Modern Algebra II, fall 2020, Instructor M.Khovanov

Homework 9, due Wednesday November 11.

1. (15 points) (a) Given a field E and an automorphism σ of E, prove that $E^\sigma = \{a \in E | \sigma(a) = a\}$ is a subfield of E.
(b) With E and σ as above, let $\tau = \sigma^2$. Explain why E^σ is a subfield of E^τ. Can you give an example of E and σ such that the inclusion $E^\sigma \subset E^\tau$ is proper (not an equality)? Can you give an example when both inclusions $E^\sigma \subset E^\tau \subset E$ are proper (neither one is an equality)?

2. (20 points) For any automorphism σ of a ring R we can define the subring R^σ of elements fixed by σ.
(a) Give a definition of R^σ.
(b) Suppose $R = F[x]$, where F is a field, and σ takes a polynomial $f(x)$ to $f(-x)$. For instance, if $f(x) = a + bx + cx^2$, then $\sigma(f)$ is the polynomial $a - bx + cx^2$. Prove that the subring R^σ of polynomials invariant under σ (equivalently, fixed by σ) is the subring $F[x^2]$ if $\operatorname{char} F \neq 2$. What happens when F has characteristic two?
(c) Suppose now $R = \mathbb{C}[x]$, where $\mathbb{C}$ is the field of complex numbers, and $\zeta = e^{2\pi i/m}$ is the first m-th root of unity as we go along the unit circle anticlockwise. To ζ assign automorphism σ of R taking $f(x)$ to $f(\zeta x)$. Write down the effect of this automorphism on an arbitrary polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then prove that the subring R^σ of invariant polynomials under this automorphism is the subring $\mathbb{C}[x^m]$.
(d) (optional) Consider the automorphism τ of $\mathbb{C}[x]$ that takes $f(x)$ to $f(x+1)$. Show that constant polynomials are the only polynomials fixed by τ.

3. (15 points) How many subfields does finite field $\mathbb{F}_{4096}$ have? What are their cardinalities? What is the order of the Frobenius automorphism of F_{4096}?