16.3 Problem Sheet: Fields

1. Let F be a field of characteristic zero and let K be a field extension of F. Suppose that $n \in \mathbb{Z}_{>0}$ is such that every $\alpha \in K$ is a root of a polynomial of degree at most n in $F[x]$. Prove that $[K : F] \le n$.

2. Let $K = \mathbb{C}(t)$. Let $E = \mathbb{C}(t^2)$ and $F = \mathbb{C}(t^2 - t)$.

   (a) Find field automorphisms σ and τ of K such that σ fixes E, τ fixes F and such that $\sigma\tau$ is of infinite order.

   (b) Prove that $E \cap F = \mathbb{C}$.

3. Let $K = \mathbb{C}(t)$. Let n be a positive integer and let $u = t^n + t^{-n}$. Define automorphisms σ and τ of K by $\sigma(t) = \zeta t$ and $\tau(t) = t^{-1}$, where $\zeta = e^{\frac{2\pi i}{n}}$.

   (a) Prove that $\mathbb{C}(u)$ is fixed by both σ and τ.

   (b) Find the minimal polynomial for t over the field $\mathbb{C}(u)$.

   (c) Prove that K is a Galois extension of $\mathbb{C}(u)$.

4. Let F be a field. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$ be two polynomials in $F[x]$.

   (a) Prove that f and g are relatively prime if and only if there do not exist nonzero polynomials $p(x)$ and $q(x)$ in $F[x]$ with $p(x)f(x) = q(x)g(x)$ and $\deg p(x) < m$, $\deg q(x) < n$.

   (b) Prove that f and g are relatively prime if and only if the determinant of the following matrix is nonzero.

$$\begin{pmatrix}
1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
a_{n-1} & 1 & \ddots & \vdots & b_{m-1} & 1 & \ddots & \vdots \\
a_{n-2} & a_{n-1} & \ddots & 0 & b_{m-2} & b_{m-1} & \ddots & 0 \\
\vdots & \vdots & \ddots & 1 & \vdots & \vdots & \ddots & 1 \\
\vdots & \vdots & \ddots & a_{n-1} & \vdots & \vdots & \ddots & b_{m-1} \\
a_0 & a_1 & \ddots & \vdots & b_0 & b_1 & \ddots & \vdots \\
0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\
\vdots & \vdots & \ddots & a_1 & \vdots & \vdots & \ddots & b_1 \\
0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0
\end{pmatrix}$$

5. Determine the Galois group of the polynomial $x^4 + 4x^2 + 2$ over $\mathbb{Q}$.

6. Show that the following polynomials are irreducible in $\mathbb{Q}[x]$:

   (a) $x^2 - 12$

   (b) $8x^3 + 4399x^2 - 9x + 2$

   (c) $2x^{10} - 25x^3 + 10x^2 - 30$.

7. Determine all irreducible polynomials of degree ≤ 4 in $\mathbb{F}_2[x]$.

8. List all monic polynomials of degree ≤ 2 in $\mathbb{F}_3[x]$. Determine which of these are irreducible.
9. Let $f(x) = x^3 - 5$. Show that $f(x)$ does not factor into three linear polynomials with coefficients in $\mathbb{Q}[\sqrt[3]{5}]$.
10. (a) Find a degree four polynomial $f(x)$ in $\mathbb{Q}[x]$ which has $\sqrt{2} + \sqrt{3}$ as a root.
    (b) Find the degree of the field extension $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ of $\mathbb{Q}$. (Possible Hint: Any factor of $f(x)$ in $\mathbb{Q}[x]$ is also a factor of $f(x)$ in $\mathbb{C}[x]$, and we can list all these factors)
11. Show that if F is a finite field of characteristic 2, then the function $x \mapsto x^2$ is a bijection. Is the same true if we remove the assumption that F is finite?
12. Show that a finite field has order a power of a prime.
13. Show that there are infinitely many irreducible polynomials of any given positive degree in $\mathbb{Q}[x]$.
14. Let F be a field of characteristic p and let q be a power of p. Let $X = \{x \in F \mid x^q = x\}$. Prove that X is a subfield of F.
15. Let K/F be a field extension. Let $f(x) \in F[x]$ be a polynomial of degree n. Suppose it has n roots in K, called $\alpha_1, \ldots, \alpha_n$. The discriminant of f is defined to be
$$D = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$
    (a) If $n = 2$, how does this relate to the high school discriminant of a quadratic?
    (b) Prove that $D \in F$ if $n \leq 3$ (actually it's true for all n, feel free to try this if you want).
    (d) Let $n = 3$, ζ be a primitive cube root of 1 and $x = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$. Show that you can write x^3 in terms of the coefficients of f and $\sqrt{D}$.
    (d) Use this to produce a cubic formula (or at least show a cubic formula exists).
16. Let α be a complex root of the irreducible polynomial $x^3 - x + 4$. Find the inverse of $\alpha^2 + \alpha + 1$ in $\mathbb{Q}[\alpha]$ explicitly, in the form $a + b\alpha + c\alpha^2$, with $a, b, c \in \mathbb{Q}$.
17. Let F be a field, and α an element that generates a field extension of F of degree 5. Prove that α^2 generates the same extension.
18. Let a be a root of the polynomial $x^3 - x + 1$. Determine the minimal polynomial for $a^2 + 1$ over $\mathbb{Q}$.
19. (a) Let $a, b, c, d \in \mathbb{C}$ with $ad - bc \neq 0$. Prove that there exists an automorphism σ of $\mathbb{C}(z)$ with $\sigma(z) = \frac{az+b}{cz+d}$ (these are called Mobius transformations)
    (b) Determine the relationship between composition of Mobius transformations and matrix multiplication.
    (c) Show that the automorphisms $\sigma(t) = it$ and $\tau(t) = t^{-1}$ of $\mathbb{C}(t)$ generate a group G that is isomorphic to the dihedral group D_4.
    (d) Let $u = t^4 + t^{-4}$. Show that u is fixed under H.
    (e) What is $[\mathbb{C}(t) : \mathbb{C}(u)]$?
20. Let p be a prime. Determine the number of monic irreducible polynomials of degree two in $\mathbb{F}_p$. In particular, show that this number is positive and deduce that there exists a field with p^2 elements.

21. Let F be a field and let $a_1, a_2, \ldots, a_n$ be the roots of a polynomial $f \in F[x]$ of degree n. Prove that $[F[a_1, \ldots, a_n] : F] \le n!$.

22. Let R be an integral domain that contains a field F as a subring and is finite dimensional when viewed as a vector space over F. Prove that R is a field.

23. Let p be a prime number and let q be a power of p. Let K be a field extension of $\mathbb{F}_p$. Let L be a subfield of K with q elements.

