Field Theory Problems

I. Degrees, etc.

1. Answer the following:
   (a) Find $u \in \mathbb{R}$ such that $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.
   (b) Describe how you would find all $w \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ such that $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

2. If $a, b \in K$ are algebraic over F are of degree m, n, respectively, with $(m, n) = 1$, show that $[F(a, b) : F] = mn$.

3. If $|F| = q < \infty$ show:
   (a) There exists a prime p such that char $F = p$.
   (b) $q = p^n$ some n.
   (c) $a^q = a$ for all $a \in F$.
   (d) If $b \in K$ is algebraic over F then $b^{q^m} = b$ for some $m > 0$.

4. Let u be a root of $f = t^3 - t^2 + t + 2 \in \mathbb{Q}[t]$ and $K = \mathbb{Q}(u)$.
   (a) Show that $f = m_{\mathbb{Q}}(u)$.
   (b) Express $(u^2+u+1)(u^2-u)$ and $(u-1)^{-1}$ in the form au^2+bu+c, for some $a, b, c \in \mathbb{Q}$.

5. Let $\zeta = \cos\frac{\pi}{6} + i \sin\frac{\pi}{6} \in \mathbf{C}$. Show that $\zeta^{12} = 1$ but $\zeta^r \neq 1$ for $1 \leq r < 12$. Show also that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ and find $m_{\mathbb{Q}}(\zeta)$.

6. Let $K = F(u)$, u algebraic over F and degree of u odd. Show that $K = F(u^2)$.

7. Let u be transcendental over F and $F < E \subseteq F(u)$. Show that u is algebraic over E.

8. If $f = t^n - a \in F[t]$ is irreducible, $u \in K$ is a root of f, and $n/m \in \mathbb{Z}$, show that $|F(u^m) : F| = \dfrac{n}{m}$. What is $m_F(u^m)$?
9. If a^n is algebraic over a field F for some $n > 0$, show that a is algebraic over F.

II. Roots, splitting fields, etc

10. If $f \in \mathbb{Q}[t]$ and K is a splitting field of f over $\mathbb{Q}$, determine $[K : \mathbb{Q}]$ if f is:
    (a) $t^4 + 1$.
    (b) $t^6 + 1$.
    (c) $t^4 - 2$.
    (d) $t^6 - 2$.
    (e) $t^6 + t^3 + 1$.

11. Find the splitting fields K for $f \in \mathbb{Q}[t]$ and $[K : \mathbb{Q}]$ if f is:
    (a) $t^4 - 5t^2 + 6$.
    (b) $t^6 - 1$.
    (c) $t^6 - 8$.

12. Let $F = \mathbb{Z}/p\mathbb{Z}$ then show:
    (a) There exists $f \in F[t]$ with $\deg f = 2$ and f irreducible.
    (b) Use the f in (a) to construct a field with p^2 elements.
    (c) If $f_1, f_2 \in F[t]$ have $\deg f_i = 2$ and f_i irreducible for $i = 1, 2$, show that their splitting fields are isomorphic.

13. Let K/F and $f \in F[t]$. Show the following:
    (a) If $\varphi : K \to K$ is an F-automorphism, then φ takes roots of f in K to roots of f in K.
    (b) If $F \subseteq \mathbb{R}$ and $\alpha = a + ib$ is a root of f with $a, b \in \mathbb{R}$ then $\bar{\alpha} = a - ib$ is also a root of f.
    (c) Let $F = \mathbb{Q}$. If $m \in \mathbb{Z}$ is not a square and $a + b\sqrt{m} \in \mathbb{C}$ is a root of f with $a, b \in \mathbb{Q}$ then $a - b\sqrt{m}$ is also a root of f in $\mathbb{C}$.

14. Prove any (field) automorphism $\varphi : \mathbb{R} \to \mathbb{R}$ is the identity automorphism.

15. Let $p_1, \ldots, p_n$ be n distinct prime numbers. Let $f = (t^2 - p_1) \cdots (t^2 - p_n) \in \mathbb{Q}[t]$. Show that $K = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$ is a splitting field of f over $\mathbb{Q}$ and $[K : \mathbb{Q}] = 2^n$. Formulate a generalization of the statement for which your proof still works.

16. Find a splitting field of $f \in F[t]$ if $F = \mathbb{Z}/p\mathbb{Z}$ and $f = t^{p^e} - t$, $e > 0$.

17. Let F be a field of characteristic $p > 0$. Show that $f = t^4 + 1 \in F[t]$ is not irreducible. Let K be a splitting field of f over F. Determine which finite field F must contain so that $K = F$.

18. Let $f = t^6 - 3 \in F[t]$. Construct a splitting field K of f over F and determine $[K : F]$ for each of the cases: $F = \mathbb{Q}, \mathbf{Z}/5\mathbf{Z}$ or $\mathbf{Z}/7\mathbf{Z}$. Do the same thing if f is replaced by $g = t^6 + 3 \in F[t]$

III. Multiple roots and separability.

19. Show the following:
    (a) If $f \in F[t]$, char $F = 0$, and the derivative $f' = 0$ show $f \in F$.
    (b) If char $F = p \neq 0$, $f \in F[t]$, and $f' = 0$, then there exists $g \in F[t]$ such that $f(t) = g(t^p)$.

