generates the cyclic group K^\times .
- (7) Let I denote the ideal $(X^3 + 2X + 2)\mathbb{F}_3[X]$ and x denote the residue class $X + I$ in the field $K = \mathbb{F}_3[X]/I$. Show that x does not generate the cyclic group K^\times . Find a generator of K^\times .

- (8) Prove that the rings $\mathbb{F}_3[x]/(x^2 + x + 2)$ and $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ are isomorphic. Construct an isomorphism.
- (9) Draw subfields lattices of the finite fields $\mathbb{F}_{3^{18}}$ and $\mathbb{F}_{2^{30}}$.
- (10) Let $f(x)$ be a separable polynomial in $\mathbb{F}_p[x]$. Show that there exists an n such that $f(x) \mid x^{p^n} - x$.
- (11) Show that the order of the Frobenius automorphism $\phi : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ is n .
- (12) Show that no finite field is algebraically closed.
- (13) Show that the field $\cup_{n=0}^{\infty} \mathbb{F}_{p^n}$ is an algebraic closure of \mathbb{F}_p .
- (14) Let K and L be subfields of \mathbb{F}_{p^n} having p^s and p^t elements respectively. How many elements does the field $K \cap L$ have ?
- (15) Define $f : K = \mathbb{F}_{p^n} \rightarrow K$ by $f(x) = x^2$.
- Show that f is surjective if $p = 2$.
 - Show that the number of elements in $f(K) = (p^n + 1)/2$.
 - Let α and β be nonzero elements of K Show that there exist $x, y \in K$ such that $\alpha x^2 + \beta y^2 = -1$, first for $p = 2$ and then for $p > 2$ by counting the number of elements in the sets $\{1 + \alpha x^2 : x \in K\}$ and $\{\beta y^2 : y \in K\}$.
- (16) Show that the product of nonzero elements of a finite field is -1 . Deduce *Wilson's theorem*: If p is a prime number then $p \mid 1 + (p - 1)!$.
- (17) Show that every element of a finite field K can be written as a sum of two squares in K .
- (18) Let K be a finite field with q elements. Define the **zeta function**

$$Z(t) = \frac{1}{1-t} \prod_p \frac{1}{1-t^{\deg p}}$$

where p ranges over all monic irreducible polynomials over K . Prove that $Z(t)$ is a rational function and determine this rational function.

7. Primitive elements

- Let $\alpha = \sqrt[3]{2}, \zeta = (-1 + \sqrt{-3})/2$ and $\beta = \alpha\zeta$.
 - Prove that for all $c \in \mathbb{Q}, \gamma = \alpha + c\beta$ is a root of a sextic of the form $x^6 + ax^3 + b$.
 - Prove that $\text{irr}(\alpha + \beta, \mathbb{Q})$ is cubic.
 - Prove that $\text{irr}(\alpha - \beta, \mathbb{Q})$ is sextic.
- Let $\alpha = \sqrt[3]{2}$, and $\omega = e^{2\pi i/3}$. Show that $\omega + c\alpha$ is a primitive element of $\mathbb{Q}(\alpha, \omega)$ for all $c \in \mathbb{Q}^\times$.
- Let $\omega = e^{2\pi i/3}$. Show that $\omega\sqrt{5}$ is a primitive element of $\mathbb{Q}(\omega, \sqrt{5})$.
- Let F be a subfield of \mathbb{C} and $a, b \in \mathbb{C}$ be algebraic elements over F . Show that there exist an integer n such that $a + nb$ is a primitive element of the field $K = F(a, b)$.

- (5) Find infinitely many primitive elements of the field $\mathbb{Q}(a, \omega)$ where a is a root of $x^3 - x + 1$.
- (6) Construct infinitely many intermediate subfields of $\mathbb{F}_p(u, v)/\mathbb{F}_p(u^p, v^p)$ where u, v are indeterminates.
- (7) Find a primitive element of \mathbb{F}_{2^4} over \mathbb{F}_2 .
- (8) Find a primitive element of the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
- (9) Let K/F be a finite separable extension of degree n . Using the primitive element theorem show that there are exactly n distinct embeddings of K into an algebraic closure F^a of F .

