Problems

1. Prove that $[\mathbf{Q}(\zeta_{20}):\mathbf{Q}] = 8$, and write down a primitive root for every subfield of $\mathbf{Q}(\zeta_{20})$.

2. Find a finite group G and a normal subgroup H such that $\Gamma = G/H$ is not abstractly isomorphic to any subgroup of G.

3. Let L/K be a finite separable extension, and let M/K denote the Galois closure of G. Let $H = \mathrm{Gal}(M/L)$.

   (a) Prove that there exists a subfield $K \subsetneq E \subsetneq L$ if and only if there exists a subgroup $H \subsetneq \Gamma \subsetneq G$.

   (b) Determine whether there exists a subfield $K \subsetneq E \subsetneq L$ in the following situations:

      i. $[L:K] = 4$ and $[M:K] = 24$

      ii. $[L:K] = 6$ and $[M:K] = 24$

      iii. $[L:K] = 6$ and $[M:K] = 60$.

4. Suppose that $x^3 - 2$ is an irreducible polynomial in $\mathbf{F}_p[x]$. Prove that $p \equiv 1 \mod 3$.

5. Let L/K be an algebraic extension, and let α and β be elements of L. Let $A = K(\alpha, \beta)$ and $B = K(\alpha\beta, \alpha + \beta)$, so there are inclusions $K \subset B \subset A \subset L$. Prove that $[B : A] = 1$ or 2, and give examples to show that both cases may occur.

6. Let K and L be fields such that there exists an inclusion map $\phi : K \to L$.

   (a) If $K = \mathbf{Q}$, prove that the degree $[L : K]$ does not depend on ϕ. In particular, the notation $[L : \mathbf{Q}]$ is unambiguous.

   (b) If $[K : \mathbf{Q}] < \infty$, prove that the degree $[L : K]$ does not depend on ϕ.

   (c) If $K = \mathbf{Q}(t)$, give examples to show that $[L : K]$ may depend on ϕ.

7. Let $f(x) = a_d x^d + \ldots + a_0 \in \mathbf{Z}[x]$ be an polynomial of degree d, and α a real root of $f(x)$.

   (a) Prove that there exists a real constant $m > 0$ such that $|f(\alpha + \epsilon)| \le m\epsilon$ for any sufficiently small real number ϵ.

   (b) If p and q are integers, and p/q is *not* a root of $f(x)$, prove that $\left| f\left(\frac{p}{q}\right)\right| \ge \frac{1}{q^d}$.

   (c) Deduce that, for p, q with $(p, q) = 1$ and p and q sufficiently large, that $\left|\alpha - \frac{p}{q}\right| \ge \frac{1}{mq^d}$.

   (d) (**Liouville**) Suppose that $\beta \in \mathbf{R}$ is a real number with the property that, for any $\epsilon > 0$, there exist infinitely many pairs of integers p and q with $(p, q) = 1$ such that
   $$\left|\beta - \frac{p}{q}\right| \le \frac{\epsilon}{q^d}.$$
   Prove that β is *not* the root of any polynomial of degree at most d.

   (e) Let $\beta_n := \sum_{k=1}^{n} \frac{1}{10^{n!}}$, and $\beta = \lim \beta_n = \sum_{k=0}^{\infty} \frac{1}{10^{n!}} = 0.110001000000000000000001\ldots$

   Show that one can write $\beta_n = p_n/q_n$ for integers p_n and q_n with $(p_n, q_n) = 1$ and $q_n = 10^{n!}$. Prove that
   $$\left|\beta - \frac{p_n}{q_n}\right| = |\beta - \beta_n| \le \frac{2}{10^{(n+1)!}} = \frac{2}{q_n^{n+1}}.$$

(f) Deduce that β is not the root of any polynomial of any degree with rational coefficients, i.e. that β is transcendental.

8. Let $\epsilon, \delta > 0$ be real numbers. Consider the real interval $S := [0,1]$. Around every rational number $p/q \in S$, consider an interval of radius $\epsilon/q^{2+\delta}$. Then the union $S(\epsilon,\delta)$ of all such intervals has area at most

$$\epsilon\left(1 + \frac{1}{2^{1+\delta}} + \frac{1}{3^{1+\delta}} + \ldots\right) = \epsilon \cdot \zeta(1+\delta) < \infty.$$

It follows that $S(\delta) = \cap_{\epsilon>0} S(\epsilon,\delta)$ has measure zero, even though it is non-empty (it contains β). It follows that, with probability one, a random $\gamma \in S$ satisfies $\left|\gamma - \frac{p}{q}\right| > \frac{\epsilon}{q^{2+\delta}}$ for some $\epsilon > 0$ and all p, q. If this were true for π, then $q^3|\pi - p/q|$ is bounded away from 0. Do you think this is true? If so, what is your guess for the p and q that minimize this expression?

9. Prove that if $x = 2\cos(\theta)$, then $x^2 - 2 = 2\cos(2\theta)$ and $x^3 - 3x = 2\cos(3\theta)$. In particular, the roots of $x^3 - 3x + 1 = 0$ are given by $\alpha_1 = 2\cos(2\pi/9)$, $\alpha_2 = 2\cos(4\pi/9)$, and $\alpha_3 = 2\cos(8\pi/9)$. It follows that α_1, α_2, and α_3 are roots of the degree 8 polynomial

$$(((t^2-2)^2-2)^2-2) = t.$$

Give explicit expressions for the other 5 roots.

10. **Chebyshev Polynomials.** Let $t = e^{i\theta}$, so that $x = \cos\theta = (t + t^{-1})/2$.

(a) Let $T_n = (t^n + t^{-n})/2$. Prove that T_n satisfies the recurrence relation

$$T_{n+1} = 2(t+t^{-1})T_n - T_{n-1} = 2xT_n - T_{n-1}.$$

(b) Deduce that $T_n = T_n(x)$ is a polynomial in x, with $T_0 = 1$, $T_1 = x$, $T_2 = 2x^2 - 1$, $T_3 = 4x^3 - 3x$, etc.

(c) Prove that $T_n(\cos\theta) = \cos n\theta$.

(d) Prove that $T_n(x)$ in the interval $[-1,1]$ takes values in $[-1,1]$.

(e) Prove that $T_n(x)$ has degree n and has exactly n roots in the interval $[-1,1]$.

(f) Prove that the splitting field L of $T_n(x)$ over $\mathbf{Q}$ is contained in $\mathbf{Q}(\zeta_{4n})$, and that that L is precisely the fixed field of complex conjugation $-1 \in (\mathbf{Z}/4n\mathbf{Z})^\times$. (Hint: what is the relationship between the splitting field of $T_n(x)$ and $T_n((t+t^{-1})/2)$?)

(g) Prove that, if $(n,m) \neq (0,0)$,

$$\int_{-1}^{-1} T_n(x)T_m(x)\frac{dx}{\sqrt{1-x^2}} = \frac{\pi\delta(n-m)}{2},$$

where $\delta(x) = 0$ if $x = 0$ and 1 if $x = 1$.

11. **Examples of Function Fields**

(a) Let $K = \mathbf{Q}(u)$ and $L = \mathbf{Q}(t)$. Prove that the inclusion $K \to L$ given by

$$u \mapsto t^2$$

makes L/K an extension of degree 2 with $\mathrm{Gal}(L/K) = \mathbf{Z}/2\mathbf{Z}$. Compute the action of $\mathrm{Gal}(L/K)$ on t.

(b) Let $K = \mathbf{Q}(u)$ and $L = \mathbf{Q}(t)$. Prove that th inclusion $K \to L$ given by

$$u \mapsto \frac{1 - 3t + t^3}{t(t-1)}$$

makes L/K an extension of degree 3. (Hint: write down a cubic over $\mathbf{Q}(u)$ with root t.)

(c) In the last example, prove that L/K is Galois with $\mathrm{Gal}(L/K) = \mathbf{Z}/3\mathbf{Z}$.

(d) In the last example, prove that there is an element $\sigma \in \mathrm{Gal}(L/K)$ of order 3 such that

$$\sigma t = \frac{1}{1-t}.$$

12. Let $\alpha_0 = 2$, $\alpha_1 = -2$, $\alpha_2 = 0$, $\alpha_3 = \sqrt{2}$, and

$$\alpha_{n+1} = \sqrt{2 + \alpha_n}.$$

Prove that $\alpha_n = 2\cos(2\pi n/2^n) = \zeta_{2^n} + \zeta_{2^n}^{-1}$ where $\zeta_{2^n} = \exp(2\pi i/2^n)$.

13. Let L/K be a finite extension of degree n. Fix a basis for L/K, and let $\alpha \in L$.

(a) Prove that the multiplication by α map: $\psi(\alpha) : L \to L$ is a K-linear map.

(b) With respect to the given basis, deduce that there exists an $n \times n$ matrix $M(\alpha) \in M_n(K)$ corresponding to $\psi(\alpha)$.

