MODEL ANSWERS TO THE NINTH HOMEWORK

1. Put an order on the elements of $\mathbb{N}$, by saying that $m \leq n$ if and only if m divides n.
2. (a) Let α be a root of $f(x)$. Then α has degree three over K, so that $M = K(\alpha)$ has degree three over K. By uniqueness, $M \simeq \mathbb{F}_{27}$ so that in particular M/K is normal. Thus $f(x)$ splits in M and $L = M$.
(b) Done in part (a).
(c) Note that a cubic $f(x)$ is reducible if and only if it has a linear factor if and only if it has a root. Thus

$$f(x) = x^3 + 2x + 1,$$

is irreducible over $\mathbb{F}_3$, as 0, 1 and 2 are not roots of $f(x)$.
(d) Every element of L is uniquely of the form

$$a + b\alpha + c\alpha^2,$$

where a, b and $c \in \mathbb{F}_3$. It is clear how add two such elements. To multiply it suffices to compute $\alpha^i\alpha^j$, for i and $j \in \{0, 1, 2\}$. If $i+j \leq 2$, then

$$\alpha^i\alpha^j = \alpha^{i+j}.$$

Otherwise we need to use the relation

$$\alpha^3 = \alpha + 2,$$

which is derived from the fact that α is a root of $f(x)$.
If $i + j = 3$, then

$$\begin{aligned} \alpha^i\alpha^j &= \alpha^3 \\ &= \alpha + 2. \end{aligned}$$

If $i + j = 4$, then

$$\begin{aligned} \alpha^i\alpha^j &= \alpha^4 \\ &= \alpha\alpha^3 \\ &= \alpha(\alpha + 2) \\ &= \alpha^2 + 2\alpha. \end{aligned}$$

This completely specifies the addition and multiplication in L.
(e) Suppose we are given $\gamma = a + b\alpha + c\alpha^2$. Then we want to find β such that

$$\gamma\beta = 1.$$

Formally, we set

$$\beta = a' + b'\alpha + c'\alpha^2.$$

Then we have

$$(a + bx + cx^2)(a' + b'x + c'x^2) = 1 + g(x)(x^3 + 2x + 1),$$

where $g(x)$ is a polynomial, which by inspection has degree at most one.

In practice solving these equations is rather involved and quite often we can just guess the inverse. For example, suppose we want to find the inverse of α itself. As

$$\alpha^3 + 2\alpha + 1 = 0,$$

we have

$$\alpha(\alpha^2 + 2) = -1,$$

so that the inverse of α is $-(\alpha^2 + 2)$.

3. (a) As L is generated by t, any automorphism of L over K is determined by its action on t and it must send t to another generator $\alpha = f(x)/g(x)$ of L. We have already seen that $L = K(\alpha)$ if and only if the maximum of the degrees of $f(x)$ and $g(x)$ is one. Thus an automorphism of L must send to

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

as the general polynomial of degree one has the form $at + b$. Of course $f(t)$ and $g(t)$ are coprime, that is, one is not a scalar multiple of the other. This is equivalent to requiring that the two vectors (a, b) and (c, d) are independent, which in turn is equivalent to the non-vanishing of the determinant,

$$ad - bc.$$

(b) Define a map

$$\rho\colon\ \mathrm{GL}(2, K) \longrightarrow \mathrm{Gal}(L/K)$$

by sending the matrix

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

to the transformation

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

It is easy, but somewhat tedious, to check that ρ is a homomorphism. ρ is clearly surjective. The kernel of ρ consists of all matrices such that

$$t = \frac{at + b}{ct + d}.$$

It is easy to see that these are precisely the scalar matrices.
4. (a) If $n = 1$, we have

$$x - \alpha$$

so that

$$\alpha$$

is the only elementary symmetric polynomial. If $n = 2$ we have

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

Thus the elementary symmetric polynomials are

$$\alpha + \beta \qquad \text{and} \qquad \alpha\beta.$$

If $n = 3$ we have

$$(x - \alpha)(x - \beta)(x - \gamma) = x^2 - (\alpha + \beta + \gamma)x^3 + (\alpha\beta + \beta\gamma + \alpha\gamma)x + \alpha\beta\gamma,$$

so that the elementary symmetric polynomials are

$$\alpha + \beta + \gamma, \qquad \alpha\beta + \alpha\gamma + \beta\gamma \qquad \text{and} \qquad \alpha\beta\gamma.$$