8. Fundamental theorem of Galois theory

- (1) Let K be a splitting field of $x^8 - 2$ over \mathbb{Q} . List all elements of $G = G(K/\mathbb{Q})$. Draw a diagram showing primitive elements of all the 15 subfields of K/\mathbb{Q} . Draw the lattice of all the 15 subgroups of G and match them with the fixed fields.
- (2) Determine all the subfields of the splitting field K of $x^8 - 2$ over \mathbb{Q} which are Galois over \mathbb{Q} .
- (3) Determine the Galois group of $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine all the subfields of the splitting field of $f(x)$.
- (4) Prove that the Galois group of $x^p - 2$, where p is a prime, is isomorphic to the group

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{F}_p \text{ and } a \neq 0 \right\}.$$

- (5) Let K be a Galois extension of F of degree p^n where p is a prime number and $n \in \mathbb{N}$. Show that there are intermediate subfields of K/F of degree p and p^{n-1} .
- (6) Let $f(x) \in \mathbb{Z}[x]$ be an irreducible quartic with Galois group S_4 over \mathbb{Q} . Let θ be a root of $f(x)$. Show that there is no field properly contained in $\mathbb{Q}(\theta)/\mathbb{Q}$. Is $\mathbb{Q}(\theta)/\mathbb{Q}$ a Galois extension ?
- (7) Show that if the Galois group of a rational cubic $f(x)$ is cyclic of order 3 then $f(x)$ has only real roots.
- (8) Consider the polynomial $f(x) = x^4 - 2x^2 - 2$.
 - (a) Show that the roots of the quartic are

$$\alpha_1 = \sqrt{1 + \sqrt{3}}, \alpha_2 = \sqrt{1 - \sqrt{3}}, \alpha_3 = -\sqrt{1 + \sqrt{3}} \text{ and } \alpha_4 = -\sqrt{1 - \sqrt{3}}.$$

- (b) Prove that $K_1 = \mathbb{Q}(\alpha_1) \neq K_2 = \mathbb{Q}(\alpha_2)$ and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.
- (c) Show that K_1, K_2 and K_1K_2 are Galois over F .
- (d) Show that $G(K_1K_2/F)$ is the Klein 4-group. Determine the automorphisms in this group.
- (e) Show that the Galois group of $f(x)$ over \mathbb{Q} is dihedral of order 8.

- (9) Show that $G(K/\mathbb{Q})$ is a cyclic group where $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$.
- (10) Let $\mathbb{C}(X)$ denote the rational function field in the indeterminate X over \mathbb{C} . Let $a \in \mathbb{C}$ and $\sigma_a : \mathbb{C}(X) \rightarrow \mathbb{C}(X)$ be the automorphism that substitutes X by $X + a$. Put $G = \{\sigma_a : a \in \mathbb{C}\}$. Show that $\mathbb{C}(X)^G = \mathbb{C}$.
- (11) Suppose that the Galois group of a field extension K/F is the Klein 4-group V_4 . Show that K/F is biquadratic.
- (12) Let $f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$ be irreducible. Show that the Galois group of $f(x)$ over \mathbb{Q} is contained in the dihedral group.
- (13) Let $E = \mathbb{Q}(r)$ where r is a root of $f(x) = x^3 + x^2 - 2x - 1$ in \mathbb{C} . Show that $f(r^2 - 2) = 0$. Determine $G(E/\mathbb{Q})$.
- (14) Let F be a field of characteristic p . Let $a \in F$ which is not of the form $b^p - b$ for any $b \in F$. Determine the Galois group over F of a splitting field of $x^p - x - a$.
- (15) Let $E = \mathbb{C}(t)$ where t is a transcendental over \mathbb{C} . Let $\omega = e^{2\pi i/3}$. Define the \mathbb{C} -automorphisms σ and τ of E by the equations $\sigma(t) = \omega t$ and $\tau(t) = 1/t$. Show that

$$\sigma^3 = \tau^2 = id \text{ and } \tau\sigma = \sigma^{-1}\tau.$$

Show that the group G of automorphisms generated by σ and τ has order 6 and $E^G = \mathbb{C}(t^3 + t^{-3})$.

