Part II

Galois Theory

Year

Paper 1, Section II

18I Galois Theory

(a) What does it mean to say that a finite extension L/K is *normal*? Show that L/K is normal if and only if L is a splitting field of some polynomial over K.

(b) Let $M/L/K$ be finite extensions. Which of the following statements are true, and which are false? Give a proof or counterexample in each case.

i) If M/K is normal then M/L is normal.

ii) If M/K is normal then L/K is normal.

iii) If M/L and L/K are normal, then M/K is normal.

(c) Let L be a splitting field of $T^4 - 7$ over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/\mathbb{Q})$ is the dihedral group of order 8. Determine all the subfields of L, and express each of them in the form $\mathbb{Q}(x)$ for some $x \in L$. Which of them are normal extensions of $\mathbb{Q}$?

Paper 2, Section II

18I Galois Theory

Let L/K be a finite extension of fields of characteristic $p > 0$.

(a) Let $x \in L$. What does it mean to say that x is *separable over* K? Show that x is separable over K if and only if its minimal polynomial is not of the form $g(T^p)$ for some $g \in K[T]$.

(b) We say that $x \in L$ is *purely inseparable* over K if for some $n \geqslant 0$, $x^{p^n} \in K$. Show that x is purely inseparable over K if and only if its minimal polynomial is of the form $T^{p^n} - y$, for some $n \geqslant 0$ and some $y \in K$.

(c) Let $g \in K[T]$ be a monic nonconstant polynomial, and $f(T) = g(T^p)$. Assume that L is a splitting field for g over K, and let M be a splitting field for f over L. Show that M is also a splitting field for f over K, and that every root of f in M is purely inseparable over L. Show also that for every $\sigma \in \mathrm{Aut}(L/K)$ there exists a unique automorphism τ of M whose restriction to L equals σ.

(d) Suppose that g is irreducible and separable. Show that $\mathrm{Aut}(M/K)$ acts transitively on the roots of f in M. Deduce that either every root of f lies in L, or every root has degree p over L.

Let $h \in K[T]$ be an irreducible monic factor of f. Show that either $h = f$, or that h is separable. Deduce that f is reducible if and only if every coefficient of g is a p-th power in K.

[*You may assume without proof the uniqueness of splitting fields, and that a nonconstant polynomial f is separable if and only if* $(f, f') = 1$.]

Paper 3, Section II

18I Galois Theory

(a) Show that a finite subgroup of the multiplicative group of a field is cyclic.

(b) What is a *primitive n-th root of unity*? Show that if K contains a primitive m-th root of unity and a primitive n-th root of unity, then it contains a primitive N-th root of unity, where N is the least common multiple of m and n.

(c) Define the *cyclotomic polynomials* Φ_n and show that they have integer coefficients. Show also that the reduction of Φ_n modulo a prime p is separable if p does not divide n.

(d) Let K be a field of characteristic zero, L a splitting field for Φ_n over K, and let $G = \mathrm{Gal}(L/K)$ be its Galois group. Write down an injective homomorphism from G into $(\mathbb{Z}/n\mathbb{Z})^\times$, and show that it is surjective if and only if Φ_n is irreducible over K.

(e) Let L be a splitting field for Φ_n over $\mathbb{Q}$. Show that the number of roots of unity in L is n if n is even, and $2n$ if n is odd. [You may assume that Φ_n is irreducible over $\mathbb{Q}$.]

Paper 4, Section II

18I Galois Theory

(a) Define the *discriminant* of a monic polynomial.

Let K be a field with $\mathrm{char}(K) \neq 2$, and let $f \in K[T]$ be a monic, separable polynomial of degree n. Show that the Galois group of f is contained in A_n if and only if the discriminant of f is a square in K.

Compute the Galois group of $T^3 - 2T + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{-19})$.

[*The discriminant of* $T^3 + aT + b$ *is* $-4a^3 - 27b^2$.]

(b) Let K be a field of characteristic 2, and $f = T^3 + aT + b \in K[T]$. Let L be a splitting field for f over K.

(i) Show that f is separable if and only if $b \neq 0$.

(ii) Assuming that f is separable, show that $g = T^2 + bT + a^3 + b^2$ splits into distinct linear factors in $L[T]$. By considering the action of the Galois group G of f on the roots of g, or otherwise, show that G is contained in A_3 if and only if g splits into linear factors in $K[T]$.

Paper 1, Section II
18H Galois Theory

(a) Let K be a field with $\operatorname{char} K \neq 2, 3$. If $f = x^3 + px + q \in K[x]$, define the *discriminant* of f, and compute it in terms of p and q.

Let L be the splitting field of f and let $G = \operatorname{Aut}(L/K)$ be the Galois group. Describe all possibilities for G. Justify your answer. [Do not assume that f is irreducible.]

Compute all subfields of L when $f = x^3 + 3x + 1 \in \mathbb{Q}[x]$. You may specify the subfields in terms of the roots; you do not need to determine the roots explicitly in terms of radicals.

(b) Let L/K be a Galois extension, and suppose $f \in L[x]$. Show that there exists a non-zero polynomial $g \in L[x]$ such that $fg \in K[x]$.

Now suppose only that L/K is a finite separable extension, and that $f \in L[x]$. Show that there exists a non-zero polynomial $g \in L[x]$ such that $fg \in K[x]$.

Paper 2, Section II
18H Galois Theory

(a) Let L be a finite field of order p^n. Suppose that $\gamma \in L$, and let $f \in \mathbb{F}_p[x]$ be the minimal polynomial of γ over $\mathbb{F}_p$. Show that $\deg f$ divides n. Prove that there is a $\gamma \in L$ for which $\deg f = n$.

Show that for every $r \geqslant 1$, there is an irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree r.

[*You may assume the tower law and the existence of splitting fields, but should prove any results about finite fields that you use.*]

(b) Suppose that K is a field and that L is a finite extension of K. Define what it means for $\alpha \in L$ to be *separable* over K. If $f \in K[x]$ is the minimal polynomial of α and $\gcd(f, f') = 1$ show that α is separable over K.

Now suppose that $L = K(\beta)$ is a finite extension of K and that $\operatorname{char} K = p$. Show there exists a unique intermediate field M with $K \subseteq M \subseteq L$, such that the following conditions hold: M is a separable extension of K, $[L : M] = p^h$ for some h, and $\gamma^{p^h} \in M$ for all $\gamma \in L$. [*Hint: If β is not separable, what is its minimal polynomial?*]

Paper 3, Section II
18H Galois Theory

(a) Let L/K be an extension of fields, and suppose that K contains a primitive nth root of unity ζ. Let $\sigma \in \mathrm{Aut}(L/K)$ be a K-automorphism of L of order n. Prove that there exists a nonzero element $\alpha \in L$ with $\sigma(\alpha) = \zeta\alpha$. What is the minimal polynomial of α over L^σ, the fixed field of σ?

(b) Define what it means for L to be an *algebraic closure* of K. Given that

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$$

is a field, show that $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. State carefully any results that you use.

(c) Let L be an algebraically closed field of characteristic zero, and $\sigma : L \to L$ a homomorphism of fields. Suppose $\sigma^d = 1$ for some $d > 0$, and let $K = L^\sigma$ be the fixed field of σ. If M/K is a finite extension, show that M/K is a Galois extension with cyclic Galois group. [*Hint: Show that there is a K-homomorphism from M to L.*] Give an example showing that the assumption that L is algebraically closed is necessary.

