Solution Sheet 4:

1. Let $K \subseteq L$ be a field extension of degree 2. Let $\alpha \in L$ and $m_{\alpha,K}$ be the minimal polynomial of α over K. Then $\deg m_{\alpha,K} \leq 2$ if $\deg m_{\alpha,K} = 1$ then α is the only root of $m_{\alpha,K}$ so $m_{\alpha,K}$ clearly splits in $L[x]$. Suppose that $\deg m_{\alpha,K} = 2$ & let $m_{\alpha,K} = x^2 + ax + b$ and let β be the other root of $m_{\alpha,K}$. Then $-a = \alpha + \beta \Rightarrow \beta = -a - \alpha \in L$ so $m_{\alpha,K}$ splits in $L[x]$.

2. First suppose that $K \subseteq L$ is normal and let $\sigma : L \to \overline{K}$ be a K-homo. As L/K is normal $L = SF_K(S)$ for $S \subseteq K[x]$. Let $f \in S$ and $\alpha \in L$ be a root of f. Then as σ is a K-homo, $\sigma(\alpha)$ is also a root of f and $\sigma(\alpha) \in L$. This shows that $\sigma(L) \subseteq L$ To see that σ is surjective* let $\beta_1 \in L$ and consider the field extension $K \subseteq K(\beta_1, .., \beta_d)$ where β_i are the roots of $m_{\alpha,K}$ in L. Then $K \subseteq K(\beta_1, .., \beta_d)$ is a finite extension, Let q be its degree. Consider the restriction of σ on $K(\beta_1, .., \beta_d)$, its image is contained in $K(\beta_1, .., \beta_d)$ hence $\sigma(K(\beta_1, .., \beta_d))$ is a sub K-vector space of $K(\beta_1, .., \beta_d)$ but σ is injective $\dim_K \sigma(K(\beta_1, .., \beta_d)) = q \Rightarrow \sigma(K(\beta_1, .., \beta_d)) = K(\beta_1, .., \beta_d) \Rightarrow \beta_1 \in \operatorname{im}\sigma$ and σ is surjective.

   *: Here we don't use that $K \subseteq L$ is normal. It suffices that $\sigma(L) \subseteq L$

   Suppose that for every K-homo. $\sigma : L \to \overline{K}$, $\sigma(L) = L$. Let $\alpha \in L$ and consider the irreducible polynomial $m_{\alpha,K}$ of α over K. Let $\beta \in \overline{K}$ be an another root of $m_{\alpha,K}$. Consider the K-isomorphism, $\psi : K(\alpha) \to K(\beta)$.
   $\alpha \mapsto \beta$.
   ψ yield a K-homo. $\tilde{\psi} : K(\alpha) \xrightarrow{\psi} K(\beta) \hookrightarrow \overline{K}$. Consider the following fact:

   Fact: Let $\phi : H \to A$ be a field homo. and A be algebraically closed. Suppose that $H \subseteq Q$ is an algebraic field extension then ϕ extends to $\Phi : Q \to A$.

   Using this fact extend $\tilde{\psi} : K(\alpha) \to \overline{K}$ to a K-homo. $\overline{\psi} : L \to \overline{K}$. Now by hypothesis $\overline{\psi}(L) = L$ so $\overline{\psi}(\alpha) = \beta \in L$ therefore L contains all the roots of $m_{\alpha,K}$ & $K \subseteq L$ is normal.

3. As L/K is finite Galois of degree $2d$, $|\mathrm{Gal}(L/K)| = 2d$. As d is odd 2^1 is the highest power of 2 dividing $2d$. Now by Sylow theorems there exists $H \leq \mathrm{Gal}(L/K)$ with $|H| = 2$. This shows that index of H is $|\mathrm{Gal}(L/K) : H| = |\mathrm{Gal}(L/K)| / |H| = d$.

