1. Let $M/K$ be a finite Galois extension, and $H_1$, $H_2$ subgroups of $\text{Gal}(M/K)$, with fixed fields $L_1$, $L_2$. Find the fixed field of $H_1 \cap H_2$, and identify the subgroup of $\text{Gal}(M/K)$ corresponding to the field $L_1 \cap L_2$.

2. Let $M/K$ be a finite Galois extension, and $L$, $L'$ intermediate fields. Show that if $\sigma : L \to L'$ is a $K$-isomorphism, then there exists $\tilde{\sigma} \in \text{Gal}(M/K)$ whose restriction to $L$ is $\sigma$.

3. Determine the Galois groups of the following polynomials in $\mathbb{Q}[x]$.
   $$x^3 + 27x - 4, \quad x^3 - 21x + 7, \quad x^3 + 3x, \quad x^3 + x^2 - 2x - 1, \quad x^3 + x^2 - 2x + 1.$$ 

4. Let $f$ be an irreducible cubic polynomial over $K$, $\text{char} K \neq 2$, and let $\delta$ be the square root of the discriminant of $f$. Show that $f$ remains irreducible over $K(\delta)$.

5. Find the Galois group of $X^4 + X^3 + 1$ over each of the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$.

6. Compute the Galois group of $X^5 - 2$ over $\mathbb{Q}$.

7. (i) Let $p$ be prime. Show that any transitive subgroup $G$ of $S_p$ contains a $p$-cycle. Show that if $G$ also contains a transposition then $G = S_p$.
   
   (ii) Prove that the Galois group of $X^5 + 2X + 6$ is $S_5$.
   
   (iii) Show that if $f \in \mathbb{Q}[X]$ is an irreducible polynomial of degree $p$ which has exactly two non-real roots, then its Galois group is $S_p$. Deduce that for $m \in \mathbb{Z}$ sufficiently large,
   $$f = X^p + mp^2(X - 1)(X - 2) \cdots (X - p + 2) - p$$

   has Galois group $S_p$.

8. What are the transitive subgroups of $S_4$? Find a monic polynomial over $\mathbb{Z}$ of degree 4 whose Galois group is $V = \{e, (12)(34), (13)(24), (14)(23)\}$.

9. (i) Let $p$ be an odd prime, and let $x \in \mathbb{F}_p$. Show that $x \in \mathbb{F}_p$ if $x^p = x$, and that $x + x^{-1} \in \mathbb{F}_p$ if either $x^p = x$ or $x^p = x^{-1}$.
   
   (ii) Apply (i) to a root of $X^2 + 1$ in a suitable extension of $\mathbb{F}_p$ to show that $-1$ is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod{4}$.
   
   (iii) Show that $x^4 = -1$ if $(x + x^{-1})^2 = 2$. Deduce that 2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod{8}$.

10. Let $k$ be any field, and let $L = k(z)$ be the function field in the variable $z$. Define mappings $\sigma, \tau : L \to L$ by the formulae
   $$\tau f(z) = f(\frac{1}{z}), \quad \sigma f(z) = f(1 - \frac{1}{z}).$$

   Show that $\sigma, \tau$ are automorphisms of $L$, and that they generate a subgroup $G \subset \text{Aut}(L)$ isomorphic to $S_3$. Show that $L^G = k(w)$ where
   $$w = \frac{(z^2 - z + 1)^3}{z^2(z - 1)^2}.$$

11. Let $K$ be a field of characteristic $p > 0$. Let $a \in K$, and let $f \in K[X]$ be the polynomial $f(X) = X^p - X - a$. Show that $f(X + b) = f(X)$ for every $b \in \mathbb{F}_p \subset K$. Now suppose that $f$ does not have a root in $K$, and let $L/K$ be a splitting field for $f$ over $K$. Show that $L = K(\alpha)$ for any $\alpha \in L$ with $f(\alpha) = 0$, and that $L/K$ is Galois, with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. 

12. Express $\sum_{i\neq j} X_i^3 X_j$ as a polynomial in the elementary symmetric polynomials.

13. Show that if $X_1, \ldots, X_n$ are indeterminates, then

$$
\begin{vmatrix}
X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \\
X_1^{n-2} & X_2^{n-2} & \cdots & X_n^{n-2} \\
\vdots & \vdots & \ddots & \vdots \\
X_1 & X_2 & \cdots & X_n \\
1 & 1 & \cdots & 1
\end{vmatrix} = \Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j)
$$

(First show that each $(X_i - X_j)$ is a factor of the determinant).

14. For an $n$-tuple $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n$, let $m_\lambda = \sum_{\mu \in S_n} \lambda^\mu$ be the sum of all the monomials obtained from $z^\lambda = z_1^{\lambda_1} \cdots z_n^{\lambda_n}$ by permuting indices, so that $\{m_\lambda \mid \lambda_1 \geq \cdots \geq \lambda_n\}$ forms a basis of $\mathbb{Z}[z_1, \ldots, z_n]S_n$.

Show that the product of two such basis elements $m_\lambda, m_\mu$ is $m_{\lambda+\mu}$ plus a sum of smaller terms in lexicographical order:

$$m_\lambda m_\mu = m_{\lambda+\mu} + \sum_{\nu < \lambda+\mu, \nu_1 \geq \cdots \geq \nu_n} c_\nu m_\nu,$$

for some integers $c_\nu$.

15. Let $\Phi_n \in \mathbb{Z}[X]$ denote the $n^{th}$ cyclotomic polynomial. Show that:

(i) If $n$ is odd then $\Phi_{2n}(X) = \Phi_n(-X)$.

(ii) If $p$ is a prime dividing $n$ then $\Phi_{np}(X) = \Phi_n(X^p)$.

(iii) If $p$ and $q$ are distinct primes then the nonzero coefficients of $\Phi_{pq}$ are alternately +1 and −1. [Hint: First show that if $1/(1 - X^p)(1 - X^q)$ is expanded as a power series in $X$, then the coefficients of $X^m$ with $m < pq$ are either 0 or 1.]

(iv) If $n$ is not divisible by at least three distinct odd primes then the coefficients of $\Phi_n$ are −1, 0 or 1.

(v) $\Phi_{3 \times 5 \times 7}$ has at least one coefficient which is not −1, 0 or 1.

16. Let $K = \mathbb{Q}(\zeta)$ be the $n^{th}$ cyclotomic field with $\zeta = e^{2\pi i/n}$. Show that under the isomorphism $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, complex conjugation is identified with the residue class of $−1 \pmod{n}$. Deduce that if $n \geq 3$, then $[K : K \cap \mathbb{R}] = 2$ and show that $K \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos 2\pi/n)$.

17. Find all the subfields of $\mathbb{Q}(e^{2\pi i/7})$. Which are Galois over $\mathbb{Q}$?

18. Let $f(X) = X^n + bX + c = \prod_{i=1}^n (X - \alpha_i)$, with $n \geq 2$. Show that

$$\alpha_i f'(\alpha_i) = (n-1)b \left( \frac{-nc}{(n-1)b} - \alpha_i \right)$$

and deduce that the discriminant of $f$ is

$$(-1)^{n(n-1)/2} \left( (1-n)^{n-1}b^n + n^ne^{n-1} \right).$$