Paper 4, Section II
18H Galois Theory

(a) Stating carefully all the theorems that you use, prove that for every integer $r > 1$ there is a Galois extension $L/\mathbb{Q}$ with Galois group $\mathbb{Z}/r\mathbb{Z}$.

(b) Suppose L_1 and L_2 are two extensions of a field K, and both L_1 and L_2 are subfields of some field M. Let L_1L_2 be the smallest subfield of M containing both L_1 and L_2. If $[L_i : K] = d_i$ and $\gcd(d_1, d_2) = 1$, show that $[L_1L_2 : K] = d_1d_2$.

(c) Let $p \geqslant 3$ be a prime number. Give examples of two non-isomorphic groups G, G' of order $p(p-1)$ containing normal subgroups N, N' of order p such that $G/N \cong G'/N'$.

Fix $p = 3$. For the groups G, G' above, give explicit examples of Galois extensions $L/\mathbb{Q}$ and $L'/\mathbb{Q}$ with $\mathrm{Aut}(L/\mathbb{Q}) \cong G$ and $\mathrm{Aut}(L'/\mathbb{Q}) \cong G'$. Identify the fixed fields L^N and $(L')^{N'}$. Justify your answer.

Now suppose $p > 3$ is an arbitrary prime. Prove that there are extensions L and L' of $\mathbb{Q}$ with $\mathrm{Aut}(L/\mathbb{Q}) \cong G$ and $\mathrm{Aut}(L'/\mathbb{Q}) \cong G'$.

Paper 1, Section II

18I Galois Theory

(a) Let $K \subseteq L$ be fields, and $f(x) \in K[x]$ a polynomial.

Define what it means for L to be a *splitting field* for f over K.

Prove that splitting fields exist, and state precisely the theorem on uniqueness of splitting fields.

Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Find a subfield of $\mathbb{C}$ which is a splitting field for f over $\mathbb{Q}$. Is this subfield unique? Justify your answer.

(b) Let $L = \mathbb{Q}[\zeta_7]$, where ζ_7 is a primitive 7th root of unity.

Show that the extension $L/\mathbb{Q}$ is Galois. Determine all subfields $M \subseteq L$.

For each subfield M, find a primitive element for the extension $M/\mathbb{Q}$ explicitly in terms of ζ_7, find its minimal polynomial, and write down $\mathrm{Aut}(M/\mathbb{Q})$ and $\mathrm{Aut}(L/M)$.

Which of these subfields M are Galois over $\mathbb{Q}$?

[*You may assume the Galois correspondence, but should prove any results you need about cyclotomic extensions directly.*]

Paper 2, Section II

18I Galois Theory

(a) Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree n, and let L be its splitting field.

(i) Suppose that f is irreducible. Compute $\mathrm{Gal}(f)$, carefully stating any theorems you use.

(ii) Now suppose that $f(x)$ factors as $f = h_1 \cdots h_r$ in $\mathbb{F}_q[x]$, with each h_i irreducible, and $h_i \neq h_j$ if $i \neq j$. Compute $\mathrm{Gal}(f)$, carefully stating any theorems you use.

(iii) Explain why $L/\mathbb{F}_q$ is a cyclotomic extension. Define the corresponding homomorphism $\mathrm{Gal}(L/\mathbb{F}_q) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ for this extension (for a suitable integer m), and compute its image.

(b) Compute $\mathrm{Gal}(f)$ for the polynomial $f = x^4 + 8x + 12 \in \mathbb{Q}[x]$. [You may assume that f is irreducible and that its discriminant is 576^2.]

Paper 3, Section II

18I Galois Theory

Define the *elementary symmetric functions* in the variables $x_1, \ldots, x_n$. State the fundamental theorem of symmetric functions.

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$, where K is a field. Define the *discriminant* of f, and explain why it is a polynomial in $a_0, \ldots, a_{n-1}$.

Compute the discriminant of $x^5 + q$.

Let $f(x) = x^5 + px^2 + q$. When does the discriminant of $f(x)$ equal zero? Compute the discriminant of $f(x)$.

Paper 4, Section II

18I Galois Theory

Let L be a field, and G a group *which acts on L by field automorphisms.*

(a) Explain the meaning of the phrase in italics in the previous sentence.

Show that the set L^G of fixed points is a subfield of L.

(b) Suppose that G is finite, and set $K = L^G$. Let $\alpha \in L$. Show that α is algebraic and separable over K, and that the degree of α over K divides the order of G.

Assume that α is a primitive element for the extension L/K, and that G is a subgroup of $\mathrm{Aut}(L)$. What is the degree of α over K? Justify your answer.

(c) Let $L = \mathbb{C}(z)$, and let ζ_n be a primitive nth root of unity in $\mathbb{C}$ for some integer $n > 1$. Show that the $\mathbb{C}$-automorphisms σ, τ of L defined by

$$\sigma(z) = \zeta_n z, \qquad \tau(z) = 1/z$$

generate a group G isomorphic to the dihedral group of order $2n$.

Find an element $w \in L$ for which $L^G = \mathbb{C}(w)$.

Paper 1, Section II

18G Galois Theory

(a) State and prove the tower law.

(b) Let K be a field and let $f(x) \in K[x]$.

(i) Define what it means for an extension L/K to be a *splitting field* for f.

(ii) Suppose f is irreducible in $K[x]$, and *char* $K = 0$. Let M/K be an extension of fields. Show that the roots of f in M are distinct.

(iii) Let $h(x) = x^{q^n} - x \in K[x]$, where $K = F_q$ is the finite field with q elements. Let L be a splitting field for h. Show that the roots of h in L are distinct. Show that $[L : K] = n$. Show that if $f(x) \in K[x]$ is irreducible, and $\deg f = n$, then f divides $x^{q^n} - x$.

(iv) For each prime p, give an example of a field K, and a polynomial $f(x) \in K[x]$ of degree p, so that f has at most one root in any extension L of K, with multiplicity p.

Paper 2, Section II

18G Galois Theory

(a) Let K be a field and let L be the splitting field of a polynomial $f(x) \in K[x]$. Let ξ_N be a primitive N^{th} root of unity. Show that $\text{Aut}(L(\xi_N)/K(\xi_N))$ is a subgroup of $\text{Aut}(L/K)$.

(b) Suppose that L/K is a Galois extension of fields with cyclic Galois group generated by an element σ of order d, and that K contains a primitive d^{th} root of unity ξ_d. Show that an eigenvector α for σ on L with eigenvalue ξ_d generates L/K, that is, $L = K(\alpha)$. Show that $\alpha^d \in K$.

(c) Let G be a finite group. Define what it means for G to be *solvable*.

Determine whether

(i) $G = S_4$; (ii) $G = S_5$

are solvable.

(d) Let $K = \mathbb{Q}(a_1, a_2, a_3, a_4, a_5)$ be the field of fractions of the polynomial ring $\mathbb{Q}[a_1, a_2, a_3, a_4, a_5]$. Let $f(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in K[x]$. Show that f is not solvable by radicals. [You may use results from the course provided that you state them clearly.]

Paper 3, Section II

18G Galois Theory

(a) Let L/K be a Galois extension of fields, with $\mathrm{Aut}(L/K) = A_{10}$, the alternating group on 10 elements. Find $[L : K]$.

Let $f(x) = x^2 + bx + c \in K[x]$ be an irreducible polynomial, $char\, K \neq 2$. Show that $f(x)$ remains irreducible in $L[x]$.

