Question 1

Let k be a field.

The definition of a k-algebra according to the assignment is a k-vector space V along with a multiplication $m\colon V \times V \to V$ satisfying

- Compatibility with scalars: $\forall \alpha \in k$ and $x, y \in V$, $\alpha \cdot m(x, y) = m(\alpha \cdot x, y) = m(x, \alpha \cdot y)$
- Right distributivity: $\forall x, y, z \in V$, $m(x + y, z) = m(x, z) + m(y, z)$
- Left distributivity: $\forall x, y, z \in V$, $m(x, y + z) = m(x, y) + m(x, z)$
- Existence of an identity element 1_V such that $\forall x \in V$, $m(x, 1_V) = m(1_V, x) = x$
- Associativity: $\forall x, y, z \in V$, $m(xy, z) = m(x, yz)$.

The above tells us that $(V, +, \times)$ is a ring, where $x \times y := m(x, y)$. (the relevant axioms are satisfied since $(V, +)$ is an abelian group, and $\times$ has the properties listed above. Note that the requirement that $0 \times v = 0 = v \times 0$ for all $v \in V$ follows from setting $\alpha = 0$ in the first dot point.) The ring A in our definition from class corresponds to this ring $(V, +, \times)$.

Our definition of a k-algebra from class had a ring homomorphism $\varphi\colon k \to A$. In this new definition, this corresponds to the map $\phi\colon k \to V$ sending

$$\alpha \mapsto \alpha \cdot 1_V$$

where $\alpha \in k$, and "$\cdot$" is the scalar multiplication of the vector space V. We can check that this is a ring homomorphism. For any $\alpha, \beta \in k$:

$$\begin{aligned}
\phi(\alpha + \beta) &= (\alpha + \beta) \cdot 1_V = \alpha \cdot 1_v + \beta \cdot 1_V = \phi(\alpha) + \phi(\beta) \\
\phi(\alpha\beta) &= (\alpha\beta) \cdot 1_V = (\alpha\beta) \cdot m(1_V, 1_V) = m(\alpha \cdot 1_V, \beta \cdot 1_V) = m(\phi(\alpha), \phi(\beta)) \\
\phi(1_k) &= 1_k \cdot 1_V = 1_V
\end{aligned}$$

where we have used properties of V being a vector space, as well as some properties of the multiplication m. Finally, we also have $\phi(k) \subseteq Z(V)$ since for all $\alpha \in k$, and $v \in V$,

$$m(\phi(\alpha), v) = m(\alpha \cdot 1_V, v) = \alpha \cdot m(1_V, v) = \alpha \cdot v = \alpha \cdot m(v, 1_V) = m(v, \alpha \cdot 1_V) = m(v, \phi(\alpha)).$$

This translation is easily reversed. Given a ring A and a ring homomorphism $\phi\colon k \to A$ such that $\phi(k) \subseteq Z(A)$, we construct the vector space V using the abelian group $(A, +)$ along with the map $\cdot\colon k \times A \to A$ defining scalar multiplication as follows:

$$\alpha \cdot v := \phi(\alpha)v$$

(where $\alpha \in k$ and $v \in A$). Most of the required properties of this scalar multiplication can be seen to be true as an immediate consequence of A being a ring and ϕ being a ring homomorphism. The only property worth elaborating on is the one that sort of looks like "associativity" of scalar multiplication: for all $\alpha, \beta \in k$ and $v \in A$:

$$(\alpha\beta) \cdot v = \phi(\alpha\beta)v = \phi(\alpha)\phi(\beta)v = \alpha \cdot (\phi(\beta)v) = \alpha \cdot (\beta \cdot v)$$

where we have used the associativity of A's multiplication in addition to ϕ being a ring homomorphism. Finally, the multiplication $m\colon A \to A$ is just taken to be the already existing multiplication in the ring A, which we will denote using $\times$. Again, most of the required properties of this multiplication are satisfied as an immediate consequence of A being a ring. We will only show the "compatibility with scalars" condition (see dot points at the very start of assignment): for all $\alpha \in k$ and $x, y \in A$

$$\alpha \cdot (x \times y) = \phi(\alpha) \times x \times y = (\alpha \cdot x) \times y$$

and

$$\alpha \cdot (x \times y) = \phi(\alpha) \times x \times y = x \times \phi(\alpha) \times y = x \times (\alpha \cdot y)$$

where we have used associativity of $\times$, as well as the fact that $\phi(x) \in Z(A)$ (so that $\phi(\alpha) \times x = x \times \phi(\alpha)$).

