SOLUTION SHEET 5:

1. (i) $K=\mathbb{Q}$, $f(x)=x^4-7$. f factorizes as

$$f(x) = (x^2-\sqrt{7})(x^2+\sqrt{7}) = (x-\sqrt[4]{7})(x+\sqrt[4]{7})(x-i\sqrt[4]{7})(x+i\sqrt[4]{7}).$$

and by Eisenstein's criterion + Gauss' lemma f is irreducible.
As $\operatorname{char}\mathbb{Q}=0$ L/K is Galois
Note that $L=\mathbb{Q}(\sqrt[4]{7},i)$ and $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[4]{7})\subseteq L$
$\Rightarrow [L:K]=[L:\mathbb{Q}(\sqrt[4]{7})]\cdot[\mathbb{Q}(\sqrt[4]{7}):\mathbb{Q}]$
and the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{7})$ is $x^2+1 \Rightarrow [L:\mathbb{Q}(\sqrt[4]{7})]=2$.
$\Rightarrow [L:K]=8 \Rightarrow |\operatorname{Gal}(L/K)|=8$

Note that $\delta\in\operatorname{Gal}(L/K)$ is determined by its action on i and $\sqrt[4]{7}$.
Let $\tau,\sigma\in\operatorname{Gal}(L/K)$ st $\sigma(i)=-i$ and $\sigma(\sqrt[4]{7})=\sqrt[4]{7}$ and
$\tau(i)=i$ $\tau(\sqrt[4]{7})=i\sqrt[4]{7}$. These are indeed K-automorphisms of L.
Moreover order of τ is 4 i.e $o(\tau)=4$ and $o(\sigma)=2$. Finally,
$\sigma\tau\sigma(i\sqrt[4]{7})=\sigma\tau(-i\sqrt[4]{7})=\sqrt[4]{7}$ & $\sigma\tau\sigma(i)=i \Rightarrow \sigma\tau\sigma=\tau^{-1}$.
$\Rightarrow \operatorname{Gal}(L/K)\cong D_8$ dihedral group on 8 elements.

There are 8 non-trivial subgroups of D_8. Here is the list:

order 2: $\{id,\tau^2\}$, $\{id,\sigma\}$, $\{id,\tau^2\sigma\}$, $\{id,\tau\sigma\}$, $\{id,\tau^3\sigma\}$.

fixed fields: $\mathbb{Q}(\sqrt{7},i)$, $\mathbb{Q}(\sqrt[4]{7})$, $\mathbb{Q}(i\sqrt[4]{7})$, $\mathbb{Q}(\sqrt[4]{7}+i\sqrt[4]{7})$, $\mathbb{Q}(\sqrt[4]{7}-i\sqrt[4]{7})$.

order 4: $\{id,\sigma,\tau^2,\tau^2\sigma\}$, $\{id,\tau\sigma,\tau^2,\tau^3\sigma\}$, $\{id,\tau,\tau^2,\tau^3\}$

fixed fields: $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(i\sqrt{7})$, $\mathbb{Q}(i)$

(ii) $K=\mathbb{F}_5$ $f=x^4-7$ Once again L/K is Galois and $\operatorname{Gal}(L/K)$ is cyclic & is generated by the Frobenius morphism. Let α be a root of $f=x^4-2$. Then as any field extension of finite fields is Galois (in particular normal) $SF_{\mathbb{F}_5}(f)=\mathbb{F}_5(\alpha)$. Now $[\mathbb{F}_5(\alpha):\mathbb{F}_5]=\deg f=4 \Rightarrow |\operatorname{Gal}(L/K)|=4$

$\Rightarrow \operatorname{Gal}(L/K)\cong\mathbb{Z}/4\mathbb{Z}$. $\Rightarrow$ only non trivial subgroup is $\mathbb{Z}/2\mathbb{Z}$ whose corresponding fixed field is $\mathbb{F}_5(\alpha^2)$. indeed x^2-7 is the minimal poly of α^2 in $\mathbb{F}_5[x]$ $\Rightarrow [\mathbb{F}_5(\alpha^2):K]=2$ and $F^2(\alpha^2)=\alpha^{50}=\alpha^{4\cdot12+2}=2^{12}\cdot\alpha^2=\alpha^2$.

