Field Theory (May 1996 - June 2008)

1996-05

8. Find the Galois group of the polynomial $3x^3 - 9x^2 + 9x - 5$ over $\mathbf{Q}$.

9. Let E be a splitting field of $x^8 - 1$ over a field F of 4 elements. Find card(E).

10. Let F be a field, and $f(x) \in F[x]$ a nonzero monic polynomial. Suppose that the zeros of $f(x)$ in a splitting field E of $f(x)$ over F are all distinct and that the set of zeros is closed under multiplication. Prove that either $f(x) = x^n - 1$ or $f(x) = x^n - x$ for some natural number n.

1997-05

6. The finite field $\mathbb{F}_{64}$ with 64 elements has how many elements of multiplicative order 9? Support your answer.

9. Let E be the splitting field of $X^{42} - 1$ over the rational field $\mathbb{Q}$. Determine the number of subfields of E.

10. Let F be a field of characteristic zero not containing a primitive n-th root of unity. Assume $f(X) = X^n - a$, $a \in F$, is irreducible. Show that the Galois group of the splitting field of $f(X)$ over F is isomorphic to a group of linear transformations of the form

$$z \mapsto bz + c$$

where $b, c \in \mathbb{Z}/n\,\mathbb{Z}$.

1997-08

7. Let E be the splitting field of $X^{35} - 1$ over the finite field $\mathbb{F}_8$ with 8 elements. Determine the cardinality $|E|$ of E. How many subfields does E have?

8. Determine the degree $[E : \mathbb{Q}]$ of the splitting field E of $X^{10} - 5$ over the rational field $\mathbb{Q}$.

9. Let F be a field and let $f(X) \in F[X]$ be a separable irreducible polynomial of degree 4. Determine, as explicitly as possible, the Galois group G, of the splitting field of $f(X)$ over F, when G has order 8.

10. Show that the splitting field E of the polynomial

$$f(X) = X^3 + X^2 - 2X - 1$$

over the rational field $\mathbb{Q}$ is obtained by adjoining a single root of $f(X)$. Find the Galois group Gal $(E/\mathbb{Q})$.

HINT: Show first that $f(X)$ divides $f(X^2 - 2)$.

2000-01

13. Determine the Galois group of the polynomial $x^p - 2$ over Q, where p is an odd prime number.

2000-09

8 The Galois Correspondence

Suppose α is a zero of a monic irreducible polynomial $f \in \mathbb{Q}[x]$ of degree 9. Then, Cauchy's theorem says that the quotient ring $K = \mathbb{Q}[x]/(f(x))$ is a field extension of $\mathbb{Q}$ of degree 9 isomorphic to $\mathbb{Q}(\alpha)$.

8.a (2) Suppose α is a real number, but none of the other zeros of f are real. Explain why K has no (non-trivial) field automorphisms.

8.b (3) Suppose there is a field M properly between K and $\mathbb{Q}$. What are the possible degrees of $M/\mathbb{Q}$?

8.c (5) Suppose the Galois closure of $K/\mathbb{Q}$ in L and $G(L/\mathbb{Q})$ is S_9. Explain why there is no field properly between K and $\mathbb{Q}$.

2001-06

5. Let $\mathbf{F}_q$ be a field of characteristic p with q elements. Let $\alpha = [\mathbf{F}_q{:}\mathbf{F}_p]$.
   - (2) a. Express q in terms of α and p; justify.
   - (3) b. Show that every extension of $\mathbf{F}_p$ is separable.
   - (3) c. Show that $\mathbf{F}_q$ is a Galois extension of $\mathbf{F}_p$: Find a polynomial over $\mathbf{F}_p$ satisfied by every element of $\mathbf{F}_q$ (justify your answer). Conclude that all fields with q elements are isomorphic.
   - (4) d. Find an automorphism ϕ of $\mathbf{F}_q$ over $\mathbf{F}_p$ with exponent α. Conclude that $G(\mathbf{F}_q/\mathbf{F}_p)$ is cycic of degree α.

2001-09

4. **The Galois Group of a degree 5 polynomial**
   Let $f(x)$ be an irreducibe degree p polynomial over Q with exactly $p-2$ real roots where p is a prime. Regard the Galois group G_f of $f(x)$ as a subgroup of S_p through its action on the roots of f.
   a. (**3 points**) Show G_f contains a 2-cycle of S_p.
   b. (**3 points**) Show $G_f = S_p$. Hint: Use that the irreducibility of f implies that G_f is transitive subgroup. Explain why p being a prime now implies G_f contains a p-cycle.
   c. (**4 points**) Let $f(x) = x^5 - 9x + 2$. Using a. and b. show that $G_f = S_5$.

2003-01

9. Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Its non-zero elements form a multiplicative group $\mathbb{F}_q^*$ which is cyclic of order $q-1$.