(b) Let $L = \mathbb{Q}[\xi_{11}]$, where ξ_{11} is a primitive 11^{th} root of unity.

Determine all subfields $M \subseteq L$. Which are Galois over $\mathbb{Q}$?

For each proper subfield M, show that an element in M which is not in $\mathbb{Q}$ must be primitive, and give an example of such an element explicitly in terms of ξ_{11} for each M. [You do not need to justify that your examples are not in $\mathbb{Q}$.]

Find a primitive element for the extension $L/\mathbb{Q}$.

Paper 4, Section II

18G Galois Theory

(a) Let K be a field. Define the *discriminant* $\Delta(f)$ of a polynomial $f(x) \in K[x]$, and explain why it is in K, carefully stating any theorems you use.

Compute the discriminant of $x^4 + rx + s$.

(b) Let K be a field and let $f(x) \in K[x]$ be a quartic polynomial with roots $\alpha_1, \ldots, \alpha_4$ such that $\alpha_1 + \cdots + \alpha_4 = 0$.

Define the *resolvant cubic* $g(x)$ of $f(x)$.

Suppose that $\Delta(f)$ is a square in K. Prove that the resolvant cubic is irreducible if and only if $Gal(f) = A_4$. Determine the possible Galois groups $Gal(f)$ if $g(x)$ is reducible.

The resolvant cubic of $x^4 + rx + s$ is $x^3 - 4sx - r^2$. Using this, or otherwise, determine $Gal(f)$, where $f(x) = x^4 + 8x + 12 \in \mathbb{Q}[x]$. [You may use without proof that f is irreducible.]

Paper 1, Section II

18F Galois Theory

(a) Suppose K, L are fields and $\sigma_1, \ldots, \sigma_m$ are distinct embeddings of K into L. Prove that there do not exist elements $\lambda_1, \ldots, \lambda_m$ of L (not all zero) such that

$$\lambda_1\sigma_1(x) + \cdots + \lambda_m\sigma_m(x) = 0 \quad \text{for all } x \in K.$$

(b) For a finite field extension K of a field k and for $\sigma_1, \ldots, \sigma_m$ distinct k-automorphisms of K, show that $m \leqslant [K : k]$. In particular, if G is a finite group of field automorphisms of a field K with K^G the fixed field, deduce that $|G| \leqslant [K : K^G]$.

(c) If $K = \mathbb{Q}(x, y)$ with x, y independent transcendentals over $\mathbb{Q}$, consider the group G generated by automorphisms σ and τ of K, where

$$\sigma(x) = y,\ \sigma(y) = -x \quad \text{and} \quad \tau(x) = x,\ \tau(y) = -y.$$

Prove that $|G| = 8$ and that $K^G = \mathbb{Q}(x^2 + y^2,\ x^2y^2)$.

Paper 2, Section II

18F Galois Theory

For any prime $p \neq 5$, explain briefly why the Galois group of $X^5 - 1$ over $\mathbb{F}_p$ is cyclic of order d, where $d = 1$ if $p \equiv 1 \mod 5$, $d = 4$ if $p \equiv 2, 3 \mod 5$, and $d = 2$ if $p \equiv 4 \mod 5$.

Show that the splitting field of $X^5 - 5$ over $\mathbb{Q}$ is an extension of degree 20.

For any prime $p \neq 5$, prove that $X^5 - 5 \in \mathbb{F}_p[X]$ does not have an irreducible cubic as a factor. For $p \equiv 2$ or $3 \mod 5$, show that $X^5 - 5$ is the product of a linear factor and an irreducible quartic over $\mathbb{F}_p$. For $p \equiv 1 \mod 5$, show that either $X^5 - 5$ is irreducible over $\mathbb{F}_p$ or it splits completely.

[*You may assume the reduction mod p criterion for finding cycle types in the Galois group of a monic polynomial over $\mathbb{Z}$ and standard facts about finite fields.*]

Paper 3, Section II

18F Galois Theory

Let k be a field. For m a positive integer, consider $X^m - 1 \in k[X]$, where either char $k = 0$, or char $k = p$ with p not dividing m; explain why the polynomial has distinct roots in a splitting field.

For m a positive integer, define the mth *cyclotomic polynomial* $\Phi_m \in \mathbb{C}[X]$ and show that it is a monic polynomial in $\mathbb{Z}[X]$. Prove that Φ_m is irreducible over $\mathbb{Q}$ for all m. [*Hint: If* $\Phi_m = fg$, *with* $f, g \in \mathbb{Z}[X]$ *and* f *monic irreducible with* $0 < \deg f < \deg \Phi_m$, *and* ε *is a root of* f, *show first that* ε^p *is a root of* f *for any prime* p *not dividing* m.]

Let $F = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1 \in \mathbb{Z}[X]$; by considering the product $(X^2 - X + 1)F$, or otherwise, show that F is irreducible over $\mathbb{Q}$.

Paper 4, Section II

18F Galois Theory

State (without proof) a result concerning uniqueness of splitting fields of a polynomial.

Given a polynomial $f \in \mathbb{Q}[X]$ with distinct roots, what is meant by its *Galois group* $\mathrm{Gal}_{\mathbb{Q}}(f)$? Show that f is irreducible over $\mathbb{Q}$ if and only if $\mathrm{Gal}_{\mathbb{Q}}(f)$ acts transitively on the roots of f.

Now consider an irreducible quartic of the form $g(X) = X^4 + bX^2 + c \in \mathbb{Q}[X]$. If $\alpha \in \mathbb{C}$ denotes a root of g, show that the splitting field $K \subset \mathbb{C}$ is $\mathbb{Q}(\alpha, \sqrt{c})$. Give an explicit description of $\mathrm{Gal}(K/\mathbb{Q})$ in the cases:

(i) $\sqrt{c} \in \mathbb{Q}(\alpha)$, and

(ii) $\sqrt{c} \notin \mathbb{Q}(\alpha)$.

If c is a square in $\mathbb{Q}$, deduce that $\mathrm{Gal}_{\mathbb{Q}}(g) \cong C_2 \times C_2$. Conversely, if $\mathrm{Gal}_{\mathbb{Q}}(g) \cong C_2 \times C_2$, show that $\sqrt{c}$ is invariant under at least two elements of order two in the Galois group, and deduce that c is a square in $\mathbb{Q}$.

Paper 4, Section II

18I Galois Theory

Let K be a field of characteristic $p > 0$ and let L be the splitting field of the polynomial $f(t) = t^p - t + a$ over K, where $a \in K$. Let $\alpha \in L$ be a root of $f(t)$.

If $L \neq K$, show that $f(t)$ is irreducible over K, that $L = K(\alpha)$, and that L is a Galois extension of K. What is $\mathrm{Gal}(L/K)$?

Paper 3, Section II

18I Galois Theory

Let L be a finite field extension of a field K, and let G be a finite group of K-automorphisms of L. Denote by L^G the field of elements of L fixed by the action of G.

(a) Prove that the degree of L over L^G is equal to the order of the group G.

(b) For any $\alpha \in L$ write $f(t, \alpha) = \Pi_{g \in G}(t - g(\alpha))$.

(i) Suppose that $L = K(\alpha)$. Prove that the coefficients of $f(t, \alpha)$ generate L^G over K.

(ii) Suppose that $L = K(\alpha_1, \alpha_2)$. Prove that the coefficients of $f(t, \alpha_1)$ and $f(t, \alpha_2)$ lie in L^G. By considering the case $L = K(a_1^{1/2}, a_2^{1/2})$ with a_1 and a_2 in K, or otherwise, show that they need not generate L^G over K.