(c) Define the *norm* $N_{L/K}(\alpha)$ and *trace* $\mathrm{Tr}_{L/K}(\alpha)$ of α from L to K to be

$$N_{L/K}(\alpha) = \det(M(\alpha)), \qquad \mathrm{Tr}_{L/K}(\alpha) = \mathrm{Trace}(M(\alpha)).$$

Prove that these quantities do not depend on the choice of basis for L/K.

(d) Prove that $N_{L/K}(\alpha) = 0$ if and only if $\alpha = 0$.

(e) If $x \in K$, show that $\mathrm{Tr}_{L/K}(x) = x[L : K]$ and $N_{L/K}(x) = x^{[L:K]}$.

(f) Prove that $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$.

(g) If $K = \mathbf{R}$ and $L = \mathbf{C}$, prove that $N_{L/K}(a + bi) = a^2 + b^2$.

(h) If $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{D})$, prove that $N_{L/K}(a + b\sqrt{D}) = a^2 - b^2 D$.

(i) If L/K is an extension of finite fields, prove that there exists at least one element $x \in L$ such that $\mathrm{Tr}_{L/K}(x) \neq 0$. If L/K is a separable extension, prove that there exists at least one element $x \in L$ such that $\mathrm{Tr}_{L/K}(x) \neq 0$.

14. In the context of the previous question, let A be the matrix associated to $\psi(\alpha)$ and some choice of basis.

(a) Let $P(x)$ denote the characteristic polynomial of A. Prove that $P(\alpha) = 0$.

(b) Suppose that $K(\alpha) = L$. Prove that $P(x)$ is the minimal polynomial of α.

(c) Suppose that $E = K(\alpha)$ and $[L : E] = m$. Prove that $P(x) = Q(x)^m$, where $Q(x)$ is the minimal polynomial of α. Hint: first consider the map $\psi_E(\alpha) : E \to E$ on E induced by multiplication by α, and show that $\psi(\alpha) = \psi_L(\alpha)$ with respect to a choice of basis is given by m block copies of $\psi_E(\alpha)$.

15. Let $f(x) = x^3 - ax^2 + bx - c$ be an irreducible degree 3 polynomial over $\mathbf{Q}$. Let L be a splitting field of $f(x)$, and let $K = \mathbf{Q}(\alpha) \subset L$ for one of the roots α of $f(x)$.

(a) Write $f(x)$ as $(x-\alpha)(x-\beta)(x-\gamma)$ in $L[X]$. Prove that

$$\begin{aligned}\alpha+\beta+\gamma &= a,\\ \alpha\beta+\alpha\gamma+\beta\gamma &= b,\\ \alpha\beta\gamma &= c.\end{aligned}$$

(b) Let $\delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$. Prove that

$$\Delta := \delta^2 = a^2b^2-4b^3-4a^3c+18abc-27c^2.$$

(c) Let $E=\mathbf{Q}(\delta)\subset L$. Prove that $[E:\mathbf{Q}]\le 2$, and that $[E:\mathbf{Q}]=2$ if and only if $\Delta\in\mathbf{Q}$ is a perfect square.

(d) Suppose that $L=K$. Prove that $\Delta\in\mathbf{Q}$ is a perfect square.

(e) For a positive integer n, show that x^3-nx+1 is irreducible unless $n=2$.

(f) Let L be a splitting field of x^3-nx+1. Prove that $[L:\mathbf{Q}]=6$ unless either:

i. $n=2$, in which case $[L:\mathbf{Q}]=2$.

ii. $n=3$, in which case $[L:\mathbf{Q}]=3$.

Hint: for $n=2$, factor the polynomial, and for $n=3$, use the first exercise. For all other n, prove that the discriminant

$$\Delta=-27-4n^3$$

is not a perfect square. Writing $\Delta=\delta^2$, consider the quantity $X^3+Y^3-Z^3$ where $Z=\delta/3+3$, $Y=\delta/3-3$, and $X=-2n$.

16. Find, explicitly, the subgroups of the following groups:

(a) $(\mathbf{Z}/16\mathbf{Z})^\times$

(b) $(\mathbf{Z}/11\mathbf{Z})^\times$

(c) $(\mathbf{Z}/60\mathbf{Z})^\times$

(d) $(\mathbf{Z}/25\mathbf{Z})^\times$

17. Draw a diagram of all the subfields of $\mathbf{Q}(\zeta_{13})$, with a line between any pair of fields $E\subset F$ indicating the degree of the corresponding extension.

18. Draw a diagram of all the subfields of $\mathbf{Q}(\zeta_{17})$, with a line between any pair of fields $E\subset F$ indicating the degree of the corresponding extension.

19. Express the following trigonometric values in terms of roots of unity and also in terms of radicals.

(a) $\tan(60^\circ)$

(b) $\sin(36^\circ)$.

(c) $\cos(30^\circ)$.

(d) $\cos(10^\circ)$.

20. Let $K=\mathbf{Q}(\sqrt{2})$ and $L=\mathbf{Q}(\sqrt[4]{2})$. Prove that $K/\mathbf{Q}$ is a splitting field, and L/K is a splitting field, but $L/\mathbf{Q}$ is *not* a splitting field of any polynomial over $\mathbf{Q}$.

21. (**Primitive Roots**) Let $K=\mathbf{F}_p$. Since $K^\times$ is cyclic, there exist elements $\varepsilon\in K^\times$ which are multiplicative generators for $K^\times$; these are called primitive roots. Let ε a primitive root.

(a) Show that the set $\{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-2}\}$ in K is precisely the set $\{1, 2, 3, 4, \ldots, p-1\}$.

(b) Suppose that $m \not\equiv 0 \mod p-1$. Prove that

$$1 + \varepsilon^m + \varepsilon^{2m} + \varepsilon^{3m} + \ldots + \varepsilon^{(p-2)m} = 0 \in K.$$

(Hint: multiply by $\varepsilon^m - 1$)

(c) Deduce that, for all $m \geq 1$, there is a congruence

$$1^m + 2^m + 3^m + \ldots + (p-1)^m \equiv \begin{cases} 0 \mod p, & m \not\equiv 0 \mod p-1, \\ -1 \mod p, & m \equiv 0 \mod p-1. \end{cases}$$

22. (**Frobenius**) Let $q = p^m$, and let $f(x) \in \mathbf{F}_q[x]$.

(a) Prove that every element α in $\mathbf{F}_q$ satisfies $\alpha^q = \alpha$.

(b) Let $K/\mathbf{F}_q$ be the splitting field of $f(x)$, and let $\beta \in K$ be a root of $f(x)$. Prove that β^q is also a root of $f(x)$.

23. Let $f(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$.

(a) Prove that $f(x)$ is irreducible.

(b) Let K be the splitting field of $f(x)$. Prove that $K \simeq \mathbf{F}_{16}$.

(c) Let α be a root of $f(x)$ in K. Determine the order of $\alpha \in K^\times$.

24. (**Algebraic Integers**) Let $K/\mathbf{Q}$ be an algebraic extension. For $\alpha \in K$, let $\mathbf{Z}[\alpha] \subset K$ denote the subring generated by the image of $\mathbf{Z}[x] \to K$ under the map that sends x to α (equivalently, elements of $\mathbf{Z}[\alpha]$ are given by polynomials in α with integral roots). Say that α is an *algebraic integer* if $\mathbf{Z}[\alpha]$ considered as a $\mathbf{Z}$-module (equivalently, abelian group) is finitely generated.

(a) Prove that $\alpha \in K$ is an algebraic integer if and only if it is a root of a *monic* polynomial $f(x) \in \mathbf{Z}[x]$.

(b) Prove that $\alpha \in K$ is an algebraic integer if and only if it is a root of an *irreducible* monic polynomial $f(x) \in \mathbf{Z}[x]$.

(c) If $\alpha \in \mathbf{Q} \subset K$, prove that α is an algebraic integer if and only if it is an actual integer.

(d) If α and β are algebraic integers in K, prove that the ring $\mathbf{Z}[\alpha, \beta]$ is finitely generated as a $\mathbf{Z}$-module.

(e) Deduce that the sum and product of two algebraic integers are algebraic.

(f) Let $\mathcal{O}_K \subset K$ denote the set of algebraic integers. Deduce that $\mathcal{O}_K$ is a subring of K.

(g) Prove that the fraction field of $\mathcal{O}_K$ is K.

(h) Suppose $[K : \mathbf{Q}] < \infty$. It is a non-trivial fact (why is it non-trivial?) that $\mathcal{O}_K$ is finitely generated as a $\mathbf{Z}$-module. Using, this, prove that as $\mathbf{Z}$-modules $\mathcal{O}_K \simeq \mathbf{Z}^d$ where $d = [K : \mathbf{Q}]$.

(i) Let D be a square-free integer. Let $K = \mathbf{Q}(\sqrt{D})$. Prove that $\mathcal{O}_K$ is equal to the ring $\mathbf{Z}[\sqrt{D}]$ if $D \equiv 2, 3 \mod 4$ and $\mathbf{Z}\left[\frac{D + \sqrt{D}}{2}\right]$ otherwise.

25. How many irreducible factors does $X^{342} - 1$ have over $\mathbf{F}_7$? What about $X^{343} - 1$? (Hint: what are the splitting fields of these polynomials?)

