EXAMPLE SHEET 3

1. Let $K \leq L$ be a finite Galois extension, and $M$ and $M'$ be intermediate fields.
   (i) What is the subgroup of $\text{Gal}(L/K)$ corresponding to the subfield $M \cap M'$?
   (ii) Show that if $\sigma : M \rightarrow M'$ is a $K$-isomorphism, then the subgroups $\text{Gal}(L/M)$ and $\text{Gal}(L/M')$ of $\text{Gal}(L/K)$ are conjugate.

2. Let $p$ be a prime and let $F$ be the field of order $p$. Let $L = F(X)$. Let $a$ be an integer with $1 \leq a < p$, and let $\sigma \in \text{Aut}_F(L)$ be the unique $K$-automorphism such that $\sigma(X) = aX$. Determine the subgroup $G \leq \text{Aut}_K(L)$ generated by $\sigma$, and also find its fixed field $L^G$.

3. Let $K \leq L$ be a Galois extension with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. Show that $\{\alpha_1, \ldots, \alpha_n\}$ is a $K$-basis for $L$ if and only if $\det \sigma_i(\alpha_j)$ is non-zero.

4. (i) Let $p$ be a prime. Show that any transitive subgroup of $S_p$ containing both a $p$-cycle and a transposition is equal to $S_p$.
   (ii) Prove that the Galois group of $f(t) = t^5 + 2t + 6$ over the rationals is $S_5$.
   (iii) Show that for a sufficiently large integer $m$, that $f(t) = t^p + mp^2(t - 1)(t - 2)\ldots(t - p + 2) - p$ has Galois group $S_p$ over the rationals.

5. (i) Let $f(t) = \Pi_{i=1}^n (t - \alpha_i)$. Show that $f'(\alpha_i) = \Pi_{j \neq i} (\alpha_i - \alpha_j)$ and deduce that the discriminant of $f(t)$ is $(-1)^{n(n-1)/2} \Pi_{i=1}^n f'(\alpha_i)$.
   (ii) Let $f(t) = t^n + bt + c = \Pi_{i=1}^n (t - \alpha_i)$ with $n$ at least 2. Show that the discriminant of $f(t)$ is $(-1)^{n(n-1)/2}((1-n)^{n-1}b^n + n^n c^{n-1})$.

6. Find the Galois group of $f(t) = t^4 + t^3 + 1$ over each of the finite fields $F$ of order 2, 3 and 4.

7. (i) Find a monic integral polynomial of degree 4 whose Galois group is $V_4$, the subgroup of $S_4$ whose elements are the identity and the double transpositions.
(ii) Let \( f(t) \) be a monic integral polynomial which is separable of degree \( n \). Suppose that the Galois group of \( f(t) \) over the rationals does not contain an \( n \)-cycle. Prove that the reduction of \( f(t) \) modulo \( p \) is reducible for every prime \( p \).

(iii) Hence exhibit an irreducible integral polynomial whose reduction mod \( p \) is reducible for every prime \( p \).

8. Compute the 12th cyclotomic polynomial \( \Phi_{12}(t) \) over the rationals.

9. Let \( L \) be the 15th cyclotomic extension of the rationals. Find all the degree two extensions of the rationals contained in \( L \).

10. Let \( p \) be a prime with \( (m,p) = 1 \). Let \( \Phi_m(t) \) be the \( m \)th cyclotomic polynomial, and consider it (mod \( p \)). Write \( \Phi_m(t) = f_1(t) \ldots f_r(t) \) to be a factorisation (mod \( p \)), where each \( f_i(t) \) is irreducible. Show that for each \( i \) the degree of \( f_i(t) \) is equal to the order of \( p \) in the unit group of the integers (mod \( m \)). Use this to write down an irreducible polynomial of degree 10 in \( F[t] \) where \( F \) is the field of two elements.

11. Let \( \Phi_n(t) \) be the \( n \)th cyclotomic polynomial over the rationals. Show that
   (i) If \( n \) is odd then \( \Phi_{2n}(t) = \Phi_n(-t) \).
   (ii) If \( p \) is a prime dividing \( n \) then \( \Phi_{np}(t) = \Phi_n(t^p) \).
   (iii) If \( p \) and \( q \) are distinct primes then the coefficients of \( \Phi_{pq}(t) \) are either +1, 0 or -1.
   (iv) If \( n \) is not divisible by at least three distinct odd primes then the coefficients of \( \Phi_n(t) \) are -1, 0 or +1.
   (v) \( \Phi_{3 \times 5 \times 7}(t) \) has at least one coefficient which is not -1, 0 or +1.

12. Let \( K \) be the field of rationals, and let \( L \) be the splitting field of \( f(t) = t^4 - 2 \) over \( K \). Show that \( \text{Gal}(L/K) \) is isomorphic to the dihedral group \( D_8 \) of order 8.

brookes@dpmms.cam.ac.uk