Math 6020 / Problem Set 11 (two pages)

Field extensions/Galois theory
- Make sure that you know/studied the Steinitz Embedding Thm and Steinitz Transitivity Thm and some of their consequences (as mentioned in class):
  - $\text{Aut}_K(\overline{K})$ acts transitively on $S_L := \{ \phi : L \to \overline{K} \mid K \text{-embedding} \}$ via $\sigma(\phi) = \sigma \circ \phi$.
  - If $L_1 \mid K$ is a subextension of $L \mid K$, then $S_L \to S_{L_1}$, $\phi \mapsto \phi_1|_{L_1}$ is surjective.
  - If $L \mid K$ is normal, and $p(t) \in K[t]$ is irreducible, then $\text{Aut}_K(L)$ acts transitively on the roots of $p(t)$ in $L$.
  - If $L_1 \mid L$ is a normal subextension of a normal extension $L \mid K$, then $\text{Aut}_K(L) \to \text{Aut}_K(L_1)$, $\sigma \mapsto \sigma_1 := \sigma|_{L_1}$ is surjective.

- Suppose that $\text{char}(K) = p > 0$, and let $p(t) \in K[t]$ be monic and irreducible. Make sure that you know the details of the proofs of the assertions from the class:
  - There are unique $c \geq 0$ and $p_c(t) \in K[t]$ monic irreducible separable s.t. $p(t) = p_c(t^p)$.
  - There is a unique monic separable polynomial $q(t)$ such that $q(t)^p = p_c(t^p)$.
  - Moreover, if $p_c(t) = \sum_k a_k t^k$ and $q(t) = \sum_k b_k t^k$, then $b_k^p = a_k$ for all $k$.

1) Find the Galois group of (the splitting field of) each of the following polynomials.
   a) $p(t) = t^3 - 10$ over $\mathbb{Q}$, respectively over $\mathbb{Q}(\sqrt[3]{3})$.
   b) $p(t) = t^4 - 5$ over $\mathbb{Q}$, respectively over $\mathbb{Q}(i)$, where $i^2 = -1$.
   c) $p(t) = t^4 - u$ over the rational function fields $\mathbb{R}(u)$, respectively $\mathbb{C}(u)$ in the variable $u$.

2) Recalling Problem 8 from HW 10, for $n \geq 1$, set $K_n = \mathbb{Q}(\mu_n)$.
   a) Show that $K_n \mid \mathbb{Q}$ is Galois and that $G_n = G(K_n \mid \mathbb{Q}) \cong (\mathbb{Z} / n\mathbb{Z})^\times$ canonically [HOW].
      In particular, what is this Galois group when $n = 5, 6, 7, 8, 12$?
   b) Find all $n$ such that $G_n$ is a cyclic group, respectively a cyclic group of odd order.
   c) Find all $m \leq n$ such that $K_m \subset K_n$ and $G(K_n \mid K_m)$ is a cyclic group.
   d) Let $K := K_n$. Show that $K_+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is Galois over $\mathbb{Q}$. What is $G(K \mid K_+)$?

3) Let $K = \mathbb{F}_p(t)$ and $L = K(\sqrt[p]{t})$, where $p = 4k + 1$ is a prime number.
   a) Find the separable subextension $L_{\text{sep}} \mid K$ of $L \mid K$ and the purely inseparable subextension $L_{\text{ins}} \mid K$ of $L \mid K$.
   b) Show explicitly in this example that $L = L_{\text{sep}} L_{\text{ins}}$ by expressing $\sqrt[p]{t}$ as a combination of elements from $L_{\text{sep}}$ and $L_{\text{ins}}$.
   c) What happens in the cases $p = 4k + 3$ or $p = 2$?