    (a) Show that if $x \in L$ then $x^q = x$ (Think about the group of units of L).

    (b) Show that
    $$L = \{x \in K \mid x^q = x\}.$$
    (Hint: the number of roots of a polynomial is at most the degree)

    (c) Deduce that K has at exactly one subfield with q elements.

    (d) Show that any two fields with q elements are isomorphic?

24. Let $K = \mathbb{Q}[\sqrt[p]{n}, \zeta]$ where n is a positive integer that is not a p-th power, p is a prime, and $\zeta = e^{\frac{2\pi i}{p}}$.

    (a) Find $[K : \mathbb{Q}]$ (Hint: What are the degrees of the intermediate field extensions?).

    (b) Show that $|\mathrm{Aut}_{\mathbb{Q}}(K)| \le p(p-1)$.

    (c) Let $\alpha = \sqrt[p]{n} + \zeta$. Prove that $K = \mathbb{Q}[\alpha]$ (if it makes it simpler, assume n is large relative to p).

    (d) Write $K = E[\zeta]$ and $K = F[\sqrt[p]{n}]$ for some appropriate subfields E and F. Deduce the existence of automorphisms σ_i and τ of K such that
    $$\sigma_i(\sqrt[p]{n}) = \sqrt[p]{n}, \quad \sigma_i(\zeta) = \zeta^i$$
    and
    $$\tau(\sqrt[p]{n}) = \zeta\sqrt[p]{n}, \quad \tau(\zeta) = \zeta.$$

    (e) Show that the automorphism group of K is isomorphic to the group of invertible matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ where the entries are in $\mathbb{F}_p$.

25. Let E be a field. Let $\mathrm{Aut}(E)$ denote the group of all field isomorphisms $\varphi : E \to E$ with composition as multiplication. Let $H \subset \mathrm{Aut}(E)$ be a subgroup. Show that $E^H = \{e \in E \mid he = e \text{ for all } h \in H\}$ is a subfield of E.

26. Let $F = \mathbb{C}(w)$. Let $f(x) = x^4 - 4x^2 + 2 - w$.

    (a) Prove that $f(x)$ is irreducible in $F[x]$. [Hint: Gauss' Lemma]

    (b) Let $K = F[x]/(f(x))$. Prove that K is not a splitting field of f. [Hint: It may be easier to identify $w = t^4 + t^{-4}$ and identify F with the corresponding subfield of $\mathbb{C}(t)$, as here you can compute the roots of f explicitly]

27. Let K be a field. Let G be a finite group of automorphisms of K and let N be a normal subgroup of G. Let $L = K^N$ and $F = K^G$. Show how you can produce an injective homomorphism $G/N \hookrightarrow \mathrm{Aut}_F(L)$. Is this an isomorphism?

28. (a) Show that $\mathrm{Aut}(\mathbb{Q})$ is the trivial group.

(b) Show that $\mathrm{Aut}(\mathbb{R})$ is the trivial group.

29. Let $p_n = x^n + y^n + z^n$ (these are the power sum symmetric functions in x, y and z).

    (a) Write p_0, p_1 and p_2 in terms of the elementary symmetric functions of x, y and z.

    (b) Find a recurrence relation relating p_n to p_{n-1}, p_{n-2} and p_{n-3}.

    (c) Can every symmetric polynomial in x, y and z be written as a polynomial in $p_0, p_1, p_2, p_3, \ldots$?

30. Let F be a field and $\delta \in F$ an element that is not a square in F (i.e., there does not exist $\alpha \in F$ such that $\alpha^2 = \delta$). Show that

$$K = \{\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix} \mid a, b \in F\} \subset M_{2\times 2}(F)$$

is a field and that it is isomorphic to $F[\sqrt{\delta}] = F[x]/(x^2 - \delta)$.

31. Let $f(x) \in \mathbb{F}_p[x]$. For any polynomial $g(x) \in F[x]$, denote $r(g(x))$ to be the remainder after dividing $g(x)$ by $f(x)$.

    Suppose $f(x) = p_1(x)p_2(x)\cdots p_k(x)$ is the factorisation of f into irreducibles. Suppose the $p_i(x)$ are all monic and distinct. Let g be a polynomial whose degree is smaller than the degree of g. Prove the following are equivalent

    (a) $r(g(x^p)) = g(x)$.

    (b) $f(x)$ divides $\prod_{i=1}^{p}(g(x) - i)$

    (c) For each i with $1 \le i \le k$, there exists s_i such that $p_i(x)$ divides $g(x) - s_i$.

32. Let $F \subseteq \mathbb{C}$ be a field and suppose that $f \in F[x]$ is an irreducible (monic) quadratic polynomial. Let the roots of f be $\alpha, \beta \in \mathbb{C}$. Show that

    (a) $F(\alpha) = F(\alpha, \beta)$

    (b) $|\mathrm{Gal}(F(\alpha)/F)| = 2$, $F(\alpha)$ is a Galois extension of F, and the non-trivial element in $\mathrm{Gal}(F(\alpha)/F)$ permutes α and β.

33. (a) Show that if a and b are rational numbers with $(a+b\sqrt{2})^2 = 1+\sqrt{2}$, then $(a-b\sqrt{2})^2 = 1-\sqrt{2}$. Use this to show that $1 + \sqrt{2}$ is not a square in $\mathbb{Q}[\sqrt{2}]$.

    (b) Let $K = \mathbb{Q}[\sqrt{1+\sqrt{2}}]$. Find $[K : \mathbb{Q}]$.

    (c) Show that $K/\mathbb{Q}$ is not Galois. [Hint: If it were Galois, then the minimal polynomial of $\sqrt{1+\sqrt{2}}$ would have four roots in K. Find those roots. Are they real?] [Comment: $K/\mathbb{Q}[\sqrt{2}]$ is Galois and $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is Galois. This example shows that being Galois is not a transitive property of field extensions.]

34. The n-th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{1\le k\le n, \gcd(n,k)=1} (x - e^{2\pi i k/n}).$$

A priori this lies in $\mathbb{C}[x]$ though we will prove a more precise result below. (Off topic aside: Although is is not experimentally clear, every integer appears as a coefficient of some cyclotomic polynomial.)

(a) If p is prime, show that $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$. Can you find a similar formula for Φ_n when n is a power of a prime?

(b) Prove that
$$\prod_{d|n} \Phi_d(x) = x^n - 1$$
and use this to show by induction on n that $\Phi_n(x) \in \mathbb{Q}[x]$. (Actually it lies in $\mathbb{Z}[x]$ and we know how to prove that too)

(c) Factor $\Phi_{12}(x)$ into irreducibles in $\mathbb{R}[x]$.

