Homework 8

1) Consider first $\mathbb{Q}(\xi)/\mathbb{Q}$. Since we have that ξ solves $x^{p}-1$ and $x \neq 1$ $\therefore$ we have that $m_\xi = x^{p-1} + \cdots + 1$ as it is irreducible by Eisenstein.

$\therefore$ we get $[\mathbb{Q}(\xi) : \mathbb{Q}] = p-1$.

Now consider the extension $\mathbb{Q}(\xi) / \mathbb{Q}(\xi + \xi^{-1})$ where we have the polynomial $x^2 - (\xi + \xi^{-1})x + 1$ which has as a root ξ as $\xi^2 - \xi^2 + 1 - 1 = 0$

$\therefore$ we have an irreducible of deg 2 so the extension has degree 2.

We get the tower

$$\begin{array}{c} \mathbb{Q}(\xi) \\ \big| \; 2 \\ \mathbb{Q}(\xi + \xi^{-1}) \\ \big| \; \therefore \frac{p-1}{2} \\ \mathbb{Q} \end{array} \left.\vphantom{\begin{array}{c} a \\ b \\ c \\ d \\ e \end{array}}\right\} p-1$$

$\therefore$ the extension asked for has degree $\frac{p-1}{2}$ $\square$

2) It suffices to show that $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ is the splitting field of some polynomial.

Let $m = (x^2-2)(x^2-3)$

which has roots $\pm\sqrt{2}, \pm\sqrt{3}$ in $\mathbb{C}$.

Consider $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ which has all roots of m and $= \mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3})$.

Claim $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q} = \mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$.

$\supset$ clear as $a(\sqrt{2}+\sqrt{3})+b$
$= a\sqrt{2}+a\sqrt{3}+b$.

$\overset{?}{\supset}$

We need to generate $\sqrt{2}$ and $\sqrt{3}$ via field ops on $\sqrt{2}+\sqrt{3}$.

Note that $(\sqrt{2}+\sqrt{3})^{-1} = \sqrt{3}-\sqrt{2}$

$\therefore (\sqrt{2}+\sqrt{3}) + (\sqrt{2}+\sqrt{3})^{-1} = 2\sqrt{3}$

$\therefore$ we can generate $\sqrt{3}$, $\therefore$ we can generate $\sqrt{2}$ $\square$

3) Claim: $k = \text{lcm}(m,n)$. Consider the field $\mathbb{F}_{p^n}$ which has multiplicative subgroup $|\mathbb{F}_{p^n}^\times| = p^n - 1$. To meet the required condition, we need that $p^n-1 \mid p^k-1$

i.e. $n \mid k$. Similarly, we need $m \mid k$.

$\therefore$ the smallest such k can be obtained by taking the $\text{l.c.m}(m,n)$.

4) $x^7-1=(x-1)(\underline{x^6+x^5+x^4+x^3+x^2+x+1})$

$f(0)=1$

$f(1)=7=2$

$f(2)=2^7-1\neq 0$

$f(-1)=1$

$f(-2)=\cancel{64-32+16-8}+4-2+1$

$32+8+2+1$

$\neq 0.$

$\therefore f$ is irreducible (degree 6)

$\therefore$ The degree of splitting field is 6.

5) Let $\alpha\in E/F$

then, we have the tower

$$\begin{array}{c} E \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

$\therefore \deg(m_\alpha)\mid [E:F]$

$\therefore \deg(m_\alpha)$ is also relatively prime to p

$\therefore (m_\alpha)'=n a_n x^{n-1}+\dots+\dots$

is not zero.

$\therefore m_\alpha, m_\alpha'$ are relatively prime.

$\therefore \alpha$ is separable ∎

6) a) Let $\alpha,\beta\in E/F$ be separable. $\therefore F(\alpha), F(\beta)$ are separable over F.

$\therefore F(\alpha,\beta)$ with minimal $f=m_\alpha m_\beta$ is also separable.

$\therefore$ the set of separable elts is closed under sums, products, inverses.

7) Assume that the extension is not purely insep i.e. $\exists\ \alpha \in E/F$ that has m_α separable. Then we can easily see that in the splitting field L of m_α, we get the extension of $E \to L$ over σ by sending α to another root of m_α in L. By contraposition, if only one extension exist, the extension is purely inseparable.

8) Consider the polynomial $(x^2-3)(x^7-5)$ and consider its splitting field over $\mathbb{Q}$.
it can be checked that the extension is Galois.
and $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$
and $|G| = [E:\mathbb{Q}] = 15$. $\square$

9) Consider the polynomial x^6+3, irreducible over $\mathbb{Q}$,
consider $\alpha = \sqrt[6]{-3}$, a root of f. Claim: $\mathbb{Q}(\alpha)$ is the splitting field of f.
It suffices to show that ξ (a 6^{th} root of unity) is in $\mathbb{Q}(\alpha)$.
Note that α^3 is a root of x^2+3. $\therefore \alpha^3 = \pm\sqrt{-3}$. Then $\xi = \frac{1 \pm \sqrt{-3}}{2}$ which is a primitive 6^{th} root of unity can be written as $\xi = \frac{1+\alpha^3}{2}$.

$\therefore [\mathbb{Q}(\alpha):\mathbb{Q}] = 6$.
We know that the Galois group embeds into S_6.
Its order is 6. $\therefore G = S_3$ ■

10) We can easily check that this is a Galois extension with $G = \mathbb{Z}_2 \times \mathbb{Z}_7$ that only has exactly one subgroup $\mathbb{Z}_7$ with index 2 in G. The result then follows by the correspondence theorem.