26. Let $E/\mathbf{Q}$ and $F/\mathbf{Q}$ be subfields of a fixed, finite extension $K/\mathbf{Q}$. Prove that $[E : \mathbf{Q}] \geq [E.F : F]$.

27. Determine all automorphisms of the following fields.

    (a) $\mathbf{Q}(\sqrt[3]{2})$.
    (b) $\mathbf{Q}(2\cos(2\pi/7))$.
    (c) $\mathbf{Q}(\sqrt{1+\sqrt{2}})$.
    (d) $\mathbf{Q}(\sqrt[3]{1+\sqrt{2}})$.

28. [**Artin–Schreier extensions**] Let E be a field of characteristic p.

    (a) If $\alpha \in E$, prove that the polynomial $p(x) = x^p - x - \alpha$ is seperable.
    (b) If β is a root of $p(x)$, show that $\beta + 1$ is also a root of $p(x)$.
    (c) Deduce that either $p(x)$ splits completely in E or $p(x)$ is irreducible.
    (d) Deduce that the splitting field F/E of $p(x)$ is either E or is cyclic of degree p.
    (e) Show that the splitting field of $x^p - x - 1$ over $\mathbf{F}_p$ is $\mathbf{F}_q$ where $q = p^p$.

29. (**Primitive Element Theorem, I**) Suppose that L/K is a finite extension, and suppose additionally that there only exists **finitely many** intermediate fields E with $K \subset E \subset L$. Assume that K is infinite. Say that an element $\theta \in L$ is *primitive* if $L = K(\theta)$. We prove (under the assumptions of the problem) that a primitive element exists.

    (a) Let $K_0 = K$. If $K_0 = L$, show (this is obvious) that L has a primitive element. If $K_0 \neq L$, show that there exists an element $\theta_1 \in L \setminus K_0$. Let $K_1 = K_0(\theta_1)$. If $K_1 = L$, show (this is obvious) that L has a primitive element. Assume that $K \subsetneq K_1 \subsetneq \ldots \subsetneq K_n \subset L$, and assume that $K_n = K(\theta_n)$. If $K_n = L$, show (this is obvious) that L has a primitive element.
    (b) If $K_n \neq L$, show there exists an element $\alpha \in L \setminus K_n$. For $\lambda \in K$, let $K_\lambda := K(\theta_n + \lambda\alpha)$. Prove that there exist $\lambda_1 \neq \lambda_2$ such that $K_{\lambda_1} = K_{\lambda_2}$.
    (c) If there is an equality of fields

    $$K(\theta_n + \lambda_1\alpha) = K(\theta_n + \lambda_2\alpha),$$

    prove that both fields are isomorphic to $K(\theta_n, \alpha)$.
    (d) Deduce that there exists $\lambda \in K$ and $\theta_{n+1} = \theta_n + \lambda\alpha$ so that $K_{n+1} := K_n(\theta_{n+1})$ strictly contains K_n.
    (e) Deduce (under the conditions of the problem) that L/K has a primitive element.
    (f) Find a primitive element for the following extensions:
        i. The splitting field of $X^3 - 2$ over $\mathbf{Q}$.
        ii. The splitting field of $X^3 - 2$ over $\mathbf{F}_7$.
        iii. The splitting field of $(X^2 - 2)(X^2 - 3)$ over $\mathbf{Q}$.

30. (**Primitive Element Theorem, II**) Let L/K be a finite extension.

    (a) Assume that L/K is separable — that is, any element $\alpha \in L$ is the root of a separable irreducible polynomial in L. Prove that there exists a normal extension (splitting field of a separable polynomial) M/K containing L.
    (b) Deduce that if L/K is separable, then L/K has only finitely many intermediate subfields.
    (c) Deduce that if L/K is separable, then L/K contains a primitive element.
    (d) Deduce that if $\mathrm{Char}(K) = 0$ or K is finite, then L/K contains a primitive element.

31. (14.4 (5)) Let p be a prime and let F be a field. Let K be a Galois extension of F whose Galois group is a p-group (i.e., the degree $[K : F]$ is a power of p). Such an extension is called a p-extension (note that p-extensions are Galois by definition).

   (a) Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.

   (b) Give an example to show that (a) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

32. Let $f(x)$ be a separable irreducible polynomial of degree d with Galois group G (That is, G is the Galois group of the splitting field of $f(x)$). What are the possible values of d for the following groups G?

   (a) The quaternion group $G = Q$ of order 8.

   (b) The alternating group $G = A_4$ of order 24.

   (c) An abelian group $G = A$ of order 60.

33. (**C is algebraically closed**). Do *not* assume that $\mathbf{C}$ is algebraically closed for this question. You may assume the intermediate value theorem for $\mathbf{R}$.

   (a) Let $g(x) \in \mathbf{C}[x]$ be a quadratic polynomial. Prove directly that $g(x)$ is reducible.

   (b) Let $f(x) \in \mathbf{R}[x]$ be a polynomial. If $\deg f(x)$ is odd, prove that $f(x)$ has a root in $\mathbf{R}$.

   (c) Deduce that if $K/\mathbf{R}$ is a finite extension, then $[K : \mathbf{R}]$ is even or $K = \mathbf{R}$.

   (d) Let $L/\mathbf{R}$ be a finite Galois extension with $G = \mathrm{Gal}(L/\mathbf{R})$. Prove that G is a power of 2. (Hint: use part (33c)).

   (e) Deduce that if $K/\mathbf{C}$ is any non-trivial finite extension, and $L/\mathbf{R}$ is the Galois closure of K, then $G = \mathrm{Gal}(L/\mathbf{C})$ is a non-trivial finite 2-group.

   (f) Deduce that if $K/\mathbf{C}$ is any non-trivial finite extension, there exists a non-trivial *quadratic* extension $E/\mathbf{C}$.

   (g) Conclude from part (33a) that $K/\mathbf{C}$ has no non-trivial finite extensions.

34. Suppose that $K = \mathbf{F}_p(X, Y)$, the field of rational functions in two variables X and Y.

   (a) Let $L = \mathbf{F}_p(X^{1/p}, Y^{1/p})$. Show that L is the splitting field of $(T^p - X)(T^p - Y)$.

   (b) Prove that $[L : K] = p^2$.

   (c) Prove that, if $\eta \in L$ is any element, then $\eta^p \in K$.

   (d) Prove that, if $\eta \in L$ is any element, then $[K(\eta) : K] = 1$ or p.

   (e) Prove that there are infinitely many subfields $K \subset E \subset L$.

35. Let $a(x)$ and $b(x)$ be irreducible polynomials of degree n over $\mathbf{Q}$, and let $A = \mathbf{Q}[x]/a(x)$, $B = \mathbf{Q}[x]/b(x)$. Suppose that K is the splitting field of both $a(x)$ and $b(x)$. Let $G = \mathrm{Gal}(K/\mathbf{Q})$, $H_A = \mathrm{Gal}(K/A)$, and $H_B = \mathrm{Gal}(K/B)$.

   (a) Prove that $\bigcap \sigma H \sigma^{-1} = 1$. for $H = H_A$ and H_B.

   (b) Prove that $|H_A| = |H_B|$.

   (c) Prove that $A \simeq B$ if and only if H_A is conjugate to H_B in G.

   (d) Prove that if $n = 2$ or $n = 3$, then $A \simeq B$.

(e) Prove that if $n = 4$, and $G = D_8$, then A is not necessarily isomorphic to B.

(f) Give an explicit example of polynomials $a(x)$ and $b(x)$ of degree 4 such that A is not isomorphic to B.

(g) Prove that if G is abelian, then $A = B = K$.

(h) Prove that if $G = S_n$, then A is isomorphic to B provided that $n \neq 6$.

36. (14.4 (5)) Let p be a prime and let F be a field. Let K be a Galois extension of F whose Galois group is a p-group (i.e., the degree $[K : F]$ is a power of p). Such an extension is called a p-extension (note that p-extensions are Galois by definition).

    (a) Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.

    (b) Give an example to show that (a) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

37. Let $f(x)$ be a separable irreducible polynomial of degree d with Galois group G (That is, G is the Galois group of the splitting field of $f(x)$). What are the possible values of d for the following groups G?

    (a) The quaternion group $G = Q$ of order 8.

    (b) The alternating group $G = A_4$ of order 24.

    (c) An abelian group $G = A$ of order 60.

38. Let $F = \mathbf{C}(x_1, x_2, \ldots, x_n)$ be the field of fractions of the polynomial ring $\mathbf{C}[x_1, \ldots, x_n]$. Let s_i denote the elementary symmetric polynomials in the x_i, that is,

$$\begin{aligned} s_1 &= x_1 + x_2 + \ldots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n \\ &\ddots \\ s_n &= x_1x_2 \ldots x_n. \end{aligned}$$

    Let $E = \mathbf{C}(s_1, \ldots, s_n)$. Prove that, with respect to the natural inclusion $E \subset F$, that:

    (a) F/E is a finite Galois extension. (Hint: identify it as a splitting field)

    (b) $\mathrm{Gal}(F/E) = S_n$.