(d) Prove that $\Phi_{12}(x)$ is irreducible in $\mathbb{Q}[x]$. (A more general fact is that $\Phi_n(x)$ is always irreducible in $\mathbb{Q}[x]$)

(e) Show that the Galois group of $\Phi_{12}(x)$ over $\mathbb{Q}$ is the Klein Four group.

(f) Let p be a prime number with $p \equiv 1 \pmod{n}$. Prove that $\Phi_n(x)$ factors into linear factors in $\mathbb{F}_p[x]$. (Possible hint: From a previous tutorial, we know the multiplicative group of a finite field is cyclic)

35. (a) Let $GL_n(\mathbb{F}_q)$ be the group of invertible $n \times n$ matrices with entries in the field $\mathbb{F}_q$ with q elements. Prove that
$$|GL_n(\mathbb{F}_q)| = \prod_{i=1}^{n} (q^n - q^{i-1})$$

(b) Can you find a formula for $|SL_n(\mathbb{F}_q)|$? ($SL_n(\mathbb{F}_q)$ is the group of $n \times n$ matrices with determinant 1) [Hint: The determinant is a group homomorphism]

(c) Let q be a power of the prime p. Show that the subgroup of upper-triangular matrices with 1's along the diagonal is a Sylow-p-subgroup of both $GL_n(\mathbb{F}_q)$ and $SL_n(\mathbb{F}_q)$.

(d) Show that every finite group is isomorphic to a subgroup of $GL_n(\mathbb{F}_q)$ for some n. [Hint: permutation matrices] [Off topic aside: There exist infinite groups that are not subgroups of $GL_n(F)$ for any field F and any n]

36. Let H be a subgroup of G. Let P be a Sylow-p-subgroup of G. (recall this means that $|P|$ is a power of p and $|G|/|P|$ is not divisible by p) Consider the action of H on G/P. Show that there exists an orbit whose size is not divisible by p.

(a) Show that every stabiliser in the H-action on G/P is conjugate to a subgroup of P, hence has order a power of p.

(b) Combine the previous results to show that H has a Sylow-p-subgroup, hence proving the first Sylow Theorem.

37. Let $F = \mathbb{Q}(\sqrt[4]{2}, i)$.

(a) Prove that F is a Galois field extension of $\mathbb{Q}$

(b) Compute $[F : \mathbb{Q}]$.

(c) Show that there exists $\tau \in \mathrm{Gal}_{\mathbb{Q}}(F)$ such that $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\tau(i) = i$. (Hint: Any automorphism must send $\sqrt[4]{2}$ to a root of $x^4 - 2$ and i to a root of $x^2 + 1$. How many possibilities does this provide and what is the size of the Galois group?).

(d) Show that the Galois group $\mathrm{Gal}_{\mathbb{Q}}(F)$ is isomorphic to the dihedral group D_4.

(e) Find the intermediate fields between $\mathbb{Q}$ and F. (have a look at Q4(b) if needed).

38. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic with three complex roots $\alpha_1, \alpha_2, \alpha_3$. Let $D = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$. Let G be the Galois group of f, thought of as a subgroup of S_3.
    (a) Show that if $\sigma \in G$ then
    $$\sigma(D) = \mathrm{sgn}(\sigma)D$$
    (Here sgn is the sign of a permutation).
    (a) Show that G is a subgroup of the alternating group A_3 if and only if $D \in \mathbb{Q}$.
    (b) Generalise this to give a criterion for when a Galois group is a subgroup of A_n for any n.

39. Up to isomorphism, there are five transitive subgroups of S_4. They are the cyclic group C_4, the Klein four group $C_2 \times C_2$, the dihedral group D_4, the alternating group A_4 and the symmetric group S_4.
    (a) Convince yourself you are aware of these groups.
    (b) Let E/F be a degree four separable field extension. Is it always the case that there exists a field $F \leq G \leq E$ with $[G : F] = 2$? Hint: Let K be the Galois closure of E (so if E is given by adjoining a root of a quartic polynomial $f(x)$, then K is the splitting field of f). Look at the list of five possibilities for $\mathrm{Gal}(K/F)$, each of which can occur. (Please assume that each of these can occur in order to solve this question, or prove it!)]

40. Let F be a field. Let G be the set of functions $f : F \to F$ of the form $f(x) = ax + b$ where $a, b \in F$ with $a \neq 0$.
    (a) Show that G is a group with the group multiplication being composition of functions (sometimes this is called the $ax + b$ group).
    (b) If F is a finite field with q elements, find $|G|$. (If $q = 5$, this gives an explicit construction of a transitive subgroup of S_5 with 20 elements).
    (c) Let $f(x) = x^5 - 2$. Find the Galois group of f over $\mathbb{Q}$.

41. Let V be a vector space over a field F. Let G be a finite group which acts linearly on V (this means that $g(\lambda v) = \lambda(gv)$ and $g(v + w) = v + w$ for all $\lambda \in F, v, w \in V$, in addition to the axioms of a group axiom $1v = v$ and $(gh)v = g(hv)$.)
    (a) Suppose that $|G| \neq 0$ in F. Let $x \in V$. Prove that $gx = x$ for all $g \in G$ if and only if there exists $y \in V$ such that
    $$x = \frac{1}{|G|} \sum_{g \in G} gy.$$
    (b) Let $F = \mathbb{Q}$ and $V = \mathbb{Q}(\sqrt[4]{2}, i)$. Let s denote complex conjugation and r the field automorphism of V with $r(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $r(i) = i$. Use the previous formula with $y = \sqrt[4]{2}$ to come up with elements of V fixed by the order two subgroups $< rs >$ and $< r^3 s >$.
    (c) Find the minimal polynomials over $\mathbb{Q}$ of the elements you found in the previous part.

42. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^4 - 2$, including their automorphisms.

43. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^5 - 1$, including their automorphisms.

44. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^3 - 1$, including their automorphisms.

45. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^3 - 7$, including their automorphisms.

46. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^4 - X^2 - 2$, including their automorphisms.

47. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^2 - 2$, including their automorphisms.

48. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^2 - 5X + 6$, including their automorphisms.

49. Analyze the poset of fields between $\mathbb{F}_2$ and the splitting field of $X^3 + X + 1$, including their automorphisms.

50. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^4 - 4X^2 - 5$, including their automorphisms.

51. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^3 - 56$, including their automorphisms.

52. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^2 - 3$, including their automorphisms.

53. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^2 - 2X - 2$, including their automorphisms.

54. Show that
$$\mathbb{Q}(\sqrt{2}, \sqrt{3}\sqrt{5})$$
is a Galois extension of $\mathbb{Q}$ and analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $\mathbb{Q}(\sqrt{2}, \sqrt{3}\sqrt{5})$, including their automorphisms.

55. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^4 - 1$, including their automorphisms.

56. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^3 - 2$, including their automorphisms.

57. Analyze the poset of fields between $\mathbb{Q}$ and the splitting field of $X^4 + 1$, including their automorphisms.

58. Show that the only continuous automorphisms of $\mathbb{C}$ are the identity and complex conjugation.

59. Let $\varphi \colon \mathbb{R} \to \mathbb{R}$ be an automorphism of $\mathbb{R}$.
    (a) Show that if $x > 0$ then $\varphi(x) > 0$.
    (b) Show that if $x > y$ then $\varphi(x) > \varphi(y)$.
    (c) Prove that $\mathrm{Aut}(\mathbb{R})$ is $\{\mathrm{id}\}$.

60. Show that $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$.

61. Let $\mathbb{F}$ be a field, $f \in \mathbb{F}[X]$ and $\mathbb{E} \supseteq \mathbb{F}$ a splitting field for f. Let $g \in \mathbb{F}[x]$ be irreducible and such that g divides f. Let $ab \in \mathbb{E}$ be two roots of g. Show that there exists and automorphism of $\mathbb{E}$ sending a to b.

62. Let $\mathbb{F} \subseteq \mathbb{C}$ be a field and suppose that $f \in \mathbb{F}[X]$ is an irreducible quadratic. Let the roots of f be $a, b \in \mathbb{C}$. Show that $\mathbb{F}(a) = \mathbb{F}(a, b)$ and $|\mathrm{Gal}(\mathbb{F}(a), \mathbb{F})| = 2$ and the nontrivial element in $\mathrm{Gal}(\mathbb{F}(a)/\mathbb{F})$ interchanges a and b.

63. Let $\mathbb{E} \supseteq \mathbb{F}$, $f \in \mathbb{F}[X]$ and $\varphi \in \mathrm{Aut}(\mathbb{E})$ and $\mathbb{F}$-automorphism. Show that if $a \in \mathbb{E}$ is a root of f then $\varphi(a)$ is also a root of f.

64. Let $\mathbb{E} \supseteq \mathbb{F}$, $f \in \mathbb{F}[X]$ and $\varphi \in \mathrm{Aut}(\mathbb{E})$ and $\mathbb{F}$-automorphism. Show that $\varphi(a)$ permutes the roots of f.

65. Let $\mathbb{E}$ be a field and let H be a subgroup of $\mathrm{Aut}(\mathbb{E})$. Show that $\mathbb{E}^H$ is a subfield of $\mathbb{E}$.

66. Show that if E is a finite filed of order p^n and $d \in \mathbb{Z}_{>0}$ divides n then E has exactly one subfield of order p^d.

67. Let F be a finite filed with p^n elements. Write down a polynomial in $F[X]$ that has no roots in F. Conclude that no finite field is algebraically closed.

68. Show that if $f \in \mathbb{F}_p[X]$ and if u is a root of f in some extension of $\mathbb{F}_p$ then u^p is also a root of f in that extension.

69. Let F be a field of size $q = p^n$. Show that every irreducible polynomial in $\mathbb{F}_p[X]$ of degree n is a factor of $X^q - X \in \mathbb{F}_p[X]$.

70. Show that if $\psi\colon E \to F$ is a (ring) homomorphism from one field to another and $\ker(\psi) \neq E$ then $\psi(1) = 1$.

71. Let $\mathbb{F}_4$ be the field containing 4 elements. Write out the addition and multiplication tables for $\mathbb{F}_4$.

72. Give an example of two infinite fields that have the same cardinality but are not isomorphic.

73. Show that if $p \in \mathbb{Z}_{\geq 0}$ is prime and $n \in \mathbb{Z}_{\geq 1}$ then there exists an irreducible polynomial of degree n.

74. Give an example of an infinite field whose characteristic is not zero.

75. Suppose that E and K are two extensions of F and let $a \in E$ and $b \in K$ be algebraic over F. Prove that $m_{a,F} = m_{b,F}$ if and only if there exists an isomorphism $\varphi\colon F(a) \to F(b)$ such that $\varphi(a) = b$ and $\varphi|_F = \mathrm{id}_F$.

76. Let $E = \{a \in R \mid a \text{ is algebraic over } \mathbb{Q}\}$. Show that E is an algebraic extension of $\mathbb{Q}$ but is not a finite extension of $\mathbb{Q}$.

77. Show that the set of algebraic numbers (over $\mathbb{Q}$) in $\mathbb{R}$ forms a subfield of $\mathbb{R}$.

78. Let F be a field and let $k \in F$ such that k is not a square in F. Show that the subset of $M_{2\times 2}(F)$ given by
$$K = \left\{ \begin{pmatrix} a & kb \\ b & a \end{pmatrix} \mid a, b \in F \right\}$$
is a field and that it is isomorphic to $F(\sqrt{k})$.

79. Find the dimension and a basis for $\mathbb{R}(\sqrt{2}+i)$ over $\mathbb{R}$.

80. Find the dimension and a basis for $\mathbb{Q}(\sqrt{2}+i)$ over $\mathbb{Q}$.

81. Find the dimension and a basis for $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$.

82. Find the dimension and a basis for $\mathbb{Q}(\sqrt{3},i)$ over $\mathbb{Q}$.

83. Show that $2^{\frac{1}{3}}$ is algebraic over $\mathbb{Q}$ and find the minimal polynomial.

84. Show that $\sqrt{3}+\sqrt{2}$ is algebraic over $\mathbb{Q}$ and find the minimal polynomial.

85. Show that $\frac{1}{2}(\sqrt{5}+1)$ is algebraic over $\mathbb{Q}$ and find the minimal polynomial.

86. Show that $\frac{1}{2}(\sqrt{3}-1)$ is algebraic over $\mathbb{Q}$ and find the minimal polynomial.

87. Find $m_{a,\mathbb{Q}}$ and $\dim_{\mathbb{Q}}(\mathbb{Q}(a))$ for $a=\sqrt{3-\sqrt{6}}$. Don't forget to prove that your answer for $m_{a,\mathbb{Q}}$ is an irreducible polynomial in $\mathbb{Q}[X]$.

88. Find $m_{a,\mathbb{Q}}$ and $\dim_{\mathbb{Q}}(\mathbb{Q}(a))$ for $a=\sqrt{(\frac{1}{3})+\sqrt{7}}$. Don't forget to prove that your answer for $m_{a,\mathbb{Q}}$ is an irreducible polynomial in $\mathbb{Q}[X]$.

89. Find $m_{a,\mathbb{Q}}$ and $\dim_{\mathbb{Q}}(\mathbb{Q}(a))$ for $a=\sqrt{2}+i$. Don't forget to prove that your answer for $m_{a,\mathbb{Q}}$ is an irreducible polynomial in $\mathbb{Q}[X]$.