- (16) Let K be a finite field with p^r elements. Let $\phi : K \rightarrow K$ where $\phi(a) = a^p$, for all $a \in K$, be the Frobenius automorphism. Find eigenvectors and eigenvalues of ϕ as an \mathbb{F}_p -linear transformation of the \mathbb{F}_p -vector space K .
- (17) Let x, y be variables. Let $a, b, c, d \in \mathbb{Z}$ and $n = |ad - bc|$. Show that $L = \mathbb{C}(x, y)$ is a Galois extension of $K = \mathbb{C}(x^a y^b, x^c y^d)$ of degree n . Find $G(L/K)$.

9. Galois groups of Quartics

- (1) Show that the resolvent cubic of $x^4 + px^2 + qx + r$ is $x^3 - px^2 - 4rx + (4pr - q^2)$.
- (2) Determine the Galois groups of the quartics: $x^4 - 2$, $x^4 + 2$, $x^4 - x + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$, and $x^4 + 4x^2 - 5$.
- (3) Show that the resolvent cubic $r(x)$ of $f(x) = x^4 + 1$ is $x(x - 2)(x + 2)$ and $G_f = V$.
- (4) Show that the Galois group of an irreducible quartic in $\mathbb{Q}[x]$ with exactly two real roots is either S_4 or D_4 .
- (5) Let α be a real root of an irreducible rational quartic whose resolvent cubic is irreducible. Show that α is not constructible by ruler and compass. Can we construct the roots of the quartic $x^4 + x - 5$ by ruler and compass ?
- (6) Put $f(x) = x^4 - 2x^2 - 1$. Show that $f(x)$ is irreducible in over \mathbb{Q} . and $r(x) = (x + 2)(x^2 + 4)$. Show that $G_f = D_4$. Find all the intermediate subfields of the splitting field K of $f(x)$ over \mathbb{Q} . Match them with the subgroups of D_4 .
- (7) Show that the discriminants of a quartic polynomial and its resolvent cubic are equal.

- (8) Substitute x by $1/y$ to calculate $\text{disc}(x^4 + ax^3 + b)$.
- (9) Find sufficient conditions on the integers a, b and c so that $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ is a Galois extension of \mathbb{Q} with cyclic Galois group of order 4.

10. Cyclotomic extensions

- (1) Show that $\mathbb{Q}[\zeta_n, \zeta_m] = \mathbb{Q}[\zeta_m + \zeta_n]$.
- (2) Determine $[\mathbb{Q}(\zeta_7, \zeta_3) : \mathbb{Q}(\zeta_3)]$.
- (3) Determine a primitive element of a subfield K of $E = \mathbb{Q}(\zeta_{13})$ so that $[K : \mathbb{Q}] = 3$.
- (4) Put $\zeta = \zeta_7$. Determine the degrees of $\zeta + \zeta^5$ and $\zeta + \zeta^5 + \zeta^8$ over \mathbb{Q} .
- (5) Put $\zeta = \zeta_{11}$ and $\alpha = \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$. Show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.
- (6) Let ν be a primitive element modulo p where p is a prime. Thus $\mathbb{F}_p^\times = \langle \nu \rangle$. Let $\zeta = \zeta_p$. Using the list $\{\zeta^{\nu^0}, \zeta^{\nu^1}, \zeta^{\nu^2}, \dots, \zeta^{\nu^{p-2}}\}$, show how to find the sum β of powers of ζ which determines a subfield $\mathbb{Q}(\beta)$ of $\mathbb{Q}(\zeta)$ so that $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$ where $d \mid (p-1)$.
- (7) Prove that if $n = p^k m$ where p is a prime and $(p, m) = 1$ then there are precisely m distinct n^{th} roots of unity over a field of characteristic p .
- (8) Let K be finite extension of \mathbb{Q} . Show that K contains only a finite number of roots of unity.
- (9) Suppose $A \in \mathbb{C}^{n \times n}$ and $A^k = I$ for some integer $k \in \mathbb{N}$. Show that A can be diagonalized. Prove that the matrix $A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$ where $\alpha \in K$ and K is a field of characteristic p satisfies $A^p = I$ and cannot be diagonalized if $\alpha \neq 0$.
- (10) Show that $n = \sum_{d \mid n} \phi(d)$ and deduce that $\phi(n) = \sum_{d \mid n} \mu(n/d)d$.
- (11) Show that $\Phi_n(x) = x^{\phi(n)}\Phi_n(1/x)$ and deduce that the coefficients of $\Phi_n(x)$ satisfy $a_k = a_{\phi(n)-k}$ for all $0 \leq k \leq \phi(n)$.
- (12) Establish the following formulas:
- $\Phi_n(x) = \Phi_m(x^{n/m})$ where m is the product of distinct prime factors of n .
 - $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ where p is coprime to n .
 - $\Phi_{2n}(x) = \Phi_n(-x)$ where $n \geq 1$ is an odd integer.
- (13) Let ζ, η and ω denote the primitive fifteenth, fifth and cube roots of unity.
- Describe all the automorphisms in $G := G(\mathbb{Q}(\zeta)/\mathbb{Q})$.
 - Show that G is isomorphic to a direct product of two cyclic groups. Construct this isomorphism.
 - Show that $\mathbb{Q}(\omega), \mathbb{Q}(\zeta), \mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\omega, \sqrt{5})$ are subfields of $\mathbb{Q}(\zeta)$.
 - Make the Galois correspondence between the subfields of $\mathbb{Q}(\zeta)$ and subgroups of G explicit.
- (14) Show that for every $N \in \mathbb{Z}$ there exists an integer n such that $\sqrt{N} \in \mathbb{Q}(\zeta_n)$.