(iii) $K=\mathbb{F}_2$ $f=x^6+1$ note that f is not irreducible. Indeed $x^6+1=(x^3+1)^2$ hence $SF_{\mathbb{F}_2}(x^6+1)=SF_{\mathbb{F}_2}(x^3+1)=SF_{\mathbb{F}_2}(x^2+x+1)$ and x^2+x+1 is irr. $\Rightarrow$ as before $[L:K]=2$ and $\operatorname{Gal}(L/K)=\mathbb{Z}/2\mathbb{Z}$ which doesn't have any non-trivial subgroups.

(iv) $K=\mathbb{Q}$, $f=x^8-1$ Note that $L=\mathbb{Q}(\omega)$ where ω is a primitive root of unity i.e $\min_{n\in\mathbb{N}_{>0}}\{n \mid \omega^n-1\}=8$. (take for instance $\omega=e^{2\pi i/8}$)
Note that $x^8-1=(x^4-1)(x^4+1)$ $\Rightarrow$ ω is a root of x^4+1 which is irreducible in $\mathbb{Q}[x]$. $\Rightarrow [L:K]=4 \Rightarrow |\operatorname{Gal}(L/K)|=4$.
Let $\sigma\in\operatorname{Gal}(L/K)$ then $\sigma(\omega)$ is a root of x^4+1. Now the roots of x^4+1 are $\omega,\omega^3,\omega^5,\omega^7$. Indeed, $\omega^4=-1\Rightarrow(\omega^3)^4=\omega^{12}=(-1)^3=-1$

and likewise for ω^5 & ω^7. Now as $Gal(L/K)$ acts transitively on the roots of x^4+1, $\exists \sigma \in Gal(L/K)$ such that $\sigma(\omega) = \omega^3$. Then $\sigma^2(\omega) = \omega^9 = \omega$ likewise $\exists \tau \in Gal(L/K)$ $\tau(\omega) = \omega^5$ and $\tau^2(\omega) = \omega$ finally $\tau\sigma(\omega) = \omega^7$. This shows that $Gal(L/K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The subgroups are

$$\{\sigma, id\}, \quad \{\tau, id\}, \quad \{\tau\sigma, id\}$$

$$\downarrow \qquad \downarrow \qquad \downarrow \qquad \omega + \omega^3$$

fixed fields : $\mathbb{Q}(\omega+\omega^3)$ $\quad$ $\mathbb{Q}(\omega+\omega^5)$ $\quad$ $\mathbb{Q}(\omega+\omega^7)$

2. An intermediate field $K \subseteq F \subseteq L$ such that $[F:K]=2$ corresponds to a subgroup H of $Gal(L/K) \cong A_4$ such that $|H| = 6$. But such a subgroup doesn't exist. Indeed there are 2 groups of order 6 up to isomorphism namely S_3 & $\mathbb{Z}/6\mathbb{Z}$. As A_4 doesn't have an element of order 6 $H \not\cong \mathbb{Z}/6\mathbb{Z}$. It can be also seen that $H \not\cong S_3$ as follows. Suppose $H \cong S_3$ then H contains 3 elements of order 2 and the identity, but these elements in A_4 form a subgroup so H has a subgroup of order 4 which is not possible.

3. (i) Let $K = \mathbb{F}_p(t)$ and $L = \mathbb{F}_p(t^{1/p})$ then $[L:K] = p$ as the minimal poly. of $t^{1/p}$ in $\mathbb{F}_p(t)[x]$ is $x^p - t$. But in L,
$$x^p - t = (x - t^{1/p})^p$$ therefore there is only one root of $x^p - t$ which is $t^{1/p}$ thus L/K is normal but this root repeated p times $\Rightarrow$ L/K not separable.

(ii) Any non-normal field extension of fields of 0 characteristic works eg $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$.

(iii) Let L be a Galois extension of K such that $Gal(L/K) \cong A_4$ *
Consider the fixed field F of $\langle(123)\rangle$. Then $[F:K] = 4$. Now an intermediate field $K \subseteq H \subseteq F$ such that $[H:K] = 2$ is also an intermediate field $K \subseteq H \subseteq L$ but $Gal(L/\mathbb{Q}) \cong A_4$ $\Rightarrow$ by exercise 2 such an extension doesn't exist