Paper 2, Section II

18I Galois Theory

Let K be a field and let $f(t)$ be a monic polynomial with coefficients in K. What is meant by a *splitting field* L for $f(t)$ over K? Show that such a splitting field exists and is unique up to isomorphism.

Now suppose that K is a finite field. Prove that L is a Galois extension of K with cyclic Galois group. Prove also that the degree of L over K is equal to the least common multiple of the degrees of the irreducible factors of $f(t)$ over K.

Now suppose K is the field with two elements, and let

$$\mathcal{P}_n = \{f(t) \in K[t] \mid f \text{ has degree } n \text{ and is irreducible over } K\}.$$

How many elements does the set $\mathcal{P}_9$ have?

Paper 1, Section II

18I Galois Theory

Let $f(t) = t^4 + bt^2 + ct + d$ be an irreducible quartic with rational coefficients. Explain briefly why it is that if the cubic $g(t) = t^3 + 2bt^2 + (b^2 - 4d)t - c^2$ has S_3 as its Galois group then the Galois group of $f(t)$ is S_4.

For which prime numbers p is the Galois group of $t^4 + pt + p$ a proper subgroup of S_4? [You may assume that the discriminant of $t^3 + \lambda t + \mu$ is $-4\lambda^3 - 27\mu^2$.]

Paper 2, Section II
16I Galois Theory

(a) Define what it means for a finite field extension L of a field K to be *separable.* Show that L is of the form $K(\alpha)$ for some $\alpha \in L$.

(b) Let p and q be distinct prime numbers. Let $L = \mathbb{Q}(\sqrt{p}, \sqrt{-q})$. Express L in the form $\mathbb{Q}(\alpha)$ and find the minimal polynomial of α over $\mathbb{Q}$.

(c) Give an example of a field extension $K \leqslant L$ of finite degree, where L is not of the form $K(\alpha)$. Justify your answer.

Paper 3, Section II
16I Galois Theory

(a) Let F be a finite field of characteristic p. Show that F is a finite Galois extension of the field F_p of p elements, and that the Galois group of F over F_p is cyclic.

(b) Find the Galois groups of the following polynomials:

(i) $t^4 + 1$ over F_3.

(ii) $t^3 - t - 2$ over F_5.

(iii) $t^4 - 1$ over F_7.

Paper 1, Section II
17I Galois Theory

(a) Let K be a field and let $f(t) \in K[t]$. What does it mean for a field extension L of K to be a *splitting field* for $f(t)$ over K?

Show that the splitting field for $f(t)$ over K is unique up to isomorphism.

(b) Find the Galois groups over the rationals $\mathbb{Q}$ for the following polynomials:

(i) $t^4 + 2t + 2$.

(ii) $t^5 - t - 1$.

Paper 4, Section II

17I Galois Theory

(a) State the Fundamental Theorem of Galois Theory.

(b) What does it mean for an extension L of $\mathbb{Q}$ to be *cyclotomic*? Show that a cyclotomic extension L of $\mathbb{Q}$ is a Galois extension and prove that its Galois group is Abelian.

(c) What is the Galois group G of $\mathbb{Q}(\eta)$ over $\mathbb{Q}$, where η is a primitive 7th root of unity? Identify the intermediate subfields M, with $\mathbb{Q} \leqslant M \leqslant \mathbb{Q}(\eta)$, in terms of η, and identify subgroups of G to which they correspond. Justify your answers.

Paper 2, Section II
16H Galois Theory

(a) Let $K \subseteq L$ be a finite separable field extension. Show that there exist only finitely many intermediate fields $K \subseteq F \subseteq L$.

(b) Define what is meant by a *normal* extension. Is $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{7}})$ a normal extension? Justify your answer.

(c) Prove Artin's lemma, which states: if $K \subseteq L$ is a field extension, H is a finite subgroup of $\mathrm{Aut}_K(L)$, and $F := L^H$ is the fixed field of H, then $F \subseteq L$ is a Galois extension with $\mathrm{Gal}(L/F) = H$.

Paper 3, Section II
16H Galois Theory

(a) Let L be the 13th cyclotomic extension of $\mathbb{Q}$, and let μ be a 13th primitive root of unity. What is the minimal polynomial of μ over $\mathbb{Q}$? What is the Galois group $\mathrm{Gal}(L/\mathbb{Q})$? Put $\lambda = \mu + \frac{1}{\mu}$. Show that $\mathbb{Q} \subseteq \mathbb{Q}(\lambda)$ is a Galois extension and find $\mathrm{Gal}(\mathbb{Q}(\lambda)/\mathbb{Q})$.

(b) Define what is meant by a *Kummer extension*. Let K be a field of characteristic zero and let L be the nth cyclotomic extension of K. Show that there is a sequence of Kummer extensions $K = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r$ such that L is contained in F_r.

Paper 1, Section II
17H Galois Theory

(a) Prove that if K is a field and $f \in K[t]$, then there exists a splitting field L of f over K. [You do not need to show uniqueness of L.]

(b) Let K_1 and K_2 be algebraically closed fields of the same characteristic. Show that either K_1 is isomorphic to a subfield of K_2 or K_2 is isomorphic to a subfield of K_1. [For subfields F_i of K_1 and field homomorphisms $\psi_i : F_i \to K_2$ with $i = 1, 2$, we say $(F_1, \psi_1) \leqslant (F_2, \psi_2)$ if F_1 is a subfield of F_2 and $\psi_2|_{F_1} = \psi_1$. You may assume the existence of a maximal pair (F, ψ) with respect to the partial order just defined.]

(c) Give an example of a finite field extension $K \subseteq L$ such that there exist $\alpha, \beta \in L \setminus K$ where α is separable over K but β is not separable over K.

Paper 4, Section II

17H Galois Theory

(a) Let $f = t^5 - 9t + 3 \in \mathbb{Q}[t]$ and let L be the splitting field of f over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to S_5. Let α be a root of f. Show that $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is neither a radical extension nor a solvable extension.

(b) Let $f = t^{26} + 2$ and let L be the splitting field of f over $\mathbb{Q}$. Is it true that $\mathrm{Gal}(L/\mathbb{Q})$ has an element of order 29? Justify your answer. Using reduction mod p techniques, or otherwise, show that $\mathrm{Gal}(L/\mathbb{Q})$ has an element of order 3.

[*Standard results from the course may be used provided they are clearly stated.*]

Paper 3, Section II

16F Galois Theory

Let $f \in \mathbb{Q}[t]$ be of degree $n > 0$, with no repeated roots, and let L be a splitting field for f.

(i) Show that f is irreducible if and only if for any $\alpha, \beta \in \text{Root}_f(L)$ there is $\phi \in \text{Gal}(L/\mathbb{Q})$ such that $\phi(\alpha) = \beta$.

(ii) Explain how to define an injective homomorphism $\tau : \text{Gal}(L/\mathbb{Q}) \to S_n$. Find an example in which the image of τ is the subgroup of S_3 generated by $(2\ 3)$. Find another example in which τ is an isomorphism onto S_3.

(iii) Let $f(t) = t^5 - 3$ and assume f is irreducible. Find a chain of subgroups of $\text{Gal}(L/\mathbb{Q})$ that shows it is a solvable group. [You may quote without proof any theorems from the course, provided you state them clearly.]

