

Problems

- Find, explicitly, the subgroups of the following groups:
 - $(\mathbf{Z}/16\mathbf{Z})^\times$
 - $(\mathbf{Z}/11\mathbf{Z})^\times$
 - $(\mathbf{Z}/60\mathbf{Z})^\times$
 - $(\mathbf{Z}/25\mathbf{Z})^\times$
- How many irreducible factors does $X^{342} - 1$ have over \mathbf{F}_7 ? (Hint: what is the splitting field of this polynomial?)
- Let E/\mathbf{Q} and F/\mathbf{Q} be subfields of a fixed, finite extension K/\mathbf{Q} . Prove that $[E : \mathbf{Q}] \geq [E.F : F]$.
- Determine all automorphisms of the following fields.
 - $\mathbf{Q}(\sqrt[3]{2})$.
 - $\mathbf{Q}(\sqrt{1 + \sqrt{2}})$.
 - $\mathbf{Q}(\sqrt[3]{1 + \sqrt{2}})$.
- [**Artin–Schreier extensions**] Let E be a field of characteristic p .
 - If $\alpha \in E$, prove that the polynomial $p(x) = x^p - x - \alpha$ is separable.
 - If β is a root of $p(x)$, show that $\beta + 1$ is also a root of $p(x)$.
 - Deduce that either $p(x)$ splits completely in E or $p(x)$ is irreducible.
 - Deduce that the splitting field F/E of $p(x)$ is either E or is cyclic of degree p .
 - Find the splitting field of $x^p - x - 1$ over \mathbf{F}_p .
- [**Field Embeddings, I**] Let E/\mathbf{Q} be a finite extension. Let K/\mathbf{Q} be a Galois extension with Galois group $G = \text{Gal}(K/\mathbf{Q})$. Let $N = \text{Hom}(E, K)$ be the set of ring homomorphisms from E to K (so 1 maps to 1).
 - Prove that either N is empty, or there exists an inclusion from E to K .
 - If $\phi \in N$, show that $\phi(E)$ is a subfield of K .
 - Prove that if $\sigma \in G$, and $\phi : E \rightarrow K$ is an element of N , then the map $\sigma.\phi$ defined by sending x to $\sigma(\phi(x))$ is an element of N .
 - Prove that this construction gives a group action of G on N .
 - Prove that the stabilizer of ϕ is $\text{Gal}(K/\phi(E))$.
 - Prove that G acts transitively on N .
 - Prove that either N is empty, or $|N| = [E : \mathbf{Q}]$.
 - Prove that for any field K (not necessarily finite or Galois) containing the splitting field of E , $N = \text{Hom}(E, K)$ has order $[E : \mathbf{Q}]$.
 - If $K = \mathbf{C}$, one can write $N = N_{\mathbf{R}} \cup N_{\mathbf{C}}$, where $N_{\mathbf{R}} = \text{Hom}(E, \mathbf{R})$, 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 $\Gamma = \text{Gal}(E/\mathbf{Q})$. Let K be any field (not necessarily finite or Galois) containing the splitting field of E . Prove that there is an action of $\Gamma = \text{Gal}(E/\mathbf{Q})$ on $N = \text{Hom}(E, K)$ 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 $\Gamma = \text{Gal}(E/\mathbf{Q})$. Let Γ act on $N = N_{\mathbf{C}}$ as in part 6k.
- 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} .
 - 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.
 - 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 $F \subseteq E^{\Phi}$.
 - 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 $[E : E^+] = 2$.
 - 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 $(1, 2)$.
7. **[Field Embeddings, II]** Let E/\mathbf{Q} be a finite extension. Let K/\mathbf{Q} be a Galois extension with Galois group $G = \text{Gal}(K/\mathbf{Q})$. Let M be the set of subfields of K that are isomorphic to E .
- Prove that M is empty, or there exists an inclusion from E to K .
 - Prove that G acts on M .
 - If $F \in M$, prove that the stabilizer of F is the normalizer N_F of $\text{Gal}(K/F)$.
 - Prove that G acts transitively on M .
 - Prove that $|M| = [G : N_F]$, for any $F \in M$.
 - Prove that $|M| = 1$ if and only if E/\mathbf{Q} is Galois.
 - If $F \in M$, let $H = K^{N_F}$. Prove that:
 - H is contained in F .
 - F/H is Galois.
 - If $H' \subset F$ is any subfield of F such that F/H' is Galois, then H' contains H .
 - H does not depend on K .
 - 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.
8. 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 $G = \text{Gal}(K/\mathbf{Q})$, $H_A = \text{Gal}(K/A)$, and $H_B = \text{Gal}(K/B)$.
- Prove that $\bigcap \sigma H \sigma^{-1} = 1$. for $H = H_A$ and H_B .
 - Prove that $|H_A| = |H_B|$.
 - 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 $n \neq 6$.
9. Determine (with proof) the degree of $\mathbf{Q}(\sqrt{3 + 2\sqrt{2}})$ over \mathbf{Q} .
10. * Prove that $\sqrt{\sqrt[3]{2} - 1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}$.
11. Determine (with proof) the degree of the splitting field of $x^{10} - 25$.
12. Let L/K be a finite extension of fields. If $x \in L$, the map $L \rightarrow L$ 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 $\text{Tr}_{L/K}(x) := \text{Trace}(M)$ and $\text{N}_{L/K}(x) := \text{Det}(M)$.
- (a) Prove that $\text{Tr}_{L/K}(x) \in K$ and $\text{N}_{L/K}(x) \in K$ for all $x \in L$.
- (b) Prove that $\text{Tr}_{L/K}(x)$ and $\text{N}_{L/K}(x)$ do not depend on the choice of basis for L over K .
- (c) Prove that $\text{Tr}_{L/K}(x + y) = \text{Tr}_{L/K}(x) + \text{Tr}_{L/K}(y)$, and $\text{N}_{L/K}(xy) = \text{N}_{L/K}(x)\text{N}_{L/K}(y)$.
- (d) If $x \in K$, show that $\text{Tr}_{L/K}(x) = x[L : K]$ and $\text{N}_{L/K}(x) = x^{[L:K]}$.
- (e) If $K = \mathbf{F}_p(t)$, and $L = \mathbf{F}_p(t^{1/p})$, prove that $\text{Tr}_{L/K}(x) = 0$ 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 $\text{Tr}_{L/K}(x) \neq 0$.
13. (14.3 (8)). Determine the splitting field of $x^p - x - a = 0$ over \mathbf{F}_p , where $a \neq 0$.
14. (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.
15. (14.5 (10)) Prove that $\mathbf{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over \mathbf{Q} .
16. (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) $x^5 + x - 1$.
17. Prove that the Galois group of the splitting field of $x^4 + ax^2 + b$ is a subgroup of D_8 .
18. (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 .
19. (14.6 (48)).
20. Draw the lattice of subfields of the splitting fields of the following polynomials.
- (a) $x^3 - 2$.
- (b) $x^4 - 7x^2 - 5$.
21. Determine whether $x^3 + 4x + 1$ is irreducible in $\mathbf{F}_5[x]$. What is its splitting field?
22. How many elements in \mathbf{F}_8 satisfy $a^5 + a + 1 = 0$?
23. Find an irreducible polynomial of degree 3 over \mathbf{F}_5 .
24. 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 a polynomial of degree p , and the splitting field of a polynomial of degree $p + 1$, where p is prime.
- Prove that G is not solvable.
 - Prove that G is not A_n or S_n unless $n = 5$.
 - Deduce that if $p = 7$, then $G = \text{GL}_3(\mathbf{F}_2)$.
 - Let $G = \text{PSL}_2(\mathbf{F}_7)$.
25. 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.
26. Prove that if K/\mathbf{Q} is a finite extension, then $K = \mathbf{Q}(\alpha)$ for some $\alpha \in K$.
27. Let K/\mathbf{Q} be a Galois extension with Galois group G . Prove there exists a unique maximal subfield $F \subset K$ such that:
- F/\mathbf{Q} is Galois with abelian Galois group.
 - F/\mathbf{Q} is Galois with solvable Galois group.
 - F/\mathbf{Q} is Galois with $[F : \mathbf{Q}]$ odd.
 - F/\mathbf{Q} is Galois with $[F : \mathbf{Q}]$ co-prime to p for any fixed prime p .
28. Let K/\mathbf{Q} be a finite extension. Let $\alpha, \beta \in K$, and let $E = \mathbf{Q}(\alpha)$ and $F = \mathbf{Q}(\beta)$.
- Let $H = \mathbf{Q}(\alpha + \beta)$. Prove that $[H : \mathbf{Q}] \leq [E : \mathbf{Q}][F : \mathbf{Q}]$.
 - * If $([E : \mathbf{Q}], [F : \mathbf{Q}]) = 1$, show that $[H : \mathbf{Q}] = [E : \mathbf{Q}][F : \mathbf{Q}]$.