39. Let $K/\mathbf{Q}$ be a Galois extension.

    (a) If $[K : \mathbf{Q}] = 2009$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.

    (b) If $[K : \mathbf{Q}] = 2010$, prove that K contains an extension E with $[E : \mathbf{Q}] = 2$.

    (c) If $[K : \mathbf{Q}] = 2011$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.

    (d) If $[K : \mathbf{Q}] = 2012$, prove that K contains an extension E with $[E : \mathbf{Q}] = 503$.

    (e) If $[K : \mathbf{Q}] = 2013$, prove that K contains an extension E with $[E : \mathbf{Q}] = 3$.

40. Determine $\mathrm{Aut}(K/\mathbf{Q})$ for the following fields, and determine which ones are Galois.

    (a) $\mathbf{Q}(\sqrt[3]{2})$.

    (b) $\mathbf{Q}(2\cos(2\pi/7))$.

(c) $\mathbf{Q}(\sqrt{1+\sqrt{2}})$.

(d) $\mathbf{Q}(\sqrt[3]{1+\sqrt{2}})$.

41. Prove that the Galois group of the splitting field of $x^4 + ax^2 + b$ is a subgroup of $D_8 \subset S_4$.

42. Let $f(x)$ be an irreducible separable polynomial over K with splitting field L. Suppose that $\mathrm{Gal}(L/K) = Q$, the quaternion group of order 8. Determine the possible degrees of $f(x)$.

43. Let L/K be an extension, and let $\alpha, \beta \in L$ be elements with $[K(\alpha) : K] = 2$ and $[K(\beta) : K] = 3$. Determine the possible degrees $[K(\alpha + \beta) : K]$.

44. [**Field Embeddings, I**] Let $E/\mathbf{Q}$ be a finite extension. Let $K/\mathbf{Q}$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Let $N = \mathrm{Hom}(E, K)$ be the set of ring homomorphisms from E to K (so 1 maps to 1).

    (a) Prove that either N is empty, or there exists an inclusion from E to K.

    (b) If $\phi \in N$, show that $\phi(E)$ is a subfield of K.

    (c) Prove that if $\sigma \in G$, and $\phi : E \to K$ is an element of N, then the map $\sigma.\phi$ defined by sending x to $\sigma(\phi(x))$ is an element of N.

    (d) Prove that this construction gives a group action of G on N.

    (e) Prove that the stabilizer of ϕ is $\mathrm{Gal}(K/\phi(E))$.

    (f) Prove that G acts transitively on N.

    (g) Prove that either N is empty, or $|N| = [E : \mathbf{Q}]$.

    (h) Prove that for any field K (not necessarily finite or Galois) containing the splitting field of E, $N = \mathrm{Hom}(E, K)$ has order $[E : \mathbf{Q}]$.

    (i) If $K = \mathbf{C}$, one can write $N = N_{\mathbf{R}} \cup N_{\mathbf{C}}$, where $N_{\mathbf{R}} = \mathrm{Hom}(E, \mathbf{R})$, and $N_{\mathbf{C}}$ consists of the homomorphisms from E to $\mathbf{C}$ which do *not* land in $\mathbf{R}$. Prove that $|N_{\mathbf{C}}|$ is even. Thus, attached to E, there are a pair of integers (r_1, r_2) such that $r_1 = |N_{\mathbf{R}}|$ and $2r_2 = |N_{\mathbf{C}}|$, so $[E : \mathbf{Q}] = r_1 + 2r_2$. The pair (r_1, r_2) is called the *signature* of E. If E has signature $(r_1, 0)$, we say that E is totally real, and if E has signature $(0, r_2)$ we say that E is totally complex.

    (j) Prove that if $E/\mathbf{Q}$ is a finite Galois extension, then E either has signature $(n, 0)$ (where $n = [E : \mathbf{Q}]$), or $[E : \mathbf{Q}] = n = 2m$ and E has signature $(0, m)$.

    (k) Suppose that $E/\mathbf{Q}$ is a finite Galois extension with $\Gamma = \mathrm{Gal}(E/\mathbf{Q})$. Let K be any field (not necessarily finite or Galois) containing the splitting field of E. Prove that there is an action of $\Gamma = \mathrm{Gal}(E/\mathbf{Q})$ on $N = \mathrm{Hom}(E, K)$ given by

    $$\sigma.\phi = \phi(\sigma^{-1}(x)).$$

    (Note that the inverse is there to ensure that $gh.(\phi) = g.(h.\phi)$.)

    (l) Suppose that $E/\mathbf{Q}$ is a Galois extension of degree $2m$ with signature $(0, m)$, and $\Gamma = \mathrm{Gal}(E/\mathbf{Q})$. Let Γ act on $N = N_{\mathbf{C}}$ as in part 44k.

        i. Show that for every $\phi \in N = N_{\mathbf{C}}$, there exists a unique element $c \in \Gamma$ of order two such that $c.\phi$ is ϕ composed with complex conjugation on $\mathbf{C}$.

        ii. Show that the elements c obtained in this way for all $\phi \in N$ are conjugate, and moreover every element that is conjugate to c occurs in this way.

        iii. Let Φ be the smallest normal subgroup of Γ containing (any) c. Prove that E^{Φ} is totally real. Moreover, if $F \subset E$ is totally real, then $F \subseteq E^{\Phi}$.

iv. If $E/\mathbf{Q}$ is Galois with *abelian* Galois group Γ, then either E is totally real, or there exists a unique totally real subfield $E^+ \subset E$ such that $[E:E^+]=2$.

v. If $E/\mathbf{Q}$ is Galois with $G = A_5$, and E is the splitting field of a degree 5 irreducible polynomial $p(x)$, prove that $F = \mathbf{Q}[x]/p(x)$ has signature $(5,0)$ or $(1,2)$.

45. [**Field Embeddings, II**] Let $E/\mathbf{Q}$ be a finite extension. Let $K/\mathbf{Q}$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Let M be the set of subfields of K that are isomorphic to E.

(a) Prove that M is empty, or there exists an inclusion from E to K.

(b) Prove that G acts on M by sending $F \in M$ to $\phi(F)$.

(c) If $F \in M$, prove that the stabilizer of F is the normalizer N_F of $\mathrm{Gal}(K/F)$.

(d) Prove that G acts transitively on M.

(e) Prove that $|M| = [G : N_F]$, for any $F \in M$.

(f) Prove that $|M| = 1$ if and only if $E/\mathbf{Q}$ is Galois.

(g) If $F \in M$, let $H = K^{N_F}$. Prove that:

i. H is contained in F.

ii. F/H is Galois.

iii. If $H' \subset F$ is any subfield of F such that F/H' is Galois, then H' contains H.

iv. H does not depend on F.

(h) Deduce that for any field $E/\mathbf{Q}$, there is a well defined minimal field $H/\mathbf{Q}$ in E such that E/H is Galois.

46. Determine (with proof) the degree of $\mathbf{Q}(\sqrt{3+2\sqrt{2}})$ over $\mathbf{Q}$.

47. **Abelian Groups as Galois Groups.** Let p be prime, and let $\Phi_{p^m}(X)$ denote the p^mth cyclotomic polynomial, given explicitly by

$$\Phi_{p^m}(X) = \frac{X^{p^m}-1}{X^{p^{m-1}}-1} = 1 + X^{p^{m-1}} + \ldots + X^{(p-1)p^{m-1}}.$$

(a) Prove that $\Phi_{p^m}(X)$ is irreducible.

(b) Let N be an integer, and let $q \neq p$ be a prime divisor of the integer $\Phi_{p^m}(N)$.

i. Prove that
$$N^{p^m} \equiv 1 \mod q.$$

ii. Prove that
$$N^{p^{m-1}} \not\equiv 1 \mod q.$$

Hint: assuming that $N^{p^{m-1}} \equiv 1 \mod q$, compute $\Phi_{p^m}(N) \mod q$.

(c) Deduce that $q \equiv 1 \mod p^m$. (Hint: consider the order of the group $\mathbf{F}_q^\times$.)

(d) Suppose that the set S of primes such that $q \equiv 1 \mod p^m$ is finite. Obtain a contradiction by considering a prime divisor q of $\Phi_{p^m}\left(p \prod_{q \in S} q\right)$.

(e) By considering subfields of $\mathbf{Q}(\zeta_M)$ where M is a product of k primes in S, prove that $(\mathbf{Z}/p^m\mathbf{Z})^k$ occurs as a Galois group of a finite extension of $\mathbf{Q}$.

(f) Prove that every finite abelian group A occurs as the Galois group of a finite extension of $\mathbf{Q}$.

48. **Resolvant cubics.** Let $f(x)$ be an irreducible degree 4 polynomial over $\mathbf{Q}$ with splitting field F and roots θ_1, θ_2, θ_3, and θ_4. Let $\alpha_{(12)} = \theta_1\theta_2 + \theta_3\theta_4$, $\alpha_{(13)} = \theta_1\theta_3 + \theta_2\theta_4$, and $\alpha_{(14)} = \theta_1\theta_4 + \theta_2\theta_3$.