4. Recall the quaternion group Q:

$$Q = \{1, i, j, k, -1, -i, -j, -k\} \qquad \begin{array}{lll} i^2=-1 & ij=-k & ik=j \\ j^2=-1 & ji=k & jk=-i \\ k^2=-1 & ki=-j & kj=i \end{array}$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of f. Let $K := \mathbb{Q}(\alpha_1, -, \alpha_4)$. Any element in $G := \mathrm{Gal}(K/\mathbb{Q})$ is determined by its action on $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Let n be the number of distinct roots then G embeds into S_n as it permutes the roots. If $n<4$ $|G| < 8$ so $G \not\cong Q$. Suppose that $n=4$ then $G \hookrightarrow S_4$. But no subgroup of S_4 is isomorphic to Q. Indeed, there are 6 elements of order 4 in Q $\{i, j, k, -i, -j, -k\}$ and there are 6 elements of order 4 in S_4 these are the 4-cycles. However, all elements of order 4 have the same square in Q but not in S_4.

5. Suppose that F/K is normal. Let $\alpha \in F$, $\tau \in \mathrm{Gal}(L/K)$ and $\sigma \in H$. Then $\tau(\alpha)$ is another root of $m_{\alpha/K}$ and is contained in F by normality. Therefore, $\sigma(\tau(\alpha)) = \tau(\alpha) \Rightarrow \tau^{-1}\sigma\tau(\alpha) = \alpha$. As this holds for all $\alpha \in F$, $\tau^{-1}\sigma\tau \in H$ and $H \trianglelefteq \mathrm{Gal}(L/K)$.

Now suppose that $H \trianglelefteq \mathrm{Gal}(L/K)$ and let α, σ be as before. Then as L/K is Galois, $m_{\alpha/K}$ splits in $L[X]$ let β be a root of $m_{\alpha/K}$. As L/K is Galois, $\mathrm{Gal}(L/K)$ acts transitively on the roots of $m_{\alpha/K}$ $\Rightarrow$ there exist $\psi \in \mathrm{Gal}(L/K)$ such that $\psi(\alpha) = \beta$. By normality of H, $\psi^{-1}\sigma\psi(\alpha) = \alpha \Rightarrow \sigma(\psi(\alpha)) = \psi(\alpha) = \beta$ $\Rightarrow \sigma(\beta) = \beta \Rightarrow \beta \in F \Rightarrow F/K$ is normal.

Suppose that $H \trianglelefteq \mathrm{Gal}(L/K)$ and define* $\phi: \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$

$$\sigma \mapsto \sigma_{|F}$$

if $\sigma \in H$ then $\sigma_{|F} = id_F$ so $H \subseteq \ker\phi$ but also the fixed field of $\ker\phi$ contains F thus $\ker\phi \subseteq H \Rightarrow H = \ker\phi$. It remains to show that ϕ is surjective.
Let $\chi \in \mathrm{Gal}(F/K)$ then by the normality of L/K χ extends to an automorphism $\bar{\chi}$ of L fixing K so we have $\bar{\chi}_{|F} = \chi$. This shows that ϕ is surjective and $\mathrm{Gal}(L/K)/_H \cong \mathrm{Gal}(F/K)$.

* Here we use that $H \trianglelefteq \mathrm{Gal}(L/K)$ therefore F/K is normal and $\sigma_F(F) \subseteq F$.

(6) (i) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$: As $\mathrm{char}\,\mathbb{Q}=0$ the extension is separable. It can be seen that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = SF_{\mathbb{Q}}((x-\sqrt{2})(x+\sqrt{2})(x+\sqrt{3})(x-\sqrt{3}))$ so the extension is normal therefore it is a Galois extension.
It is clear that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4 \Rightarrow |G|=4$ where $G=\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$.
Note that there are 2 groups of order 4 which are $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ & $\mathbb{Z}/4\mathbb{Z}$.
Take $\tau\in G$ then $\tau(\sqrt{2})=\pm\sqrt{2}$ indeed τ permutes the roots of the polynomial x^2-2, likewise $\tau(\sqrt{3})=\pm\sqrt{3}$, in any case we get $\tau^2=id_G$
Therefore $G\cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ and the elements are given by:

$\{id,\tau,\sigma,\tau\sigma\}$ where $\tau(\sqrt{2})=-\sqrt{2}$ $\sigma(\sqrt{2})=\sqrt{2}$ $\tau\sigma(\sqrt{2})=-\sqrt{2}$
$\tau(\sqrt{3})=\sqrt{3}$ $\sigma(\sqrt{3})=-\sqrt{3}$ $\tau\sigma(\sqrt{3})=-\sqrt{3}$

non trivial
There are 3 subgroups, $H_1=\{id,\tau\}$, $H_2=\{id,\sigma\}$, $H_3=\{id,\tau\sigma\}$.
Clearly the fixed field of H_1 is $\mathbb{Q}(\sqrt{3})$ that of H_2 is $\mathbb{Q}(\sqrt{2})$.
Notice that $\sqrt{6}$ is fixed by H_3 thus the fixed field of H_3 is $\mathbb{Q}(\sqrt{6})$.
Finally the fixed field of the subgroup $\{id\}$ is $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

(ii) $\mathbb{Q}\subseteq\mathbb{Q}(\eta)$: As before separability is clear. To see normality note that $\mathbb{Q}(\eta)=SF_{\mathbb{Q}}(x^5-1)$.