11. Solvable Galois extensions

- (1) Show that the polynomials $f(x) = x^5 - 14x + 7$, $g(x) = x^5 - 7x^2 + 7$ and $h(x) = x^7 - 10x^5 + 15x + 5$ are not solvable by radicals over \mathbb{Q} .
- (2) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p . Suppose that $f(x)$ has exactly two non-real roots. Show that $f(x)$ is not solvable by radicals over \mathbb{Q} .
- (3) Let K be a subfield of \mathbb{C} . Let $p(x) = x^3 + px + q$ be an irreducible polynomial in $K[x]$. Let r be a root of $p(x)$. Let $u = a + br + cr^2 \in K(r) \setminus K$. Determine $g(x) := \text{irr}(u, K)$. Let $\Delta = -4p^3 - 27q^2$. Show that $K(r)$ is a radical extension of K if and only if -3Δ is a square in K .
- (4) Let x_1, x_2, x_3 be indeterminates and let s_1, s_2, s_3 be the elementary symmetric polynomials in these indeterminates. Show that $\mathbb{Q}(x_1, x_2, x_3)$ is not a radical extension of $\mathbb{Q}(s_1, s_2, s_3)$ but $\mathbb{Q}(\zeta_3)(x_1, x_2, x_3)$ is a radical extension of $\mathbb{Q}(s_1, s_2, s_3)$.
- (5) Let G be the Galois group of an irreducible quintic over \mathbb{Q} . Show that $G = A_5$ or S_5 if G has an element of order 3.
- (6) Find Galois groups of the Taylor polynomials $T_n(x) = \sum_{i=0}^{i=n} x^i/i!$ for $n \leq 4$.
- (7) Is every Galois extension of degree 10 solvable by radicals?
- (8) Let ζ be a primitive 7th root of unity and let $\alpha = \zeta + \zeta^{-1}$. Show that $f(x) = \text{irr}(\alpha, \mathbb{Q}) = x^3 + x^2 - 2x - 1$. Solve for the roots of $f(x)$ to express ζ in terms of radicals over \mathbb{Q} .
- (9) Show that S_n and A_n are not solvable groups for $n \geq 5$ by using the following line of argument: Let $G < S_n$ be a subgroup containing all the 3-cycles. Let $H < G$ be a normal subgroup of G such that G/H is abelian. Then show that H contains all the 3-cycles. Hint: Define the commutator of g and h to be the element $[g, h] = g^{-1}h^{-1}gh$. Then for the natural map $\pi : G \rightarrow G/H$, $\pi([g, h]) = 1$, whence $[g, h] \in H$. Find the commutator $[(ikr), (jkv)]$.
- (10) Show: (a) A p -group is solvable. (b) A group of order pq where p and q are distinct primes is solvable. (c) A group of order pqr where p, q and r are distinct primes is solvable.