   (a) Let m be a positive integer. Prove that

   $$\sum_{x\in\mathbb{F}_q} x^m = \begin{cases} -1 & \text{if } (q-1) \mid m \\ 0 & \text{otherwise} \end{cases}$$

   (b) Let $n > d$ be positive integers. Let $f(x_1, \ldots, x_n)$ be a polynomial of total degree d in n-variables with coefficients in $\mathbb{F}_q$. Let $N(f)$ denote the number of solutions of the equation

   $$f(x_1, \ldots, x_n) = 0, \; x_i \in \mathbb{F}_q.$$

   Prove that $N(f)$ is divisible by p.

11. Let K be the splitting field over $\mathbb{Q}$ of the polynomial

$$f(x) = (x^2 - 2x - 1)(x^4 - 1).$$

Determine the Galois group G of $f(x)$ and determine all the intermediate fields explicitly.

2004-09

4. Let F be the splitting field of $x^{10} - 1$ over $\mathbf{Q}$. Find $\mathrm{Gal}(F/\mathbf{Q})$, both as an abstract group, and as a group of explicitly described automorphisms of F.

7. Let $\mathbf{F}_q$ be a finite field with q elements, and K a finite extension of $\mathbf{F}_q$. Let $n = [K : \mathbf{F}_q]$.

   (a) How many elements does K have? Explain.

   (b) Show that every extension of $\mathbf{F}_q$ is separable.

   (c) Show that K is a Galois extension of $\mathbf{F}_q$.

   (d) Exhibit an automorphism σ of K of order n, such that σ restricts to the identity automorphism of $\mathbf{F}_q$. Conclude that $\mathrm{Gal}(K/\mathbf{F}_q)$ is cyclic.

8. Suppose $f(x) \in \mathbf{Q}[x]$ is irreducible and let K denote its splitting field.

   (a) Suppose $\mathrm{Gal}(K/\mathbf{Q}) = Q_8$ (the quaternion group of order 8). What are the possibilities for the degree of f?

   (b) Suppose $\mathrm{Gal}(K/\mathbf{Q}) = D_8$ (the dihedral group of order 8). What are the possibilities for the degree of f?

2005-06

(10 points) 7. Suppose p is a prime number and L/K is a field extension of degree p.

(a) Prove that if $K = \mathbb{Q}$, then L/K is separable.
(b) Prove that if $K = \mathbb{F}_p$, then L/K is separable.
(c) Give an example of a field extension L/K of degree p that is *not* separable.

(13 points) 8. Let K be the splitting field over $\mathbb{Q}$ of $x^8 - 1$.

(a) Find $[K : \mathbb{Q}]$.
(b) Describe the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$, both as an abstract group and as a set of automorphisms.
(c) Find explicitly all subgroups of G and the corresponding subfields of K under the Galois correspondence.

2006-06

(8) (10 points) Let q be a prime power and n a positive integer.

(a) Prove that the map ϕ defined by $\phi(x) = x^q$ is an automorphism of $\mathbb{F}_{q^n}$ that fixes $\mathbb{F}_q$.

(b) Prove that the automorphism ϕ of part (a) generates $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

2007-06

1 (10 points). Let $\mathbf{Q}$ be the field of rational numbers. Find a field F such that $\mathrm{Gal}(F/\mathbf{Q}) = D_8$, the dihedral group with 8 elements. Prove your answer.

2 (10 points). Let $\mathbf{F}_q$ denote the finite field of q elements. Show that the order of the special linear group $SL_n(\mathbf{F}_q)$ is

$$q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1),$$

and the order of the projective special linear group $PSL_n(\mathbf{F}_q)$ is

$$\frac{1}{(n, q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1).$$

7 (10 points). Let F be a finite field and let K be a finite extension of F. Show that both the norm map and the trace map from K to F are surjective. Is the same statement true if K and F are number fields (finite extensions of $\mathbf{Q}$)?

2007-09

2 (10 points). Show that every finite field is perfect, i.e., every extension of finite fields is separable.

3 (10 points). Let p be an odd prime number.

a) Show that $\mathbf{Q}(e^{2\pi i/p})$ contains a unique quadratic extension of $\mathbf{Q}$.

b) Find a field F such that $\mathrm{Gal}(F/\mathbf{Q}) = \mathbf{Z}/3\mathbf{Z}$. Prove your answer.

2008-06

3. Factor the polynomial $x^4 + 1 \in F[x]$ and find the splitting field over F if the ground field F is:

(a) $\mathbb{Q}$

(b) $\mathbb{F}_2$

(c) $\mathbb{R}$

5. Let K be the splitting field of $X^{49} - 1$ over $\mathbb{Q}$. Determine the number of fields F such that $\mathbb{Q} \subseteq F \subseteq K$.