MODEL ANSWERS TO THE SEVENTH HOMEWORK

1. First we check that this map is well-defined. We have to check that if

$$\frac{f_1}{g_1} = \frac{f_2}{g_2},$$

then

$$\frac{(Df_1 \cdot g_1 - f_1 \cdot Dg_1)}{g_1^2} = \frac{(Df_2 \cdot g_2 - f_2 \cdot Dg_2)}{g_2^2},$$

which is an easy check. Note that

$$D(f/1) = \frac{(Df \cdot 1 - f \cdot D1)}{1^2} = D(f),$$

so this does indeed extend the formal derivative.
Now observe that the formal derivative, which is a function

$$D\colon K(t) \longrightarrow K(t)$$

is linear in the numerator, that is the function

$$K[t] \longrightarrow K(t)$$

which sends f to

$$\frac{(Df \cdot g - f \cdot Dg)}{g^2},$$

is linear. This is clear, as it is the sum of

$$\frac{Df}{g} \qquad \text{and} \qquad -\frac{fDg}{g^2},$$

the composition of two linear functions is linear and multiplying by a fixed scalar is linear. Now

$$D(f_1/g_1 + f_2/g_2) = D(f_1g_2/(g_1g_2) + f_1g_1/(g_1g_2)),$$

and so the formal derivative is linear.
Now we turn to proving Leibniz's rule, that is

$$D(uv) = D(u)v + uD(v),$$

where u and v are rational functions. Suppose that $u = f/g$ and $v = h/k$. Then the argument to the LHS is $(fh)/(gk)$ and so the LHS

is

$$D(uv) = \frac{(D(fh) \cdot gk - fh \cdot D(gk))}{g^2k^2}$$
$$= \frac{(hgkDf + fgkDh - fhkDg - fhgDk)}{g^2k^2}$$

Now consider the RHS,

$$D(u)v + uD(v) = \frac{h\,(Df \cdot g - f \cdot Dg)}{kg^2} + \frac{f\,(Dh \cdot k - h \cdot Dk)}{gk^2}$$
$$= \frac{(hkDf \cdot g - hkf \cdot Dg + fgDh \cdot k - fgh \cdot Dk)}{g^2k^2}.$$

As both are the same, the result follows.
2. First note that any polynomial over a field of characteristic zero is separable. Secondly, we proved in class that a finite extension of a finite field is separable, so that every polynomial over a finite field is separable. (Indeed the minimum polynomial of any element must divide $x^q - x$ for some q, and this has no repeated roots). So every polynomial listed is automatically separable.
3. Note that to prove that a finite extension is normal, it suffices to prove that it is the splitting field of some polynomial.
(1) Note that $\mathbb{Q}(\sqrt{-5})$ is a splitting field for $x^2 - 5$, so the extension is normal.
(2) The polynomial $x^7 - 5$ has a root in $\mathbb{Q}(\alpha)$, since α is a root. However the other six roots of this polynomial are not real, so the polynomial does not split in this field. It follows that this extension is not normal.
(3) Not normal, for the same reason as in (3).
4. Let L/K be an extension of degree two. Let $\alpha \in L$. The minimum polynomial of α has degree one or two, so that α is a root of a monic polynomial of degree two with coefficients in K. Any such polynomial has the form

$$f(x) = x^2 + ax + b.$$

In a splitting field, we have

$$x^2 + ax + b = (x - \alpha)(x - \beta).$$

Multipyling out, we have

$$-a = \alpha + \beta,$$

so that $\beta = -a - \alpha \in L$. But then $f(x)$ splits in L.

5. M/K is separable by definition. Suppose that α is in L, let $f(x)$ be the minimum polynomial over M and let $g(x)$ be the minimum polynomial over K. Then $g(x)$ is separable, by definition and $f(x)$ divides $g(x)$. It follows then that $f(x)$ has no repeated roots.
6. No. Let α be the positive square root of 2 and let β be the positive real fourth of 2. Let $L = \mathbb{Q}(\beta)$, $M = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}$. Then M/K is quadratic, $\beta^2 = \alpha$ and so $M \subset L$ and L/M is quadratic. Thus L/M and M/K are normal extensions. However L/K is not normal. For example, β is a root of $x^4 - 2$, but $x^4 - 2$ does not split in L.
7. Let $L = \mathbb{F}(s,t)$, where $\mathbb{F}$ is any finite field of characteristic p, and let $K = \mathbb{F}(s^p, t^p) = \mathbb{F}(u,v)$. Then $s^p = u$ and $t^p = v$, so that s is a root of $x^p - u$ and t is a root of $x^p - v$. It follows that L/K is finite. As s and t are independent variables, it is clear that L/K is an extension of degree p^2, by the Tower Law.
Let $\alpha = s + kt$, where k is any element of K. Then

$$\begin{aligned} \alpha^p &= (s+kt)^p \\ &= s^p + k^p t^p \\ &= u + k^p v. \end{aligned}$$

