Galois Theory: Example Sheet 2 of 4

1. Let F be a finite field with q elements. Find a formula in terms of q for the number of monic irreducible quadratics in $F[X]$. Deduce that F cannot be algebraically closed. Find all irreducible polynomials in $\mathbb{F}_2[X]$ of degree at most 4.

2. (i) Let $u = X_1 + \omega X_2 + \omega^2 X_3$ and $v = X_1 + \omega^2 X_2 + \omega X_3$ where $\omega = e^{2\pi i/3}$. Find expressions for $u^3 + v^3$ and uv in terms of the elementary symmetric polynomials $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$ and $s_3 = X_1X_2X_3$.
(ii) Express $\sum_{i \neq j} X_i^3 X_j \in \mathbb{Z}[X_1, \ldots, X_n]$ as a polynomial in the elementary symmetric polynomials.

3. (i) Let $f(X) = \prod_{i=1}^n (X - \alpha_i)$. Show that $f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$, and deduce that $\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\alpha_i)$.
(ii) Let $f(X) = X^n + bX + c = \prod_{i=1}^n (X - \alpha_i)$, with $n \geqslant 2$. Show that
$$\alpha_i f'(\alpha_i) = (n-1)b \left(\frac{-nc}{(n-1)b} - \alpha_i \right)$$
and deduce that
$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \left((1-n)^{n-1} b^n + n^n c^{n-1} \right).$$

4. Show directly from the definition that any quadratic extension is normal. Give an example of a cubic extension which is normal, and another which is not normal.

5. (i) Let K be a field of characteristic $p > 0$ such that every element of K is a p^{th} power. Show that any irreducible polynomial over K is separable.
(ii) Deduce that if F is a finite field, then any irreducible polynomial over F is separable.
(iii) A field is said to be *perfect* if every finite extension of it is separable. Show that any field of characteristic zero is perfect, and that a field of characteristic $p > 0$ is perfect if and only if every element is a p^{th} power.

6. Let K be a field of characteristic $p > 0$, and let α be algebraic over K. Show that α is inseparable over K if and only if $K(\alpha) \neq K(\alpha^p)$, and that if this is the case, then p divides $[K(\alpha) : K]$. Deduce that if L/K is a finite inseparable extension of fields of characteristic p, then p divides $[L : K]$.

7. Let $M/L/K$ be finite extensions. Show that M is separable over K if and only if both M/L and L/K are separable extensions.

8. Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3}$. For which $c \in \mathbb{Q}$ do we have $K = \mathbb{Q}(\sqrt[3]{2} + c\omega)$?

9. Which of the quadratic extensions from Question 2 on Example Sheet 1 are Galois?

10. Let L/K be a finite Galois extension, and F, F' intermediate fields.

    (i) What is the subgroup of $\mathrm{Gal}(L/K)$ corresponding to the subfield $F \cap F'$?

    (ii) Show that if $\sigma\colon F \xrightarrow{\simeq} F'$ is a K-isomorphism, then the subgroups $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/F')$ of $\mathrm{Gal}(L/K)$ are conjugate.

11. Show that $L = \mathbb{Q}(\sqrt{2}, i)$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group G. Write down the lattice of subgroups of G and the corresponding subfields of L.

12. Show that $L = \mathbb{Q}(\sqrt[4]{2}, i)$ is a Galois extension of $\mathbb{Q}$, and show that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to D_8, the dihedral group of order 8. Write down the lattice of subgroups of D_8 (be sure you have found them all!) and the corresponding subfields of L, which you should give explicitly in terms of generators, for example $F = \mathbb{Q}(\sqrt{2}, i)$ or $F = \mathbb{Q}(\sqrt[4]{2}(1+i))$. Which intermediate fields are Galois over $\mathbb{Q}$?

Further problems

13. Let K be a field and $c \in K$. If m, n are coprime positive integers, show that $X^{mn} - c$ is irreducible if and only if both $X^m - c$ and $X^n - c$ are irreducible. [One way is easy. For the other, use the Tower Law.]

14. We say that α is *purely inseparable* over K if either $\alpha \in K$ or $\mathrm{char}\, K = p > 0$ and for some $n \geqslant 1$, $\alpha^{p^n} \in K$. We say that an algebraic extension L/K is purely inseparable if every element of L is purely inseparable over K.

    Let L/K be a finite extension, and $L_0 = \{\alpha \in L \mid \alpha \text{ is separable over } K\}$. Show that L_0 is a subfield of L which is separable over K, and that L is purely inseparable over L_0.

15. Let $L = \mathbb{F}_p(X, Y)$ be the field of rational functions in two variables over the finite field $\mathbb{F}_p$ (i.e., the field of fractions of $\mathbb{F}_p[X, Y]$). Let K be the subfield $\mathbb{F}_p(X^p, Y^p)$. Show that for any $f \in L$ we have $f^p \in K$, and deduce that L/K is not a simple extension (i.e., not of the form $K(\alpha)$).

16. (i) Let $f = g/h$ be a non-constant rational function in $K(X)$ where g, h are coprime polynomials. By finding a polynomial in $K(f)[T]$ with X as a root, and proving that it is irreducible, show that $[K(X) : K(f)] = \max(\deg g, \deg h)$.

    (ii) Deduce that $\mathrm{Aut}(K(X)/K) \cong \mathrm{PGL}_2(K)$.

17. Show that the only field homomorphism $\mathbb{R} \to \mathbb{R}$ is the identity map.