The minimal polynomial of η over $\mathbb{Q}$ is given by $x^4+x^3+x^2+x+1$ hence $[\mathbb{Q}(\eta):\mathbb{Q}]=4 \Rightarrow |G|=4$ where $G:=\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$. Consider the $\mathbb{Q}$-automorphism τ given by $\tau(\eta)=\eta^2$. Note that such a τ exists as Galois groups act transitively on the roots of minimal polynomials. It can be seen that iterating τ we obtain all the roots of $x^4+x^3+x^2+x+1$ and the order of τ is 4. This shows that $G\cong\mathbb{Z}/4\mathbb{Z}$.
The only non trivial subgroup is $H:=\{id,\tau^2\}$. Observe that H fixes $\eta^2+\eta^3$ thus the fixed field of H contains $\mathbb{Q}(\eta^2+\eta^3)$. It can be also seen that $m_{\eta^2+\eta^3,\mathbb{Q}}=x^2+x-1$ thus $[\mathbb{Q}(\eta^2+\eta^3):\mathbb{Q}]=2$ which shows that the fixed field is $\mathbb{Q}(\eta^2+\eta^3)$.

(7) (i) Let $\mathrm{char}\,K=p>0$ and $q=p^e$. Then $\mathrm{char}\,L=p$ and $|L|=p^\ell$ for some ℓ such that $e|\ell$.

Consider the chain of field extensions, $\mathbb{F}_p\subseteq K\subseteq L$ and recall that $K=SF_{\mathbb{F}_p}(x^q-x)$ and $L=SF_{\mathbb{F}_p}(x^{p^\ell}-x)$ moreover $x^{p^\ell}-x$ is separable thus the extension $\mathbb{F}_p\subseteq L$ is separable. This shows that $K\subseteq L$ is separable. To see that $K\subseteq L$ is normal note that $L=SF_K(x^{p^\ell}-x)$.

(ii) Denote the Frobenius morphism by F. By the above description of K it is clear that $F(k)=k$ $\forall k\in K$. This shows that $F\in\mathrm{Gal}(L/K)$.
Note that $[L:K]=\ell/e$ so if we show that the order of F is ℓ/e we are done. Suppose that the order of F is n. Then $F^n(t)=t$ for all $t\in L$. But $F^n(t)=t^{p^{en}}$ this shows that t is a root of $x^{p^{en}}-x$ and this polynomial has at most p^{en} roots so if all the elements of L are roots then $p^{en}\geq p^\ell \Rightarrow n\geq \ell/e \Rightarrow n=\ell/e$.

non-zero
(iii) Let $\alpha\in L$ let us compute the norm of $\alpha\in L$. Recall that for $\alpha\in L$ such that $[K(\alpha):K]=t$ and $[L:K(\alpha)]=\ell/et$ the characteristic polynomial of the matrix $M_\alpha: L\to L$ corresponding to multiplication

by α is given by $(m_{\alpha,K})^{\ell/et}$. As $K \subseteq K\alpha$ is Galois,

$m_{\alpha,K} = \prod_{\sigma \in Gal(K(\alpha)/K)} (x - \sigma(\alpha))$ and the characteristic polynomial of M_α is

$\chi(M_\alpha) = \left(\prod_{\sigma \in Gal(K(\alpha)/K)} (x - \sigma(\alpha))\right)^{\ell/et}$. Now recall that

