1. Let \( \alpha \) and \( \beta \) be elements of a finite extension \( L/K \).
   (a) If \( [K(\alpha) : K] \) is odd show that \( K(\alpha) = K(\alpha^2) \).
   (b) If the degree of the minimal polynomials \( P_\alpha(X) \) (of \( \alpha \) over \( K \)) and \( P_\beta(X) \) (of \( \beta \) over \( K \)) are coprime show that \( P_\alpha(X) \) is irreducible over \( K(\beta) \).
   (c) If \( K \) has characteristic \( p \) which does not divide \([L : K]\) show that \( \alpha \) is separable over \( K \).

   Proof. (1): \( K(\alpha)/K(\alpha^2)/K \) are extensions and so \( [K(\alpha) : K(\alpha^2)] \) divides the odd number \( [K(\alpha) : K] \). The former is either 1 or 2 and since the latter is odd we deduce that \( K(\alpha) = K(\alpha^2) \).

   (2): Note that \( \deg P_\alpha = [K(\alpha) : K] \). Let \( Q \) be the minimal polynomial of \( \alpha \) over \( K(\beta) \). Clearly \( Q | P_\alpha \) and we need equality. Since \( [K(\beta)(\alpha) : K(\beta)] = \deg Q \) it suffices to show that \( [K(\alpha, \beta) : K(\beta)] = \deg P_\alpha = [K(\alpha) : K] \). But \( [K(\alpha) : K] = \deg P_\alpha \) and \( [K(\beta) : K] = \deg P_\beta \) are coprime and so from class \( [K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K] \) and so we deduce \( [K(\alpha, \beta) : K(\beta)] = [K(\alpha) : K] \).

   (3): Note that \( \deg P_\alpha = [K(\alpha) : K] | [L : K] \) and so \( \deg P_\alpha \) is coprime to \( p \). If \( P_\alpha \) inseparable we know there exists some polynomial \( Q \) such that \( P_\alpha(X) = Q(X^p) \) and so \( p | \deg Q = \deg P_\alpha \), contradiction.

2. Let \( L/K \) be a finite extension and \( K_1, K_2 \) be two subextensions of \( K \) such that \( [K_2 : K] = 2 \) and \( K_1 \cap K_2 = K \). Show that \( [K_1K_2 : K] = [K_1 : K][K_2 : K] \).

   Proof. Let \( u, v \) be a basis of \( K_2 \) over \( K \). If \( [K_1K_2 : K] < [K_1 : K][K_2 : K] \) then from class \( u \) and \( v \) must be linearly dependent over \( K_1 \). Let \( a, b \in K_1 \) not both 0 such that \( au + bv = 0 \). Say \( a \neq 0 \). Then \( u/v = -b/a \). But the LHS is in \( K_2 \) and the RHS is in \( K_1 \) and the only possibility is that \( u/v = -b/a \in K_1 \cap K_2 = K \). But then \( u \) and \( v \) are linearly dependent over \( K \) contradicting the fact that they form a basis.

3. Suppose \( K \) is not perfect. Show that there exist inseparable irreducible polynomials in \( K[X] \).

   Proof. Since \( K \) is not perfect there exists \( a \in K \) such that \( a \) is not of the form \( b^p \). Therefore \( X^p - a \in K[X] \) does not split completely over \( K \). Let \( P(X) \) be any irreducible factor of \( X^p - a \) of degree \( \geq 2 \). Let \( \alpha \) be a root of \( P(X) \). Then \( \alpha \notin K \) because \( \alpha^p = a \). Moreover, \( X^p - a = X^p - \alpha^p = (X - \alpha)^p \) and \( P(X) | (X - \alpha)^p \). We deduce that \( P(X) \) is inseparable as all its roots are equal to \( \alpha \).

4. Let \( \alpha = \sqrt[3]{5} \).
   (a) Is \( \mathbb{Q}(i\alpha^2) \) normal over \( \mathbb{Q} \)?
   (b) Is \( \mathbb{Q}(\alpha + i\alpha) \) normal over \( \mathbb{Q}(i\alpha^2) \)?
   (c) Is \( \mathbb{Q}(\alpha + i\alpha) \) normal over \( \mathbb{Q} \)?
Proof. Note that every quadratic extension is normal. Indeed, if \( L = K(\alpha) \) where \( \alpha \) satisfies a polynomial \( X^2 - aX + b = 0 \) then the other root \( \beta \) of this polynomial is \( a - \alpha \in L \) and so \( L \) is the splitting field of \( X^2 - aX + b \) over \( K \) and so it is normal.

(1): \( \sigma x^2 = \sqrt{a} \) so \( Q(\sigma x^2) \) is quadratic and therefore normal over \( Q \).

(2): Write \( x = \alpha + i\alpha \). Then \( x^2 = \alpha^2(1 + i)^2 = 2i\alpha^2 \) and so \( Q(\alpha + i\alpha) \) is quadratic and therefore normal over \( Q(\alpha i\alpha^2) \).

