Some problems on field and Galois theory

B.Sury

April 2010

Q 1.
Let K be any field and $a \in K$. Suppose m, n are relatively prime. Prove that $X^{mn} - a$ is irreducible over K if, and only if, both $X^m - a$ and $X^n - a$ are.

Q 2.
Find the splitting field over $\mathbf{Q}$ of :
(i) $X^4 - X^2 + 4$; what is its degree?
(ii) $X^p - q$ where p, q are (not necessarily distinct) primes; deduce that $X^p - q$ is irreducible over $\mathbf{Q}(e^{2i\pi/p})$.
Hint for (ii) : p and $p-1$ are co-prime.

Q 3.
If L/K is an algebraic extension and A is a subring of L containing K, prove that A is a subfield.

Q 4.
Determine what the characteristic must be for the following polynomial to have a multiple root. In each case, determine the multiple roots and their multiplicities.
(i) $X^4 + X + 1$.
(ii) $X^4 + 2X^3 + 3X^2 + 8X + 1$.
Hint : For instance, in case (i), see what $\alpha^4 + \alpha + 1 = 0 = 4\alpha^3 + 1$ implies.

Q 5.
If $q = p^n$ and $\alpha \in \mathbf{F}_q$, show that

$$(X - \alpha)(X - \alpha^p)(X - \alpha^{p^2}) \cdots (X - \alpha^{p^{n-1}}) \in \mathbf{F}_p[X].$$

Q 6.
Let $F = Spl(X^{13} - 1, \mathbf{F}_3)$. Prove that $[F : \mathbf{F}_3] = 3$.

Q 7.
Determine the Galois group of $X^p - 2$ over $\mathbf{Q}$ for an odd prime p.

Q 8.
If K is any field and $f \in K[X]$ is irreducible, prove that all roots of f in any splitting field of f over K have the same multiplicity.

Q 9.
Describe (with brief explanations) the Galois group of $K = \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ over $\mathbf{Q}$ where $p_1, \cdots, p_n$ are distinct primes. Compute, using the fundamental theorem of Galois theory, the number of intermediate fields between $\mathbf{Q}$ and K.

Q 10.
Find the partial fraction decomposition of $\frac{1}{x^n-1}$ over $\mathbf{Q}$.
Hint : Think of the irerducible factorization of $x^n - 1$ over $\mathbf{Q}$.

Q 11.
Find a Galois extension of $\mathbf{Q}$ whose Galois group cyclic of order 13.

Q 12.
If $f \in \mathbf{F}_p[X]$ is a product of irreducible factors of degrees $d_1, d_2, \cdots, d_r$, then show that the splitting field of f over $\mathbf{F}_p$ has degree $\mathrm{LCM}(d_1, d_2, \cdots, d_r)$.

Q 13.
Let $\alpha \in \overline{\mathbf{F}_p}$, the algebraic closure of $\mathbf{F}_p$.
Prove that $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = \min\ \{n : \alpha^{\frac{p^n-1}{p-1}} \in \mathbf{F}_p\}$.

Q 14.
Let $f \in K[X]$ be irreducible, K any field. If α is a root of f, and $\deg f = 15$, show that f cannot decompose over $K(\alpha)$ as
$f = (\deg 1)(\deg 1)(\deg 1)(\deg 2)(\deg 2)(\deg 8)$ in $K(\alpha)[X]$.

Q 15.
Determine all the natural numbers n for which the angle of n° can be constructed using a ruler and a compass.

Q 16.
Let n be a natural number and Φ_n be the minimal polynomial of $e^{2i\pi/n}$ over $\mathbf{Q}$; that is, the cyclotomic polynomial of degree $\phi(n)$. For any integer a, show that any prime factor p of $\Phi_n(a)$ with $p \not| n$ must satisfy $p \equiv 1 \bmod n$.

Q 17.
Let Char. $K = p > 0$, and let $a \in K$. If the polynomial $X^p - X - a$ is reducible in $K[X]$, prove that all its roots lie in K.

Q 18.
Let Char. $K = p > 0$. Suppose L/K is a finite extension such that $p \not| [L : K]$. Show that L/K is separable.

Q 19.
Prove that $K = Spl(X^3 - 3X + 1, \mathbf{Q})$ is not a radical extension of $\mathbf{Q}$.

Q 20.
(a) If $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$ are extensions of degrees m, n over $\mathbf{Q}$ which are relatively prime, prove that $min(\alpha, \mathbf{Q})$ remains irreducible in $\mathbf{Q}(\beta)[X]$.
(b) Using (a), determine the number of irreducible factors of $1 + X + \cdots + X^{p-1}$ in $\mathbf{Q}(2^{1/n})$ where $n \geq p$ are both primes.

Q 21.
Let n be any natural number. Determine the degree of $\mathbf{Q}(Cos\frac{2\pi}{n})$ over $\mathbf{Q}$. Is this a Galois extension of $\mathbf{Q}$? Justify. Find all the conjugates of $Cos\frac{2\pi}{n}$ over $\mathbf{Q}$.

Q 22.
If $n > 1$ is odd, then prove that $\mathbf{Q}(\zeta_d)$ cannot contain an n-th root of 2 for any d.

Q 23.
Let E/F be an extensions of finite fields. Prove that the norm map from E to F is surjective.

Q 24.
Let K be an algebraic extension of $\mathbf{Z}/p\mathbf{Z}$. Show that the map

$$Frob_p : K \to K; a \mapsto a^p$$

is an automorphism of K onto itself. Deduce that all polynomials over K are separable.
Hint for the last statement : For an irreducible, inseparable polynomial f, one has $f(X) = g(X^p)$ for some g.