Paper 4, Section II

17F Galois Theory

(i) Prove that a finite solvable extension $K \subseteq L$ of fields of characteristic zero is a radical extension.

(ii) Let $x_1, \ldots, x_7$ be variables, $L = \mathbb{Q}(x_1, \ldots, x_7)$, and $K = \mathbb{Q}(e_1, \ldots, e_7)$ where e_i are the elementary symmetric polynomials in the variables x_i. Is there an element $\alpha \in L$ such that $\alpha^2 \in K$ but $\alpha \notin K$? Justify your answer.

(iii) Find an example of a field extension $K \subseteq L$ of degree two such that $L \neq K(\sqrt{\alpha})$ for any $\alpha \in K$. Give an example of a field which has no extension containing an 11th primitive root of unity.

Paper 2, Section II

17F Galois Theory

(i) State the fundamental theorem of Galois theory, without proof. Let L be a splitting field of $t^3 - 2 \in \mathbb{Q}[t]$. Show that $\mathbb{Q} \subseteq L$ is Galois and that $\text{Gal}(L/\mathbb{Q})$ has a subgroup which is not normal.

(ii) Let Φ_8 be the 8th cyclotomic polynomial and denote its image in $\mathbb{F}_7[t]$ again by Φ_8. Show that Φ_8 is not irreducible in $\mathbb{F}_7[t]$.

(iii) Let m and n be coprime natural numbers, and let $\mu_m = \exp(2\pi i/m)$ and $\mu_n = \exp(2\pi i/n)$ where $i = \sqrt{-1}$. Show that $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$.

Paper 1, Section II

17F Galois Theory

(i) Let $K \subseteq L$ be a field extension and $f \in K[t]$ be irreducible of positive degree. Prove the theorem which states that there is a 1-1 correspondence

$$\mathrm{Root}_f(L) \longleftrightarrow \mathrm{Hom}_K\left(\frac{K[t]}{\langle f\rangle}, L\right).$$

(ii) Let K be a field and $f \in K[t]$. What is a splitting field for f? What does it mean to say f is separable? Show that every $f \in K[t]$ is separable if K is a finite field.

(iii) The primitive element theorem states that if $K \subseteq L$ is a finite separable field extension, then $L = K(\alpha)$ for some $\alpha \in L$. Give the proof of this theorem assuming K is infinite.

Paper 4, Section II

18H Galois Theory

(i) Let G be a finite subgroup of the multiplicative group of a field. Show that G is cyclic.

(ii) Let $\Phi_n(X)$ be the nth cyclotomic polynomial. Let p be a prime not dividing n, and let L be a splitting field for Φ_n over $\mathbb{F}_p$. Show that L has p^m elements, where m is the least positive integer such that $p^m \equiv 1 \pmod{n}$.

(iii) Find the degrees of the irreducible factors of $X^{35}-1$ over $\mathbb{F}_2$, and the number of factors of each degree.

Paper 3, Section II

18H Galois Theory

Let L/K be an algebraic extension of fields, and $x \in L$. What does it mean to say that x is separable over K? What does it mean to say that L/K is separable?

Let $K = \mathbb{F}_p(t)$ be the field of rational functions over $\mathbb{F}_p$.

(i) Show that if x is inseparable over K then $K(x)$ contains a pth root of t.

(ii) Show that if L/K is finite there exists $n \geqslant 0$ and $y \in L$ such that $y^{p^n} = t$ and $L/K(y)$ is separable.

Show that Y^2+tY+t is an irreducible separable polynomial over the field of rational functions $K = \mathbb{F}_2(t)$. Find the degree of the splitting field of X^4+tX^2+t over K.

Paper 2, Section II

18H Galois Theory

Describe the Galois correspondence for a finite Galois extension L/K.

Let L be the splitting field of X^4-2 over $\mathbb{Q}$. Compute the Galois group G of $L/\mathbb{Q}$. For each subgroup of G, determine the corresponding subfield of L.

Let L/K be a finite Galois extension whose Galois group is isomorphic to S_n. Show that L is the splitting field of a separable polynomial of degree n.

Paper 1, Section II

18H Galois Theory

What is meant by the statement that L is a *splitting field* for $f \in K[X]$?

Show that if $f \in K[X]$, then there exists a splitting field for f over K. Explain the sense in which a splitting field for f over K is unique.

Determine the degree $[L : K]$ of a splitting field L of the polynomial $f = X^4 - 4X^2 + 2$ over K in the cases (i) $K = \mathbb{Q}$, (ii) $K = \mathbb{F}_5$, and (iii) $K = \mathbb{F}_7$.

Paper 4, Section II

18I Galois Theory

(i) Let $\zeta_N = \mathrm{e}^{2\pi i/N} \in \mathbb{C}$ for $N \geqslant 1$. For the cases $N = 11, 13$, is it possible to express ζ_N, starting with integers and using rational functions and (possibly nested) radicals? If it is possible, briefly explain how this is done, assuming standard facts in Galois Theory.

(ii) Let $F = \mathbb{C}(X, Y, Z)$ be the rational function field in three variables over $\mathbb{C}$, and for integers $a, b, c \geqslant 1$ let $K = \mathbb{C}(X^a, Y^b, Z^c)$ be the subfield of F consisting of all rational functions in X^a, Y^b, Z^c with coefficients in $\mathbb{C}$. Show that F/K is Galois, and determine its Galois group. [*Hint: For $\alpha, \beta, \gamma \in \mathbb{C}^\times$, the map $(X, Y, Z) \longmapsto (\alpha X, \beta Y, \gamma Z)$ is an automorphism of F.*]

Paper 3, Section II

18I Galois Theory

Let p be a prime number and F a field of characteristic p. Let $\mathrm{Fr}_p : F \to F$ be the Frobenius map defined by $\mathrm{Fr}_p(x) = x^p$ for all $x \in F$.

(i) Prove that Fr_p is a field automorphism when F is a finite field.

(ii) Is the same true for an arbitrary algebraic extension F of $\mathbb{F}_p$? Justify your answer.

(iii) Let $F = \mathbb{F}_p(X_1, \ldots, X_n)$ be the rational function field in n variables where $n \geqslant 1$ over $\mathbb{F}_p$. Determine the image of $\mathrm{Fr}_p : F \to F$, and show that Fr_p makes F into an extension of degree p^n over a subfield isomorphic to F. Is it a separable extension?

Paper 2, Section II

18I Galois Theory

For a positive integer N, let $\mathbb{Q}(\boldsymbol{\mu}_N)$ be the cyclotomic field obtained by adjoining all N-th roots of unity to $\mathbb{Q}$. Let $F = \mathbb{Q}(\boldsymbol{\mu}_{24})$.

(i) Determine the Galois group of F over $\mathbb{Q}$.

(ii) Find all $N > 1$ such that $\mathbb{Q}(\boldsymbol{\mu}_N)$ is contained in F.

(iii) List all quadratic and quartic extensions of $\mathbb{Q}$ which are contained in F, in the form $\mathbb{Q}(\alpha)$ or $\mathbb{Q}(\alpha, \beta)$. Indicate which of these fields occurred in (ii).

[Standard facts on the Galois groups of cyclotomic fields and the fundamental theorem of Galois theory may be used freely without proof.]

Paper 1, Section II

18I Galois Theory

(i) Give an example of a field F, contained in $\mathbb{C}$, such that X^4+1 is a product of two irreducible quadratic polynomials in $F[X]$. Justify your answer.

