

Homework 10 : Due Monday, May 9

Notation: Throughout this assignment, let $\xi_n = e^{2\pi i/n} \in \mathbb{C}$.

Problem 1: Let $\mathbb{Q} \prec F$ be a Galois extension and suppose that $\text{Gal}_{\mathbb{Q}} F \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Show that there exist squarefree integers $c, d \in \mathbb{Z}$ such that $F = \mathbb{Q}(\sqrt{c}, \sqrt{d})$.

Problem 2: Let K be a field of prime characteristic p . Let F be a splitting field of $f(x) = x^n - 1$ over K . Write $n = p^k m$ where $p \nmid m$. Show that $f(x)$ has exactly m distinct roots in F .

Problem 3:

- a. Show that $\Phi_n(0) = 1$ for all $n \geq 2$.
- b. Let p be prime. Find an explicit formula for $\Phi_{p^2}(x)$.
- c. Suppose that n is odd. Show that $\xi_{2n} \in \mathbb{Q}(\xi_n)$ by finding an explicit formula for ξ_{2n} in terms of ξ_n . Conclude that $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{2n})$.
- d. Suppose that $n \geq 3$ is odd. Show that $\Phi_{2n}(x) = \Phi_n(-x)$.

Problem 4: Let p be an odd prime. In this problem, we show that the only degree two extension of \mathbb{Q} inside $\mathbb{Q}(\xi_p)$ is:

$$\begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv_4 1 \\ \mathbb{Q}(i\sqrt{p}) & \text{if } p \equiv_4 3 \end{cases}$$

Letting $m = (-1)^{(p-1)/2}$, we have $m = 1$ if $p \equiv_4 1$ and $m = -1$ if $p \equiv_4 3$. With this notation, we can consolidate the above two calling them both $\mathbb{Q}(\sqrt{mp})$.

- a. Show that $\mathbb{Q}(\xi_p)$ has a unique subfield E with $[E : \mathbb{Q}] = 2$.
- b. Show that $(1 - \xi)(1 - \xi^2) \cdots (1 - \xi^{p-1}) = p$. (*Hint:* Think about $\Phi_p(x)$)
- c. Show that there exists $k \in \mathbb{Z}$ with $(1 - \xi)(1 - \xi^2) \cdots (1 - \xi^{p-1}) = m\xi^k[(1 - \xi)(1 - \xi^2) \cdots (1 - \xi^{(p-1)/2})]^2$.
- d. Show that there exists $u \in \mathbb{Q}(\xi)$ with $u^2 = mp$.
- e. Show that $\mathbb{Q}(\sqrt{mp})$ is the unique field E from part a.

Problem 5: Show that $\sqrt[3]{2} \notin \mathbb{Q}(\xi_n)$ for all $n \in \mathbb{N}^+$.