12. Cyclic extensions

- (1) Let L be the splitting field of $x^{10} - 1$ over \mathbb{Q} in \mathbb{C} . Is L a cyclic extension of \mathbb{Q} ?
- (2) Let $K = \mathbb{Q}(\sqrt[n]{a})$ where a is a positive rational number. Suppose $[K : \mathbb{Q}] = n$ and E is any subfield of K with $[E : \mathbb{Q}] = d$. Prove that $E = \mathbb{Q}(\sqrt[d]{a})$. **Hint:** Consider $N_{K/E}(\sqrt[n]{a})$.
- (3) Let K be as in exercise ???. Prove that if n is odd, then K has no nontrivial subfields that are Galois over \mathbb{Q} and if n is even, then the only nontrivial subfield of K that is Galois over \mathbb{Q} is $\mathbb{Q}(\sqrt{a})$.

- (4) **(Kummer generators for cyclic extensions)** Let F be a field so that $\text{char}(F)$ does not divide n and let F have a primitive n^{th} root ζ of unity. Let K be a cyclic extension of F so that $[K : F] = d \mid n$. Then $K = F(\sqrt[n]{a} =: c)$ for some nonzero $a \in F$. Let $G(K/F) = \langle \sigma \rangle$.
- Show that $\sigma(c) = \zeta c$ for some primitive d^{th} root ζ of unity.
 - Suppose $K = F(\sqrt[n]{a}) = F(\sqrt[n]{b})$. Show that $\sigma(c)/c = \left(\sigma(\sqrt[n]{b})/\sqrt[n]{b}\right)^i$ for some integer i coprime with d . Conclude that σ fixes the element $c/(\sqrt[n]{b})^i$.
 - Prove that $K = F(\sqrt[n]{a}) = F(\sqrt[n]{b})$ if and only if $a = b^i e^n$ and $b = a^j f^n$ for some $e, f \in F$.
- (5) Show that if E is a finite field and F is a subfield, then $N_{E/F} : E^\times \rightarrow F^\times$ is surjective.
- (6) Let $E = \mathbb{Q}(\sqrt{m})$ where $m < 0$ is an integer. Show that E cannot be embedded in a cyclic quartic field over \mathbb{Q} .

13. Luröth's theorem and Galois group of $F(t)/F$

Let t denote an indeterminate in this section.

- Show that $\mathbb{C}(t)$ is a Galois extension of $\mathbb{C}(t^n + t^{-n})$. Find the Galois group of this extension.
- Let k be a field with 4 elements and put $F = k(t^4 + t)$ and $E = k(t)$. Show that E/F is a Galois extension. Find the Galois group of E/F and describe primitive elements of all the subfields of E/F .
- Let F be a field and let $G := G(F(t)/F)$. Show that G is generated by the automorphisms $\tau_b : t \mapsto t + b$, $\rho_a : t \mapsto at$ ($a \neq 0$) and $\sigma : t \mapsto t^{-1}$.
- Let k be a finite field with q elements. Let $G := G(k(t)/k)$. Prove the following:
 - $o(G) = q^3 - q$.
 - $k(t)^G = k(y)$ where $y = (t^{q^2} - t)^{q+1}/(t^q - t)^{q^2+1}$.
 - Put $H_1 = \{t \mapsto at + b : a \neq 0, b \in k\}$. Then $k(t)^{H_1} = k((t^q - t)^{q-1})$.
 - Let $H_2 = \{t \mapsto t + b : b \in k\}$. Then $k(t)^{H_2} = k(t^q - t)$.
- Let $k := \mathbb{F}_3$. Let $G := G(k(t)/k)$ and $F = k(t)^G$. Prove that $G \simeq S_4$ by examining the action of G on lines in the two dimensional k -vector space k^2 .
- Let the notation be as in the exercise ???. Prove that there is a unique subfield E of $k(t)/F$ such that $[E : F] = 2$. Find primitive elements of subfields of $k(t)$ containing E .
- Let $L = \mathbb{Q}(t)$. Define \mathbb{Q} -automorphisms σ, τ of L by $\sigma(t) = -t$ and $\tau(t) = 1/t$. Find the fixed field L^G of the group generated by σ and τ .