Polynomial Equations and Fields Sample Solution- University of Toronto

(1) Suppose that F is a subfield of $\mathbb{C}$, $f(x) \in F[x]$ is irreducible over F and G is the Galois group of $f(x)$ over F.

a) Prove that if $|G| > \deg f(x)$, then G is nonabelian.

b) Prove or disprove: If $|G| = \deg f(x)$, then G is abelian.

(2) Suppose that $F \leq E \leq \mathbb{C}$, $[E : F] = 100$, E is Galois over F and $G = \mathrm{Gal}(E/F)$ contains a subgroup H such that $|H| = 25$. Use Galois theory to prove that $H \lhd G$.

(3) Let $F \leq \mathbb{C}$. Suppose that $f(x) \in F[x]$ is monic, irreducible over F and $\deg f(x) = 6$. Let E be the splitting field of $f(x)$ over F and let $G = \mathrm{Gal}(E/F)$. Assume that $[E : F] = 12$ and assume that there exists $\sigma \in G$ such that $|\sigma| = 3$. Let $H = \langle \sigma \rangle$ and $K = E^H$.

a) Prove that if $\alpha \in E$ and $f(\alpha) = 0$, then $E = K(\alpha)$.

b) Determine how $f(x)$ factors as a product of irreducible polynomals in $K[x]$. What is the number of irreducible factors of $f(x)$ in $K[x]$ and what are their degrees? (*Hint*: How are $m_{\alpha,K}(x)$ and H related?)

① (a) Suppose that $|G| > \deg f$

As a result of the assumptions of the question we have there exists E such that $G = \mathrm{Gal}(E/F)$ and $F \leq E \leq \mathbb{C}$.

G is transitive group. Hence, if G is abelian then from $G \cong H$ such that $H \leq S_n$ we have $|G| = n$, where $n = \deg f$.

Notice that all abelian transitive subgroups of S_n have degree n. Hence $|G| > \deg f \Rightarrow G$ is nonabelian

(b) Now, suppose that $|G| = \deg f$

Let $F = \mathbb{Q}$ and $f(x) = x^6 - 2$. Let G be a Galois group of $f(x)$ over $\mathbb{Q}$.

$|G| = 6 = \deg f$ But G is not abelian, because f has at least to nonreal distinct roots and at least one real root and we can see $G \cong S_3$.

(2) By the Galois theory for finite Galois groups we have $|G| = [E:F] = 100$.

$|H| = 25 \implies [G:H] = 4$

Now by the Sylow theorems if r be the number of Sylow 5-subgroup of order 25 then:

$r \geq 1$

$r \equiv 1 \pmod{5}$

$r \leq (4 = \frac{100}{25}) \implies r = 1$

Sylow p-subgroup is unique iff Normal. Hence, $H \trianglelefteq G$.

Polynomial Equations and Fields Sample Solution- University of Toronto

(3) (a) α is the root of f. f has linear decomposition over E. $[E:F]=12$; Hence, $|G|=12 > \deg f$.
So G is nonabelian. $G \cong T \leqslant S_6$ and $|\sigma|=3$.
Hence $G \cong A_4$ or $G \cong S_3 \times S_2$. f is irreducible over F. Hence $G \cong A_4$.
All proper subgroups of A_4 are abelian.

$$\left.\begin{array}{l}\sigma(\alpha)=\sigma^2(\alpha)=id(\alpha)=\alpha \\ \alpha \in E\setminus F\end{array}\right\} \Rightarrow K(\alpha) \subseteq E \quad (*)$$

Now suppose $a \in E$. $f(x)$ is the minimal polynomial of α. Hence, by definition of K, $f(x)$ is linearly decomposable over $K(\alpha)$.
E is the splitting field of $f(x)$. Hence, if $K(\alpha) \subseteq E$ then $K(\alpha)=E$. $(**)$ By $(*)$ and $(**)$ we have $K(\alpha)=E$

(3) (b) For all α such that $f(\alpha)=0$, we have $E=K(\alpha)$.
By comparing $m_{\alpha,K}(x)$ and H we have
$\deg m_{\alpha,K}(x) = 1$ or 3.

If $m_{\alpha,K}(x)=1$ then by $E=K(\alpha)$, for all α we have $m_{\alpha,K}(x)=1$. Hence, $K=E$. That is impossible.
Therefore for all α such that $f(\alpha)=0$, we have $m_{\alpha,K}(x)=3$.
$f(x) = q(x)\, r(x)$ such that q and r are monic and irreducible over K and $\deg q = \deg r = 3$