(ii) Let F be any extension of degree 3 over $\mathbb{Q}$. Prove that the polynomial X^4+1 is irreducible over F.

(iii) Give an example of a prime number p such that X^4+1 is a product of two irreducible quadratic polynomials in $\mathbb{F}_p[X]$. Justify your answer.

[Standard facts on fields, extensions, and finite fields may be quoted without proof, as long as they are stated clearly.]

Paper 4, Section II

18H Galois Theory

Let $F = \mathbb{C}(X_1, \ldots, X_n)$ be a field of rational functions in n variables over $\mathbb{C}$, and let $s_1, \ldots, s_n$ be the elementary symmetric polynomials:

$$s_j := \sum_{\{i_1,\ldots,i_j\} \subset \{1,\ldots,n\}} X_{i_1} \cdots X_{i_j} \in F \qquad (1 \leqslant j \leqslant n)\,,$$

and let $K = \mathbb{C}(s_1, \ldots, s_n)$ be the subfield of F generated by $s_1, \ldots, s_n$. Let $1 \leqslant m \leqslant n$, and $Y := X_1 + \cdots + X_m \in F$. Let $K(Y)$ be the subfield of F generated by Y over K. Find the degree $[K(Y) : K]$.

[Standard facts about the fields F, K and Galois extensions can be quoted without proof, as long as they are clearly stated.]

Paper 3, Section II

18H Galois Theory

Let $q = p^f$ $(f \geqslant 1)$ be a power of the prime p, and $\mathbb{F}_q$ be a finite field consisting of q elements.

Let N be a positive integer prime to p, and $\mathbb{F}_q(\boldsymbol{\mu}_N)$ be the cyclotomic extension obtained by adjoining all Nth roots of unity to $\mathbb{F}_q$. Prove that $\mathbb{F}_q(\boldsymbol{\mu}_N)$ is a finite field with q^n elements, where n is the order of the element q mod N in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ of the ring $\mathbb{Z}/N\mathbb{Z}$.

Explain why what is proven above specialises to the following fact: the finite field $\mathbb{F}_p$ for an odd prime p contains a square root of -1 if and only if $p \equiv 1 \pmod 4$.

[Standard facts on finite fields and their extensions can be quoted without proof, as long as they are clearly stated.]

Paper 2, Section II

18H Galois Theory

Let K, L be subfields of $\mathbb{C}$ with $K \subset L$.

Suppose that K is contained in $\mathbb{R}$ and L/K is a finite Galois extension of odd degree. Prove that L is also contained in $\mathbb{R}$.

Give one concrete example of K, L as above with $K \neq L$. Also give an example in which K is contained in $\mathbb{R}$ and L/K has odd degree, but is *not* Galois and L is not contained in $\mathbb{R}$.

[Standard facts on fields and their extensions can be quoted without proof, as long as they are clearly stated.]

Paper 1, Section II

18H Galois Theory

List all subfields of the cyclotomic field $\mathbb{Q}(\boldsymbol{\mu}_{20})$ obtained by adjoining all 20th roots of unity to $\mathbb{Q}$, and draw the lattice diagram of inclusions among them. Write all the subfields in the form $\mathbb{Q}(\alpha)$ or $\mathbb{Q}(\alpha, \beta)$. Briefly justify your answer.

[The description of the Galois group of cyclotomic fields and the fundamental theorem of Galois theory can be used freely without proof.]

Paper 1, Section II

18H Galois Theory

Let K be a field.

(i) Let F and F' be two finite extensions of K. When the degrees of these two extensions are equal, show that every K-homomorphism $F \to F'$ is an isomorphism. Give an example, with justification, of two finite extensions F and F' of K, which have the same degrees but are not isomorphic over K.

(ii) Let L be a finite extension of K. Let F and F' be two finite extensions of L. Show that if F and F' are isomorphic as extensions of L then they are isomorphic as extensions of K. Prove or disprove the converse.

Paper 2, Section II

18H Galois Theory

Let $F = \mathbb{C}(x, y)$ be the function field in two variables x, y. Let $n \geqslant 1$, and $K = \mathbb{C}(x^n + y^n, xy)$ be the subfield of F of all rational functions in $x^n + y^n$ and xy.

(i) Let $K' = K(x^n)$, which is a subfield of F. Show that K'/K is a quadratic extension.

(ii) Show that F/K' is cyclic of order n, and F/K is Galois. Determine the Galois group $\mathrm{Gal}(F/K)$.

Paper 3, Section II

18H Galois Theory

Let $n \geqslant 1$ and $K = \mathbb{Q}(\boldsymbol{\mu}_n)$ be the cyclotomic field generated by the nth roots of unity. Let $a \in \mathbb{Q}$ with $a \neq 0$, and consider $F = K(\sqrt[n]{a})$.

(i) State, without proof, the theorem which determines $\mathrm{Gal}(K/\mathbb{Q})$.

(ii) Show that $F/\mathbb{Q}$ is a Galois extension and that $\mathrm{Gal}(F/\mathbb{Q})$ is soluble. [When using facts about general Galois extensions and their generators, you should state them clearly.]

(iii) When $n = p$ is prime, list all possible degrees $[F : \mathbb{Q}]$, with justification.

Paper 4, Section II

18H Galois Theory

Let K be a field of characteristic 0, and let $P(X) = X^4 + bX^2 + cX + d$ be an *irreducible* quartic polynomial over K. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be its roots in an algebraic closure of K, and consider the Galois group $\mathrm{Gal}(P)$ (the group $\mathrm{Gal}(F/K)$ for a splitting field F of P over K) as a subgroup of S_4 (the group of permutations of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$).

Suppose that $\mathrm{Gal}(P)$ contains $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$.

(i) List all possible $\mathrm{Gal}(P)$ up to isomorphism. [*Hint: there are 4 cases, with orders 4, 8, 12 and 24.*]

(ii) Let $Q(X)$ be the *resolvent cubic* of P, i.e. a cubic in $K[X]$ whose roots are $-(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, $-(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$ and $-(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$. Construct a natural surjection $\mathrm{Gal}(P) \to \mathrm{Gal}(Q)$, and find $\mathrm{Gal}(Q)$ in each of the four cases found in (i).

(iii) Let $\Delta \in K$ be the discriminant of Q. Give a criterion to determine $\mathrm{Gal}(P)$ in terms of Δ and the factorisation of Q in $K[X]$.

(iv) Give a specific example of P where $\mathrm{Gal}(P)$ is abelian.

Paper 1, Section II

18H Galois Theory

Let $\mathbb{F}_q$ be a finite field with q elements and $\overline{\mathbb{F}}_q$ its algebraic closure.

(i) Give a non-zero polynomial $P(X)$ in $\mathbb{F}_q\,[X_1, \ldots, X_n]$ such that

$$P(\alpha_1, \ldots, \alpha_n) = 0 \qquad \text{for all } \alpha_1, \ldots, \alpha_n \in \mathbb{F}_q\,.$$

(ii) Show that every irreducible polynomial $P(X)$ of degree $n > 0$ in $\mathbb{F}_q[X]$ can be factored in $\overline{\mathbb{F}}_q[X]$ as $\big(X-\alpha\big)\big(X-\alpha^{q}\big)\big(X-\alpha^{q^2}\big)\cdots\big(X-\alpha^{q^{n-1}}\big)$ for some $\alpha \in \overline{\mathbb{F}}_q$. What is the splitting field and the Galois group of P over $\mathbb{F}_q$?