90. Show that every finite extension is algebraic.

91. Show that p is irreducible.

92. Let F be a field and $D\colon F[X]\to F[X]$ the map given by

$$D(a_0+a_1X+\cdots+a_nX)=a_1+2a_2X+\cdots na_nX^{n-1}.$$

   (a) (a)] Show that $D(fg)=D(f)g+fD(g)$.
   (b) Suppose that $f\in F[X]$ is irreducible. Show that if $D(f)\neq 0$ then f has no multiple root in any extension field of F.
   (c) Show that if F has characteristic 0 and $f\in F[X]$ is irreducible then f has no repeated roots.

93. Let $K=\mathbb{Q}[\sqrt[6]{2},e^{\frac{\pi i}{3}}]$. Find $[K:\mathbb{Q}]$.

94. Let $K=\mathbb{Q}[\sqrt[6]{2},e^{\frac{\pi i}{3}}]$. Prove that K is a Galois extension of $\mathbb{Q}$.

95. Let $K=\mathbb{Q}[\sqrt[6]{2},e^{\frac{\pi i}{3}}]$. Show that there exists an element $\sigma\in\mathrm{Gal}_{\mathbb{Q}}(K)$ such that

$$\sigma(\sqrt[6]{2})=e^{\frac{\pi i}{3}}\sqrt[6]{2}\qquad\text{and}\qquad\sigma(e^{\frac{\pi i}{3}})=e^{\frac{\pi i}{3}}.$$

96. Let $K=\mathbb{Q}[\sqrt[6]{2},e^{\frac{\pi i}{3}}]$. Let γ be such that $\mathbb{Q}[\gamma]$ is the inteermediate field between K and $\mathbb{Q}$ that corresponds to the cyclic subgroup generated by σ under the main theorem of Galois theory. Is $\mathbb{Q}[\gamma]$ a Galois extension of $\mathbb{Q}$?

97. Let $f=x(x-1)(x-2)+(x+1)(x+2)$. Determine whether or not $\mathbb{F}_5[x]/f\mathbb{F}_5[x]$ is a field.

98. For which $c \in \mathbb{F}_5$ does the equation $y^2 - c = 0$ have a solution in $\mathbb{F}_5[x]/f\mathbb{F}_5[x]$.

99. Let $f = x^3 + x^2 + x + 2$.
    (a) Prove that $\mathbb{F}_3[x]/f\mathbb{F}_3[x]$ is a field.
    (b) For which $c \in \mathbb{F}_3$ does the equation $y^2 - c$ have a solution in $\mathbb{F}_3[x]/f\mathbb{F}_3[x]$?

100. Let $K = \mathbb{C}(t)$. Define automorphisms σ and τ of K by $\sigma(t) = 1 - t$ and $\tau(t) = \frac{1}{t}$. Let

$$w = \frac{(t^2 - t + 1)^3}{t^2(t-1)^2} \qquad \text{and} \qquad F = \mathbb{C}(w).$$

    (a) Prove that $\sigma(w) = w$ and $\tau(w) = w$.
    (b) Find a polynomial $f \in F[x]$ of degree 6 which has t as a root. What are the other 5 roots of f in K?
    (c) Let G be the group generated by the automorphisms σ and τ. Prove that $F = K^G$. You may use without proof that $G \cong S_3$, the symmetric group on 3 letters.
    (d) How many fields are there with $F \subseteq E \subseteq K$?
    (e) How many of the fields from part (d) are Galois extensions of F?

101. Recall the definition of the Frobenius homomorphism and explicitly describe its action on $\mathbb{F}_4$ and $\mathbb{F}_8$ element by element.

102. For each element of $\mathbb{F}_4$ and $\mathbb{F}_8$ determine its irreducible polynomial over $\mathbb{F}_2$.

103. What is $\sin(30°)$?

104. The triple angle formula for $\sin\theta$ is $\sin(3\theta) = 3\sin(\theta) - 4\sin(\theta)^3$. Use this formula to decide (with proof) whether it is possible to trisect a $30°$ angle using compass and straightedge.

105. Let $F \subseteq K$ be a field extension and let $a \in K$. Under which condition do we call a algebraic over F? Under which condition do we call a transcendental over F?

106. Let $F \subseteq K$ be a field extension and let $a \in K$. Assume that a is algebraic over F. What is the definition of the irreducible polynomial of a over F?

107. Let $F \subseteq K$ be a field extension and let $a \in K$. Assume that F and K are finite fields. Determine (with proof) whether a is algebraic or transcendental.

108. What is the dimension of $\mathbb{C}$ over $\mathbb{Q}$?

109. Let K be a field. What is the definition of the characteristic of K?

110. Let $F \subseteq K$ be a field extension. Prove that $\mathrm{char}(F) = \mathrm{char}(K)$.

111. Prove that finite fields have prime power order.

112. Recall the construction of the field $E = \mathbb{Q}(\sqrt[4]{2})$.

113. Let F be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Decide whether $E = \mathbb{Q}(\sqrt[4]{2})$ is equal to F.

114. Let F be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Identify the automorphism group of F over $\mathbb{Q}$.

115. State the four equivalent definitions of a Galois extension and prove that they are equivalent.

116. Let F be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Prove that F is a Galois extension of $\mathbb{Q}$.

117. Let F be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Write down the Galois correspondence, including automorphism groups, for F over $\mathbb{Q}$.

118. Let $F \subseteq K$ be a Galois extension. How exactly does the Galois coresspondence relate intemediate field extensions with subgroups of the Galois group?

119. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Find the irreducible polynomial of ζ_6 over $\mathbb{Q}$.

120. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Find the irreducible polynomial of ζ_9 over $\mathbb{Q}$.

121. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Find the irreducible polynomial of ζ_6 over $\mathbb{Q}(\zeta_3)$.

122. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Find the irreducible polynomial of ζ_9 over $\mathbb{Q}(\zeta_3)$.

123. Let E and F be fields with $E \supseteq F$ and let $a \in E$ such that $\deg(a, F) = 7$. Show that $F(a) = F(a^3)$.

124. Let $E \supseteq \mathbb{F}_3$ be an extension and let $f = x^2 + 1 \in \mathbb{F}_3[x]$.
    (a) Let $a \in E$ be a root of F. Find a basis $\mathcal{B}$ for the extension $\mathbb{F}_3(a) \supseteq \mathbb{F}_3$ considered as a vector space over $\mathbb{F}_3$. What is the cardinatlity of $\mathbb{F}_3(a)$?
    (b) Using your result from (a) write down the elements of the field $\mathbb{F}_9$ (in terms of the basis $\mathcal{B}$.
    (c) Find a generator for the group $\mathbb{F}_9(a)^\times$.