   (a) Let $S = \{\alpha_{12}, \alpha_{13}, \alpha_{23}\}$. Prove that $G = \mathrm{Gal}(L/\mathbf{Q})$ acts on this set.

   (b) Let $H = \mathrm{Gal}(L/\mathbf{Q}(\alpha_{12}))$. Deduce that $[G : H] = 1$, 2, or 3.

   (c) Deduce that the polynomial $g(x) = (X - \alpha_{12})(X - \alpha_{13})(X - \alpha_{14})$ has coefficients in $\mathbf{Q}$.

   (d) If $[G : H] = 3$, prove that $G = A_4$ or S_4.

   (e) If $[G : H] = 1$ or 2, prove that G has order dividing 8.

   (f) Prove that $G \subset A_4$ if and only if $\delta = \prod_{i>j}(\theta_i - \theta_j) \in \mathbf{Q}$.

   (g) Prove that G has order dividing 8 if and only if $g(x)$ has a rational root.

   (h) Let E be the splitting field of $g(x)$. Prove that $\mathrm{Gal}(F/E) = K \cap G$, where K is the Klein 4-group of S_4.

   (i) Suppose that $f(x) = x^4 + ax^3 + bx^2 + cx + d$. Prove that

   $$g(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - c^2 - a^2 d.$$

   (j) Prove that if $G \subset A_4$ has 2-power order and acts transitively on 4 points then $G = K$.

   (k) Using $g(x)$, compute the Galois groups of the following polynomials:

      i. $x^4 + x + 1$. Show $G \not\subset A_4$ and $|G| \nmid 8$ so $G = S_4$.

      ii. $x^4 + 8x + 12$. Show $G \subset A_4$ and $|G| \nmid 8$ so $G = A_4$.

      iii. $x^4 + x^2 + 2$. Show $G \not\subset A_4$ and $|G||8$. Then distinguish between $\mathbf{Z}/4\mathbf{Z}$ and D.

      iv. $x^4 + x^3 + x^2 + x + 1$. Show $G \not\subset A_4$ and $|G||8$. Then distinguish between $\mathbf{Z}/4\mathbf{Z}$ and D.

      v. $x^4 + 1$. Show $G \subset A_4$ and $|G||8$ so $G = K$.

49. **Imprimitive subgroups.** Let G act on a set A of n points. Recall that G is imprimitive (equivalently, not primitive) if and only if there does exists a decomposition

   $$A = \coprod A_i$$

   of A into distinct sets A_i such that:

   - There is at least one i such that $|A_i| \geq 2$.
   - If $g \in G$ and a, $a' \in A_i$, then $g.a$ and $g.a'$ both lie in A_j for some j.

   Let G be a finite group which acts on a set A.

   (a) If G is not transitive, prove that G is not imprimitive by taking A_i to be the orbits of G.

   (b) Say that G is 2-transtive if, for any two pairs (a_1, a_2) and (a_1', a_2') of distinct elements of A, there exists a $g \in G$ such that $g(a_1) = a_1'$ and $g(a_2) = a_2'$. If G is 2-transitive, prove that G is primitive.

   (c) If G is transitive, but not primitive, prove that $|A_i| = |A_j|$ for all i and j.

   (d) Deduce that if G is transitive, and $|A|$ is prime, then G is primitive.

   (e) Suppose that G is transitive, imprimitive, and acts faithfully on A.

      i. Let B denote the set of sets $\{A_i\}$. Prove that G acts transitively on B.

      ii. Show there exists integers a, b, and n such that $|A| = n$, $|B| = b$, $|A_i| = a$ for all i, and $ab = n$.

iii. Let H denote the kernel of G acting on B. Prove that H is isomorphic to a subgroup of $(S_a)^b = S_a \times S_a \times \ldots S_a$.

iv. Prove that G/H is isomorphic to a subgroup of S_b.

v. Deduce that G has order dividing $b! \cdot (a)!^b$.

vi. Let N be any group which acts faithfully and transitively on a points, and let Γ be any group which acts faithfully and transitively on b points. Prove that there is a group $N \wr \Gamma$ which acts faithfully, transitively, and imprimitively on a set A of order $n = ab$ points, where G preserves a decomposition of A into sets A_i of order $|A_i| = a$, where the action of G onto the set B of sets $\{A_i\}$ factors through Γ, and where the kernel of this action is $H = N^b$.

vii. Prove that G is subgroup of $S_a \wr S_b$.

(f) Prove that the 2-Sylow of S_4 is $S_2 \wr S_2$.

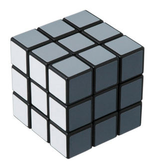
(g) Prove that the 3-Sylow of S_9 is $\mathbf{Z}/3\mathbf{Z} \wr \mathbf{Z}/3\mathbf{Z}$.

(h) If N is the p-Sylow of S_{p^n}, prove that $N \wr \mathbf{Z}/p\mathbf{Z}$ is the p-Sylow of $S_{p^{n+1}}$.

(i) Deduce that any p-group is a subgroup of $\mathbf{Z}/p\mathbf{Z} \wr \mathbf{Z}/p\mathbf{Z} \wr \mathbf{Z}/p\mathbf{Z} \ldots \mathbf{Z}/p\mathbf{Z}$.

(j) Deduce that any p-group is solvable.

(k) Find out what a Rubix cube is.



(l) Let G be the group defined by the possible combinations of moves.

(m) Prove that the action of G on the $9 \cdot 6 = 54$ has orbits of size 24, 24, and 6 orbits of size 1.

(n) Prove that G admits a quotient N which is a subgroup of S_{24} by showing that some quotient acts faithfully on the corner squares.

(o) Prove that the action of N on the corner squares is imprimitive, by taking A_i to be the triples of squares along each corner.

(p) Deduce that N is a subgroup of $S_3 \wr S_8$, and hence $|N|$ divides $3!^8 \cdot 8! = 67722117120$.

(q) Prove that the stabilizer H in N of the cubes always preserves the orientation of the triple of colours around the corners, and hence that H is actually a subgroup of $(\mathbf{Z}/3\mathbf{Z})^8$.

(r) Deduce that N is a subgroup of $(\mathbf{Z}/3\mathbf{Z}) \wr S_8$, and hence $|N|$ divides $3^8 \cdot 8! = 264539520$. (Actually, N has index 2 in $(\mathbf{Z}/3\mathbf{Z}) \wr S_8$.)

(s) Let M be the quotient on which G acts on the edge squares of the cube. Prove that M is a subgroup of S_{24}.

(t) Prove that M acts imprimively on the set of edges, since it preserves the squares on each pair.

(u) Deduce that M is a subgroup of $\mathbf{Z}/2\mathbf{Z} \wr S_{12}$.

(v) Prove that G is a subgroup of $M \oplus N$.

(w) Deduce that G is a subgroup of

$$(\mathbf{Z}/3\mathbf{Z}) \wr S_8 \oplus (\mathbf{Z}/2\mathbf{Z}) \wr S_{12},$$

and hence that G has order dividing

$$|G| = 3^8 \cdot 8! \cdot 2^{12} \cdot 12! = 519024039293878272000.$$

(In fact, it turns out that G has index 12 in this group.)

50. Let L/K be Galois with Galois group Γ. Let M/L be Galois with Galois group N. Show that the Galois closure N/K of M/K is Galois with Galois group a subgroup of $N \wr \Gamma$.

51. Let $f(x)$ be an irreducible polynomial over $\mathbf{Q}$ of degree b, and let $g(x)$ be arbitrary of degree a. Prove that the Galois group of $f(g(x))$ is a subgroup of $S_a \wr S_b$.

52. **Iterated Polynomials.** Let $f(x)$ be an irreducible quadratic polynomial. Let

$$f_n(x) = f(f(f(\cdots f(x))\cdots)))$$

where f is iterated n times.

Prove that the Galois group of $f_n(x)$ is a subgroup of the 2-Sylow P_{2^n} of S_{2^n}.

   (a) If $f(x) = x^2 - 2$, prove that $f_n(x)$ is irreducible.
   (b) If $f(x) = x^2 - 2$, prove that the Galois group of $f_n(x)$ is $\mathbf{Z}/2^n\mathbf{Z}$. (Hint: what is $f_n(t + t^{-1})$? Compare with question 10).
   (c) Find an explicit polynomial $f(x)$ such that $f_n(x)$ has Galois group $P_{2^n} \subset S_{2^n}$ for all n.

53. Prove that $\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}$.

54. (14.5 (10) Prove that $\mathbf{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbf{Q}$.

55. (See 14.6 (2),(4),(5),(6),(7),(8),(9),(10)) Determine the Galois group of the following polynomials:

   (a) $x^3 - x^2 - 4$.
   (b) $x^3 - 2x + 4$.
   (c) $x^3 - x + 1$.
   (d) $x^3 + x^2 - 2x - 1$.
   (e) $x^4 - 25$.
   (f) $x^4 + 4$.
   (g) $x^4 + 3x^3 - 3x - 2$.
   (h) $x^4 + 8x + 12$.
   (i) $x^4 + 4x - 1$.
   (j) $x^5 + x - 1$.

