MODEL ANSWERS TO THE EIGHTH HOMEWORK

1. By assumption

$$t = \frac{f(x)}{g(x)},$$

for polynomials $f(x)$ and $g(x) \in K[x]$. As $K[x]$ is a UFD, we may assume that $f(x)$ and $g(x)$ have no common factors.
Let

$$p(u) = g(u)t - f(u) \in K(t)[u].$$

Clearly x is a zero of this polynomial. We check that $p(u)$ is irreducible.

$$p(u) \in K[t][u],$$

and the content of $p(u)$ is one. By Gauss' Lemma it suffices to show that $p(u)$ is irreducible in $K[t][u]$. But $p(u)$ is clearly irreducible in $K[u][t]$, since $p(u)$ is a linear polynomial in t and the content is one, by construction.
The degree of $p(u)$, as a polynomial in u, is the maximum degree of $f(u)$ and $g(u)$. Thus

$$[K(x) : K(t)] = \max(\deg f, \deg g).$$

2. First note that the group S_3, has the following presentation.
Generators: a, b
Relations: $a^2 = b^3 = e$, $aba = b^2$.
Indeed $S_3 \simeq D_3$ and we have already seen that this is a presentation of D_3.
Let σ be the map given as $t \longrightarrow 1 - t$ and τ the map $t \longrightarrow 1/t$. Then σ^2 and τ^2 are both the identity. Consider $a = \sigma$, $b = \sigma\tau$. It is easy, but tedious, to check that a and b satisfy the given relations, so that G is indeed isomorphic to S_3.
A more sophisticated and certainly more satisfying way to proceed is as follows: Think of σ and τ as acting on $K \cup \{\infty\}$, in the obvious way (∞ being defined as $1/0$). Then σ and τ permute the three elements 0, 1 and ∞. In fact σ fixes ∞ and switches 0 and 1, and τ switches 0 and ∞ and fixes 1. Thus we get a natural map from G to S_3, the group of permutations of $\{0, 1, \infty\}$. It suffices to prove that the kernel is trivial. It is easy to check that in fact G is a subgroup of the group of all automorphisms of the form

$$t \longrightarrow \frac{at + b}{ct + d},$$

where $ad - bc \neq 0$.
In fact recall that we may identify a point of $K \cup \{\infty\}$ with a point of $K^2 - \{0\}/\sim$, where we indentify two points if they lie on the same line through the origin (∞ then corresponds to the vertical line, a line of infinite slope), so that

$$\mathbb{P}^1 = \mathbb{P}(K^2) = K \cup \{\infty\}.$$

In this way we can associate a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

to the transformation (again two matrices which are multiples of each other correspond to the same transformation, so strictly speaking we have an equivalence class of matrices, that is, an element of $\mathrm{PGL}(2, K)$). But if a matrix has more than two eigenvectors, then it must be a scalar matrix and hence correspond to the identity transformation. Thus the given representation of G is an isomorphism.
Let $L = K(t)$. It suffices to exhibit a rational function

$$j = j(t) = \frac{f(t)}{g(t)},$$

of t, where

$$\max(\deg f(t), \deg g(t)) = 6.$$

Indeed let $M = L^G$ and $N = K(j)$. By (1)

$$[L : N] = [K(t) : K(j)] = 6.$$

As j is invariant, $N \subset M$ and by the fundamental theorem of Galois theory

$$[L : M] = 6.$$

Alternatively note that it is easy to exhibit subfields F of L which contain M, such that $[L : F] = 2$ or $[L : F] = 3$.
So how do we exhibit any invariant rational funtions? Let us start with finding something invariant under σ. Since σ switches t and $1 - t$, it is clear that the product $t(1 - t)$ is invariant under σ. Further it is clear that if we set $F = K(t(1 - t))$, then

$$[L : F] = 2.$$

Similarly since τ switches t and $1/t$, the sum $t + 1/t$ is invariant under τ.
Let $\phi = \sigma \circ \tau$. Then $\phi(t) = 1 - 1/t = (t - 1)/t$. Now the orbit of G acting on t is

$$\{\, t, 1 - t, 1/t, (t - 1)/t, t/(t - 1), 1/(1 - t) \,\}.$$

The action of ϕ on this orbit decomposes this orbit into two subsets of size three,

$$\{\, t, (t-1)/t, 1/(1-t) \,\} \qquad \text{and} \qquad \{\, 1-t, 1/t, t/(t-1) \,\}.$$

Thus both

$$t + (t-1)/t + 1/(t-1) \qquad \text{and} \qquad (1-t) + 1/t + t/(t-1),$$

are invariant under ϕ. Since τ obviously switches the two subsets above, τ fixes

$$j_0 = (t + (t-1)/t + 1/(1-t))((1-t) + 1/t + t/(t-1)).$$

Since G is generated by ϕ and τ, j_0 is fixed by G. As j_0 has degree six on top and four on the bottom, we are done. In fact the function

$$j(t) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2},$$

is quite famous (it is even called the j-function, $\lambda = t$ of course). The strange choice of factor of 2 is actually chosen so that things work out well when we work over a field of characteristic two.

