Solution Sheet #2:

1.(i)(ii) As $[L:K]\neq 1$ there exists $\alpha \in L\setminus K$ and we have the following chain of extensions $K \subseteq K(\alpha) \subseteq L$.

Thus $[K(\alpha):K] \mid [L:K]$, also $[L:K]=2 \Rightarrow [K(\alpha):K]=2$ because $K(\alpha)\neq K$. This also implies that $L=K(\alpha)$.

Now $K(\alpha) \cong K[x]/(m_{K,\alpha})$ where $m_{K,\alpha}$ is the minimal polynomial of α over K.
as $[K(\alpha):K]=2$ then $\deg m_{K,\alpha}=2$.

Write $m_{\alpha,K}= x^2+ax+b$ with $a,b\in K$. Note that α is a root of $m_{\alpha,K}$
$\Rightarrow$ we have $\alpha^2+a\alpha+b=0 \Leftrightarrow \alpha^2+a\alpha=-b\in K$

If $\operatorname{char} K\neq 2$ we have $(\alpha+\frac{a}{2})^2=\alpha^2+a\alpha+\frac{a^2}{4}=\frac{a^2}{4}-b\in K$
$\Rightarrow (\alpha+\frac{a}{2})^2\in K$ and as $K(\alpha)=K(\alpha+\frac{a}{2})$ we are done.

If $\operatorname{char} K=2$ and $a=0$ then $\alpha^2\in K$ and we are done. Suppose that $a\neq 0$. Then $\frac{\alpha^2}{a^2}+\frac{a\alpha}{a^2}=\frac{\alpha^2}{a^2}+\frac{\alpha}{a}\in K$
moreover $K(\alpha)=K(\frac{\alpha}{a})$ and we are done.

2. If there exists F an intermediate field between K and L then $[F:K]\mid[L:K]$ but $[L:K]=p$ for some p prime
$\Rightarrow [F:K]=1$ or $[F:K]=p$, in the former case $F\cong K$ and in the latter case $F\cong L$ as then $[L:F]=1$.

3. (i) First note that $K(\alpha^2)\subseteq K(\alpha)$ so $K(\alpha^2)$ is an intermediate field extension between K and $K(\alpha)$.
Now suppose that $K(\alpha^2)\neq K(\alpha)$. Note that α is a root of $x^2-\alpha^2\in K(\alpha^2)[x]$ therefore $[K(\alpha):K(\alpha^2)]\leq 2$ but it is not equal to $1 \Rightarrow [K(\alpha):K(\alpha^2)]=2$.
But then $[K(\alpha):K(\alpha^2)]\mid[K(\alpha):K]$ which contradicts that $[K(\alpha):K]$ is odd. $\Rightarrow K(\alpha^2)=K(\alpha)$.

(ii) Consider the field extension $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[4]{2})$ clearly $\mathbb{Q}(\sqrt{2})\neq\mathbb{Q}(\sqrt[4]{2})$
As an easier example, we can take the extension $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})$ clearly $\mathbb{Q}=\mathbb{Q}(2)\neq\mathbb{Q}(\sqrt{2})$.

4. Write $f=\sum_{i=1}^d a_i x^i$ where $a_i\in K$. Let $\varphi\in \operatorname{Aut}(K/L)$ such that $\varphi(\beta)\neq\beta$, notice that $\varphi(\beta)$ is a root of f indeed,
$$0=\varphi(0)=\varphi\left(\sum_{i=1}^d a_i\beta^i\right)=\sum_{i=1}^d \varphi(a_i)\varphi(\beta)^i=\sum_{i=1}^d a_i\,\varphi(\beta)^i$$
let $G:=\operatorname{Aut}(K/L)$ and observe that as f has finitely many roots thus the orbit $G\beta$ is finite.

let $G\beta=\{\beta_1,\dots,\beta_k\}$. Consider the polynomial $g=\prod_{i=1}^k(x-\beta_i)$ observe that the coefficient of x^j in g is given by

$\sum_{\{i_1,\dots,i_{k-j}\}\subseteq\{1,\dots,k\}} \beta_{i_1}\cdots\beta_{i_{k-j}}$. It can be seen that permuting the β_i don't change these coefficients. In particular the coefficients of g are fixed under the action of G. By hypothesis $\forall a \in L\setminus K$ $\exists \phi \in G$ such that $\phi(a) \neq a$. This shows that coefficients of g belong to K and $g \in K[X]$.

Finally, notice that $g \mid f$ but f is minimal by hypothesis. Therefore $f=g$ and G acts transitively on the roots of f.

5. We leave it to the reader to verify that φ is a homomorphism of fields and show that φ fixes K and admits an inverse.

$a + b\alpha \in K \Leftrightarrow b=0$ therefore for $a \in K$ $\varphi(a) = \varphi(a+0\alpha) = a+0+0\alpha = a$.

We claim that $\varphi^2 = \mathrm{id}$. Indeed,

$\varphi(\varphi(a+b\alpha)) = \varphi(a+b+b\alpha) = a+b+b+b\alpha = a+2b+b\alpha = a+b\alpha$

6. It suffices to show that every polynomial in $\mathbb{A}[X]$ has a root in $\mathbb{A}$. Let $f = \sum_{i=1}^{d} a_i x^i \in \mathbb{A}[X]$ and β be a root of f.

We can think of f as a polynomial over $\mathbb{Q}(a_1,\dots,a_n)$ then β is contained in $\mathbb{Q}(a_1,\dots,a_n,\beta)$ a finite field extension of $\mathbb{Q}(a_1,\dots,a_n)$. Notice that $\mathbb{Q}(a_1,\dots,a_n)/\mathbb{Q}$ is also a finite field extension as each a_i is algebraic. This shows that $\mathbb{Q}(a_1,\dots,a_n,\beta)/\mathbb{Q}$ is a finite field extension. As $\mathbb{Q}(\beta)$ is an intermediate field between these two fields, $\mathbb{Q}(\beta)/\mathbb{Q}$ is also finite and β is algebraic $\Rightarrow \beta \in \mathbb{A}$.

7. Suppose that x is transcendental over $K(y)$. Recall that α is transcendental over $k \Leftrightarrow k(\alpha) \cong \mathrm{Frac}\, k[\alpha]$.

Consider the following commutative diagram:

$$\begin{array}{ccc} K(y)(x) & \cong \mathrm{Frac}((\mathrm{Frac}\,K[y])[x]) \cong & \mathrm{Frac}(K[y][x]) \\ \text{\rotatebox{90}{$\cong$}} & & \text{\rotatebox{90}{$\cong$}} \\ K(x)(y) & \mathrm{Frac}((\mathrm{Frac}\,K[x])[y]) \cong & \mathrm{Frac}(K[x][y]) \\ & \text{\rotatebox{90}{$\cong$}} & \\ & \mathrm{Frac}(K(x)[y]) & \end{array}$$

This shows that $K(x)(y) \cong \mathrm{Frac}(K(x)[y])$. Which shows that y is transcendental over $K(x)$.

Changing the roles of x and y yields the other implication.