125. Let $f = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ and let E be the splitting field of f over $\mathbb{Q}$.
    (a) State the fundamental Theorem of Galois theory.
    (b) Show that $[E : \mathbb{Q}] = 4$.
    (c) Find the Galois group $\mathrm{Gal}(E/\mathbb{Q})$.
    (d) Describe explicitly the intermediate fields $\mathbb{Q} \subseteq L \subseteq E$ and the Galois correspondence between the set of subgroups of $\mathrm{Gal}(E/\mathbb{Q})$ and the set of intermediate fields.
    (e) Specify β such that $E = \mathbb{Q}(\beta)$.

126. Find a basis of $\mathbb{Q}(i, 2^{1/3})$ as a vector space over $\mathbb{Q}$.

127. Let $f = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$. Give an explicit description of a field E that contains $\mathbb{F}_2$ and an element $a \in E$ that is a root of f.

128. Let $g \in \mathbb{Q}[X]$ be irreducible and let $n = \deg(g)$. Let $a \in \mathbb{C}$ be a root of g. Show that there are exactly n injective ring homomorphisms $\mathbb{Q}(a) \to \mathbb{C}$.

129. Let $p, n \in \mathbb{Z}_{>0}$ with p prime. Given that there exists a field of size p^n show that there is an irreducible polynomial of degree n in $\mathbb{F}_p[X]$.

130. Let F be a.finite field. Show that F is not algebraically closed.

131. Let E be a finite field and let F_1 and F_2 be subfields of E. Show that if $|F_1| = |F_2|$ then $F_1 = F_2$.

132. Let E and F be fields with $E \supseteq F$. Define the Galois group of the extension.

133. State the fundamental theorem of Galois theory.

134. Let F be a field and let $E \supseteq F$ be an extension with $[E : F] = 2$. Prove that E is a Galois extension of F.

135. Give an example of a finite extension E of $\mathbb{Q}$ that is not Galois.

136. Let $f = x^4 + 1 \in \mathbb{Q}[X]$ and let $E \subseteq \mathbb{C}$ be the splitting field of f over $\mathbb{Q}$ and let $F = \mathbb{Q}(i)$.

   (i) Show that $E \supseteq F$.
   (ii) Find $E : F]$.
   (iii) Find the Galois group $G = G(E/F)$.
   (iv) List all subfields of E that contain F and for each give the corresponding subgroup of G.

137. Let $f = x^4 + 1 \in \mathbb{Q}[X]$ and let $E \subseteq \mathbb{C}$ be the splitting field of f over $\mathbb{Q}$ and let $F = \mathbb{Q}(i)$.

   (i) Show that complex conjugation induces a $\mathbb{Q}$-automorphism of E.
   (ii) Denote by $\tau \in G(E/\mathbb{Q})$ the autormorphism from (i). Show that the subgroup of $G(E/Q)$ generated by τ is not normal in $G(E/Q)$.

138. Let $p \in \mathbb{Z}_{>0}$ be prime, let $n \in \mathbb{Z}_{>0}$ and let $\mathbb{F}$ be a finite field of size p^n.

   (a) Show that the map $\varphi\colon \mathbb{F} \to \mathbb{F}$ given by $\varphi(x) = x^p$ is an isomorphism.
   (b) Show that φ has order n.
   (c) Show that every automorphism of $\mathbb{F}$ is a power of φ.

139. Define what it means to say that an element $a \in \mathbb{E} \supseteq \mathbb{F}$ is algebraic over $\mathbb{F}$.

140. Determine the irreducible polynomial $\mathrm{irr}(a, \mathbb{F})$ for $a = \sqrt{3} + \sqrt{5}$, where $\mathbb{F} = \mathbb{Q}$.

141. Determine the irreducible polynomial $\mathrm{irr}(a, \mathbb{F})$ for $a = \sqrt{3} + \sqrt{5}$, where $\mathbb{F} = \mathbb{Q}(\sqrt{15})$.

142. Let R be an integral domain and let $\mathbb{F} \subseteq R$ be a subfield of R. Show that if R is finite dimension as a vector space over $\mathbb{F}$ then R is a field.

143. Let $\zeta = e^{2\pi i/7}$.

   (a) What is the irreducible polynomial $f = \mathrm{irr}(\zeta, \mathbb{Q})$ of ζ over $\mathbb{Q}$?
   (b) Show that $\mathbb{E} = \mathbb{Q}(\zeta)$ is the splitting field of f over $\mathbb{Q}$.
   (c) Show that the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is cyclic.
   (d) List all intermediate fields $\mathbb{F}$ with $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{Q}(\zeta)$ and for each give the group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

144. Let $\mathbb{K} = \mathbb{Q}(\omega, \sqrt{5})$, where $\omega = e^{2\pi i/3}$.

   (a) Find a basis for $\mathbb{K}$ over $\mathbb{Q}$.
   (b) Show that $\mathbb{K}$ is a Gaois extension of $\mathbb{Q}$ and describe the Galois group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.
   (c) Let $\beta = \omega + \sqrt{5} \in \mathbb{K}$. Compute the orbit of β under the action of G on K.
   (d) Use your answer to part (c) to write down $\mathrm{irr}(\beta, \mathbb{Q})$, the irreducible polynomial of β over $\mathbb{Q}$.

145. Let $\mathbb{F}$ be a field and $\mathbb{E} \supseteq \mathbb{F}$ an extension field. Let φ be an automorphism of $\mathbb{E}$ satsifying $\varphi(x) = x$ for all $x \in \mathbb{F}$. Show that if $a \in \mathbb{E}$ is a root of $f \in \mathbb{F}[X]$ then $\varphi(a)$ is a root of f.