29. 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 $K \rightarrow K$ given by multiplication by $a + b\sqrt[3]{2}$. What is the trace of this matrix?
30. 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.
31. 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.
32. 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.
33. Find (with proof) all the subfields of $\mathbf{Q}(\sqrt[4]{2}, \sqrt{-1})$.
34. Prove that $\mathbf{Q}(\sqrt[6]{-3})$ is the splitting field of $x^6 + 3$.
35. Determine whether the following fields are Galois over \mathbf{Q} :
- $\mathbf{Q}(\sqrt{1 + \sqrt{2}})$
 - $\mathbf{Q}(\sqrt{2} + \sqrt{3})$
36. Prove that if L/K has Galois group $\text{Gal}(L/K) \simeq A_4$, then L does not contain any quadratic extension F/K .
37. Suppose that $f(x)$ is an irreducible polynomial of degree 3 over a perfect field K .
- Let L/K be the splitting field of $f(x)$. Prove that $G := \text{Gal}(L/K)$ is either $\mathbf{Z}/3\mathbf{Z}$ or S_3 .
 - 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 .
 - Let $\Delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \delta)$. Prove that $\sigma\Delta = \Delta$. Deduce that Δ lies in the fixed field F of $\langle \sigma \rangle$.
 - If $G = \mathbf{Z}/3\mathbf{Z}$, prove that $\Delta \in \mathbf{Q}$.
 - If $G = S_3$, prove that there exists a $\tau \in G$ such that $\tau\Delta = -\Delta$. Deduce that $\Delta \notin \mathbf{Q}$, but $\Delta^2 \in \mathbf{Q}$.
 - Deduce that $G = S_3$ if and only if the element $\Delta \in \mathbf{Q}$ is not a perfect square.
 - If $f(x) = x^3 + px + q$, prove that