(3): \( \sigma x = \alpha + i\alpha \). If \( Q(x) \) were normal over \( Q \) then all the roots of the minimal polynomial of \( x \) would be in \( Q(x) \). But \( x^2 = 2i\alpha^2 = 2\sqrt{a} \) so the minimal polynomial is \( x^2 + 20 = 0 \) \( ([Q(x) : Q] = \lceil Q(x) : Q(\alpha^2) \rceil) = 2 = 2 \cdot 2 \). The four roots are \( x = \alpha \pm \alpha \mp i\alpha \). If all four were in \( Q(x) \) then \( \alpha = (x + \alpha - i\alpha)/2 \in Q(x) \) and therefore \( i \in Q(x) \). We'd deduce that \( Q(x) = Q(i, \alpha) \). But \( \alpha \in \mathbb{R} \) and so \( Q(\alpha) \subset \mathbb{R} \) from where we'd get \( Q(i) \cap Q(\alpha) = Q \). From the previous problem we'd get that \( [Q(i, \alpha) : Q] = 2 \cdot 4 = 8 \) contradicting that \( [Q(x) : Q] = 4 \). We conclude that \( Q(x) \) is not normal over \( Q \).

5. Let \( p \) be a prime and \( \alpha \in \mathbb{F}_p^\times \).

(a) Let \( Q(X) = X^p - X - a \). Show that \( Q(X + 1) = Q(X) \).

(b) Show that the splitting field \( K \) of \( Q(X + 1) \) is a normal separable extension of degree \( p \). [Hint: Use (a).]

(c) Determine the set \( \text{Aut}(K/\mathbb{F}_p) \). [Hint: Use (a).]

\( K \) is an Artin-Schreier extension.

Proof. (1): \( Q(X + 1) = (X + 1)^p - (X + 1) - a = X^p + 1^p - X - 1 - a = Q(X) \).

(2): Suppose \( \alpha \) is a root of \( Q \). Then \( Q(\alpha) = Q(\alpha + 1) = \cdots = Q(\alpha + p - 1) = 0 \) and so the roots of \( Q \) are distinct equal to \( \alpha, \alpha + 1, \ldots, \alpha + p - 1 \). Thus \( K = \mathbb{F}_p(\alpha, \alpha + 1, \ldots, \alpha + p - 1) = \mathbb{F}_p(\alpha) \) is normal and separable over \( \mathbb{F}_p \). It remains to show that \( Q \) is irreducible. Part (3) shows that \( \text{Aut}(K/\mathbb{F}_p) \) has \( p \) elements and from class \( p = [\text{Aut}(K/\mathbb{F}_p)] \leq [K : \mathbb{F}_p] = \text{deg \, min}_a(X) \leq p \). We conclude that \( \text{min}_a(X) = Q(X) \) which is then irreducible.

(3): We know from class that \( [\text{Aut}(K/\mathbb{F}_p)] \leq [K : \mathbb{F}_p] = \text{deg \, min}_a \leq \text{deg \, Q(X)} = p \). It suffices to exhibit \( p \) automorphisms in \( \text{Aut}(K/\mathbb{F}_p) \). Note that \( K = \mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha] \). For \( 0 \leq k \leq p - 1 \) define \( \sigma_k : \mathbb{F}_p[\alpha] \to \mathbb{F}_p[\alpha] \) defined by \( \sigma_k(R(\alpha)) = R(\alpha + k) \) for \( R \in \mathbb{F}_p[X] \). This is clearly an isomorphism with inverse \( \sigma_{-k} \). Note that if \( R \) is constant then \( \sigma_k(R) = R \) so \( \sigma_k \in \text{Aut}(K/\mathbb{F}_p) \). All the automorphisms \( \sigma_0, \ldots, \sigma_{p-1} \) are distinct (they take \( a \) to distinct elements) so \( \text{Aut}(K/\mathbb{F}_p) = \{\sigma_0, \ldots, \sigma_{p-1}\} \).

6. Suppose \( \sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q}) \).

(a) Show that if \( x > 0 \) then \( \sigma(x) > 0 \) and conclude that \( \sigma \) is an increasing function.

(b) Show that if \( |x - y| < \frac{1}{n} \) then \( |\sigma(x) - \sigma(y)| < \frac{1}{n} \) and conclude that \( \sigma \) is continuous.

(c) Show that \( \text{Aut}(\mathbb{R}/\mathbb{Q}) = \{\text{id}\} \).

Proof. (1): If \( x \geq 0 \) then \( \sigma(x) = \sigma(\sqrt{x})^2 = \sigma(\sqrt{x})^2 \geq 0 \). Equality occurs iff \( \sigma(\sqrt{x}) = 0 \) iff \( \sqrt{x} = 0 \) iff \( x = 0 \). If \( x < y \) then \( y - x > 0 \) so \( \sigma(y) - \sigma(x) = \sigma(y - x) > 0 \).

(2): Suppose \( -1/n < x - y < 1/n \). Then \( -1/n = \sigma(-1/n) < \sigma(x) - \sigma(y) < \sigma(1/n) = 1/n \). This \( |\sigma(x) - \sigma(y)| < 1/n \). For \( \delta > 1/n \) take \( \varepsilon = 1/n \) in the definition of continuity so \( \sigma \) is continuous.