146. Let $f \in \mathbb{Q}[X]$ be irreducible with $\deg(f) = 3$ and let $\mathbb{E} \subseteq \mathbb{C}$ be the splitting field of f.
   (i) Show that the Galois group $G(\mathbb{E}/Q)$ is isomorhpic to S_3 or C_3.
   (ii) Show that if f has a root that is not real then $G(\mathbb{E}/\mathbb{Q}) \cong S_3$.
147. State the Fundamental theorem of Galois theory.
148. Let $f = X^7 - 1 \in \mathbb{Q}[X]$ and let $\mathbb{E} \subseteq \mathbb{C}$ be the splitting field of f.
   (i) Find the Galois group G of $\mathbb{E}$.
   (ii) List all subfields of $\mathbb{E}$ and for each give the corresponding subgroup of G.
   (iii) For each subfield of $\mathbb{E}$ give a primitive element.
   (iv) Which subfields of $\mathbb{E}$ are Galois extensions of $\mathbb{Q}$?
149. Define the degree of a field extension $\mathbb{E} \supseteq \mathbb{F}$ and determine the degree of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$.
150. Let L be a finite extension of a field K and let $f \in K[x]$ be an irreducible polynomial over K of degree at least 2. Show that if $[L : K]$ and $\deg(f)$ are coprime then f has no root in L.
151. Explain why it is not possible to construct (with straight-edge and compass) a line segment whose length is $2^{1/3}$.
152. Let F be a field. Define the term *splitting field* of a polynomial $f \in F[x]$.
153. Let F be a field. Let $f \in F[x]$. Show that a splitting field of f exists.
154. Show that $\mathbb{Q}(5^{1/3})$ is not the splitting field of any polynomial over $\mathbb{Q}$.
155. State the main theorem of Galois theory.
156. Let $E = \mathbb{Q}(2^{1/3}, e^{2\pi i/3})$.
   (i) Show that E is a Galois extension of $\mathbb{Q}$.
   (ii) List all intermediate fields lying between $\mathbb{Q}$ and E.
   (iii) Which of the intermediate fields are Galois extensions of $\mathbb{Q}$?
157. Let E and F be fields with F a subfield of E. What does it mean to say that $a \in E$ is algebraic over F?
158. Let E and F be fields with F a subfield of E. Let $a \in E$ be algebraic over F. Denote by $F(a)$ the smallest subfield of E that contains F and q. Prove that $[F(a) : F] = \deg(a, F)$.
159. Let E and F be fields with F a subfield of E. Let $a \in E$ be algebraic over F. Denote by $F[a]$ the smallest subring of E that contains both F and a. Prove that $F(a) = F[a]$.
160. Show that $X^2 - 3$ and $X^2 - 2X - 2$ have the same splitting field K over $\mathbb{Q}$.
161. Let K be the splitting field of $X^2 - 3$ over $\mathbb{Q}$. Find $[K : \mathbb{Q}]$.
162. Let $F = \mathbb{Z}/3\mathbb{Z}$ be the field with three elements and let $f = X^3 - X + 1$.
   (i) Show that f is irreducible over F.
   (ii) How many elements are there in $E = \mathbb{F}[X]/(f)$?

(iii) Determine the inverse of the element $a = X = (f) \in E$.

(iv) Show that $Y^3 - Y + 1$ splits completely into linear factors in $E[Y]$ and find these factors.

163. State the main theorem of Galois theory.

164. Let K be the splitting field of the polynomial $X^5 - 1 \in \mathbb{Q}[X]$.

    (i) Determine the Galois group $G(K/\mathbb{Q})$.

    (ii) Give the correspondence between subfields of K and subgroups of $G(K/\mathbb{Q})$.

165. Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. Show that there is an extension field K of F in which $f(x)$ has a root.

166. Find a basis for $\mathbb{Q}(i, \sqrt{5})$ as a vector space over $\mathbb{Q}$.

167. Define what it means to say that an element $a \in \mathbb{C}$ is algebraic over $\mathbb{Q}$.

168. Find the minimal polynomial over $\mathbb{Q}$ of $(i\sqrt{3} - 1)/2$.

169. Suppose that $a \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ and let $n = \deg(a, \mathbb{Q})$. Show that there are exactly n injective field homomorphisms $\mathbb{Q}(q) \to \mathbb{C}$.

170. Let K be the splitting field of the polynomial $x^3 - 11 \in \mathbb{Q}[x]$. Determine the Galois group $G(K/\mathbb{Q})$.

171. Let K be the splitting field of the polynomial $x^3 - 11 \in \mathbb{Q}[x]$. Give the correspondence between subfields of K and subgroups of $G(K/\mathbb{Q})$.

172. Let K be the splitting field of the polynomial $x^3 - 11 \in \mathbb{Q}[x]$. Which of the subfields are Galois extensions of $\mathbb{Q}$?

173. Let F be a finite field of characteristic p. Show that there exists $r \in \mathbb{Z}_{>0}$ such that the number of elements in F is p^r.

174. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

    (i) Calculate $[E : \mathbb{Q}]$.

    (ii) Find an element $a \in E$ for which $E = \mathbb{Q}(a)$.

175. Suppose that $a \in \mathbb{R}$ is a constructible number. What can be said about the degree of a over $\mathbb{Q}$.

176. Let $r \in R$ be a root of the polynomial $x^3 + 3x + 1$. Explain why it is not possible to construct, with straight-edge and compass, a circle of radius r.

177. Show that the set of real numbers that are algebraic over $\mathbb{Q}$ is a subfield of $\mathbb{R}$.

178. Find the Galois group of the extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$. Explain why it is a Galois extension and list the correspondence between subgroups of $G(K/Q)$ and subfields $Q \subseteq L \subseteq K$.

179. Let K be the splitting field of $f(x) = x^3 - 2$ in $\mathbb{Q}[x]$.

    (i) Calculate $[K : \mathbb{Q}]$.

    (ii) Find a basis for K as a Q-vector space.

    (iii) Identify the Galois group $G(K/Q)$ and identify it.

(iv) Write down a field L such that $Q \subseteq L \subseteq K$ and L is not a Galois extension of $\mathbb{Q}$.

180. Suppose that $a \in \mathbb{R}$ is a constructible number. What can be said about the dimension of $\mathbb{Q}(a)$ as a vector space over $\mathbb{Q}$?

181. Is it possible to construct a regular 9-gon with straight-edge and compass? Explain. What about a regular 6-gon?

182. Find the Galois groups of $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$ and list the correspondence between subgroups of $G(K/\mathbb{Q})$ and subfields $L \subseteq K$.

183. Find the Galois groups of $K = \mathbb{Q}(e^{2\pi i/3})$ over $\mathbb{Q}$ and list the correspondence between subgroups of $G(K/\mathbb{Q})$ and subfields $L \subseteq K$.

184. Prove that there is no proper subfield of $\mathbb{Q}(e^{2\pi i/3})$ other than $\mathbb{Q}$.

185. Let K be the splitting field of the polynomial $f(x) = x^4 - 3$.

    (a) Calculate $[K : \mathbb{Q}]$.
    (b) Find a basis $\mathcal{B}$ for K as a $\mathbb{Q}$-vector space.
    (c) Give the size of the Galois group $G(K/Q)$ and identify it.
    (d) Write down a field L such that $\mathbb{Q} \subseteq L \subseteq K$ and L is not a Galois extension of $\mathbb{Q}$.

186. Let $a \in \mathbb{R}$ be a constructible number. What can be said about the degree of the extension $\mathbb{Q}(a)$ of $\mathbb{Q}$?