20. Show if x is transcendental over F, then $t^2 - x \in F(x)[t]$ is irreducible.

21. Suppose that char $F = p \neq 0$. Show the following;
    (a) The map $F \to F$ given by $x \mapsto x^p$ is a monomorphism. Denote its image by F^p.
    (b) If K/F is algebraic and $\alpha \in K$ is separable over $F(\alpha^p)$, then $\alpha \in F(\alpha^p)$.
    (c) Every finite field is perfect, i.e., every algebraic extension is separable.

22. Suppose that char $F = p \neq 0$. Show the following:
    (a) If K/F is separable then $K = F(K^p)$.
    (b) Suppose that K/F is finite and $K = F(K^p)$. If $\{x_1, ..., x_n\} \subset K$ is linearly independent over F, then so is $\{x_1^p, ..., x_n^p\}$.
    (c) If K/F is finite and $K = F(K^p)$, then K/F is separable.

23. Let K/F. Show the following:
    (a) If $\alpha \in K$ is separable over F, then $F(\alpha)/F$ is separable.
    (b) If $\alpha_1, ..., \alpha_n \in K$ are separable over F, then $F(\alpha_1, ..., \alpha_n)/F$ is separable.
    (c) Let $F_{\text{sep}} = \{\alpha \in K \mid \alpha \text{ separable over } F\}$. Then F_{sep} is a field.

24. Show any algebraic extension of a perfect field is perfect.

25. Let F_o be a field of characteristic $p > 0$, $F = F_o(t_1^p, t_2^p)$, and $L = F_o(t_1, t_2)$. Show
    (a) Show if $\theta \in L \setminus F$, then $[F(\theta) : F] = p$.
    (b) There exist infinitely many fields K satisfying $F < K < L$. [Cf. Problem **V**:45.]

IV. Normality, Galois Theory

26. Show the following:
    (a) If $K/\mathbb{Q}$ and $\sigma \in \text{Aut } K$, then σ fixes $\mathbb{Q}$.
    (b) The fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

27. A **primitive nth root of unity** is an element $z \in \mathbb{C}$ such that $z^n = 1$ and $z^r \neq 1$ for $1 \leq r < n$. Show the following:
    (a) There exist $\phi(n) := |\{d \mid 1 \leq d \leq n,\ (d, n) = 1\}|$ primitive nth roots of unity.
    (b) If ω is a primitive nth root of unity, then $\mathbb{Q}(\omega)$ is a splitting field of $t^n - 1 \in \mathbb{Q}[t]$ and $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal.
    (c) If $\omega_1, ..., \omega_{\phi(n)}$ are the $\phi(n)$ primitive nth roots of unity of $t^n - 1 \in \mathbb{Q}[t]$ and $\sigma \in \text{Aut } \mathbb{Q}(\omega_1)$, then $\sigma(\omega_1) = \omega_i$ for some i, $1 \leq i \leq \phi(n)$.

28. Continued from Problem **IV**:27. Show
    (a) Let $\Phi_n(t) = (t - \omega_1) \cdots (t - \omega_{\phi(n)})$. Then show $\Phi_n(t) \in \mathbb{Q}[t]$. $\Phi_n(t)$ is called the nth **cyclotomic polynomial**.
    (b) $\Phi_n(t) \in \mathbb{Z}[t]$.

29. Continued from Problem **IV**:28. Show
    (a) $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible.
    (b) Calculate $\Phi_n(t)$ for $n = 3, 4, 6, 8$ explicitly and show directly that $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible.

30. Suppose you knew that, for any integers a and n with $(a, n) = 1$, there are infinitely many primes p that are congruent to a modulo n (this is a famous theorem of Dirichlet). Conclude that every finite abelian group occurs as a Galois group over the rational numbers. (The corresponding statement when the "abelian" is eliminated is an open problem.)

31. Let $K = \mathbb{Q}(r)$ with r a root of $t^3 + t^2 - 2t - 1 \in \mathbb{Q}[t]$. Let $r_1 = r^2 - 2$. Show that r_1 is also a root of this polynomial. Find $G(K/\mathbb{Q})$ and show that $K/\mathbb{Q}$ is normal.

32. Let K be a splitting field of $t^5 - 2 \in \mathbb{Q}[t]$.
    (a) Find $G(K/\mathbb{Q})$.
    (b) Show that there exists a group monomorphism $G(K/\mathbb{Q}) \to S_5$.
    (c) Find all subgroups of $G(K/\mathbb{Q})$ and the corresponding fields.