3. Let G be a finite group. Instead of starting with K and constructing a Galois extension L with Galois group G (which problem is extemely hard) the idea is to start with L and construct K. In fact it was proved in class that if G acts on L (that is G is a group of automorphisms of L) and K is the fixed field, then L/K is Galois, with Galois group G. Now any finite group G is a subgroup of S_n, for some n (Cayley's Theorem). So it suffices to prove that S_n may be realised as the set of automorphisms of some field L.

Let K be any field and $L = K(x_1, x_2, \ldots, x_n)$, where $x_1, x_2, \ldots, x_n$ are indeterminates over K. Note that L is the field of fractions of the polynomial ring $R = K[x_1, x_2, \ldots, x_n]$. Given a permutation $\sigma \in S_n$, let σ act on the variables $x_1, x_2, \ldots, x_n$ in the obvious way,

$$\sigma(x_i) = x_{\sigma(i)}.$$

By the universal property of a polynomial ring, there is an induced ring homomorphism

$$f \colon R \longrightarrow R,$$

which acts on the variables as indicated. As f permutes the generators of R over K, it follows that f is an isomorphism (in fact the inverse of f is given by the map induced by the inverse of σ). But then, by the universal property of the field of fractions, there is an induced automorphism

$$\phi \colon L \longrightarrow L$$

In this way, we realise S_n as a group of automorphisms of L.

4. Let G be the Galois group of L/K. Then G has order a power of 2, so that G is a Sylow 2-subgroup. Thus by Sylow's Theorems, there is a tower of subgroups of G, such that each group is normal in the next and each quotient has order two. By the Fundamental Theorem, this gives us a sequence of subfields, each of which is quadratic over the previous field. As the characteristic is not two, we are done.
5. (a) The group $\mathbb{Z}_2 \times \mathbb{Z}_2$, as in question 6.
(b) ω is a root of $x^2 + x + 1$, which we have already seen is irreducible. Thus the Galois group is $\mathbb{Z}_2$.
6. (a) We first check that

$$x^4 - 3x^2 + 4$$

is irreducible. By Gauss it is enough to check this over $\mathbb{Z}$. If there were a linear factor, we would have an integer root, necessarily a divisor of 4. But ± 1, ± 2 and ± 4 are not roots of this polynomial. The only other possibility is that we can factor as

$$x^4 - 3x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d),$$

where a, b, c and d are all integers. Looking at the coefficient of x^3, we have $a = -c$ and looking at the constant coefficient, we have $bd = 4$. Looking at the linear term, we have $b = d$, so that $b = d = \pm 2$. Looking at the quadratic term, we have

$$-3 = b + d - a^2,$$

clearly impossible.
Now consider

$$y^2 - 3y + 4.$$

This has roots

$$\frac{3 \pm \sqrt{-7}}{2}.$$

Thus the four roots of $x^2 - 3x + 4$ are the two pairs of square roots. Call α and β one of each. I claim that, up to sign, $\alpha\beta = 2$. One way to see this is to calculate directly

$$\begin{aligned} \alpha\beta &= \frac{((3 + \sqrt{-7})(3 - \sqrt{-7}))^{1/2}}{2} \\ &= \frac{(9 + 7)^{1/2}}{2} \\ &= 2. \end{aligned}$$

Here is another. Suppose that I have a monic polynomial of degree n, which splits as

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n),$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $f(x)$. Then I can compare terms and identify the coefficients by multiplying out. In particular the constant term is the product of the roots,

$$a_0 = (-1)^n \alpha_1 \alpha_2 \ldots \alpha_n.$$

In our case the roots are $\pm\alpha$ and $\pm\beta$ so that

$$(\alpha\beta)^2 = 4.$$

Let $L = \mathbb{Q}(\alpha)$. Then L/K has degree four. But $\beta = 4/\alpha \in L$, so that $f(x)$ splits in L. Hence the Galois group has order four and it is either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. As α and β are roots of the same irreducible polynomial, there is an automorphism which carries one to the other. The same automorphism must carry $-\alpha$ to $-\beta$. Similarly there is an automorphism that carries α to $-\alpha$ and β to $-\beta$. Thus there are two elements of order two, and we must have $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(b) and (d).

$$\begin{aligned} x^4 - 3x^2 + 4 &= x^4 + x^2 \\ &= x^2(x^2 + 1) \\ &= (x(x+1))^2. \end{aligned}$$

Thus this polynomial splits in $\mathbb{F}_2$ and the Galois group is trivial.
(c)

$$x^4 - 3x^2 + 4 = x^4 + 1.$$

Now $x^4 + 1$ does not have any roots over $\mathbb{F}_3$. Suppose it were reducible. Then