56. Let $K/\mathbf{Q}$ be a Galois extension.

   (a) If $[K : \mathbf{Q}] = 2009$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.
   (b) If $[K : \mathbf{Q}] = 2010$, prove that K contains an extension E with $[E : \mathbf{Q}] = 2$.
   (c) If $[K : \mathbf{Q}] = 2011$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.
   (d) If $[K : \mathbf{Q}] = 2012$, prove that K contains an extension E with $[E : \mathbf{Q}] = 503$.
   (e) If $[K : \mathbf{Q}] = 2013$, prove that K contains an extension E with $[E : \mathbf{Q}] = 3$.

(f) If $[K : \mathbf{Q}] = 2014$, prove that K contains an extension E with $[E : \mathbf{Q}] = 19$.

(g) If $[K : \mathbf{Q}] = 2015$, prove that K contains an extension E with $[E : \mathbf{Q}] = 13$.

(h) If $[K : \mathbf{Q}] = 2016$, prove that K contains an extension E with $[E : \mathbf{Q}] = 63$.

57. Determine (with proof) the degree of the splitting field of $x^{10} - 25$.

58. (14.4 (5)) Let p be a prime and let F be a field. Let K be a Galois extension of F whose Galois group is a p-group (i.e., the degree $[K : F]$ is a power of p). Such an extension is called a p-extension (note that p-extensions are Galois by definition).

    (a) Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.

    (b) Give an example to show that (a) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

59. Prove that the Galois group of the splitting field of $x^4 + ax^2 + b$ is a subgroup of D_8.

60. (14.6 (3)) Let $q = p^n$. Prove that for any $a, b \in \mathbf{F}_q$, if $x^3 + ax + b$ is irreducible, then $-4a^3 - 27b^2$ is a square in $\mathbf{F}_q$.

61. (14.6 (48)).

62. Consider the polynomial $p(x) = x^5 - x^4 + 2x^2 - 2x + 2$.

    (a) Prove that $p(x)$ is irreducible mod 3, and hence irreducible, and deduce that the Galois group G of its splitting field is a transitive subgroup of S_5.

    (b) Prove that $p(x)$ has exactly one real root, and hence G contains an element of order 2.

    (c) Prove that the discriminant of $p(x)$ is $2^6 \cdot 17^2$, and conclude that the Galois group G of the splitting field of $p(x)$ is a subgroup of A_5.

    (d) Show that the transitive subgroups of A_5 are A_5, $\mathbf{Z}/5\mathbf{Z}$, and D_5.

    (e) Prove that
    $$p(x) \equiv (x-3)(x-2)(x^3 + 4x^2 + 3x + 4) \mod 11.$$

    (f) Deduce that $G = A_5$.

63. Draw the lattice of subfields of the splitting fields of the following polynomials.

    (a) $x^3 - 2$.

    (b) $x^4 - 7x^2 - 5$.

64. Show that the polynomial $x^5 - 4x + 2$ is not solvable in terms of radicals.

65. Determine whether $x^3 + 4x + 1$ is irreducible in $\mathbf{F}_5[x]$. What is its splitting field?

66. How many elements in $\mathbf{F}_8$ satisfy $a^5 + a + 1 = 0$?

67. Find an irreducible polynomial of degree 3 over $\mathbf{F}_5$.

68. Let $E/\mathbf{Q}$ be a Galois extension.

    (a) Show that E cannot be both the splitting field of an irreducible polynomial of degree 5 *and* of degree 7.

(b) Suppose E is the splitting field of an polynomial of degree p, and the splitting field of a polynomial of degree $p+1$, where p is prime.

   i. Prove that G is not solvable.

   ii. Prove that G is not A_n or S_n unless $n=5$.

   iii. Deduce that if $p=7$, then $G = \mathrm{GL}_3(\mathbf{F}_2)$.

69. Show that if the splitting field of $f(x)$ is Galois with Galois group A_n, then the discriminant $\Delta^2 = \prod_{i>j}(\alpha_i - \alpha_j)^2$ of $f(x)$ is positive.

70. Prove that if $K/\mathbf{Q}$ is a finite extension, then $K = \mathbf{Q}(\alpha)$ for some $\alpha \in K$.

71. Let $K/\mathbf{Q}$ be a Galois extension with Galois group G. Prove there exists a unique maximal subfield $F \subset K$ such that:

   (a) $F/\mathbf{Q}$ is Galois with abelian Galois group.

   (b) $F/\mathbf{Q}$ is Galois with solvable Galois group.

   (c) $F/\mathbf{Q}$ is Galois with $[F:\mathbf{Q}]$ odd.

   (d) $F/\mathbf{Q}$ is Galois with $[F:\mathbf{Q}]$ co-prime to p for any fixed prime p.

72. Let $K/\mathbf{Q}$ be a finite extension. Let $\alpha, \beta \in K$, and let $E = \mathbf{Q}(\alpha)$ and $F = \mathbf{Q}(\beta)$.

   (a) Let $H = \mathbf{Q}(\alpha+\beta)$. Prove that $[H:\mathbf{Q}] \le [E:\mathbf{Q}][F:\mathbf{Q}]$.

   (b) If $([E:\mathbf{Q}],[F:\mathbf{Q}]) = 1$, show that $[H:\mathbf{Q}] = [E:\mathbf{Q}][F:\mathbf{Q}]$.

73. Find a basis for the vector space $K = \mathbf{Q}(\sqrt[3]{2})$ over $\mathbf{Q}$. With respect to this basis, write down the matrix associated to the $\mathbf{Q}$-linear map $K \to K$ given by multiplication by $a + b\sqrt[3]{2}$. What is the trace of this matrix?

74. Let p be prime, and let ζ be a primitive pth root of unity. Prove that

$$\prod_{i=1}^{p-1}(1-\zeta^i) = p.$$

75. Suppose the polynomial $f(x)$ of degree 3 in $\mathbf{Q}[x]$ is irreducible. Prove that $f(x)$ considered as a polynomial over $\mathbf{Q}(\sqrt{2})[x]$ is still irreducible.

76. Let K be field of characteristic zero and suppose that $\zeta_p \in K$. Let L/K be an extension with $\mathrm{Gal}(L/K) = \langle\sigma\rangle = \mathbf{Z}/p\mathbf{Z}$.

   (a) Think of L as a p-dimensional vector space over K, and let $\sigma : L \to L$ be the corresponding K-linear map induced by σ. Let M denote the corresponding matrix for some choice of basis. Prove that $M^p = I$.

   (b) Prove that the characteristic polynomial of M^p is exactly $X^p - 1$, and deduce that the eigenvalues of M are precisely ζ^k for $k = 0, \ldots, p-1$.

   (c) Deduce that L/K has a basis $x_0, x_1, \ldots, x_{p-1}$ such that

$$\sigma x_i = \zeta^i x_i$$

   for all i.

(d) Compute this basis explcitly when $K = \mathbf{Q}(\zeta_4) = \mathbf{Q}(i)$ and $L/K = \mathbf{Q}(\zeta_5, i)$ with $p = 5$.

77. Let L/K be a Galois extension, and suppose that any intermediate field $L/F/K$ is either L or K. Prove that $[L : K]$ is prime.

78. Let L/K be a finite extension, and suppose that any intermediate field $L/F/K$ is either L or K. Show by example that $[L : K]$ does not have to be prime.

79. Find (with proof) all the subfields of $\mathbf{Q}(\sqrt[4]{2}, \sqrt{-1})$.

80. Prove that $\mathbf{Q}(\sqrt[6]{-3})$ is the splitting field of $x^6 + 3$.

81. Determine whether the following fields are Galois over $\mathbf{Q}$:
   (a) $\mathbf{Q}(\sqrt{1 + \sqrt{2}})$
   (b) $\mathbf{Q}(\sqrt{2} + \sqrt{3})$

82. Prove that if L/K has Galois group $\mathrm{Gal}(L/K) \simeq A_4$, then L does not contain any quadratic extension F/K.