33. Let char $F = p \neq 0$ and $a \in F$. Let $f = t^p - t - a \in F[t]$. Show the following:
    (a) f has no multiple roots.
    (b) If α is a root of f, then so is $\alpha + k$ for all $0 \leq k \leq p - 1$.
    (c) f is irreducible if and only if f has no root in F.
    (d) Suppose that $a \neq b^p - b$ for any $b \in F$. Find $G(K/F)$ where K is a splitting field of $t^p - t - a \in F[t]$.

34. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, u)$ where $u^2 = (9 - 5\sqrt{3})(2 - \sqrt{2})$. Show that K/Q is normal and find $G(K/\mathbb{Q})$.

35. Let $F \subset E \subset K$. If K/E and E/F are both normal, is K/F normal? Prove or give a counterexample.

36. Let $f, g \in F[t]$ be relatively prime and suppose that $u = f/g$ lies in $F(t) \setminus F$.
    (a) Show that $F(t)/F(u)$ is finite of degree $d = \max\{\deg(f), \deg(g)\}$.
    (b) $G(F(t)/F)$ consists of all F-automorphisms of $F(t)$ mapping t to $(at+b)/(ct+d)$ where $a, b, c, d \in F$ satisfies $ad - bc \neq 0$.

37. Suppose that K/F is Galois with Galois group $G(K/F) \cong S_n$. Show that K is the splitting field of an irreducible polynomial in $F[t]$ of degree n over F.

38. Let K be a splitting field of $f \in \mathbb{Q}[t]$. Find $K, G(K/F)$ and all intermediate fields if
    (a) $f = t^4 - t^2 - 6$.
    (b) $f = t^3 - 3$.

39. Suppose that L/F is a finite Galois extension and $L/K/F$, an intermediate field. Let $N = N_{G(L/F)}(G(L/K))$ denote the normalizer of $G(L/K)$ in $G(L/F)$. Show that L^N is the smallest subfield of K with K/L^N Galois.

40. Suppose that K/F is Galois. Let $F \subset E \subset K$ and L the smallest subfield of K containing E and such that L/F is normal. Show that $G(K/L) = \bigcap_{\sigma \in G(K/F)} \sigma G(K/E)\sigma^{-1}$.

41. Suppose that K/F is Galois, p a prime, and $p^r \mid [K : F]$ but $p^{r+1} \nmid [K : F]$. Show that there exist fields L_i, $1 \leq i \leq r$, satisfying $F \subseteq L_r < L_{r-1} < \cdots < L_1 < L_0 = K$ such that L_i/L_{i+1} is normal, $[L_i : L_{i+1}] = p$ and $p \nmid [L_r : F]$.

V. Miscellaneous

42. Suppose the $|K| = p^m$ and $F \subset K$. Show that $|F| = p^n$ for some n with $n \mid m$. Moreover, $G(K/F)$ is generated by the **Frobenius automorphism** $\alpha \mapsto \alpha^{p^n}$.

43. Show if F is a finite field, $n \in \mathbb{Z}^+$, then there exists an irreducible polynomial $f \in F[t]$ of degree n.

44. Show if F is a finite field, then every element in F is a sum of two squares.

45. Show if K is not a finite field and u, v are algebraic and separable over K, then there exists an element $a \in K$ such that $K(u, v) = K(u + av)$. Is this true if $|K| < \infty$ with $K(u) < K(u, v)$ and $K(v) < K(u, v)$?

46. Let $F = \mathbb{R}$. Let $f = t^3 - a_1 t^2 - a_2 t - a_3 \in \mathbb{R}[t]$. Show:
    (a) The discriminant $\Delta = -4a_1^3 a_3 + a_1^2 a_2^2 - 18 a_1 a_2 a_3 + 4a_2^3 - 27 a_3^2$.
    (b) f has multiple roots if and only if $\Delta = 0$.
    (c) f has three distinct real roots if and only if $\Delta > 0$.
    (d) f has one real root and two non-real roots if and only if $\Delta < 0$.

47. Let $x^3 + px + q$ be irreducible over a finite field K of characteristic not 2 or 3. Show that $-4p^3 - 27q^2$ is a square in K.

48. Let f be an irreducible quartic over a field K of characteristic zero, G the Galois group of f, and u a root of f. Show that there is no field properly between K and $K(u)$ if

and only if $G = A_4$ or $G = S_4$. (This will explode the myth that there must be an intermediate field when the dimension is not prime.)

49. Let K be a subfield of the real numbers, f an irreducible quartic over K. Suppose that f has exactly two real roots. Show that the Galois group of f is either S_4 or of order 8.

50. Let K/F be a finite extension. Suppose that F has no nontrivial extensions of odd degree and K has no extensions of degree two. Show that F is perfect and K is algebraically closed.

(**) (Extra Credit.) Let char $F = 0$. Suppose that $f \in F[t]$ is irreducible of prime degree and K/F a splitting field of f. Then f is solvable by radicals if and only if $K = F(r_i, r_j)$ for any two roots, r_i, r_j of $f \in K$.