MODEL ANSWERS TO THE SIXTH HOMEWORK

1. $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$. There are many ways to see this; for example $x^n - 2 \in \mathbb{Q}[x]$ is irreducible, by Eisenstein. If α is a root of $x^n - 2$ then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ and so $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq n$ by the tower law.
2. Note first that G is naturally a subset of the set of all functions from L to L. The set of all such functions forms a group, where the multiplication is defined as composition of functions.
Hence it suffices to prove that G is closed under multiplication and inverses, that is, that the composition and inverse of an automorphism that fixes K, is an automorphism that fixes K. But the composition and inverse of a function that fixes K certainly fixes K and it is not hard to check that composition and inverse of an automorphism is an automorphism.
3. Clearly H is a subset of G. On the other hand $H = \mathrm{Gal}(L/M)$, so that H is also a group. Thus H is a subgroup.
4. As G fixes K, clearly $K \subset M \subset L$, and so it suffices to prove that M is closed under addition, additive inverses, multiplication and multiplicative inverses. We check closure under addition; the other cases are just as straightforward. Suppose that m and $n \in M$. We have to check that $m + n$ is fixed by every element of H. Pick $\phi \in H$. Then $\phi(m) = m$ and $\phi(n) = n$.

$$\begin{aligned} \phi(m+n) &= \phi(m) + \phi(n) \\ &= m + n. \end{aligned}$$

As ϕ was arbitrary, $m + n \in M$, as required.
5. Suppose that $m \in L^K$. Then $\phi(m) = m$, for every $\phi \in K$. As $H \subset K$, it follows that $\phi(m) = m$, for every $\phi \in H$. Thus $m \in L^H$ and so $L^K \subset L^H$.
Suppose that $\phi \in \mathrm{Gal}(L/N)$. Then $\phi(n) = n$, for every $n \in N$. As $M \subset N$, it follows that $\phi(m) = m$, for every $m \in M$. Thus $\phi \in \mathrm{Gal}(L/M)$ and so $\mathrm{Gal}(L/N) \subset \mathrm{Gal}(L/M)$.
6. Pick $\phi \in H$. Then $\phi(m) = m$, for every $m \in L^H = M$. Thus $\phi \in \mathrm{Gal}(L/M) = K$. Hence $H \subset K$.
7. Pick $m \in M$. Then $\phi(m) = m$, for all $\phi \in \mathrm{Gal}(L/M)$. Thus $m \in N$ and $M \subset N$.
8. First we check that $[L : \mathbb{Q}] = 8$. We already know that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

By the tower law, it suffices to check that

$$[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})]=2.$$

For this, we just need to check that

$$\sqrt{5}\notin\mathbb{Q}(\sqrt{2},\sqrt{3}).$$

A basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is given by 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$. We just need to check that no linear combination is a root of x^2-5. Now

$$(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})^2=(a^2+2b^2+3c^2+6d^2)+2((ab+3cd)\sqrt{2}+(ac+2bd)\sqrt{3}+(ad+bc)\sqrt{6}).$$

If this is equal to 5 we have

$$a^2+2b^2+3c^2+6d^2=5\qquad ab+3cd=0\qquad ac+2bd=0\qquad\text{and}\qquad ad+bc=0.$$

Consider the last three equations. If one of the variables is zero then at least two of the variables are zero. But the equation

$$mx^2=5$$

has no rational solutions for $m\in\{1,2,3,6\}$. If none of a, b, c and d is zero then the last equation gives us

$$a=-\frac{bc}{d}.$$

If we substitute into the third equation we get

$$bc^2=2bd^2.$$

Cancelling we get

$$c^2=2d^2,$$

which is not possible.
Thus $[L:\mathbb{Q}]=8$. Thus the degree of an intermediary field M is two or four. Note that

$$\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{6}),\ \mathbb{Q}(\sqrt{10}),\ \mathbb{Q}(\sqrt{15}),\ \mathbb{Q}(\sqrt{30}),$$

are all intermediary fields of degree two, as each field is generated by an element α, whose square is rational. Conversely, we have seen in class that if $M/\mathbb{Q}$ has degree two, then there is an $\alpha\in M$ such that $M=\mathbb{Q}(\alpha)$, where $\alpha^2\in\mathbb{Q}$. Now, by repeated application of the tower law, a basis for $L/\mathbb{Q}$ is given as

$$1,\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{6},\sqrt{10},\sqrt{15},\sqrt{30}.$$

Thus a general element α of L is given by

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30},$$

for some rational numbers a, b, c, d, e, f, g and h. It is easy to see that the only way the square is rational is if there are no cross-terms, so

that all but one coefficient is in fact zero. Thus the list above certainly exhausts all possible quadratic intermediary fields.
Now consider classifying all quartic extensions. Again it is easy to write down quite a few examples of quartic extensions

$$\mathbb{Q}(\sqrt{2},\sqrt{3}),\ \mathbb{Q}(\sqrt{2},\sqrt{15}),\ \mathbb{Q}(\sqrt{2},\sqrt{5}),\ \mathbb{Q}(\sqrt{3},\sqrt{5}),\mathbb{Q}(\sqrt{3},\sqrt{10}),\ \mathbb{Q}(\sqrt{5},\sqrt{6}),\ \mathbb{Q}(\sqrt{5},\sqrt{30}).$$