$Gal(L/K)/_{Gal(L/K(\alpha))} \cong Gal(K(\alpha)/K)$ and $|Gal(L/K(\alpha))| = \ell/et$

therefore for each $\sigma \in Gal(K(\alpha)/K)$ there exist ℓ/et many elements $\{\sigma_i\}_{i=1}^{\ell/et} \subseteq Gal(L/K)$ such that $\forall \beta \in K(\alpha)$ $\sigma_i(\beta) = \sigma(\beta)$. In particular,

$$\underbrace{(x - \sigma(\alpha)) \cdot \_\_\_ \cdot (x - \sigma(\alpha))}_{\ell/et \text{ times}} = \prod_{i=1}^{\ell/et} (x - \sigma_i(\alpha))$$

Applying this to every element in $Gal(K(\alpha)/K)$, we can write

$\chi(M_\alpha) = \prod_{\sigma \in Gal(L/K)} (x - \sigma(\alpha))$. Therefore, the norm $N(\alpha)$ of α is given by $N(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma(\alpha)$. Recall that $Gal(L/K) \cong \mathbb{Z}/_{\frac{\ell}{e}}\mathbb{Z}$ is generated by the Frobenius $F: \alpha \mapsto \alpha^q$ thus,

$$N(\alpha) = \prod_{i=0}^{\ell/e} \alpha^{q^i} = \alpha^{1+q+\dots+q^{\ell/e}} = \alpha^{(q^{\ell/e}-1)/q-1}$$

Now we know that $\alpha^{p^\ell} - \alpha = 0$ or if $\alpha \neq 0$ $\alpha^{p^\ell - 1} - 1 = 0$.
Moreover $K = SF_{\mathbb{F}_p}(x^{p^e} - x)$. Take $\beta \in K^\times$ then we claim that $\beta^{q-1/q^{\ell/e}-1} \in L$. Indeed,

$$\left(\beta^{q-1/q^{\ell/e}-1}\right)^{p^\ell - 1} - 1 = \left(\beta^{q-1/p^\ell - 1}\right)^{p^\ell - 1} - 1 = \beta^{q-1} - 1 = 0.$$

This shows that for $\beta \in K$, $N(\beta^{q-1/q^{\ell/e}-1}) = \beta$.

(8) First of all note that x^4+x+1 is irreducible and separable. Moreover it's roots are given by $\alpha, \alpha^2, \alpha^4, \alpha^8$ (these are all distinct because clearly $\alpha \neq \alpha^2$, moreover $\alpha^4+\alpha+1=0 \Rightarrow \alpha^4=\alpha+1$, likewise $\alpha^8=\alpha^2+1$). This shows that $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is normal $\Rightarrow$ $\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha)$ is Galois $\Rightarrow$ $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=4=\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$. As elements of $\mathrm{Gal}(\mathbb{F}_p(\alpha):\mathbb{F}_p)$ permute the roots $\alpha, \alpha^2, \alpha^4, \alpha^8$ it is clear that $\mathrm{Gal}(\mathbb{F}_p(\alpha), \mathbb{F}_p) \cong \mathbb{Z}/4\mathbb{Z}$ generated by the Frobenius $x \mapsto x^2$.
The only subgroup of order 2 of $\mathbb{Z}/4\mathbb{Z}$ is given by $\mathbb{Z}/2\mathbb{Z}$ which is generated by $x \mapsto x^4$. Now notice that

$$(\alpha+\alpha^2)^4 = \alpha^4+\alpha^8 = \alpha+1+\alpha^2+1 = \alpha+\alpha^2$$

Therefore $\alpha+\alpha^2 \in L^H$ moreover $\alpha+\alpha^2 \notin \mathbb{F}_2$ as if $\alpha+\alpha^2=0$ or $\alpha+\alpha^2=1$ this relation would yield a polynomial of degree 2 for which α is a root but the minimal polynomial of α is x^4+x+1.
Finally notice that $(\alpha+\alpha^2)^2+(\alpha+\alpha^2)+1 = \alpha^2+\alpha^4+\alpha+\alpha^2+1 = \alpha^4+\alpha+1 = 0$

$\Rightarrow$ $\alpha^2+\alpha$ is a root of x^2+x+1 $\Rightarrow$ $[\mathbb{F}_p(\alpha^2+\alpha):\mathbb{F}_p]=2$.
By the Galois correspondence $[L^H:\mathbb{F}_p]=2$ and there is only one intermediate field of degree 2 between $\mathbb{F}_p$ and $\mathbb{F}_p(\alpha)$ by the uniqueness of H. This shows that $L^H=\mathbb{F}_p(\alpha^2+\alpha)$.