(3): Any \( x \in \mathbb{R} \) is a limit \( x = \lim q_n \) with \( q_n \in \mathbb{Q} \). Since \( \sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q}) \) is continuous \( \sigma(x) = \lim \sigma(q_n) = \lim q_n = x \) so \( \sigma = \text{id} \).
7. Let \( K \) be any field and \( x \) a variable. Recall that \( \text{PGL}(2, K) \) is the quotient \( \text{GL}(2, K)/K \times I_2 \) of invertible \( 2 \times 2 \) matrices by the normal subgroup of scalar matrices. Show that
\[
\text{Aut}(K(x)/K) \cong \text{PGL}(2, K)
\]
via \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}(2, K) \) mapping to the automorphism \( \sigma_\gamma(f(x)) = f \left( \frac{ax + b}{cx + d} \right) \). [Hint: If \( \sigma \in \text{Aut}(K(x)/K) \) then \( K(x) = K(\sigma(x)) \). What does \( \sigma(x) \) look like?]

Proof. If \( \sigma \in \text{Aut}(K(x): K) \) then \( K(x) \cong \text{K}(\sigma(x)) \). But \( \sigma(x) \in K(x) \) so we conclude that \( K(x) = K(\sigma(x)) \). But \( \sigma(x) = P(x)/Q(x) \) is a rational function and from homework 6 we know that \( [K(x): K(\sigma(x))] = \max(\text{deg} P, \text{deg} Q) \). Thus \( P \) and \( Q \) are linear and so \( \sigma(x) = \frac{ax + b}{cx + d} \) for some matrix \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). Similarly \( \sigma^{-1}(x) = \frac{ux + v}{wx + t} \) for some matrix \( \eta = \begin{pmatrix} u & v \\ w & t \end{pmatrix} \). Since \( \sigma(\sigma^{-1}(x)) = x \) we conclude that \( \gamma \eta = I_2 \) and so \( \gamma \in \text{GL}(2, K) \). If \( R(x) \) is any rational function then \( \sigma(R(x)) = R(\sigma(x)) = R(\frac{ax + b}{cx + d}) \) as desired.

If \( \lambda \in K^\times \) the it’s clear that \( \sigma_\gamma = \sigma_{\lambda \gamma} \). Suppose \( \sigma_\gamma = \sigma_{\gamma'} \) for two matrices \( \gamma, \gamma' \in \text{GL}(2, K) \). Then \( \frac{ax + b}{cx + d} = \frac{a'x + b'}{c'x + d'} \) as rational functions. There are two ways of proceeding. One way is to multiply everything out and do a case-by-case analysis. This is somewhat unpleasant to write out, but quite straightforward. We get \( a' = a, ad = c'd + b'c \) and \( b' = b + d' \) and so on. Another is to notice that the equality of the two rational functions is equivalent to the matrix \( x \begin{pmatrix} a & a' \\ c & c' \end{pmatrix} + \begin{pmatrix} b & b' \\ d & d' \end{pmatrix} \) has 0 determinant. If \( \begin{pmatrix} a & a' \\ c & c' \end{pmatrix} \) is invertible, then we’d deduce that \( \begin{pmatrix} b & b' \\ d & d' \end{pmatrix} \begin{pmatrix} a & a' \\ c & c' \end{pmatrix}^{-1} \) has 0 characteristic polynomial which is impossible. Therefore \( \det \begin{pmatrix} a & a' \\ c & c' \end{pmatrix} = 0 \). The matrices \( \gamma \) and \( \gamma' \) are invertible and so the matrix \( \begin{pmatrix} a & a' \\ c & c' \end{pmatrix} \) has nonzero columns. Thus the determinant 0 condition implies there exists \( \lambda \in K^\times \) such that \( a = \lambda a' \), \( c = \lambda c' \).

We have \( \sigma_\gamma = \sigma_{\gamma'} = \sigma_{\lambda \gamma} \) and so \( \frac{ax + b}{cx + d} = \frac{ax + \lambda b'}{cx + \lambda d'} \). We get \( \frac{ax + b}{cx + d} = \frac{cx + d}{cx + \lambda d'} \). This implies \( \frac{ax + b}{cx + d} = \frac{d - \lambda d'}{d - \lambda d'} \). If the numerators are nonzero we’d get that \( \frac{ax + b}{cx + \lambda d'} = \frac{b - \lambda b'}{d - \lambda d'} \in K \). But \( [K(x): K(LHS)] = 1 \) as at least one of \( a, c \) is nonzero (homework 6). This is a contradiction and so \( b = \lambda b' \) and \( d = \lambda d' \). Thus \( \gamma = \lambda \gamma' \).

Thus \( \text{GL}(2, K) \to \text{Aut}(K(x)/K) \) sending \( \gamma \) to \( \sigma_\gamma \) factors through \( \text{PGL}(2, K) \to \text{Aut}(K(X)/K) \) and this maps is injective and surjective. \( \square \)