Problem 1:

Let $k \subset K$ and $k \subset L$ be finite field extensions contained in some field.

In the following, I freely use the fact that $\dim(U)\dim(V) = \dim(UV)/\dim(U \cap V)$ for any vector spaces U and V over the same field.

Part a:

First, $[KL : L][L : k] = [KL : k]$.

So this means that

$$\begin{aligned}\frac{[K : k]}{[KL : L]} &= \frac{\dim(K)}{\frac{\dim(KL)}{\dim(L)}} \\ &= \frac{\dim(K)\dim(L)}{\dim(KL)}\end{aligned}$$

That is, we have reduced this problem to the following one; if $[KL : k] \leq [K : k][L : k]$, then the right hand side is at least 1.

So $[K : k] \geq [KL : L]$ if we manage to solve the following part.

Part b:

We know that both K and L are algebraic over k, because they're finite extensions. Let $K = k(\alpha_1, \alpha_2 \ldots \alpha_n)$ and $L = k(\beta_1, \beta_2 \ldots \beta_m)$ (with all of the al_is and β_is outside of k). Now, KL is the smallest field containing both K and L. So it must contain all of the α_is and β_is. So $KL = k(\alpha_1, \alpha_2 \ldots \alpha_n, \beta_1, \beta_2 \ldots \beta_m)$. This means that $[KL : k] \leq [K : k][L : k]$ (it may have been "less than", as there may have been some redundancy in the α_is and the β_is.

Part c:

Let $K \cap L = k$. We know that both K and L are algebraic over k, because they're finite extensions. Let $K = k(\alpha_1, \alpha_2 \ldots \alpha_n)$ and $L = k(\beta_1, \beta_2 \ldots \beta_m)$ (with all of the al_is and β_is outside of k). Note that all of the α_is are linearly independent from the β_is, else K and L intersect outside of k. Now, KL is the smallest field containing both K and L. So it must contain all of the α_is and β_is. So $KL = k(\alpha_1, \alpha_2 \ldots \alpha_n, \beta_1, \beta_2 \ldots \beta_m)$. This means that $[KL : k] = [K : k][L : k]$.

The converse is false. Consider $k = \mathbb{Q}$, $L = \mathbb{Q}(2^{1/3})$, $K = \mathbb{Q}(2^{1/3}e^{2\pi/3})$. It is clear that $[LK : k] = 3$ (both of those roots has the same minimal polynomial, $x^3 - 2$), but $[L : k][K : k] = 9$.

Problem 2:

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Then $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 * 2 = 4$. (The minimal polynomial of $\sqrt{2}$ in $\mathbb{Q}[x]$ is $x^2 - 2$, a polynomial with $\sqrt{3}$ as a root in $\mathbb{Q}(\sqrt{2})[x]$ is $x^2 - 3$, and $\sqrt{3}$ isn't in $\mathbb{Q}(\sqrt{2})$.

Now, $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$; first, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset K$, because $\sqrt{2} + \sqrt{3} \in K$; that is, all of the right hand side's generators are in K, so $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset K$. Next, we have that

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \frac{-\sqrt{2}+\sqrt{3}}{5}$$

So $\sqrt{2} - \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Adding (or subtracting) $\sqrt{2} + \sqrt{3}$ to this and dividing by 2 shows us that $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, so all of K's generators are in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$; $K \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Problem 3:

Let $k \subset K$ be an algebraic field extension.

Then every k-homomorphism $\delta : K \to K$ is a monomorphism; this is immediate, as discussed in class.

Next, let $a \in K$. Then a is the root of some $f \in k[x]$, because the extension is algebraic.

Now, for all $b \in K$, $\delta(f(b)) = f(\delta(b))$; this is because δ fixes all of the coefficients of f.

So if b is a root of f that is in K, then

$$\begin{aligned} \delta(f(b)) &= f(\delta(b)) \\ 0 &= f(\delta(b)) \end{aligned}$$

Note that $\delta(b)$ is also in K, so this means that δ permutes the roots of f that are in K. (There's finitely many of them, and δ is a one-to-one map, so it's a permuation.)

This means that there's a $b \in K$ such that $\delta(b) = a$, for all $a \in K$.

So δ is onto. So δ is a one-to-one and onto k-homomorphism, it is an isomorphism.

Problem 4:

If k is finite, then k^* is cyclic: this is example 5.8 a.

If k^* is cyclic, then it is a finitely generated abelian group; we can apply the fundamental theorem of finitely generated abelian groups to it. In particular, we have that k^* is either group-isomorphic to $\mathbb{Z}/n$ for some $n \in \mathbb{N}$ or k^* is group-isomorphic to $\mathbb{Z}$.

If k^* is group-isomorphic to $\mathbb{Z}$, this means that $(-1_k)(-1_k) = 1_k$, but this means that (-1_k) maps to an element of order 1 or 2 in $\mathbb{Z}$. But $\mathbb{Z}$ has no elements of order 2; this means that -1_k has order 1 in k^*, which means that $-1_k = 1_k$.

So k has characteristic 2. That is, $\mathbb{F}_2 \subset k$ is a field extension. Because k^* is cyclic, we have that $\mathbb{F}_2(a) = k$ for some $a \in k$. Moreover, a is algebraic; (I don't know how to show this and I give up.)

So k is an algebraic field extension of a finite field. So k is a finite extension of a finite field, it is finite; but this contradicts the fact that k^* is infinte, so k^* cannot have been isomorphic to $\mathbb{Z}$.

So k^* is group-isomorphic to $\mathbb{Z}/n$ for some $n \in \mathbb{N}$.

So k^* is isomorphic to a finite group; $k^* = k \setminus \{0\}$ is finite, so k is finite.

So k is finite if and only if k^* is cyclic.

Problem 5:

Let k be a field, and let $k(x)$ be the field of rational functions of k.