It follows that α is a root of the polynomial $x^p - (u + k^p v)$. Thus $K(\alpha) \neq L$, as α has degree p over K. By the proof of (7.23), if L/K were primitive then for some k, α would generate L, a contradiction, as L/K does not have degree p.
8. Consider the polynomial $x^2 - \alpha \in L(\alpha)[x]$. It suffices to prove that this polynomial is irreducible. By Gauss this is the same as saying that $x^2 - \alpha \in L[\alpha][x] = L[x][\alpha]$ is irreducible, which is clear, as this is a linear polynomial in α.
9. Let M consist of all elements α of L such that the minimum polynomial of α splits in L. Suppose that Σ/K is a normal extension. Pick $\alpha \in \Sigma$. Then the minimum polynomial of α splits in Σ, so that it certainly splits in L. Hence $\alpha \in M$ and so $\Sigma \subset M$. In particular $K \subset M \subset L$, as $x - \alpha \in K[x]$ splits in L, whenever $\alpha \in K$.
We want to prove that M is a subfield of L. Given α and β in M, it suffices to prove that $K(\alpha, \beta) \subset M$. Let $f(x)$ be the product of the minimum polynomials of α and β. Then $f(x)$ splits in L as α and β belong to M. Let $\Sigma \subset M$ be a splitting field for $f(x)$. Then Σ/K is normal as it is a splitting field. Thus $K(\alpha,\beta) \subset \Sigma \subset M$. Thus M is a field. It is clear that M/K is normal.
10. Pick $l \in M = K(M_1, M_2)$. We want to prove the minimum polynomial of l splits in L. Now there exists $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_n$ such that $l \in M = K(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n)$. As $\alpha_i \in M_1$,

the minimum polynomial of α_i splits in M_1. Similarly the minimum polynomial of β_j splits in M_2. Hence the product of the minimum polynomials splits in M. Let $\Sigma \subset L$ be the corresponding splitting field. Then Σ/K is normal and by construction $l \in \Sigma$. But then, as the minimum polynomial of l splits in Σ, it certainly splits in M. Thus M/K is normal.

Now let $M = M_1 \cap M_2$. Let $\alpha \in M$ and let $m(x)$ be the minimum polynomial of α. As m splits in M_1, all the roots of $m(x)$ are contained in M_1. Similarly the same roots are contained in M_2. But then $m(x)$ splits in M and so M/K is normal.

11. Clearly it suffices to count the number of monic irreducible polynomials of degree d and then multiply the answer by $q-1$, the number of non-zero scalars.

Suppose that $m(x)$ is a monic polynomial of degree d. Then $m(x)$ has a root in a field extension of degree d. But all fields of cardinality q^d are isomorphic. Thus every polynomial of degree d splits in the same field $\mathbb{F}$ of cardinality q^d.

Note that $\mathbb{F}$ is separable over $\mathbb{F}_q$. Therefore a monic polynomial $m(x)$ of degree d has d distinct roots in $\mathbb{F}$ and each of these d roots has $m(x)$ as minimum polynomial. So we just need to count the number of possible roots and divide by d.

Suppose $\alpha \in \mathbb{F}$ and let $m(x)$ be its minimum polynomial. If $m(x)$ ha degree d then $\mathbb{F}_q(\alpha) \subset \mathbb{F}$ has degree d over $\mathbb{F}_q$, so that $\mathbb{F}_q(\alpha) = \mathbb{F}$. If $m(x)$ has smaller degree then $\mathbb{F}_q(\alpha) \neq \mathbb{F}$. Thus $m(x)$ has degree d if and only if α lives in no smaller field. The intermediary fields correspond to divisors e of d. There is one such for each divisor; it is the splitting field of $x^{q^e} - x$. By inclusion-exclusion the number of polynomials of degree d is

$$\frac{(q-1)}{d}\left(q^d - \sum_e q^e + \sum_f q^f - \dots\right),$$

where the first sum ranges over all e such that d/e is a prime, the second sum ranges over all f such that d/f is a product of two distinct primes, and so on.

12. γ is clearly a root of the polynomial

$$f(x) = (x^2-2)^2 - 2 = x^4 - 4x^2 + 2.$$

By Eisenstein, applied with $p = 2$, $f(x)$ is irreducible. Thus $L = \mathbb{Q}(\gamma)/\mathbb{Q} = K$ has degree four. Now the four roots of $f(x)$, in $\mathbb{C}$ are

$$\pm\sqrt{(2 \pm \sqrt{2})}.$$

Now clearly L contains $\sqrt{2} = \gamma^2 - 2$.

We have

$$\begin{aligned}\gamma\gamma' &= \left(\sqrt{(2+\sqrt{2})}\right)\left(\sqrt{(2-\sqrt{2})}\right)\\ &= \sqrt{(2+\sqrt{2})(2-\sqrt{2})}\\ &= \sqrt{4-2}\\ &= \sqrt{2} \in L.\end{aligned}$$

As L is a field, it follows that $\sqrt{(2-\sqrt{2})} \in L$, and so $f(x)$ splits in L. Thus L/K is a splitting field for $f(x)$ and so L/K is Galois, as all polynomials over a field of characteristic zero are separable.
In particular the Galois group must have order four and there are only two groups of order 4, the cyclic group of order four $\mathbb{Z}_4$ and the product of two cyclic groups of order two $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Consider $M = \mathbb{Q}(\sqrt{2})$. We have $L/M/K$. As $x^2 - 2$ is irreducible over $\mathbb{Q}$, there is an automorphism of M which switches $\sqrt{2}$ and $-\sqrt{2}$. We may extend this to an automorphism of L, in two ways. Pick one and call it σ. Then σ is determined by its action on anyone of the roots of $f(x)$, and it must send a root to another root, that is σ induces a permutation of the roots. Suppose that $\sigma(\gamma) = -\gamma$. Then $\sigma(\gamma') = -\gamma'$ and as $\gamma\gamma' = \sqrt{2}$, σ fixes $\sqrt{2}$. But this contradicts the fact that σ extends π.
Thus $\sigma(\gamma) = \gamma'$ (possibly switching σ) and by the same token as before $\sigma(\gamma') = -\gamma$. Thus σ^2 is not the identity and so the Galois group is cyclic, generated by σ. It follows, by the Galois correspondence, that M is the only proper intermediary field, as G has only one proper subgroup.