Problems

1. 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) $(\mathbf{Z}/25\mathbf{Z})^\times$
2. 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.
3. 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.
4. 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) $\cos(10^\circ)$.
5. How many irreducible factors does $X^{342} - 1$ have over $\mathbf{F}_7$? (Hint: what is the splitting field of this polynomial?)
6. Let $E/\mathbf{Q}$ and $F/\mathbf{Q}$ be subfields of a fixed, finite extension $K/\mathbf{Q}$. Prove that $[E : \mathbf{Q}] \geq [E.F : F]$.
7. 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) $\mathbf{Q}(\sqrt[3]{1+\sqrt{2}})$.
8. [**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 $q = p^p$.
9. [**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 9k.

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 $(1, 2)$.

10. [**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.

(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 K.

(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.

11. Let $a(x)$ and $b(x)$ be 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 $n \neq 6$.

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

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

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

15. Let L/K be a finite extension of fields. If $x \in L$, the map $L \to L$ determined by multiplication by x is a K-linear homomorphism. Hence, if we fix a basis for L/K, x determines a matrix M. Let $\mathrm{Tr}_{L/K}(x) := \mathrm{Trace}(M)$ and $\mathrm{N}_{L/K}(x) := \mathrm{Det}(M)$.

(a) Prove that $\mathrm{Tr}_{L/K}(x) \in K$ and $\mathrm{N}_{L/K}(x) \in K$ for all $x \in L$.

(b) Prove that $\mathrm{Tr}_{L/K}(x)$ and $\mathrm{N}_{L/K}(x)$ do not depend on the choice of basis for L over K.

(c) Prove that $\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$, and $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$.

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

(e) If $K = \mathbf{F}_p(t)$, and $L = \mathbf{F}_p(t^{1/p})$, prove that $\mathrm{Tr}_{L/K}(x) = 0$ for all $x \in L$.

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

16. (14.3 (8)). Determine the splitting field of $x^p - x - a = 0$ over $\mathbf{F}_p$, where $a \neq 0$.

17. (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.

18. (14.5 (10) Prove that $\mathbf{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbf{Q}$.

19. (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) $x^5 + x - 1$.

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

21. (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 $\mathbf{F}_q$.

22. (14.6 (48)).

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

    (a) Prove that $p(x)$ is irreducible, and hence 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 splitting field of $p(x)$ has Galois group A_5.

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

    (a) $x^3 - 2$.
    (b) $x^4 - 7x^2 - 5$.

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

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

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

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

29. 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 $G = \mathrm{GL}_3(\mathbf{F}_2)$.

iv. Let $G = \mathrm{PSL}_2(\mathbf{F}_7)$.

30. 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.

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

32. 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.

33. 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 $[H : \mathbf{Q}] \leq [E : \mathbf{Q}][F : \mathbf{Q}]$.

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

34. 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?

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

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

36. 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.

37. 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.

38. 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.

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

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

41. Determine whether the following fields are Galois over $\mathbf{Q}$:

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

(b) $\mathbf{Q}(\sqrt{2}+\sqrt{3})$

42. 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.

43. 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. $x^3 - 21x - 7$

44. 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 $\mathrm{Gal}(L/K) \subset A_n$.

45. 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.

46. 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.

47. 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.

48. 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 $K = \mathbf{Q}(\alpha)$.

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

50. 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.

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

52. 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 $\mathbf{F}_q^\times$?]

53. 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 $\mathbf{F}_p$.

54. 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) $x^{11} - 1$.

55. 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.

56. Prove that If $K/\mathbf{Q}$ and $L/\mathbf{Q}$ have different degrees, then $K \cap L = \mathbf{Q}$.

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

58. Let $K/\mathbf{Q}$ be a Galois extension of degree 2009. Prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.