4. Define $K := SF_{\mathbb{Q}}(f)$. First note that $\mathbb{Q} \subseteq K$ is Galois and $G := Gal(K/\mathbb{Q})$ permutes the p many roots of f transitively (as $\mathbb{Q} \subseteq K$ is normal) thus G is a subgroup of S_p. Write $K = \mathbb{Q}(r_1, r_2, \dots, r_p)$ where r_i are the roots of f.
Now consider the intermediate extension $\mathbb{Q} \subseteq \mathbb{Q}(r_1) \subseteq K$, as $[\mathbb{Q}(r_1):\mathbb{Q}] = p$ $p \mid [K:\mathbb{Q}]$. This implies that $p \mid |G|$, by Cauchy thm. there exists an element σ of order p in G. It is not hard to see that in S_p the only element of order p is a cycle of length p.
Note that the two non-real roots are conjugate to each other and complex conjugation $\bar{\cdot}$ is in $Gal(K/\mathbb{Q})$. Let r_1, r_2 be the two non-real roots then $\bar{\cdot}$ exchanges r_1 & r_2 and fixes all the other roots. Therefore in S_p $\bar{\cdot}$ corresponds to a 2-cycle.
Now we show that the subgroup generated by a p-cycle σ and a transposition in S_p is S_p. Suppose wlog that $\bar{\cdot}$ corresponds to the transposition (12). Now there exist some number $1 \leq i \leq p-1$ such that $\sigma^i(1) = 2$ and σ^i is also a p-cycle as its order is p. We can write $\sigma^i = (12\dots)$.
From group theory we know that a transposition (12) & an n-cycle $(12\dots)$ generates S_n. So we are done.

5. First of all notice that $\alpha^2 \cdot \beta^2 = b$ and $-\alpha^2 - \beta^2 = a$. We claim that $\mathbb{Q}(\omega, \alpha) = L$ where $\omega = \frac{\alpha}{\beta} - \frac{\beta}{\alpha}$. Clearly $\mathbb{Q}(\omega,\alpha) \subseteq L$ to see the inclusion notice that $\omega = \frac{\alpha^2 - \beta^2}{\beta\alpha}$ and $\beta^2 \in \mathbb{Q}(\alpha)$ as $-\beta^2 = a + \alpha^2$ this shows that $\beta \in \mathbb{Q}(\alpha, \omega)$. Now notice that $[\mathbb{Q}(\omega):\mathbb{Q}] \leq 2$ indeed $\omega^2 \in \mathbb{Q}$ (this can be shown by doing some algebraic manipulations).
Suppose that $\omega \notin \mathbb{Q}$.
Now consider the following chain of extensions. $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\omega, \alpha)$
Thus $\mathbb{Q}(\alpha)$ is a fixed field of $Gal(L/\mathbb{Q})$. Moreover as $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ we have that

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\omega,\alpha)^H$$ for H some subgroup of order two of $Gal(L/\mathbb{Q})$.

Let $H = \{id, \sigma\}$ then $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = -\beta$.
Now consider $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\alpha, \omega)$. As before $\mathbb{Q}(\omega) = \mathbb{Q}(\omega,\alpha)^T$ for some subgroup T of $Gal(L/\mathbb{Q})$ of order 4.
Let $\tau \in T$ then $\tau(\alpha) \neq \alpha$. If $\tau(\alpha) = -\alpha$ then $\tau(\omega) = \frac{-\alpha}{\tau(\beta)} + \frac{\tau(\beta)}{\alpha}$ and $\tau(\omega) = \omega \Leftrightarrow \tau(\beta) = -\beta$.
If $\tau(\alpha) = \beta$ then $\tau(\omega) = \frac{\beta}{\tau(\beta)} - \frac{\tau(\beta)}{\beta}$ and $\tau(\omega) = \omega \Leftrightarrow \tau(\beta) = -\alpha$
in this case τ has order 4. Likewise if $\tau(\alpha) = -\beta$, τ has order 4.
This shows that T contains an element of order 4 as each element of T fits into one of these cases thus $T \cong \mathbb{Z}/4\mathbb{Z}$.
Finally we can see that τ, σ in $Gal(L/\mathbb{Q})$ generates $D_8 \Rightarrow Gal(L/\mathbb{Q}) \cong D_8$.

If $\omega \in \mathbb{Q}$. Then ω is fixed by $Gal(L/\mathbb{Q})$ hence by the above argument $|Gal(L/\mathbb{Q})| = 4$ & $Gal(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

If $Gal(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ then $L = \mathbb{Q}(\alpha)$. The only permutations τ of the roots of f of order 4 are $\tau(\alpha) = \pm\beta$, $\tau(\beta) = \mp\alpha$ both of these fix ω so $Gal(L/\mathbb{Q})$ fix ω and $\omega \in \mathbb{Q}$.