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 $\sigma : M \to M'$ 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 $K$ 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. Write down the lattice of subgroups of $D_8$ and the corresponding subfields of $L$. Which intermediate fields are Galois over $K$?
3. (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.
4. 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.
5. (i) Let $f(t) = \prod_{i=1}^{n}(t-\alpha_i)$. Show that $f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$ and deduce that the discriminant of $f(t)$ is $(1)^{n(n-1)/2}\prod_{i=1}^{n}f'(\alpha_i)$.
   (ii) Let $f(t) = t^n + bt + c = \prod_{i=1}^{n}(t-\alpha_i)$ with $n$ at least 2. Show that the discriminant of $f(t)$ is $(-1)^{n(n-1)/2}(1-n)^{n-1}b^n + n^nc^{n-1})$.
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. (i) Let \( p \) be an odd prime, and let \( K \) and \( F \) be the fields of \( p \) and \( p^n \) elements respectively. Let \( x \in F \). Show that \( x \in K \) if and only if \( x^p = x \) and that \( x + x^{-1} \in K \) if and only if either \( x^p = x \) or \( x^p = x^{-1} \).

(ii) Apply (i) to a root of \( t^2 + 1 \) in a suitable extension of \( K \) to show that \(-1\) is a square in \( K \) if and only if \( p = 1 \mod 4 \).

(iii) Show that \( x^4 = -1 \) if and only if \((x + x^{-1})^2 = 2 \). Deduce that \( 2 \) is a square in \( K \) if and only if \( p = 1 \) or \( p = -1 \mod 8 \).

9. 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 \( L^G \).

10. Compute the Galois group of \( f(t) = t^5 - 2 \) over the rationals.

brookes@dpmms.cam.ac.uk