(iii) Let n be a positive integer and $\Phi_n(X)$ be the n-th cyclotomic polynomial. Recall that if K is a field of characteristic prime to n, then the set of all roots of Φ_n in K is precisely the set of all primitive n-th roots of unity in K. Using this fact, prove that if p is a prime number not dividing n, then p divides $\Phi_n(x)$ in $\mathbb{Z}$ for some $x \in \mathbb{Z}$ if and only if $p = an + 1$ for some integer a. Write down Φ_n explicitly for three different values of n larger than 2, and give an example of x and p as above for each n.

Paper 2, Section II

18H Galois Theory

(1) Let $F = \mathbb{Q}(\sqrt[3]{5}\,, \sqrt{5}\,, i)$. What is the degree of $F/\mathbb{Q}$? Justify your answer.

(2) Let F be a splitting field of $X^4 - 5$ over $\mathbb{Q}$. Determine the Galois group $\mathrm{Gal}(F/\mathbb{Q})$. Determine all the subextensions of $F/\mathbb{Q}$, expressing each in the form $\mathbb{Q}(x)$ or $\mathbb{Q}(x, y)$ for some $x, y \in F$.

[*Hint: If an automorphism ρ of a field X has order 2, then for every $x \in X$ the element $x + \rho(x)$ is fixed by ρ.*]

Paper 3, Section II

18H Galois Theory

Let K be a field of characteristic 0. It is known that soluble extensions of K are contained in a succession of cyclotomic and Kummer extensions. We will refine this statement.

Let n be a positive integer. The n-th cyclotomic field over a field K is denoted by $K(\boldsymbol{\mu}_n)$. Let ζ_n be a primitive n-th root of unity in $K(\boldsymbol{\mu}_n)$.

(i) Write $\zeta_3 \in \mathbb{Q}(\boldsymbol{\mu}_3)$, $\zeta_5 \in \mathbb{Q}(\boldsymbol{\mu}_5)$ in terms of radicals. Write $\mathbb{Q}(\boldsymbol{\mu}_3)/\mathbb{Q}$ and $\mathbb{Q}(\boldsymbol{\mu}_5)/\mathbb{Q}$ as a succession of Kummer extensions.

(ii) Let $n > 1$, and $F := K(\zeta_1, \zeta_2, \ldots, \zeta_{n-1})$. Show that $F(\boldsymbol{\mu}_n)/F$ can be written as a succession of Kummer extensions, using the structure theorem of finite abelian groups (in other words, roots of unity can be written in terms of radicals). Show that every soluble extension of K is contained in a succession of Kummer extensions.

Paper 4, Section II

18H Galois Theory

Let K be a field of characteristic $\neq 2, 3$, and assume that K contains a primitive cubic root of unity ζ. Let $P \in K[X]$ be an irreducible cubic polynomial, and let α, β, γ be its roots in the splitting field F of P over K. Recall that the Lagrange resolvent x of P is defined as $x = \alpha + \zeta\beta + \zeta^2\gamma$.

(i) List the possibilities for the group $\mathrm{Gal}(F/K)$, and write out the set $\{\sigma(x) \mid \sigma \in \mathrm{Gal}(F/K)\}$ in each case.

(ii) Let $y = \alpha + \zeta\gamma + \zeta^2\beta$. Explain why x^3, y^3 must be roots of a quadratic polynomial in $K[X]$. Compute this polynomial for $P = X^3 + bX + c$, and deduce the criterion to identify $\mathrm{Gal}(F/K)$ through the element $-4b^3 - 27c^2$ of K.

Paper 1, Section II

18H Galois Theory

Define a K-*isomorphism*, $\varphi : L \to L'$, where L, L' are fields containing a field K, and define $\mathrm{Aut}_K(L)$.

Suppose α and β are algebraic over K. Show that $K(\alpha)$ and $K(\beta)$ are K-isomorphic via an isomorphism mapping α to β if and only if α and β have the same minimal polynomial.

Show that $\mathrm{Aut}_K K(\alpha)$ is finite, and a subgroup of the symmetric group S_d, where d is the degree of α.

Give an example of a field K of characteristic $p > 0$ and α and β of the same degree, such that $K(\alpha)$ is not isomorphic to $K(\beta)$. Does such an example exist if K is finite? Justify your answer.

Paper 2, Section II

18H Galois Theory

For each of the following polynomials over $\mathbb{Q}$, determine the splitting field K and the Galois group G.

(1) $x^4 - 2x^2 - 25$.

(2) $x^4 - 2x^2 + 25$.

Paper 3, Section II

18H Galois Theory

Let $K = \mathbb{F}_p(x)$, the function field in one variable, and let $G = \mathbb{F}_p$. The group G acts as automorphisms of K by $\sigma_a(x) = x + a$. Show that $K^G = \mathbb{F}_p(y)$, where $y = x^p - x$.

[State clearly any theorems you use.]

Is K/K^G a separable extension?

Now let

$$H = \left\{ \begin{pmatrix} d & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_p, d \in \mathbb{F}_p^* \right\}$$

and let H act on K by $\begin{pmatrix} d & a \\ 0 & 1 \end{pmatrix} x = dx + a$. (The group structure on H is given by matrix multiplication.) Compute K^H. Describe your answer in the form $\mathbb{F}_p(z)$ for an explicit $z \in K$.

Is K^G/K^H a Galois extension? Find the minimum polynomial for y over the field K^H.

Paper 4, Section II

18H Galois Theory

(a) Let K be a field. State what it means for $\xi_n \in K$ to be a *primitive* nth root of unity.

Show that if ξ_n is a primitive nth root of unity, then the characteristic of K does not divide n. Prove any theorems you use.

(b) Determine the minimum polynomial of a primitive 10th root of unity ξ_{10} over $\mathbb{Q}$.

Show that $\sqrt{5} \in \mathbb{Q}(\xi_{10})$.

(c) Determine $\mathbb{F}_3(\xi_{10})$, $\mathbb{F}_{11}(\xi_{10})$, $\mathbb{F}_{19}(\xi_{10})$.

[*Hint: Write a necessary and sufficient condition on q for a finite field $\mathbb{F}_q$ to contain a primitive* 10*th root of unity.*]

1/II/18H **Galois Theory**

Find the Galois group of the polynomial $f(x) = x^4 + x^3 + 1$ over

(i) the finite field $\mathbf{F}_2$, (ii) the finite field $\mathbf{F}_3$,

(iii) the finite field $\mathbf{F}_4$, (iv) the field $\mathbf{Q}$ of rational numbers.

[Results from the course which you use should be stated precisely.]

2/II/18H **Galois Theory**

(i) Let K be a field, $\theta \in K$, and $n > 0$ not divisible by the characteristic. Suppose that K contains a primitive nth root of unity. Show that the splitting field of $x^n - \theta$ has cyclic Galois group.

(ii) Let L/K be a Galois extension of fields and ζ_n denote a primitive nth root of unity in some extension of L, where n is not divisible by the characteristic. Show that $\mathrm{Aut}(L(\zeta_n)/K(\zeta_n))$ is a subgroup of $\mathrm{Aut}(L/K)$.

(iii) Determine the minimal polynomial of a primitive 6th root of unity ζ_6 over $\mathbf{Q}$.

Compute the Galois group of $x^6 + 3 \in \mathbf{Q}[x]$.

3/II/18H **Galois Theory**

Let L/K be a field extension.

