(1) Prove that the formal derivative $D_X$ of a polynomial satisfies:
   i. $D_X(f(X) + g(X)) = D_X(f(X)) + D_X(g(X))$,
   ii. $D_X(f(X)g(X)) = D_X(f(X))g(X) + f(X)D_X(g(X))$.
   iii. Deduce that $D_X : k[X] \to k[X]$ is a group homomorphism of $(k[X], +)$.
   iv. Find the kernel of $D_X$ if characteristic of $k$ is 0.
   v. Find the kernel of $D_X$ if characteristic of $k$ is $p > 0$.

(2) How many polynomials are there of degree 4 in $F_2[X]$? How many of them are irreducible? How many of them are separable? Prove that the product of all irreducible polynomials in $F_2[X]$ of degree 1, 2 and 4 is $X^{16} - X$.

(3) For any prime $p$ and any non-zero element $a \in F_p$, the polynomial $X^p - X + a$ is irreducible and separable. (Hint: Prove that if $x$ is a root then so is $x + 1$.)

(4) i. Prove that $x^{p^n} - 1 = \prod_{\alpha \in (F_{p^n} \setminus \{0\})} (x - \alpha)$.
   ii. Deduce that $\prod_{\alpha \in (F_{p^n} \setminus \{0\})} (x - \alpha) = (-1)^{p^n}$.
   iii. For $p$ odd and $n = 1$ deduce Wilson’s theorem: $(p - 1)! = -1 \pmod{p}$.

(5) Prove that for any $f(X) \in F_p[X]$ we have $(f(X))^p = f(X^p)$.

(6) A field $k$ is called perfect if every extension of $k$ is a separable extension.
   i. Show that every field of characteristic 0 is perfect.
   ii. Show that every finite field is perfect.

(7) Give an example of an $f(X) \in Q[X]$ that has no zeroes in $Q$ but whose zeroes in $C$ are all of multiplicity 3. Does this contradict the fact that $Q$ is perfect? Why?

(8) Let $K = k(\alpha_1, \cdots, \alpha_n)$ be a finite algebraic extension of $k$. Show that any element $\sigma \in Aut(K/k)$ is uniquely determined by its action on the generators $\alpha_1, \cdots, \alpha_n$, i.e. by $\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$.

(9) Let $G$ be a subgroup of $Aut(L/k)$ and $\sigma_1, \cdots, \sigma_k$ be generators of the group $G$. Show that a subfield $K$ is fixed by $G$ if and only if it is fixed by the generators $\sigma_1, \cdots, \sigma_k$.

(10) For any complex number $z = a + b\sqrt{-1}$, we define its complex conjugate to be the number $\bar{z} := a - b\sqrt{-1}$.
   i. Show that complex conjugation is an automorphism of $C$.
   ii. Determine the subfield of $C$ fixed by complex conjugation.

(11) Find $Aut(Q(\sqrt{2})/Q(\sqrt{2}))$.

(12) Let $k$ be a field and consider the field of rational functions in the variable $x$, i.e. consider the field $k(x)$.
   i. Show that the map $x \mapsto x + 1$ extends to an automorphism of $k(x)$.
   ii. Find the subfield of $k(x)$ fixed by this automorphism.

(13) Let $f(X) \in F_2[X]$ and let $\alpha$ be a root of $f$. Show that $f(X)$ splits in $F_2(\alpha)$.

(14) Find the Galois group of the polynomial $f(X) = X^3 - 2 \in Q[X]$.

(15) Find the Galois group of the polynomial $f(X) = X^p - 2 \in Q[X]$; where $p$ is a prime number.

(16) Find the Galois group of the polynomial $f(X) = X^8 - 3 \in Q[X]$. 

A. ZEYTÎN
(17) Recall that two elements $\alpha, \beta \in K$ are said to be conjugate over $k$ if there is an element $\sigma \in \text{Aut}(K/k)$ so that $\sigma(\alpha) = \beta$. Find all conjugates of given elements in the indicated fields:

i. $\sqrt{p}$ and $3 + \sqrt{p} \in \mathbb{Q}(\sqrt{p})$; where $p$ is a prime number.

ii. $\sqrt{2} + \sqrt{3}, \sqrt{2} + \sqrt{5}$ and $\sqrt{3} + \sqrt{5}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.

(18) Prove that

i. an automorphism of a field $K$ maps elements that are squares of elements in $K$ to elements in $K$ what are squares of elements in $K$, that is for any element $\alpha \in K$ with the property that $\alpha = \beta^2$ for some $\beta \in K$, there exists some $\beta' \in K$ so that $\sigma(\alpha) = (\beta')^2$; where $\sigma \in \text{Aut}(K/k)$ arbitrary.

ii. an automorphism of real numbers sends positive numbers to positive numbers.

iii. for $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ and for $a, b \in \mathbb{R}$ with $a < b$, $\sigma(a) < \sigma(b)$

iv. the group $\text{Aut}(\mathbb{R}/\mathbb{Q}) = \{1\}$, i.e. the trivial group.

(19) Let $f(X) \in \mathbb{Q}[X]$ is a polynomial of degree 3. Prove that if the Galois group of this polynomial is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ then all the roots of $f(X)$ are real. Find such an $f$. What is the other possibility?

(20) Let $K/k$ be a field extension. Recall that two elements $\alpha, \beta \in K$ are said to be conjugate over $k$ if there is an element $\sigma \in \text{Aut}(K/k)$ so that $\sigma(\alpha) = \beta$.

i. Prove that two elements are conjugate if and only if their minimal polynomials, $f_\alpha(X)$ and $f_\beta(X)$ in $k[X]$, are the same.

ii. Let $d = \deg(f_\alpha)$. Define

$$\varphi_{\alpha, \beta} : k(\alpha) \rightarrow k(\beta)$$

$$\left(a_0 + a_1 \alpha + \cdots + a_{d-1} \alpha^{d-1}\right) \mapsto \left(a_0 + a_1 \beta + \cdots + a_{d-1} \beta^{d-1}\right)$$

Show that $\varphi_{\alpha, \beta}$ is a field homomorphism.

iii. Show that the map $\varphi_{\alpha, \beta}$ is an isomorphism if and only if $\alpha$ and $\beta$ are conjugate.

iv. Let $f(X) \in \mathbb{R}[X]$ be any polynomial. Show that complex zeroes of $f$ come in conjugate pairs, i.e. show that for $a, b \in \mathbb{R}$ if $f(a + b\sqrt{-1}) = 0$ then $f(a - b\sqrt{-1}) = 0$, too.

(21) Show that the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is not Galois by showing that the Galois group is trivial.