Suppose that M is a quartic extension that contains $\sqrt{2}$. Then $M/\mathbb{Q}(\sqrt{2})$ is quadratic. Arguing as before, it follows that M is generated over $\mathbb{Q}(\sqrt{2})$ be an element α whose square lies in $\mathbb{Q}(\sqrt{2})$. Now a basis for $L/\mathbb{Q}(\sqrt{2})$ is given by 1, $\sqrt{3}$, $\sqrt{5}$ and $\sqrt{15}$. Thus

$$\alpha = a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}.$$

As before it is easy to see that the condition that α^2 lies in $\mathbb{Q}(\sqrt{2})$ implies that all cross-terms vanish, so that all but one coefficient is zero. Arguing similarly for the other quadratic extensions, it follows that the list given above exhausts all quartic extensions provided we can show that a quartic extension must contain a quadratic one.
Now we turn to the problem of computing the Galois group and all of its subgroups. Let ϕ be an automorphism of L. Then ϕ is determined by its action on the generators of L. Now $\phi(\sqrt{2})$ must a root of x^2-2, so that

$$\phi(\sqrt{2}) = \pm\sqrt{2}, \qquad \phi(\sqrt{3}) = \pm\sqrt{3} \qquad \text{and} \qquad \phi(\sqrt{5}) = \pm\sqrt{5}.$$

In particular G has at most eight elements. Now we turn to the problem of showing that there is an automorphism $\phi_{\sqrt{2}}$ which switches the sign of $\sqrt{2}$ and fixes the other two signs. Note first that we may find

$$\sigma\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}),$$

such that $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$ Indeed $\sqrt{2}$ and $-\sqrt{2}$ are both roots of the same irreducible polynomial. Now the extension $L/\mathbb{Q}(\sqrt{2})$ is a splitting field for $(x^2-3)(x^2-5)$. It follows that we may find an extension $\phi_{\sqrt{2}}$ of σ that fixes $\sqrt{3}$ and $\sqrt{5}$.
Similarly we may find $\phi_{\sqrt{3}}$ and $\phi_{\sqrt{5}}$. Let H be the group they generate inside G. Note that each of these elements has degree two and that they commute with each other. It follows that H is an abelian group, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. As H and G both have eight elements, in fact $H = G$.
Thus G has seven subgroups of order two, given by the seven non-zero elements of G, each of which has order two. To find all subgroups of order four is a little more involved. The trick is to identify G with $\mathbb{F}_2^3$ and to realise that a subgroup of order four corresponds to a linear subspace of dimension two. But a plane in a three dimensional space

is the same as a line in the dual space, and so there are seven planes as well, that is, seven subgroups of order four.
Let M be an intermediary field of order 4. Let $H = \mathrm{Gal}(L/M)$. Then H is a subgroup of G. Now L/M is quadratic and so there is a $\beta \in L$ such that $L = M(\beta)$, where $\beta^2 \in M$. Thus the order of H is two (one can either change the sign of β or not). It follows that $M \subset L^H$. By inspection, L^H is always a quartic extension of K, and so $M = L^H$. But then there are at most seven quartic extensions.
We note that the lattice of subgroups and intermediary fields are the same (but with an upside-down identification).
9.

$$t^3 - 1 = (t-1)(t^2 + t + 1),$$

and $t^2 + t + 1$ is irreducible. Thus it suffices to find a splitting field for $t^2 + t + 1$. Let ω be a root of $t^2 + t + 1$. Then $\omega^3 = 1$ and so ω^2 is the other root,

$$\begin{aligned}(\omega^2)^3 &= (\omega^3)^2 \\ &= 1^2 \\ &= 1.\end{aligned}$$

Thus $\mathbb{Q}(\omega)$ is in fact a splitting field for $t^3 - 1$. The degree of the extension is two. Of course we may always represent ω as $\exp(2\pi i/3)$.
Consider $t^4 + 5t^2 + 6$. This factors as

$$(t^2 + 2)(t^2 + 3),$$

so that $\mathbb{Q}(\sqrt{-2}, \sqrt{-3})$. Just as the case with $\sqrt{2}$, $\sqrt{3}$, the degree of this field extension is 4.
Finally consider $t^6 - 8$. Suppose that ω is a primitive sixth root of unity, and let α be a positive sixth root of 8, that is a positive square root of 2. Then the roots of $t^6 - 8$ are $\omega^i \alpha$, where i ranges from 0 up to 5. Thus a splitting field is given as $\mathbb{Q}(\alpha, \omega)$. Now ω is a cube root of -1. Put differently,

$$x^6 - 1 = (x^3 - 1)(x^3 + 1),$$

and the roots of the first factor are cube roots of 1, so that ω is a root of the second factor. It is easy to check that $x^3 + 1$ is irreducible over $\mathbb{Q}$. Thus ω has degree three over $\mathbb{Q}$. On the other hand $\sqrt{2}$ has degree two over $\mathbb{Q}$. As 2 and 3 are coprime the degree of the splitting field is 6.
10. Note first that any two splitting fields define isomorphic extensions of K, so that we are free to go through the construction given in class and check the result for the splitting field so constructed.

We proceed by induction on n. If $n = 1$, then f is linear, f splits in L and so $L = K$. Now suppose that $n > 1$. Suppose that f is reducible, so that $f = gh$, where g and h have degree a and b respectively. Then $n = a + b$. Let M/K be a splitting field for g over K and let L/M be a splitting field for h over M. Then L/K is a splitting field for the product f. By induction

$$[M : K]|a! \qquad \text{and} \qquad [L : M]|b!.$$

Thus

$$[L : K] = [L : M][M : K]|a!b!$$

and as $a!b!$ divides $(a + b)! = n!$, we are done in this case.
Finally suppose that f is irreducible. We first adjoin a root α of f. Thus we get a field extension $K(\alpha)/K$, which has degree n, as f is irreducible. Now

$$f(x) = (x - \alpha)g(x),$$

where $g(x) \in K(\alpha)[x]$. As the degree of $g(x)$ is $n - 1$, by induction

$$[L : K(\alpha)]|(n - 1)!.$$

Arguing as before, the result follows.