(a) State what it means for $\alpha \in L$ to be algebraic over K, and define its degree $\deg_K(\alpha)$. Show that if $\deg_K(\alpha)$ is odd, then $K(\alpha) = K(\alpha^2)$.

[You may assume any standard results.]

Show directly from the definitions that if α, $\beta \in L$ are algebraic over K, then so too is $\alpha + \beta$.

(b) State what it means for $\alpha \in L$ to be separable over K, and for the extension L/K to be separable.

Give an example of an inseparable extension L/K.

Show that an extension L/K is separable if L is a finite field.

4/II/18H **Galois Theory**

Let $L = \mathbf{C}(z)$ be the function field in one variable, $n > 0$ an integer, and $\zeta_n = e^{2\pi i/n}$.

Define $\sigma, \tau : L \to L$ by the formulae

$$(\sigma f)(z) = f(\zeta_n z), \qquad (\tau f)(z) = f(1/z),$$

and let $G = \langle \sigma, \tau \rangle$ be the group generated by σ and τ.

(i) Find $w \in \mathbf{C}(z)$ such that $L^G = \mathbf{C}(w)$.

[You must justify your answer, stating clearly any theorems you use.]

(ii) Suppose n is an odd prime. Determine the subgroups of G and the corresponding intermediate subfields M, with $\mathbf{C}(w) \subseteq M \subseteq L$.

State which intermediate subfields M are Galois extensions of $\mathbf{C}(w)$, and for these extensions determine the Galois group.

1/II/18F **Galois Theory**

Let $L/K/M$ be field extensions. Define the *degree* $[K : M]$ of the field extension K/M, and state and prove the tower law.

Now let K be a finite field. Show $\#K = p^n$, for some prime p and positive integer n. Show also that K contains a subfield of order p^m if and only if $m|n$.

If $f \in K[x]$ is an irreducible polynomial of degree d over the finite field K, determine its Galois group.

2/II/18F **Galois Theory**

Let $L = K(\xi_n)$, where ξ_n is a primitive nth root of unity and $G = \mathrm{Aut}(L/K)$. Prove that there is an injective group homomorphism $\chi : G \to (\mathbb{Z}/n\mathbb{Z})^*$.

Show that, if M is an intermediate subfield of $K(\xi_n)/K$, then M/K is Galois. State carefully any results that you use.

Give an example where G is non-trivial but χ is not surjective. Show that χ is surjective when $K = \mathbb{Q}$ and n is a prime.

Determine all the intermediate subfields M of $\mathbb{Q}(\xi_7)$ and the automorphism groups $\mathrm{Aut}(\mathbb{Q}\ (\xi_7)/M)$. Write the quadratic subfield in the form $\mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Q}$.

3/II/18F **Galois Theory**

(i) Let K be the splitting field of the polynomial $x^4 - 3$ over $\mathbb{Q}$. Describe the field K, the Galois group $G = \mathrm{Aut}(K/\mathbb{Q})$, and the action of G on K.

(ii) Let K be the splitting field of the polynomial $x^4 + 4x^2 + 2$ over $\mathbb{Q}$. Describe the field K and determine $\mathrm{Aut}(K/\mathbb{Q})$.

4/II/18F **Galois Theory**

Let $f(x) \in K[x]$ be a monic polynomial, L a splitting field for f, $\alpha_1, \ldots, \alpha_n$ the roots of f in L. Let $\triangle(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ be the *discriminant* of f. Explain why $\triangle(f)$ is a polynomial function in the coefficients of f, and determine $\triangle(f)$ when $f(x) = x^3 + px + q$.

Compute the Galois group of the polynomial $x^3 - 3x + 1 \in \mathbb{Q}[x]$.

1/II/18H **Galois Theory**

Let K be a field and f a separable polynomial over K of degree n. Explain what is meant by the Galois group G of f over K. Show that G is a transitive subgroup of S_n if and only if f is irreducible. Deduce that if n is prime, then f is irreducible if and only if G contains an n-cycle.

Let f be a polynomial with integer coefficients, and p a prime such that $\overline{f}$, the reduction of f modulo p, is separable. State a theorem relating the Galois group of f over $\mathbb{Q}$ to that of $\overline{f}$ over $\mathbb{F}_p$.

Determine the Galois group of the polynomial $x^5 - 15x - 3$ over $\mathbb{Q}$.

2/II/18H **Galois Theory**

Write an essay on ruler and compass construction.

3/II/18H **Galois Theory**

Let K be a field and m a positive integer, not divisible by the characteristic of K. Let L be the splitting field of the polynomial $X^m - 1$ over K. Show that $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$.

Now assume that K is a finite field with q elements. Show that $[L : K]$ is equal to the order of the residue class of q in the group $(\mathbb{Z}/m\mathbb{Z})^*$. Hence or otherwise show that the splitting field of $X^{11} - 1$ over $\mathbb{F}_4$ has degree 5.

4/II/18H **Galois Theory**

Let K be a field of characteristic different from 2.

Show that if L/K is an extension of degree 2, then $L = K(x)$ for some $x \in L$ such that $x^2 = a \in K$. Show also that if $L' = K(y)$ with $0 \neq y^2 = b \in K$ then L and L' are isomorphic (as extensions of K) if and only b/a is a square in K.

Now suppose that $F = K(x_1, \ldots, x_n)$ where $0 \neq x_i^2 = a_i \in K$. Show that F/K is a Galois extension, with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \leqslant n$. By considering the subgroups of $\mathrm{Gal}(F/K)$, show that if $K \subset L \subset F$ and $[L : K] = 2$, then $L = K(y)$ where $y = \prod_{i \in I} x_i$ for some subset $I \subset \{1, \ldots, n\}$.

1/II/18G **Galois Theory**

Let L/K be a field extension. State what it means for an element $x \in L$ to be *algebraic* over K. Show that x is algebraic over K if and only if the field $K(x)$ is finite dimensional as a vector space over K.

State what it means for a field extension L/K to be *algebraic*. Show that, if M/L is algebraic and L/K is algebraic, then M/K is algebraic.

2/II/18G **Galois Theory**

Let K be a field of characteristic 0 containing all roots of unity.

(i) Let L be the splitting field of the polynomial $X^n - a$ where $a \in K$. Show that the Galois group of L/K is cyclic.

(ii) Suppose that M/K is a cyclic extension of degree m over K. Let g be a generator of the Galois group and $\zeta \in K$ a primitive m-th root of 1. By considering the resolvent

$$R(w) = \sum_{i=0}^{m-1} \frac{g^i(w)}{\zeta^i}$$

of elements $w \in M$, show that M is the splitting field of a polynomial $X^m - a$ for some $a \in K$.

3/II/18G **Galois Theory**

Find the Galois group of the polynomial

$$x^4 + x + 1$$

over $\mathbb{F}_2$ and $\mathbb{F}_3$. Hence or otherwise determine the Galois group over $\mathbb{Q}$.

[*Standard general results from Galois theory may be assumed.*]

4/II/18G **Galois Theory**

(i) Let K be the splitting field of the polynomial

$$x^4 - 4x^2 - 1$$

over $\mathbb{Q}$. Show that $[K : \mathbb{Q}] = 8$, and hence show that the Galois group of $K/\mathbb{Q}$ is the dihedral group of order 8.

(ii) Let L be the splitting field of the polynomial

$$x^4 - 4x^2 + 1$$

over $\mathbb{Q}$. Show that $[L : \mathbb{Q}] = 4$. Show that the Galois group of $L/\mathbb{Q}$ is $C_2 \times C_2$.