83. Suppose that $f(x)$ is an irreducible polynomial of degree 3 over a perfect field K.
   (a) Let L/K be the splitting field of $f(x)$. Prove that $G := \mathrm{Gal}(L/K)$ is either $\mathbf{Z}/3\mathbf{Z}$ or S_3.
   (b) Let the roots of $f(x)$ be α, β, and γ. Prove there is a $\sigma \in G$ sending α to β, β to γ, and γ to α.
   (c) Let $\Delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \delta)$. Prove that $\sigma\Delta = \Delta$. Deduce that Δ lies in the fixed field F of $\langle \sigma \rangle$.
   (d) If $G = \mathbf{Z}/3\mathbf{Z}$, prove that $\Delta \in \mathbf{Q}$.
   (e) If $G = S_3$, prove that there exists a $\tau \in G$ such that $\tau\Delta = -\Delta$. Deduce that $\Delta \notin \mathbf{Q}$, but $\Delta^2 \in \mathbf{Q}$.
   (f) Deduce that $G = S_3$ if and only if the element $\Delta \in \mathbf{Q}$ is not a perfect square.
   (g) If $f(x) = x^3 + px + q$, prove that
   $$\alpha\beta\gamma = -q, \qquad \alpha\beta + \alpha\gamma + \beta\gamma = p, \qquad \alpha + \beta + \gamma = 0.$$
   (h) Deduce that
   $$\Delta^2 = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \delta)^2 = -4p^3 - 27q^2.$$
   (i) Compute the Galois groups G of the following cubics, as well as their quadratic subfields when $G = S_3$.
      i. $x^3 - 2$.
      ii. $x^3 - x - 1$.
      iii. $x^3 - 21x - 7$

84. Generalize the last problem. Let $f(x)$ be irreducible of degree n with coefficients in K, and let $G = \mathrm{Gal}(L/K)$ be thought of as a subgroup of S_n via the permutation action of the roots. If the roots of $f(x)$ in L are α_i, prove that if $\Delta = \prod_{i>j}(\alpha_i - \alpha_j)$, then $\Delta^2 \in K$, and $\Delta \in K$ if and only if $\mathrm{Gal}(L/K) \subset A_n$.

85. Let α be an algebraic number, and suppose that $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is odd. Prove that $[\mathbf{Q}(\alpha^2), \mathbf{Q}]$ is odd.

86. Let L/K be a finite Galois extension. Let $\sigma \in \mathrm{Gal}(L/K)$, and suppose that $K \subset F \subset L$. Prove that if $\sigma(F)$ is contained in F, then $\sigma(F)$ equals F.

87. Let $f(x) = x^4 + ax^2 + b \in K[x]$. Let L be the splitting field of K.

 (a) Prove that $[L : K]$ has order dividing 8. [Hint: show that $f(x)$ partially factors over the splitting field of $x^2 + ax + b$]

 (b) Prove that $\mathrm{Gal}(L/K)$ is a subgroup of D_8.

88. Let p and q be distinct primes. Let $K = \mathbf{Q}(\sqrt{p}, \sqrt{q})$.

 (a) Prove that $\mathrm{Gal}(K/\mathbf{Q}) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

 (b) Find all subfields of K.

 (c) Show there is an element $\alpha \in K$ such that $K = \mathbf{Q}(\alpha)$.

89. Let $S = \{p_1, p_2, \ldots, p_n\}$ be n distinct primes.

 (a) Let Σ denote the set consisting of non-trivial products of distinct elements of S. Prove that $|\Sigma| = 2^n - 1$.

 (b) If D_1 and D_2 denote elements of Σ, prove that $\mathbf{Q}(\sqrt{D_1}) \simeq \mathbf{Q}(\sqrt{D_2})$ if and only if $D_1 = D_2$.

 (c) Let $K = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Prove that K is the splitting field of

$$(X^2 - p_1)(X^2 - p_2) \cdots (X^2 - p_n).$$

 (d) Prove that $\mathrm{Gal}(K/\mathbf{Q})$ is a subgroup of $(\mathbf{Z}/2\mathbf{Z})^n$.

 (e) Prove that K has at least $2^n - 1$ subfields of degree 2.

 (f) Prove that $\mathrm{Gal}(K/\mathbf{Q}) = (\mathbf{Z}/2\mathbf{Z})^n$, and deduce that $[K : \mathbf{Q}] = 2^n$.

90. Let $L/\mathbf{Q}$ be Galois with $\mathrm{Gal}(L/\mathbf{Q}) = Q = \{\pm i, \pm j, \pm k, \pm 1\}$, the quaternion group of order 8. Prove that any quadratic subfield of $K \subset L$ is a real quadratic field; that is, admits a ring homomorphism injection $K \to \mathbf{R}$.

91. Find an irreducible polynomial with splitting field $\mathbf{F}_{32}$.

92. Let L/K be a finite extension of fields, and let R be a ring that contains K and is contained inside L, so $K \subset R \subset L$. Prove that R is a field.

93. If L/K is an extension of degree 2, prove that L is the splitting field of some polynomial in $K[x]$.

94. Suppose that $\mathbf{F}_{p^f}$ be the splitting field of $x^{17} - 1$ over $\mathbf{F}_p$. Prove that:

 (a) If $p = 2$, then $f = 8$.

 (b) If $p = 3$, then $f = 16$.

 (c) If $p = 17$, then $f = 1$.

 (d) For all p, f divides 16.

 [Hint: what is the order of $\mathbf{F}_q^\times$?]

95. Prove that the roots of $x^4 + 10x^2 + 1$ are $\pm\sqrt{2} \pm \sqrt{3}$.

 (a) Deduce that $x^4 + 10x^2 + 1$ is irreducible over $\mathbf{Q}$.

(b) Prove that 2 and 3 are both squares in $\mathbf{F}_{p^2}$ for any prime p, and deduce that $x^4 + 10x^2 + 1$ is never irreducible over $\mathbf{F}_p$.

96. Find the splitting fields of the following polynomials, and draw the lattice of subfields.

(a) $x^4 + 1$.

(b) $x^4 + 2$.

(c) $x^3 - 3$.

(d) $x^4 + 4$.

(e) $x^5 - 5$.

(f) $x^{11} - 1$.

97. (**Gauss Sums**) Let $p > 2$ be prime, and let $G = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$, where ζ is a primitive pth root of unity, and where $a \in G$ sends ζ to ζ^a.

(a) Say that $a \not\equiv 0 \mod p$ is a quadratic residue if it is a square; that is, $a \equiv x^2 \mod p$. Prove that G has a unique subgroup H of consisting of quadratic residues.

(b) For $a \not\equiv 0 \mod p$, define the quadratic residue symbol as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue,} \\ -1 & a \text{ is not quadratic residue.} \end{cases}$$

Prove that the map $G \to \{\pm 1\} = \mathbf{Z}/2\mathbf{Z}$ sending a to (a/p) is a homomorphism with kernel H.

(c) Prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

(d) Let $\chi := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a = \sum_{a \in G} \left(\frac{a}{p}\right) \zeta^a \in \mathbf{Q}(\zeta)$. Prove that, for $g \in G$, $g\chi = \left(\frac{a}{p}\right) \chi$.

(e) Deduce that χ^2 is fixed by G and hence $\chi^2 \in \mathbf{Q}$. Deduce that either $\chi = 0$, or χ generates the unique quadratic subfield $K := \mathbf{Q}(\zeta)^H \subset \mathbf{Q}(\zeta)$.

(f) Prove that if one chooses any embedding of $\mathbf{Q}(\zeta)$ into $\mathbf{C}$, then complex conjugation acts on $\mathbf{Q}(\zeta)$ by $-1 \in G$, that is, $\zeta \mapsto \zeta^{-1}$.

(g) Prove that if one chooses any embedding of $\mathbf{Q}(\zeta)$ into $\mathbf{C}$, then the absolute value squared $|x|^2$ of the image of $x \in \mathbf{Q}(\zeta) \subset \mathbf{C}$ is equal to $x \cdot cx$. If $p \geq 5$, show that the absolute value of $|1+\zeta|$ depends on the choice of embedding $\mathbf{Q}(\zeta) \to \mathbf{C}$. In contrast, show that the absolute value of $|\chi^2|$ does not depend on the embedding. (use (97e))

(h) Prove that $|\chi^2| = \chi \cdot c\chi = \left(\sum_{a \in G} \left(\frac{a}{p}\right) \zeta^a\right) \left(\sum_{b \in G} \left(\frac{b}{p}\right) \zeta^{-b}\right) = \sum_{a,b \in G} \left(\frac{ab}{p}\right) \zeta^{a-b}$.

(i) By replacing a by ab in the sum above, show that

$$|\chi^2| = \sum_{a,b \in G} \left(\frac{a}{p}\right) \zeta^{(a-1)b}.$$

(j) Prove that $\sum_{b \in G} \zeta^{(a-1)b}$ equals $p - 1$ if $a = 1 \in G$ and equals -1 for all other $a \in G$.

(k) Deduce that $|\chi^2| = \sum_{a,b \in G} \left(\frac{ab}{p}\right) \zeta^{a-b} = p + \sum_{a \in G} \left(\frac{a}{p}\right)(-1) = p$.

(l) Show that complex conjugation $c = -1$ lies in H if and only if $p \equiv 1 \mod 4$. (use (97c))

(m) Show that $c\chi = \chi$ if $c \in H$ and $c\chi = -\chi$ if $c \notin H$. Deduce that if $\mathbf{Q}(\zeta) \subset \mathbf{C}$, then χ is either real or purely imaginary depending on whether $c \in H$. (use (97d))

(n) Let $p^* = p$ if $p \equiv 1 \mod 4$ and $-p$ if $p \equiv -1 \mod 4$. Prove that $\chi^2 = p^*$, and deduce that the quadratic subfield K of $\mathbf{Q}(\zeta)$ is equal to $\mathbf{Q}(\sqrt{p^*})$.