Finally if $n = 4$ we have

$$(x - \alpha)(x - \beta)(x - \gamma)(x - \delta) = x^4 - (\alpha + \beta + \gamma + \delta)x^3$$
$$+(\alpha\beta+\beta\gamma+\alpha\gamma+\alpha\delta+\beta\delta+\gamma\delta)x-(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)x+\alpha\beta\gamma\delta,$$

so that the elementary symmetric polynomials are

$$\alpha+\beta+\gamma+\delta, \quad \alpha\beta+\alpha\gamma+\beta\gamma+\alpha\delta+\beta\delta+\gamma\delta, \quad \alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta \quad \text{and} \quad \alpha\beta\gamma\delta.$$

(b) Let K be any field and set $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are indeterminates over K. S_n acts on L in the obvious way. Let M be the fixed field. Then L/M is Galois, with Galois group S_n. Let N be the intermediary field generated by the elementary symmetric polynomials. Then $N \subset M$. On the other hand, the polynomial

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

splits in L and by definition $f(x) \in N[x]$, as the elementary symmetric polynomials are the coefficients of $f(x)$. Thus L/N is a splitting field for $f(x)$. In particular L/N has degree at most $n!$ (proved in a previous hwk). By the Tower Law, $M = N$. Now a polynomial is symmetric if and only if it lies in M. But the elements of N are precisely the rational functions of the elementary symmetric polynomials so every symmetric polynomial is a rational function of the elementary symmetric polynomials.

(c) Consider squaring $\alpha+\beta+\gamma$. We get

$$(\alpha+\beta+\gamma)^2=\alpha^2+\beta^2+\gamma^2+2(\beta\gamma+\alpha\gamma+\alpha\beta).$$

Thus

$$\alpha^2+\beta^2+\gamma^2=(\alpha+\beta+\gamma)^2-2(\beta\gamma+\alpha\gamma+\alpha\beta).$$

(d) Comparing coefficients, we have

$$\alpha+\beta+\gamma-a \qquad \text{and} \qquad \beta\gamma+\alpha\gamma+\alpha\beta=b.$$

Thus

$$\alpha^2+\beta^2+\gamma^2=a^2-2b.$$

5. (a) This is basically completing the square. Thus the automorphism

$$x\longrightarrow x-\frac{a_{n-1}}{n}$$

will work.
For the cubic, we use

$$x\longrightarrow x-\frac{a}{3}.$$

We get

$$\begin{aligned}
y^3+ay^2+by+c&=\left(x-\frac{a}{3}\right)^3+a\left(x-\frac{a}{3}\right)^2+b\left(x-\frac{a}{3}\right)+c\\
&=\left(x^3-ax^2+\frac{a^2}{3}x-\frac{a^3}{3^3}\right)+a\left(x^2-2\frac{a}{3}x+\frac{a^2}{3^2}\right)+b\left(x-\frac{a}{3}\right)+c\\
&=x^3+\left(\frac{a^2}{3}-\frac{2a^2}{3}+b\right)x+\left(-\frac{a^3}{3^3}+\frac{a^3}{3^2}-b\frac{a}{3}\right)+c\\
&=x^3+\left(b-\frac{a^2}{3}\right)x+\left(\frac{2a^3}{3^3}-\frac{ab}{3}\right)+c\\
&=x^3+\frac{1}{3}\left(3b-a^2\right)x+\frac{1}{27}\left(2a^3-9ab+27c\right)\\
&=x^3+px+q.
\end{aligned}$$

Comparing coefficients, we get

$$p=\frac{1}{3}\left(3b-a^2\right) \qquad \text{and} \qquad q=\frac{1}{27}\left(2a^3-9ab+27c\right).$$

(b) If $g(x)$ has roots α, β and γ, then the discriminant is the determinant of the product

$$\begin{pmatrix}1&1&1\\ \alpha&\beta&\gamma\\ \alpha^2&\beta^2&\gamma^2\end{pmatrix}\begin{pmatrix}1&\alpha&\alpha^2\\ 1&\beta&\beta^2\\ 1&\gamma&\gamma^2\end{pmatrix}.$$

On the other hand, comparing coefficients, we have

$$\alpha+\beta+\gamma=0, \qquad \beta\gamma+\alpha\gamma+\alpha\beta=p \qquad \text{and} \qquad \alpha\beta\gamma=-q.$$

Thus if we expand the product above, we get

$$\begin{pmatrix} 3 & 0 & \alpha^2+\beta^2+\gamma^2 \\ 0 & \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 \\ \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 & \alpha^4+\beta^4+\gamma^4 \end{pmatrix}.$$

We turn to computing the sums of powers of the roots. We have already seen that

$$\alpha+\beta+\gamma=0.$$

Squaring both sides we get

$$\begin{aligned} 0 &= \alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\dots) \\ &= \alpha^2+\beta^2+\gamma^2+2p. \end{aligned}$$