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

Looking at the term of degree three, we have

$$0 = a + c,$$

so that $c = -a$. Looking at the constant term we have $bd = 1$, so that $b = d$. Thus

$$x^4 + 1 = (x^2 + ax + b)(x^2 - ax + b).$$

Now consider the quadratic term. We have

$$0 = 2b - a^2.$$

Thus $a^2 = 2b$. Thus $b = 2$ and $a = 1$. Thus $x^4 + 1$ is the product of two quadratics. The splitting field of either polynomial is a quadratic extension. As their is only one quadratic extension, namely $\mathbb{F}_9/\mathbb{F}_3$, it follows that both quadratics split in the same field extension. Thus the Galois group is $\mathbb{Z}_2$.

7. The only non-trivial cases are 3(a) and 4(a). In the first case, there are three proper subgroups, all normal, corresponding to the three intermediate fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{10})$.
The second case is almost identical. One intermediate field is obvious

$$\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{-7}),$$

which is the fixed field of the automorphism that sends α to $-\alpha$.
Consider the automorphism that switches α and β. Obviously $\alpha\beta$ and $\alpha + \beta$ are invariant. The first is unfortunately equal to 2, so we get nothing from this. But $\alpha + \beta$ certainly does not look like a rational number, so it should generate our fixed field.
Now to compute $\alpha + \beta$ look at the coefficient of x^2,

$$x^4 - 3x^2 + 4 = (x - \alpha)(x - \beta)(x + \alpha)(x + \beta) = (x^2 - \alpha^2)(x - \beta^2).$$

Thus

$$-3 = -\alpha^2 - \beta^2,$$

so that

$$\alpha^2 + \beta^2 = 3.$$

Now expand

$$\begin{aligned}(\alpha + \beta)^2 &= \alpha^2 + 2\alpha\beta + \beta^2 \\ &= (\alpha^2 + \beta^2) + 2(\alpha\beta) \\ &= 3 + 2 \cdot 2 \\ &= 7.\end{aligned}$$

Thus

$$\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\sqrt{7}).$$

The final fixed field is

$$\mathbb{Q}(i) = \mathbb{Q}(\sqrt{7}\sqrt{-7}) = \mathbb{Q}(\alpha - \beta) \quad \text{or compute as above.}$$

Challenge Problems: 8. We proceed in a similar fashion to question 2. First note that any symmetry of a tetrahedron is determined by its action on the vertices, of which there are four. So the group of symmetries of a tetrahedron is a subgroup of S_4. On the other hand, the action is certainly transitive and the stabiliser of a vertex has order three. Thus the group of symmetries has order $12 = 3 \cdot 4$ and it must in fact be $A_4 \subset S_4$.
We are indeed given 12 symmetries. It suffices then to check we get the right group.
The elegant way to proceed is to think again of G acting on points of $K \cup \{\infty\}$. Consider the six points $\{0, \pm 1, \pm i, \infty\}$. It is easy to check that the given automorphisms permute these points. We have already

seen that any element of G that fixes these points (or indeed any three of them) must be the identity, so that G is a subgroup of S_6.
Now we want G to act on 4 things. If we think of these points as being points of the Riemann sphere, with the south pole corresponding to zero, the north pole to infinity, and the equator to the unit circle, then these points correspond to the points of an octahedron. There are then eight faces (all triangles) so that there are four sets of opposite faces. It follows then that we get a representation of G into S_4, which is easily seen to be faithful (that is, any element of G which fixes all four pairs of faces, must be the identity). The image of G is then a subgroup of order 12 and so it is automatically A_4.
9. Note that L/K is the splitting field of

$$f(x) = (x^2 - p_1)(x^2 - p_2)(x^2 - p_3)\dots(x^2 - p_n).$$

Thus L/K is Galois. Moreover, by repeated adjoining square roots and applying the Tower Law, it follows that

$$[L : K] \leq 2^n.$$

Thus it suffices to prove that the Galois group G has order at least 2^n. By Eisenstein, $x^2 - p$ is irreducible, where p is any prime. Suppose that $\alpha \in L$ is a root of $x^2 - p$, where $p = p_i$. Let $M = K(\alpha)$. Then M/K is quadratic and we may find $\pi\colon M \longrightarrow M$ sending α to $-\alpha$. Now L/M is a splitting field for $f(x)/(x^2 - p)$, so that there is an automorphism $\phi = \phi_i$ of L that fixes α_j, $j \neq i$ and sends α_i to $-\alpha_i$, so that ϕ extends π.
The group H generated by $\phi_1, \phi_2, \dots, \phi_n$ is easily seen to have at least 2^n elements. Note that we have also proved that $H = G$ and that G is isomorphic to a product of n copies of the cyclic group of order two.