Question 10

(i) What's the problem? $\sigma|_L \longrightarrow ?$ Certainly $\sigma|_L : L \longrightarrow M$. So we've a K-monomorphism $L \longrightarrow M$ but $L : K$ is normal. 10.4 looks relevant, but doesn't give the whole story.

Since, by definition, $\sigma|_L : L \longrightarrow M$ and $L : K$ is normal, we may apply Theorem 10.5 with $\sigma = \tau$. Thus $\sigma|_L$ is a K-automorphism of L.

(ii) Must prove the homomorphism property: $(\sigma\tau)|_L = \sigma|_L\tau|_L$. Why (i)? To ensure $\sigma|_L$ can compose with $\tau|_L$.

Let $\sigma, \tau \in \Gamma(M : K)$. Since $\sigma|_L$ and $\tau|_L$ are K-automorphisms of L, by part (i), $\sigma|_L\tau|_L$ is defined.

Let $x \in L$; then

$$\begin{aligned}(\sigma|_L\tau|_L)(x) &= \sigma|_L(\tau(x))\\ &= (\sigma\tau)(x)\\ &= (\sigma\tau)|_L(x).\end{aligned}$$

Hence $(\sigma\tau)|_L = \sigma|_L\tau|_L$, i.e. $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$, and ϕ is a group homomorphism.

Kernel? If $\phi(\sigma)$ is the identity, then $\sigma|_L$ is the identity map on L, i.e. $\sigma|_L$ fixes L.

If $\sigma|_L$ is the identity, then σ fixes L. Hence

$\sigma \in \Gamma(M : L)$.

That means σ is an L-automorphism of M.

Containment *both* ways.

Conversely, if $\sigma \in \Gamma(M : L)$, then σ fixes L and so $\sigma|_L$ is the identity. Thus $\mathrm{Ker}(\phi) = \Gamma(M : L)$.

(iii) Isomorphism Theorem.

$\mathrm{Im}(\phi)$ is a subgroup of $\Gamma(L : K)$ and, by the First Isomorphism Theorem, $\mathrm{Im}(\phi) \cong \Gamma(M : K)/\Gamma(M : L)$. Thus $\Gamma(M : K)/\Gamma(M : L)$ is isomorphic to a subgroup of $\Gamma(L : K)$.

(iv) For this we need an intermediate field. $\mathbf{Q}(\sqrt{2})$ looks possible.

Consider $M = \mathbf{Q}(\sqrt[4]{2})$, $L = \mathbf{Q}(\sqrt{2})$, $K = \mathbf{Q}$. Since M contains exactly two zeros of $t^4 - 2$, $\Gamma(M : \mathbf{Q}) \cong \mathbf{C}_2$. But $\Gamma(M : L) = \mathbf{C}_2$ because $\sigma \in \Gamma(M : K)$ defined by

$\sigma(\sqrt[4]{2}) = (-\sqrt[4]{2})$

fixes L. Hence $\Gamma(M : K)/\Gamma(M : L)$ has order 1. But $\Gamma(L : K)$ has order 2. ($\sqrt{2} \longmapsto -\sqrt{2}$ is a non-identity automorphism.) Thus $\Gamma(M : K)/\Gamma(M : L)$ is isomorphic to a proper subgroup of $\Gamma(L : K)$.

Question 11

(i) Must put in all cube roots of 7, and explain why this includes putting in all cube roots of 1.

Let α be the real cube root of 7. Then the splitting field for $t^3 - 7$ over $\mathbf{Q}$ must contain α.

The other cube roots of 7 are $\omega\alpha$ and $\omega^2\alpha$, where ω is a non-real cube root of 1. Since the splitting field contains α and $\omega\alpha$, it also contains $\omega\alpha/\alpha = \omega$. So the splitting field contains $\mathbf{Q}(\alpha, \omega)$. But $t^3 - 7$ certainly splits in $\mathbf{Q}(\alpha, \omega)$, so this is the required splitting field.

(ii) Split the extension into two simple pieces $\mathbf{Q}(\alpha) : \mathbf{Q}$ and $\mathbf{Q}(\alpha, \omega) : \mathbf{Q}(\alpha)$.

Since p is irreducible (Eisenstein with $q = 7$), it is the minimum polynomial of α over $\mathbf{Q}$, so $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$.

Since $\mathbf{Q}(\alpha) \subseteq \mathbf{R}$ and $\omega \notin \mathbf{R}$, $\omega \notin \mathbf{Q}(\alpha)$.

Tempting to try $t^3 - 1$ as the minpol, but it's divisible by $t - 1$.

Thus the minimum polynomial of ω over $\mathbf{Q}(\alpha)$ has degree at least 2. But ω is a zero of $t^2 + t + 1$, so that is its minimum polynomial over $\mathbf{Q}(\alpha)$, therefore $[\mathbf{Q}(\alpha, \omega) : \mathbf{Q}(\alpha)] = 2$. Now

$$\begin{aligned}[\mathbf{Q}(\alpha, \omega) : \mathbf{Q}] &= [\mathbf{Q}(\alpha, \omega) : \mathbf{Q}(\alpha)] \times [\mathbf{Q}(\alpha) : \mathbf{Q}]\\ &= 6.\end{aligned}$$