(Here and elsewhere we adopt the convention that dots represent the obvious symmetric terms.) Thus

$$\alpha^2+\beta^2+\gamma^2=-2p.$$

Now multiply both sides by $\alpha+\beta+\gamma$.

$$0=\alpha^3+\beta^3+\gamma^3+(\alpha^2\beta+\dots).$$

On the other hand, multiplying $\alpha+\beta+\gamma$ and $\alpha\beta+\dots$

$$0=(\alpha^2\beta+\dots)+3\alpha\beta\gamma.$$

So

$$\alpha^3+\beta^3+\gamma^3=-3q.$$

Now for the fourth powers. Consider squaring $\alpha^2+\beta^2+\gamma^2$.

$$4p^2=(\alpha^4+\beta^4+\gamma^4)+2(\alpha^2\beta^2+\dots).$$

Now square $\alpha\beta+\dots$.

$$p^2=(\alpha^2\beta^2+\dots)+2(\alpha^2\beta\gamma+\dots).$$

Finally multiplying $\alpha+\beta+\gamma$ with $\alpha\beta\gamma$ we get,

$$0=\alpha^2\beta\gamma+\dots.$$

Thus

$$\alpha^4+\beta^4+\gamma^4=2p^2.$$

Putting all this together we want to compute the following determinant

$$\begin{aligned} \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} &= 3\begin{vmatrix} -2p & -3q \\ -3q & 2p^2 \end{vmatrix} - 2p\begin{vmatrix} 0 & -2p \\ -2p & 0 \end{vmatrix} \\ &= -27q^2-4p^3. \end{aligned}$$

6. We have

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = \Phi_1(x)\Phi_3(x)\Phi_2(x)\Phi_6(x).$$

Hence

$$(x + 1)\Phi_6(x) = \Phi_2(x)\Phi_6(x) = x^3 + 1.$$

Now

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

where $y = -x$. Thus

$$\Phi_6(x) = x^2 - x + 1.$$

We have

$$x^{10} - 1 = (x^5 - 1)(x^5 + 1) = \Phi_1(x)\Phi_5(x)\Phi_2(x)\Phi_{10}(x).$$

Hence

$$(x + 1)\Phi_{10}(x) = \Phi_2(x)\Phi_{10}(x) = x^5 + 1.$$

Now

$$\begin{aligned} x^5 + 1 &= -(y^5 - 1) \\ &= -(y - 1)(y^4 + y^3 + y^2 + 1) \\ &= (x + 1)(x^4 - x^3 + x^2 - x + 1), \end{aligned}$$

where $y = -x$. Thus

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

We have

$x^{30}-1 = (x^{15}-1)(x^{15}+1) = (\Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x))(\Phi_{10}(x)\Phi_6(x)\Phi_{30}(x))$

Therefore

$$(x^5 + 1)(x^2 - x + 1)\Phi_{30}(x) = \Phi_2(x)\Phi_{10}(x)\Phi_6(x)\Phi_{30}(x) = x^{15} + 1.$$

Now

$$\begin{aligned} x^{15} + 1 &= -(y^3 - 1) \\ &= -(y - 1)(y^2 + y + 1) \\ &= (x^5 + 1)(x^{10} - x^5 + 1), \end{aligned}$$

where $y = (-x)^5$. Thus

$$(x^2 - x + 1)\Phi_{30}(x) = x^{10} - x^5 + 1.$$

After some work one gets

$$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

7. We want to determine the isomorphism classes of the abelian groups U_7, U_{20}, U_{60}.
If p is a prime then U_p are the units in the field $\mathbb{F}_p$ so that U_p is always cyclic of order $p-1$. Hence U_7 is cyclic of order 6, $U_7 \simeq \mathbb{Z}_6$.
By the Chinese remainder theorem, $U_{20} = U_4 \times U_5 = \mathbb{Z}_2 \times \mathbb{Z}_4$ and $U_{60} = U_3 \times U_4 \times U_5 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.
8. Let $f(x) = x^3 - 2x + 1$, considered over $\mathbb{Q}$. Let L/K be a splitting field.
First observe that all of the roots of $f(x)$ are real. Indeed the derivative of $f(x)$ is $3x^2 - 2$, which has two real roots. Thus $L \subset \mathbb{R}$.
Now $\Delta = -4(-2)^3 - 27(1)^2 = 5$. So L must contain $\mathbb{Q}(\delta)$, where δ is a root of $x^2 - 5$ (ie. $\delta = \sqrt{5}$). Let G be the Galois group of L/K. It follows that G is isomorphic to S_3. As S_3 is solvable, it follows that $f(x)$ is solvable by radicals.
Clearly the extension $M/\mathbb{Q}$ is radical. The problem is that L/M is not. Indeed suppose it were. Then there would be $\alpha \in L$ such that $\alpha^3 = a$. But then α is a root of $x^3 - a$. As L/K is Galois, then so is L/M and so $x^3 - a$ would split in L.
In particular $x^3 - 1$ would split in L. But then L is not a subset of $\mathbb{R}$, a contradiction.
9. Suppose that β is a root of

$$f(x) = x^p - x - a,$$

so that

$$\beta^p = \beta + a.$$

Then

$$\begin{aligned}(\beta+1)^p &= \beta^p + 1 \\ &= \beta + a + 1 \\ &= (\beta + 1) + a.\end{aligned}$$