(o) Now suppose that $\mathbf{Q}(\zeta) \to \mathbf{C}$ sends ζ to the very specific choice $e^{2\pi i/p} \in \mathbf{C}$. Let $\sqrt{p^*}$ denote the complex number which is either positive if $p^* > 0$ or has positive imaginary part if $p^* < 0$. We know that $\chi^2 = p^*$ so $\chi = \pm\sqrt{p^*}$. Determine the correct sign in this formula for $p = 3$, 5, 7, and 11.

(p) (*) Determine the sign in part (97o) for all p.

(a) Let L be the splitting field of the polynomial $x^4 - x - 1$ over $\mathbf{Q}$, and denote the roots by α_1, α_2, α_3, and α_4. You may assume that $G = \mathrm{Gal}(L/\mathbf{Q}) = S_4$.

   i. Determine the number n of subfields E of L. (Thus two fields $E \subset L$ and $F \subset L$ count as one if and only if $E = F$ inside L.)

   ii. Determine the number m of subfields E of L up to isomorphism. (Thus two fields $E \subset L$ and $F \subset L$ count as one if and only if there is an isomorphism $E \simeq F$.)

   iii. For each of the n subfields E in part (97(a)i), write down a primitive element $\theta \in L$; that is, an element $\theta \in L$ such that $E = \mathbf{Q}(\theta) \subset L$.

   iv. For each of the n subfields E and elements θ of part (97(a)iii), write down the irreducible polynomial of θ in $\mathbf{Q}[x]$.

98. **Kummer Extensions.** Let K be a field of characteristic zero containing the splitting field of $x^n - 1$. Let L/K be Galois with $\mathrm{Gal}(L/K) = \mathbf{Z}/n\mathbf{Z}$.

(a) Let ζ be a primitive nth root of unity in K, and let A and B denote the following matrices:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \dots & \zeta^{n-1} \\ \\ 1 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^8 & \dots & \zeta^{2(n-1)} \\ & \ddots & & & & & \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \zeta^{3(n-1)} & \zeta^{4(n-1)} & \dots & \zeta^{(n-1)^2} \end{pmatrix} = \left(\zeta^{ij}\right)_{i,i=0}^{n-1},$$

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta^{-1} & \zeta^{-2} & \zeta^{-3} & \zeta^{-4} & \dots & \zeta^{-(n-1)} \\ \\ 1 & \zeta^{-2} & \zeta^{-4} & \zeta^{-6} & \zeta^{-8} & \dots & \zeta^{-2(n-1)} \\ & \ddots & & & & & \\ 1 & \zeta^{-(n-1)} & \zeta^{-2(n-1)} & \zeta^{-3(n-1)} & \zeta^{-4(n-1)} & \dots & \zeta^{-(n-1)^2} \end{pmatrix} = \left(\zeta^{-ij}\right)_{i,i=0}^{n-1}.$$

Prove that $A.B = n.I$.

(b) Suppose that $\theta \in L$. Show that

$$x_k = \sum_{i=0}^{n-1} \zeta^{-ik} \sigma^k \theta$$

satisfies $\sigma x_k = \zeta^k x_k$.

(c) Let $f(x)$ be a degree n polynomial over K whose splitting field is L. Let θ be a root of $f(x)$. Prove that

$$\theta = \frac{1}{n}\sum_{i=0}^{n-1} x_i,$$

where x_i are defined as above.

(d) Prove that $x_i^n \in K$.

(e) Let $K = \mathbf{Q}(\zeta_5)$, and let L be the subfield of $\mathbf{Q}(\zeta_5, \zeta_{11})$ of degree 5 over K, and let $\theta = \zeta_{11} + \zeta_{11}^{-1}$. Prove that θ is a root of

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0.$$

(f) Suppose that $\sigma\zeta_{11} = \zeta_{11}^2$, so that $\sigma x = x^2 - 2$. Prove that

$$x_0^5 = -1$$

$$\begin{aligned}
x_1^5 &= 385y^3 + 110y^2 + 220y - 66\\
x_2^5 &= -110y^3 + 110y^2 + 275y - 176\\
x_3^5 &= -165y^3 - 385y^2 - 275y - 451\\
x_4^5 &= -110y^3 + 165y^2 - 220y - 286
\end{aligned}$$

(g) Suppose that $\zeta_5 = e^{2\pi i/5}$. Show that

$$y = \frac{\sqrt{5}-1}{4} + \sqrt{-\frac{5+\sqrt{5}}{8}}.$$

Deduce that

$$x_0^5 = -1$$

$$x_1^5 = -\left(\frac{11(89+25\sqrt{5})}{4}\right) + \frac{55(13-5\sqrt{5})}{2}\sqrt{-\frac{5+\sqrt{5}}{8}} \sim -398.48 + 47.5915i,$$

$$x_2^5 = -\left(\frac{11(89-25\sqrt{5})}{4}\right) + 55(3+2\sqrt{5})\sqrt{-\frac{5+\sqrt{5}}{8}} \sim -91.0203 + 390.853i,$$

$$x_3^5 = -\left(\frac{11(89-25\sqrt{5})}{4}\right) - 55(3+2\sqrt{5})\sqrt{-\frac{5+\sqrt{5}}{8}} \sim -91.0203 - 390.853i,$$

$$x_4^5 = -\left(\frac{11(89+25\sqrt{5})}{4}\right) - \frac{55(13-5\sqrt{5})}{2}\sqrt{-\frac{5+\sqrt{5}}{8}} \sim -398.48 - 47.5915i,$$

(h) Deduce that $2\cos(2\pi/11)$ is equal to

$$\begin{aligned}
&\frac{1}{5}\left(-1 + \sqrt[5]{-\left(\frac{11(89+25\sqrt{5})}{4}\right) + \frac{55(13-5\sqrt{5})}{2}\sqrt{-\frac{5+\sqrt{5}}{8}}} + \sqrt[5]{-\left(\frac{11(89-25\sqrt{5})}{4}\right) + 55(3+2\sqrt{5})\sqrt{-\frac{5+\sqrt{5}}{8}}}\right.\\
&\left. + \sqrt[5]{-\left(\frac{11(89-25\sqrt{5})}{4}\right) - 55(3+2\sqrt{5})\sqrt{-\frac{5+\sqrt{5}}{8}}} + \sqrt[5]{-\left(\frac{11(89+25\sqrt{5})}{4}\right) - \frac{55(13-5\sqrt{5})}{2}\sqrt{-\frac{5+\sqrt{5}}{8}}}\right)\\
&\sim \frac{1}{5}\left(-1 + (2.63611 - 2.0127i) + (2.07016 - 2.59122i) + (2.07016 + 2.59122i) + (2.63611 + 2.0127i)\right)
\end{aligned}$$

where the last line indicates which 5th root in $\mathbf{C}$ one is considering.

99. Let $f(x) \in \mathbf{Q}[x]$ be an irreducible polynomial of degree d. Suppose that $K = \mathbf{Q}[x]/f(x)$. Prove if $K/\mathbf{Q}$ is a splitting field, then the roots of $f(x)$ are either all real or none of them are real.

100. Prove that If $K/\mathbf{Q}$ and $L/\mathbf{Q}$ have co-prime degrees, then $K \cap L = \mathbf{Q}$.

101. Prove that if L/K is a finite extension, and M/L is a finite extension, then there is an equality $[M : K] = [M : L][L : K]$.

102. Let $f(x)$ be a separable polynomial over $\mathbf{F}_p[x]$ of degree n. Suppose that $f(x)$ factors as

$$f(x) = \prod f_i(x),$$

where $f_i(x)$ are irreducible of degree r_i for $\sum r_i = n$. Let $K/\mathbf{F}_p$ be the splitting field of $f(x)$, and let $G \subset S_n$ where $G = \mathrm{Gal}(K/\mathbf{F}_p)$ acts on the roots. Prove that G is generated by an element $\sigma \in S_n$ whose cycle decomposition is a product of disjoint cycles of length r_i.

103. Prove that there does not exist a separable polynomial $f(x)$ of degree 4 over $\mathbf{F}_2$ whose corresponding Galois group $G \subset S_4$ is generated by $\sigma = (12)(34)$.

104. Let $K/\mathbf{Q}$ be an extension of degree n.

   (a) Prove that if $n = p$ is prime, then $K/\mathbf{Q}$ has no intermediate subfields except $\mathbf{Q}$ and K.

   (b) Let $L/\mathbf{Q}$ be the Galois closure of K, let $G = \mathrm{Gal}(L/\mathbf{Q})$, and $H = \mathrm{Gal}(L/K)$. Prove that the number of intermediate subfields between K and $\mathbf{Q}$ is the number of subgroups Γ of G containing H.

   (c) Prove that if $G = S_n$ with $n = [K : \mathbf{Q}]$ then there are no intermediate subfields.

   (d) Suppose that $n = 6$. Decide whether the following situations are possible:

      i. There exists a unique intermediate proper subfield $\mathbf{Q} \subset E \subset K$, and $[E : \mathbf{Q}] = 2$.

      ii. There exists a unique intermediate proper subfield $\mathbf{Q} \subset E \subset K$, and $[E : \mathbf{Q}] = 3$.