187. Explain why it is not possible to construct with straight-edge and compass a line segment whose length is that of an edge of a cube of volume 5.

188. Let K be the splitting field of the polynomial $x^3 - 7 \in \mathbb{Q}[x]$. Find the Galois group of K as an extension of $\mathbb{Q}$.

189. Let K be the splitting field of the polynomial $x^3 - 7 \in \mathbb{Q}[x]$. Exhibit an intermediate subfield L, $\mathbb{Q} \subseteq L \subseteq K$ such that L is not a Galois extension of $\mathbb{Q}$.

190. Let $K = \mathbb{Q}(\omega, \sqrt{5})$ where $\omega = e^{2\pi i/3}$. Find a basis of K over $\mathbb{Q}$.

191. Let $K = \mathbb{Q}(\omega, \sqrt{5})$ where $\omega = e^{2\pi i/3}$. Show that K is a Galois extension of $\mathbb{Q}$ and describe the Galois group $G = G(K/\mathbb{Q})$.

192. Let $\beta = \omega + \sqrt{5} \in K$. Compute the orbit of β under the action of G on K.

193. If a number $a \in \mathbb{R}$ is constructible what can be said about the degree of the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$?

194. Is π constrictible?

195. Explain why it is not possible to construct with ruler and compass a line segment whose length is the length of an edge of a cube of volume 2.

196. Find the Galois group G of the splitting field K of $x^4 - 4x^2 - 5$ as an extension of $\mathbb{Q}$. Explicitly write down the correspondence between the subgroups of G and the intermediate subfields of K.

197. Let $K = \mathbb{Q}(\omega, \sqrt[3]{7})$, where $\omega = e^{2\pi i/3}$. Show that $K/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$ and describe the Galois group $G = G(K/\mathbb{Q})$.

198. Let $K = \mathbb{Q}(\omega, \sqrt[3]{7})$, where $\omega = e^{2\pi i/3}$. Find the subgroup of the Galois group $G = G(K/\mathbb{Q})$ corresponding to the intermediate field $L = \mathbb{Q}(\sqrt[3]{7})$ under the Galois correspondence and show that $L/\mathbb{Q}$ is not a Galois extension.

199. Let $K = \mathbb{Q}(\omega, \sqrt[3]{7})$, where $\omega = e^{2\pi i/3}$. Find a basis for K as a vector space over $\mathbb{Q}$.

200. Given that π is a transcendental number, explain why it is not possible to contruct (by ruler and compass) a square whose area is the same as the unit circle.

201. Explain why it is not possible to construct (by ruler and compass) a line segment whose length is the length of a side of a cube of volume 2.

202. Find the Galois group G of the splitting field K of $x^4 - x^2 - 2$ as an extension of $\mathbb{Q}$. Explicitly write down the correspondence between the subgroups of G and the intermediate subfields of K.

203. Let $K = \mathbb{Q}(\omega, \sqrt[3]{5})$, where $\omega = e^{2\pi i/3}$.

    (i) Find a basis of K as a vector space over $\mathbb{Q}$.

    (ii) Show that $K/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$ and describe the Galois group $G = G(K/\mathbb{Q})$.

    (iii) Find the subgroup of G corresponding to the intermediate field $L = \mathbb{Q}(\sqrt[3]{5})$ under the Galois correspondence and show that $L/\mathbb{Q}$ is not a Galois extension.

204. If a number $\alpha \in \mathbb{R}$ is constructible what can be said about the degree of the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$?

205. Explain why it is not possible to construct with ruler and compass a line segment whose length is the length of a side of a cube with volume 2.

206. Find the Galois group G of the splitting field K of $x^3 - 5$ as an extension of $\mathbb{Q}$. Explicitly write down the correspondence between the subgroups of G and the intermediate subfields of K. Exhibit an intermediate subfield L of K such that $L/\mathbb{Q}$ is not a Galois extension.

207. Let $K = \mathbb{Q}(\omega, \sqrt{7})$, where $\omega = e^{2\pi i/3}$. Let $\beta = \omega + \sqrt{7}$ which is an element of K.

    (i) Find a basis for K over $\mathbb{Q}$.

    (ii) Show that $K/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$ and describe the Galois group $G = G(K/\mathbb{Q})$.

    (iii) Compute the orbit of β under the action of G.

    (iv) What is the degree of the irreducible polynomial of β?

    (v) Explain why your answer to (iv) shows that β is a primitive element for $K/\mathbb{Q}$.

208. Let $K = \mathbb{Q}(\sqrt{2 - \sqrt{3}})$.

    (a) Find the degree of K over $\mathbb{Q}$.

    (b) Show that K is a splitting field of the minimal polynomial of $\sqrt{2 - \sqrt{3}}$ over $\mathbb{Q}$.

209. Show that $\mathbb{Q}[2^{1/4}]$ is not the splitting field of any polynomal over $\mathbb{Q}$.

210. Let $i = \sqrt{-1}$. Show that $\mathbb{Q}[2^{1/4}, i]$ is the splitting field of a polynomial over $\mathbb{Q}$.

211. Let E be the smallest field extension of $\mathbb{Q}$ containing $\omega = e^{2\pi i/5}$.
    (a) Find a basis for E over $\mathbb{Q}$.
    (b) Show that E is the splitting field of an irreducible polynomial over $\mathbb{Q}$.
    (c) Find the Galois group of $E/\mathbb{Q}$.
    (d) Show that there is only one subfield of E containing $\mathbb{Q}$ which is different from E and $\mathbb{Q}$.

212. Let $f(x)$ be the minimal polynomial of $\sqrt{-2}+\sqrt{3}$ over $\mathbb{Q}$.
    (a) Determine $f(x)$.
    (b) Find the splitting field K of $f(x)$ and determine the Galois group of K over $\mathbb{Q}$.

213. (a) Show that the polynomial $f(x) = x^3 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$.
    (b) Let η denote a root of $f(x)$. Determine the number of elements and the degree of $\mathbb{F}_2(\eta)$ over $\mathbb{F}_2$.
    (c) Show that η^2 and $\eta^2+\eta+1$ are roots of f.
    (d) Show $\mathbb{F}_2(\eta)$ is the splitting field of f.
    (e) Prove that the only proper subfield of $\mathbb{F}_2(\eta)$ is $\mathbb{F}_2$.

214. Find the minimal polynomial of $(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$.

215. Determine the degree of the field extension $\mathbb{Q}(\sqrt{5}, 2^{1/3})$ over $\mathbb{Q}$.

216. Is it possible to construct by ruler and compass an angle of $\pi/9$?

217. Define the degree of a field extension and determine the degree of $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ over $\mathbb{Q}$.

218. Is it possible to trisect an angle of $3t$ degrees if $\cos(3t) = \frac{1}{3}$?