MATH 7752 - HOMEWORK 11
DUE FRIDAY 04/29/22

(1) In this problem you will need the following two definitions.
Definition 1: Let L/F be a finite separable extension and let $\overline{F}$ be an algebraic closure of F containing L. A subfield L' of $\overline{F}$ is called **conjugate to L over F** if $L' = \sigma(L)$ for some F-embedding $\sigma : L \to \overline{F}$. (Note: L/F is Galois if and only if the only conjugate to L over F is itself.)
Definition 2: A finite extension K/F is called a **p-extension** if K/F is **Galois** and $\mathrm{Gal}(K/F)$ is a p-group.
  (a) Let L/F be a separable extension of degree n and let K be the Galois closure of L over F. Prove that K can be written as a compositum $L_1 L_2 \cdots L_n$, where $L_1, \ldots, L_n$ are (not necessarily distinct) conjugates of L over F.
  (b) Let K/F and L/F be finite p-extensions. Prove that KL/F is also a p-extension.
  (c) Suppose that K/L and L/F are both p-extensions, and let M be the Galois closure of K over F (note: we do not know whether K/F is Galois or not). Prove that M/F is also a p-extension.
  (d) Now assume only that L/F is a separable extension with $[L : F] = p^r$, for some $r \geq 1$. Let M be the Galois closure of L over F. Prove that $[M : F]$ need not be a power of p.

(2) Let $f(x)$ and $g(x)$ be irreducible polynomials in $\mathbb{F}_p[x]$ of the same degree. Let $F = \mathbb{F}_p[x]/(f(x))$. Prove that $g(x)$ splits completely over F.

(3) Consider the polynomial $f(x) = x^4 - 2x^2 - 5 \in \mathbb{Q}[x]$.
  (a) Determine the Galois group G of the splitting field K of $f(x)$ over $\mathbb{Q}$.
  (b) Find all subgroups of G and their corresponding fixed fields. Which of those are normal extensions of $\mathbb{Q}$?

(4) Let p and q be distinct primes with $q > p$, and let K/F be a Galois extension of degree pq. Prove the following:
(a) There exists a field L with $F \subset L \subset K$ and $[L : F] = q$.
(b) There exists a **unique** field M with $F \subset M \subset K$ and $[M : F] = p$.

(5) Prove the following analogue of Kummer's theorem for abelian extensions: Let $n \in \mathbb{N}$ and let F be a field containing a primitive n^{th} root of unity.
  (a) Let K/F be a finite Galois extension such that $G = \mathrm{Gal}(K/F)$ is abelian of exponent n. Then there exists $a_1, \ldots, a_t \in F$ such that $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$. More precisely, there exists $\alpha_1, \ldots, \alpha_t \in K$ such that $K = F(\alpha_1, \ldots, \alpha_t)$ and $\alpha_i^n \in F$ for all i.
  (b) Conversely, suppose that $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$ for some $a_1, \ldots, a_t \in F$. Prove that K/F is Galois and $G = \mathrm{Gal}(K/F)$ is abelian of exponent n. **Hint:** For part (b) use one of the problems from the previous homework.

(6) Let F be a field containing a primitive n^{th} root of unity. Let $a, b \in F$ be such that the polynomials $f(x) = x^n - a$, and $g(x) = x^n - b$ are both irreducible over F. Consider the Kummer extensions $F(\alpha)$, $F(\beta)$, where α is a root of $f(x)$ and β is a root of $g(x)$. Prove that $F(\alpha) = F(\beta)$ if and only if $\beta = c\alpha^r$, for some $c \in F$ and some integer r which is coprime to n (equivalently, if and only if $b = c^n a^r$, for some $c \in F$ and some $(r, n) = 1$).