4) Let $\alpha = \sqrt{2} \in \mathbb{R}$, $\beta = \sqrt{3 + \sqrt{2}} \in \mathbb{R}$ and consider $K = \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\beta)$.
   a) Describe the normal closures $K^n \mid \mathbb{Q}$ and $L^n \mid \mathbb{Q}$ of $K \mid \mathbb{Q}$ and $L \mid \mathbb{Q}$.
   b) Describe the Galois groups $G(K^n \mid \mathbb{Q})$ and $G(L^n \mid \mathbb{Q})$. 

Due: Th, Dec 7, 2023
5) In the notation from Problem 4) above, answer the following:
   a) Find a primitive element of \( M := \mathbb{Q}(\alpha, \beta) \) over \( \mathbb{Q} \).
   b) What is \( M^n \) and \( G(M^n|\mathbb{Q}) \)?

6) Consider the rational function fields \( \mathbb{F}_p(t) \) and \( \mathbb{F}_p(t, u) \). Prove/disprove/answer:
   a) Every normal finite extension of \( \mathbb{F}_p(t) \) has a primitive element.
   b) Every normal finite extension of \( \mathbb{F}_p(t, u) \) has a primitive element.

The Frobenius endomorphism

- Recall that a field \( K \) is called perfect, if \( K \) does not have any purely inseparable extensions. In particular, if \( \text{char}(K) = 0 \), then \( K \) is perfect. Further, if \( \text{char}(K) = p > 0 \), then \( K \) is perfect iff every \( a \in F \) is a \( p \)-power.
- Let \( \text{char}(K) = p > 0 \). Then the map \( F : K \to K, x \mapsto x^p \) is a field morphism (why), and \( F \) is an isomorphism iff \( K \) is perfect (why). Terminology: \( F \) is the Frobenius endomorphism.

7) Let \( K \) be a field with \( \text{char}(K) = p > 0 \) and \( L|K \) denote algebraic extensions. Prove/disprove:
   a) \( F \) commutes with all field morphisms \( \sigma : F \to F \), i.e., \( F \circ \sigma = \sigma \circ F \).
   b) \( K \) is perfect iff \( F(K) = K \) iff all \( L|K \) are perfect iff all \( L|K \) are separable.
   b) If \( K \) is a finite field, then \( K \) is perfect, and every finite \( L|K \) has a primitive element.

Cyclotomic polynomials in \( \text{char} = p > 0 \).

- Recall the discussion form HW 10 about roots of unity and cyclotomic polynomials \( \Phi_n \).

8) Let \( K = \mathbb{F}_{p^e} \) be a finite field, \( p = \text{char}(K) \), and \( F : K \to K \) the Frobenius. Prove/disprove/answer:
   a) \( K \) is the fixed field of \( F^e \) acting on \( K \).
   b) For \( m \geq 1 \) there is a unique \( L|K \) of degree \( m \), and \( L|K \) is cyclic with \( G(L|K) = \langle F^e \rangle \).
   c) \( \Phi_n(t) \in K[t] \) is never irreducible.
   d) How many irreducible factors does \( \Phi_n(t) \) have over \( K \)?

[Hints: To a): \( F^e(x) = x \iff x^{p^e} = x \iff x^{p^e-1} = 1 \iff x \in \mu_{p^e-1} \), etc. To b): \( [L:K] = m \iff |L| = p^m \iff L^\times = \mu_{p^m-1} \) (why), etc. To c) & d): \( F^e \) acts on \( \mu_n \) by raising to the \( p^e \)-power, hence the orbit of every \( \zeta \in \mu_n \) is \( \{\zeta_1 = \zeta, \zeta_2 = \zeta^{p^e}, \ldots\} \) and has length the minimal \( d \) such that \( \zeta^{p^e d} = \zeta \) (why). Conclude: If \( \zeta \in \mu_n \) is a primitive \( n^{1/k} \) root of unity, then \( d \) is the order of \( \zeta^{p^e} \in (\mathbb{Z}/n\mathbb{Z})^\times \) (why). Compare that with \( \deg \Phi_n(t) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n), \) etc.]