MATH5725: Galois Theory (2014, S2) Problem Set 2

1. Let p be a positive prime number. Put

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbf{Q}[X]$$

so that

$$X^p - 1 = (X-1)\Phi_p(X).$$

(a) Show that if $K/\mathbf{Q}$ is a splitting field for Φ_p and $\zeta \in K$ is a root of Φ_p then ζ^j is too if $1 \leq j \leq p-1$.
(b) Using (a), show that $K = \mathbf{Q}(\zeta)$. Show every element of K has a representation of the form $\sum_{0\leq i\leq p-1} a_i\zeta^i$ with $a_i \in \mathbf{Q}$ (this representation is not unique, but you do not need to show that for this part of the question). Show that

$$(\sum_{0\leq i\leq p-1} a_i\zeta^i) + (\sum_{0\leq i\leq p-1} b_i\zeta^i) = \sum_{0\leq i\leq p-1} (a_i+b_i)\zeta^i$$

and that

$$(\sum_{0\leq i\leq p-1} a_i\zeta^i)(\sum_{0\leq j\leq p-1} b_j\zeta^j) = \sum_{0\leq n\leq p-1} (\sum_{i+j\equiv n \mod p} a_ib_j)\zeta^n.$$

(Hint: use the isomorphism $\mathbf{Q}[X]/(\Phi_p) \to K : X + (\Phi_p) \mapsto \zeta$).
(c) Show that if $\lambda \in (\mathbf{Z}/p)^*$ and $\sum a_i\zeta^i \in K$ that

$$\sigma_\lambda : K \longrightarrow K : \sum a_i\zeta^i \mapsto \sum a_i\zeta^{\lambda i}$$

respects addition and multiplication (use the formulas in (b) and the fact that $\lambda(i+j) \equiv \lambda i + \lambda j \bmod p$).
Show that $\sigma_\lambda(1+\zeta+\cdots\zeta^{p-1}) = 1+\zeta+\cdots\zeta^{p-1}$, i.e. that σ_λ is well-defined.
Conclude that σ_λ is a field automorphism (i.e show it is surjective, it is injective automatically as a ring homomorphism of fields is always injective (because a field has no ideals other than the zero ideal)).
(d) Show that $\sigma_\lambda(a) = a$ if $a \in \mathbf{Q}$.
(e) Let g be a monic irreducible polynomial over $\mathbf{Q}$ such that $g(\zeta) = 0$. Using (d), show that $g(\sigma_\lambda(\zeta)) = 0$. Conclude that $\Phi_p \mid g$ and hence $g = \Phi_p$.
(f) Conclude that Φ_p is irreducible and that $\mathbf{Q}(\zeta_p) \cong \mathbf{Q}[X]/(\Phi_p)$ has degree $p-1$ over $\mathbf{Q}$ and therefore that $1, \zeta, \cdots, \zeta^{p-2}$ is a basis for K over $\mathbf{Q}$. You might consult the literature for alternative proofs that Φ_p is irreducible.

2. Let $f(X) \in \mathbf{Q}[X]$ by given by

$$f(X) = X^4 - 10X^2 + 1.$$

(a) Show that the roots of f have the form $\pm\sqrt{5 \pm 2\sqrt{6}}$.
(b) Put $K = \mathbf{Q}(\sqrt{5+2\sqrt{6}}, \sqrt{5-2\sqrt{6}})$, show that K is a splitting field for f.
(c) Calculate the square of $\sqrt{2} \pm \sqrt{3}$; conclude that $\sqrt{2} \pm \sqrt{3} \in K$.
(d) Show that $\sqrt{2}, \sqrt{3} \in K$.
(e) By considering dimensions, show that $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. Conclude that $\sqrt{2}$ and $\sqrt{3}$ can be written as polynomial expressions of $\sqrt{2}+\sqrt{3}$. Try finding formulas for $\sqrt{2}, \sqrt{3}$ in terms of $\sqrt{2}+\sqrt{3}$.