SOLUTION SHEET #3

(1) (i) From the course we know that degree 2 extensions are normal
$\Rightarrow$ L/F & $F/\mathbb{Q}$ are normal.
We claim that $L/\mathbb{Q}$ is not normal. The minimal polynomial of $\sqrt[4]{2}$ is given by $m_{\sqrt[4]{2},\mathbb{Q}} = x^4-2$.
Write

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

Now if $L/\mathbb{Q}$ is normal then $m_{\sqrt[4]{2},\mathbb{Q}}$ splits into linear factors in $L[x]$. However $L \subseteq \mathbb{R}$ and $i \notin L \Rightarrow x^4-2$ doesn't split.
Thus $L/\mathbb{Q}$ is not normal.

(ii) Consider the morphism $\varphi: F \to F$ given by $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ with $a,b \in \mathbb{Q}$. Suppose that it extends to a morphism $\tilde{\varphi}: L \to L$ then

$$\tilde{\varphi}(\sqrt{2}) = \tilde{\varphi}((\sqrt[4]{2})^2) = \tilde{\varphi}(\sqrt[4]{2})^2 = \varphi(\sqrt{2}) = -\sqrt{2}.$$

This shows that $\tilde{\varphi}(\sqrt[4]{2})^2 = -\sqrt{2}$, which is not possible.

(2) Write $f = g.h$ for two polynomials $g,h \in L[x]$. Suppose that g is not a constant polynomial and let α be a root of g.

We can express $[L(\alpha):K]$ in two different ways.

$$\underbrace{[L(\alpha):L]}_{=k}.\underbrace{[L:K]}_{=m} = [L(\alpha):K] = \underbrace{[L(\alpha):K(\alpha)]}_{=\ell}.\underbrace{[K(\alpha):K]}_{=n}$$

thus we obtain the relation $m.k = n.\ell$ with $k,\ell \in \mathbb{N}_{>0}$.
It can be easily seen that $[L(\alpha):L] \leq [K(\alpha):K]$ i.e. $k \leq n$ which also implies that $\ell \leq m$. Now the condition $\gcd(n,m)=1$ implies that $k=n$ and $\ell=m$. In particular $\deg g = \deg f$ and we are done.

(3) The chain of extensions $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt[4]{2})$ works.

(4) It is not hard to see that α is a root of f with multiplicity ≥ 2 $\Leftrightarrow$ $f(\alpha)=0$ AND $f'(\alpha)=0$ where f' is the formal derivative of f.

Now let $n=[L:K]$ & $\alpha \in L \setminus K$ and let f be the minimal poly. of α over K, note that $k := \deg f$ divides n.

Write $f = \sum_{i=0}^{n} a_i x^i$ with $a_i \in K$. The leading coefficient of f' is $n.a_n$ which is non zero as $a_n \neq 0$ & $n \neq 0$ because $\operatorname{char} K \nmid n$.
In conclusion, $\deg f' = k-1$. $\Rightarrow \operatorname{char} K \nmid k$.

Now suppose that f has a root β in then $f(\beta)=0$ & $f'(\beta)=0$

but $\deg f' < \deg f$ which contradicts the fact that f is the minimal polynomial of β over K.

(5) This is basically Ex 4 from worksheet 2.

To see this, notice that $\forall \alpha \in L \setminus K$ by definition of K, $\sigma(\alpha) \neq \alpha$ moreover $\sigma \in Aut(L/K)$ as $\sigma|_K = id_K$.

Now let $G = \langle \sigma \rangle \leq Aut(L/K)$ be the subgroup generated by σ.

To show that L/K is normal it suffices to show that $\forall \alpha \in L \setminus K$ $m_{\alpha,K}$ splits over L. We show this by showing that G acts transitively on the roots of $m_{\alpha,K}$.

This can be shown by mimicking the proof of Ex 4 worksheet 2.

Question: Why do we require that σ has infinite order?

(6) (i) First, it is clear that F/K is separable as $\forall \alpha \in F \Rightarrow \alpha \in L$ and $m_{\alpha,K}$ splits into linear terms in its splitting field as L/K is separable.

Now let $\beta \in L$ and consider $m_{\beta,L} \in L[x]$. As β is a root of $m_{\beta,K}$ then $m_{\beta,L} \mid m_{\beta,K}$ in $L[x]$ therefore $m_{\beta,L} \mid m_{\beta,K}$ in $SF_L(m_{\beta,K})$. But $m_{\beta,K}$ splits into linear factors in $SF_L(m_{\beta,K})$ as L/K is separable.

(ii) Let $\alpha \in L$. If $\alpha \in F$ then as F/K is purely inseparable the only root of $m_{\alpha,K}$ is α and $m_{\alpha,K}$ splits in $L[x]$.

