Assignment 17

Extensions of Finite Fields, Splitting Fields

1. Let L_1/K_1 and L_2/K_2 be two field extensions and $\varphi : L_1 \longrightarrow L_2$ an isomorphism of fields such that $\varphi(K_1) = K_2$. Prove that $[L_1 : K_1] = [L_2 : K_2]$.

2. Let p be a prime number. By factoring $X^{p-1} - 1$ over $\mathbb{F}_p$, show that
$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

3. Let $f = X^3 - X + 1 \in \mathbb{F}_3[X]$.
   (a) Show that f is irreducible in $\mathbb{F}_3[X]$.
   (b) Show that if E is a splitting field and $\rho \in E$ is a root, then so are $\rho + 1$ and $\rho - 1$.
   (c) Construct a splitting field of f and write out its multiplication table.
   (d) Write down explicitly the action of $\mathrm{Gal}(E/\mathbb{F}_3)$ on the elements of E.

4. Let p be a prime number.
   (a) Show that an element of order p in S_p is a p-cycle.
   (b) Show that a transposition and a p-cycle generated S_p.