Thus $\beta + 1$ is a root of $f(x)$. So

$$\beta, \quad \beta + 1, \quad \beta + 2, \quad \ldots \beta + p - 1.$$

are p distinct roots of $f(x)$. As a polynomial of degree p can have at most p roots, these are all the roots. In particular $L = K(\beta)$. Let G be the Galois group of L/K.
Define a map

$$f\colon G \longrightarrow \mathbb{Z}_p$$

by sending σ to i, where $\sigma(\beta) = \beta + i$. f is injective as β is a generator of L. Pick σ and $\tau \in G$ and suppose that $\sigma(\beta) = \beta + i$ and $\tau(\beta) = \beta + j$. Then

$$\begin{aligned}(\tau \circ \sigma)(\beta) &= \tau(\beta + i) \\ &= \tau(\beta) + i \\ &= \beta + i + j.\end{aligned}$$

Thus $f(\tau\sigma) = i + j$ and so f is also a group homomorphism. As G is then a subgroup of $\mathbb{Z}_p$, there are only two possibilities. Either G is trivial, which happens if and only if $L = K$ or L/K is cyclic of order p.

10. Note that the trace is invariant under the action of G, since we only permute the terms of the sum. It follows that f is indeed a map

$$f \colon L \longrightarrow K.$$

Let α and β be two elements of L. Then

$$\begin{aligned}f(\alpha + \beta) &= \sum_{\sigma \in G} \sigma(\alpha + \beta) \\ &= \sum_{\sigma \in G} \sigma(\alpha) + \sum_{\sigma \in G} \sigma(\beta) \\ &= f(\alpha) + f(\beta).\end{aligned}$$

Now suppose that $\alpha \in L$ and that $k \in K$. Then

$$\begin{aligned}f(k\alpha) &= \sum_{\sigma \in G} \sigma(k\alpha) \\ &= k \sum_{\sigma \in G} \sigma(\alpha) \\ &= k f(\alpha).\end{aligned}$$

Thus f is certainly a K-linear map.

11. We have

$$\begin{aligned}\sigma(\alpha) &= \sigma((p-1)\beta + (p-2)\sigma(\beta) + \cdots + 2\sigma^{p-3}(\beta) + \sigma^{p-2}(\beta)) \\ &= (p-1)\sigma(\beta) + (p-2)\sigma^2(\beta) + \cdots + 2\sigma^{p-2}(\beta) + \sigma^{p-1}(\beta) \\ &= \alpha + f(\alpha) \\ &= \alpha + 1.\end{aligned}$$

Now consider $a = \alpha^p - \alpha$. We have

$$\begin{aligned}\sigma(a) &= \sigma(\alpha^p - \alpha) \\ &= \sigma(\alpha)^p - \sigma(\alpha) \\ &= (\alpha + 1)^p - \alpha - 1 \\ &= \alpha^p + 1 - \alpha - 1 \\ &= \alpha^p - \alpha \\ &= a.\end{aligned}$$

Thus a is invariant under σ and hence the whole Galois group. But then $a \in K$. Clearly α is a root of $f(x) = x^p - x - a$ and as $\alpha \notin K$ and the degree of L/K is prime, $L = K(\alpha)$. But then $f(x)$ must be irreducible, as the degree of α is equal to the degree of the minimal polynomial. Thus L/K is a splitting field for $f(x)$, as L/K is normal. We are done by 7.

12. (i) Recall that as ϕ runs over G, so does $\phi\sigma$. Thus the numerator and denominator of the norm of α will be a product of the images of α under the action of G, only in a different order. Thus numerator and denominator cancel and the norm of α is one (note that for this result, we don't need G to be cyclic).

(ii) Set

$$\beta = \sigma(\alpha^{p-1})\sigma^2(\alpha^{p-2}) \dots \sigma^{p-2}(\alpha^2)\sigma^{p-1}(\alpha).$$

Just as in 7, it is easy to see that

$$\sigma(\beta) = \alpha\beta,$$

as $N(\alpha) = 1$. On the other hand β is clearly non-zero and so we are free to divide through by β.