$$\alpha\beta\gamma = -q, \quad \alpha\beta + \alpha\gamma + \beta\gamma = p, \quad \alpha + \beta + \gamma = 0.$$
 - Deduce that

$$\Delta^2 = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \delta)^2 = -4p^3 - 27q^2.$$
 - Compute the Galois groups G of the following cubics, as well as their quadratic subfields when $G = S_3$.
 - $x^3 - 2$.
 - $x^3 - x - 1$.
 - $x^3 - 21x - 7$.

38. Generalize the last problem. Let $f(x)$ be irreducible of degree n with coefficients in K , and let $G = \text{Gal}(L/K)$ 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 $\text{Gal}(L/K) \subset A_n$.
39. 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.
40. Let L/K be a finite Galois extension. Let $\sigma \in \text{Gal}(L/K)$, and suppose that $K \subset F \subset L$. Prove that if $\sigma(F)$ is contained in F , then $\sigma(F)$ equals F .
41. Let $f(x) = x^4 + ax^2 + b \in K[x]$. Let L be the splitting field of K .
- Prove that $[L : K]$ has order dividing 8. [Hint: show that $f(x)$ partially factors over the splitting field of $x^2 + ax + b$]
 - Prove that $\text{Gal}(L/K)$ is a subgroup of D_8 .
42. Let p and q be distinct primes. Let $K = \mathbf{Q}(\sqrt{p}, \sqrt{q})$.
- Prove that $\text{Gal}(K/\mathbf{Q}) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
 - Find all subfields of K .
 - Show there is an element $\alpha \in K$ such that $K = \mathbf{Q}(\alpha)$.
43. Find an irreducible polynomial with splitting field \mathbf{F}_{32} .
44. 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.
45. If L/K is an extension of degree 2, prove that L is the splitting field of some polynomial in $K[x]$.
46. Suppose that \mathbf{F}_{p^f} be the splitting field of $x^{17} - 1$ over \mathbf{F}_p . Prove that:
- If $p = 2$, then $f = 8$.
 - If $p = 3$, then $f = 16$.
 - If $p = 17$, then $f = 1$.
 - For all p , f divides 16.
- [Hint: what is the order of \mathbf{F}_q^\times ?]
47. Prove that the roots of $x^4 + 10x^2 + 1$ are $\pm\sqrt{2} \pm \sqrt{3}$.
- Deduce that $x^4 + 10x^2 + 1$ is irreducible over \mathbf{Q} .
 - 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 .
48. Find the splitting fields of the following polynomials, and draw the lattice of subfields.
- $x^4 + 1$.
 - $x^4 + 2$.
 - $x^3 - 3$.
 - $x^4 + 4$.
 - $x^5 - 5$.

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

49. 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.
50. Prove that If K/\mathbf{Q} and L/\mathbf{Q} have co-prime degrees, then $K \cap L = \mathbf{Q}$.
51. Prove that if L/K is a finite extension, and M/L is a finite extension, then $[M : K] = [M : L][L : K]$.
52. Let K/\mathbf{Q} be a Galois extension of degree 2009. Prove that $\text{Gal}(K/\mathbf{Q})$ is abelian.