School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet VI: Galois groups, the Galois correspondence and the Fundamental Theorem of Galois Theory

1. Let F be a field *not* of characteristic 2 and let K be an extension of F of degree 2. Show that K is a Galois extension of F.

2. Find an example of field extensions $F \subseteq K \subseteq L$ such that K is a Galois extension of F, L is a Galois extension of K, but L is not a Galois extension of F.

   [Hint: Consider $\sqrt[4]{2}$.]

3. Let n be a natural number and $F = \mathbb{Q}(\sqrt[n]{2})$. Show that $|F : \mathbb{Q}| = n$. Show that $\mathrm{Gal}(F/\mathbb{Q})$ is trivial or cyclic of order 2 according to whether n is odd or even.

4. Let $f(X) = X^4 + 5X^2 + 5$ over $\mathbb{Q}$.

   (a) Show that $f(X)$ is irreducible over $\mathbb{Q}$.

   (b) Find a splitting field K for $f(X)$ over $\mathbb{Q}$.

   (c) Find an element of order 4 in $\mathrm{Gal}(K/\mathbb{Q})$.

   (d) Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

5. Let $f(X) = X^8 - 1$ over $\mathbb{Q}$.

   (a) Factorize $f(X)$ into irreducible polynomials over $\mathbb{Q}$.

   (b) Find a splitting field K for $f(X)$ over $\mathbb{Q}$.

   (c) Determine the elements of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

   (d) Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

6. Describe the Galois group $\mathrm{Gal}(\mathbb{Q}(i + \sqrt{3})/\mathbb{Q})$.

7. For each of the following field extensions, find the Galois group, find all of its subgroups, and find the subfield corresponding to each subgroup under the Galois correspondence. Determine which of the subfields are normal.

   (a) The splitting field of $X^3 - 1$ over $\mathbb{Q}$.

   (b) The splitting field of $X^3 - 2$ over $\mathbb{Q}$.

   (c) The splitting field of $X^4 - 1$ over $\mathbb{Q}$.

   (d) The splitting field of $X^5 - 1$ over $\mathbb{Q}$.

   (e) The splitting field of $X^6 - 1$ over $\mathbb{Q}$.

   (f) The splitting field of $X^6 + X^3 + 1$ over $\mathbb{Q}$.

   (g) $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$ over $\mathbb{Q}$.

   (h) The splitting field of $X^4 - 2$ over $\mathbb{Q}(i)$.

8. Let $f(X) = X^5 - 5X^4 + 5$ over some finite field F. For each of the following groups G either finite a finite field F such that the Galois group of $f(X)$ over F is isomorphic to G, or prove that no such field F exists.

   (a) The trivial group $\mathbf{1}$.

   (b) The Klein 4-group $V_4 \cong C_2 \times C_2$.

   (c) The cyclic group C_5 of order 5.

   (d) The cyclic group C_6 of order 6.

   (e) The cyclic group C_{10} of order 10.

   (f) The symmetric group S_5 of degree 5.

9. Let $f(X)$ be an irreducible polynomial over the finite field $\mathbb{F}_p$ (where p is a prime number). Show that if α is a root of $f(X)$ in some extension field, then $\mathbb{F}_p(\alpha)$ is a splitting field for $f(X)$ over $\mathbb{F}_p$.

   In each of the following cases, let α be a root of $f(X)$. Show that $f(X)$ is irreducible over $\mathbb{F}_p$ and express the roots of $f(X)$ as polynomials in α of degree less than the degree of $f(X)$ [that is, express the roots in terms of our standard basis for the usual extension $\mathbb{F}_p(\alpha)$ over $\mathbb{F}_p$]:

   (a) $f(X) = X^2 + 1,\ \ p = 7$;

   (b) $f(X) = X^3 + 2X^2 + X + 1,\ \ p = 3$.