Q 25.
Let K be any field and let $\mathcal{M}$ denote the set of all monic irreducible polynomials in $K[X]$. For each $f = c_n(f) + c_{n-1}(f)X + \cdots + c_1(f)X^{n-1} + X^n$, consider independent variables $X_i(f); 1 \leq i \leq n$ and the elements $s_1(f), \cdots, s_n(f)$ of the polynomial ring $A = K[X_i(f); f \in \mathcal{M}, i \leq deg(f)]$ defined by

$$s_n(f) + s_{n-1}(f)X + \cdots + s_1(f)X^{n-1} + X^n = \prod_{i=1}^{n}(X - X_i(f)).$$

If I denotes the ideal in A generated by all elements of the form $s_i(f) - c_i(f)$, verify :
(i) I is a proper ideal,
(ii) each $f \in \mathcal{M}$, considered as a polynomial over A/I, splits into linear factors.

Hint for (i) : You may assume that for any finite set of polynomials over K, there is a field extension of K where all of them split.

Q 26.
Let $K/\mathbf{Q}$ be a finite extension. Denote by $\sigma_1, \cdots, \sigma_n$ all the $\mathbf{Q}$-embeddings of K in an algebraic closure $\bar{\mathbf{Q}}$ containing K. For any n-tuple $(v_1, \cdots, v_n)$ of elements of K, consider the $n \times n$ matrix $M(v_1, \cdots, v_n)$ whose (i, j)-th entry is $\sigma_j(v_i)$. Define the discriminant $\mathrm{disc}(v_1, \cdots, v_n)$ to be $\det M(v_1, \cdots, v_n)^2$.
(i) Prove that $\mathrm{disc}(v_1 \cdots, v_n) \neq 0$ if, and only if, the v_i's form a $\mathbf{Q}$-basis of K and that, modulo squares, it is independent of the basis.
(ii) Prove $\mathrm{disc}(v_1, \cdots, v_n) = \det(\ \mathrm{tr}_{K/\mathbf{Q}}(v_i v_j))$.
Hint :
You may use the fact proved in class that for a finite separable extension, $\mathrm{tr}(x) = \sum_i \sigma_i(x)$.
(iii) If K is Galois over $\mathbf{Q}$, prove that there exists a normal basis that is, there exists $v \in K$ such that $\{\sigma(v) : \sigma \in \mathrm{Gal}\ (K/\mathbf{Q})\}$ is a $\mathbf{Q}$-basis of K.

Q 27. (Richard Brauer)
Let $p \geq 5$ be any prime. Let $n_1 < n_2 < \cdots < n_{p-2}$ be even integers. Let $n > \frac{\sum n_i^2}{2}$ be any even integer. Prove that the polynomial

$$f = (X^2 + n)(X - n_1)(X - n_2) \cdots (X - n_{p-2}) - 2$$

is irreducible over $\mathbf{Q}$ and has exactly $p-2$ real roots. Deduce that the Galois group of f is S_p.

Q 28.
For $f \in \mathbf{Z}[X]$ monic, irreducible and any prime p not dividing disc f, the Galois group of (f mod p) over $\mathbf{F}_p$ can be regarded as a subgroup of $\mathrm{Gal}_{\mathbf{Q}}(f)$. Use this to show that for any n, there exists f with $\mathrm{Gal}_{\mathbf{Q}}(f) \cong S_n$.
Hint : You may refer to some textbook (P.M.Cohn, Dummit-Foote etc.) if you want to.

Q 29.
Let $f \in K[X]$ be irreducible, K any field. Let α be any root of f in a splitting field. Define $r_K(f, \alpha)$ to be the number of roots of f in $K(\alpha)$.
(i) Prove $r_K(f, \alpha)$ is independent of the choice of α.
(ii) Prove that $r_K(f, \alpha)$ divides the separability degree of $\mathrm{Spl}_K(f)$ over K.
(iii) If f is also taken to be separable, prove that $r_K(f, \alpha) = [N_G(H) : H]$ where G is the Galois group of f over K and H is the stabilizer of α.
(iv) If L/K is any field extension (not necessarily algebraic), prove that the number of roots of f in L is a multiple of $r_K(f)$.

(v) Use (iv) to show that of deg $f = 15$, then f cannot decompose over some $K(\alpha)$ as
$f = (\text{degree } 1)(\text{degree } 1)(\text{degree } 1)(\text{degree } 2)(\text{degree } 2)(\text{degree } 8)$ in $K(\alpha)[X]$.

Q 30.
Let K_1, K_2 be algebraically closed fields containing fields E_1, E_2 respectively. Suppose that S_1, S_2 are transcendence bases of K_1 and K_2 over E_1 and E_2 respectively. If S_1 and S_2 are in bijection, prove that every isomorphism from E_1 onto E_2 extends to an isomorphism from K_1 onto K_2.
Deduce that $\mathbf{C}$ has uncountably many proper subfields which are isomorphic to it.

Q 31.
If E/F is a finitely generated field extension and E_0 is an intermediate field (that is, $E \supset E_0 \supset F$), prove that E_0 is also finitely generated over F.

Q 32.
Recall that a transcendence basis S of E over F is said to be a separating transcendence basis if E is separable (algebraic) over $F(S)$.
Let char $F = p > 0$ and let t be a transcendental element (of some field extension of F) over F. Consider the field E generated over F by $\{t, a_1, a_2, a_3, \cdots\}$ where a_i is a root of $X^{p^i} - t \in F(t)[X]$. Show that every finitely generated subfield of E containing F has a separating transcendence basis over F but that E itself does not. In other words, E is separable over F (in the general sense) but is not separably generated over F.
Hint : If need be, you may use Maclane's criterion which defines separability for a general extension by 3 equivalent properties.