Now suppose $\alpha \in L \setminus F$ write $m_{\alpha,F} = \prod_{i=1}^{n} (x - a_i)$ with $a_i \in L$. and $m_{\alpha,F} = \sum_{i=1}^{n} c_i x^i$ with $c_i \in F$ let $\operatorname{char} K = p > 0$. As L/K is purely insep.
$\forall i \in \{1, -, n\}$ there exists p^{k_i} st $c_i^{p^{k_i}} \in K$ choose m big enough such that $c_i^{p^m} \in K$ $\forall i$.
Keeping in mind that $\operatorname{char} K = \operatorname{char} F = p > 0$ we have,

$$(m_{\alpha,F})^{p^m} = \left(\sum_{i=1}^{n} c_i x^i\right)^{p^m} = \sum_{i=1}^{n} c_i^{p^m} x^{i \cdot p^m} \in K[x].$$

Moreover we can also write $(m_{\alpha,F})^{p^m} = \left(\prod_{i=1}^{n} (x - a_i)\right)^{p^m}$ $= \prod_{i=1}^{n} (x - a_i)^{p^m}$ so $(m_{\alpha,F})^{p^m}$ splits in $L[x]$.
Finally note that α is a root of $(m_{\alpha,F})^{p^m}$ therefore $m_{\alpha,K} \mid (m_{\alpha,F})^{p^m}$ but as $(m_{\alpha,F})^{p^m}$ splits in $L[x]$ so does $m_{\alpha,K}$ thus L/K is normal.

(7) First note that we need $\operatorname{char} K = p > 0$ to get inseparable extensions.

Let $K = \mathbb{F}_p(t)$ (the field of rational functions / K) and let $L = \mathbb{F}_p(t^{1/pq})$ where $q \neq p$ is a prime number. We claim that L/K is inseparable & not normal.

To see this note that $f := m_{t^{1/pq},K} \in \mathbb{F}_p(t)[x]$ is given by
$f(x) = x^{pq} - t$
this is not separable as for instance in L, $f(x)$ factors as

$$f(x) = x^{pq} - (t^{1/pq})^{pq} = (x^q - t^{1/p})^p$$ thus $t^{1/pq}$ is a multiple root.
Now consider the polynomial irreducible polynomial

$$g(x) = x^q - t \in K[x]$$
note that g has a root in L given by $(t^{1/pq})^p = t^{1/q}$.
However it doesn't split in $L[x]$ as L doesn't contain the qth roots of unity.

This gives an infinite family of non-normal inseparable extensions.

(8) (i) First note that for $\beta \in L$

$$\begin{aligned} f(M_\alpha)(\beta) &= M_\alpha^n(\beta) + a_{n-1} M_\alpha^{n-1}(\beta) + \_\_\_ + a_1 M_\alpha(\beta) + a_0 . \beta \\ &= \alpha^n . \beta + a_{n-1} \alpha^{n-1} \beta + \_\_\_ + a_1 \alpha . \beta + a_0 . \beta \\ &= f(\alpha) . \beta = 0 \quad \text{as } f = \min_K(\alpha). \end{aligned}$$

This shows that $f(M_\alpha) = 0$. Moreover as f is the minimal polynomial of α a similar argument shows that f is the minimal polynomial of M_α.

By Cayley-Hamilton theorem f divides the characteristic polynomial of M_α.

Let $N_\alpha : K(\alpha) \to K(\alpha)$ be the multiplication map by α. Then again $f(N_\alpha) = 0$ and f divides $\chi(N_\alpha)$ the characteristic polynomial of N_α. However $\deg \chi(N_\alpha) \leq d$ therefore $f = \chi(N_\alpha)$.

Recall that $\{1, \alpha, \_, \alpha^{n-1}\}$ is a K-basis for $K(\alpha)$. Let $\{e_1, -, e_d\}$ be a $K(\alpha)$-basis of L. Then

$\{e_1, \alpha e_1, -, \alpha^{n-1} e_1, e_2, \alpha e_2, -, \alpha^{n-1} e_2, \_\_, e_d, -, \alpha^{n-1} e_d\}$ is a K-basis of L.

The matrix M_α in this basis is given by,

$$M_\alpha = \begin{pmatrix} N_\alpha & & 0 \\ & N_\alpha & \\ & & \ddots & \\ 0 & & & N_\alpha \end{pmatrix} \quad \text{thus } \chi(M_\alpha) = \chi(N_\alpha)^d = f^d.$$

(ii) Recall that given an $n \times n$ matrix M, $\det M$ is given by the constant term in $\chi(M)$ & $(-1)^{n-1} \operatorname{tr} M$ is given by the coefficient of x^{n-1} in $\chi(M)$.

Applying this to f^d yields the result.