Question 2

(a)

To construct $\mathbb{F}_{16}$, we'll start by letting the elements of $\mathbb{F}_4$ be $0, 1, a, a+1$, where $a^2 = a+1$. We want to find irreducible polynomials of degree 2, since we'd like to construct a field with $16 = 4^2$ elements. Now, note that it suffices to just consider monic polynomials, since multiplying the any polynomial $p(x) \in \mathbb{F}_4[x]$ by a nonzero element of $\mathbb{F}_4$ doesn't change the principal ideal of $p(x)$. To find these monic irreducible polynomials of degree 2, we just eliminate the polynomials that can be factorised into two linear factors, i.e. we eliminate each of

- $x^2 = x \cdot x$
- $x^2 + x = x \cdot (x+1)$
- $x^2 + ax = x \cdot (x+a)$
- $x^2 + (a+1)x = x \cdot (x+a+1)$
- $x^2 + 1 = (x+1) \cdot (x+1)$
- $x^2 + (a+1)x + a = (x+1) \cdot (x+a)$
- $x^2 + ax + a + 1 = (x+1) \cdot (x+a+1)$
- $x^2 + a + 1 = (x+a) \cdot (x+a)$
- $x^2 + x + 1 = (x+a) \cdot (x+a+1)$
- $x^2 + a = (x+a+1) \cdot (x+a+1)$

So, the only monic irreducible polynomials (over $\mathbb{F}_4$) with degree 2 are:

$$p_1(x) = x^2 + x + a, \qquad p_2(x) = x^2 + x + a + 1, \qquad p_3(x) = x^2 + ax + 1$$

$$p_4(x) = x^2 + ax + a, \qquad p_5(x) = x^2 + (a+1)x + 1, \qquad p_6(x) = x^2 + (a+1)x + a + 1.$$

Thus, we can construct $\mathbb{F}_{16}$ by taking $\mathbb{F}_4[x]/(p(x))$, where $p(x)$ can be any of the six monic irreducible polynomials listed above. (Note that $\mathbb{F}_4[x]/(p(x))$ is indeed a field since $p(x)$ irreducible $\implies$ $(p(x))$ is prime (since $F_4[x]$ is a PID) $\implies$ $(p(x))$ is maximal $\implies$ $\mathbb{F}_4[x]/(p(x))$ is a field.)

Now we construct isomorphisms between these. Let c and b be the cosets of x in the source and target fields and let $\mathbb{F}_4[x]/(p_s(x))$ and $\mathbb{F}_4[x]/(p_t(x))$ be the source and target fields respectively. To define our isomorphism $f\colon \mathbb{F}_4[x]/(p_s(x)) \to \mathbb{F}_4[x]/(p_t(x))$ we just need to specify the image of c and make sure that $p_s(f(c)) = 0$. (Everything else will just work out, e.g. since it's a ring homomorphism between fields, it's automatically injective, hence bijective since target and source have same number of elements.)

In the below table, we specify the image of c in terms of b (recall c and b are the cosets of x in the source and target fields respectively).

target field is $\mathbb{F}_4[x]/(p_t(x))$

source field is $\mathbb{F}_4[x]/(p_s(x))$: $s\backslash t$	1	2	3	4	5	6
1	b	$b+a$	$(a+1)b+1$	$(a+1)b+a$	$ab+a$	ab
2	$b+a$	b	$(a+1)b+a+1$	$(a+1)b$	ab	$ab+a$
3	$ab+a$	$ab+1$	b	$b+1$	$(a+1)b+1$	$(a+1)b+a$
4	$ab+a+1$	ab	$b+1$	b	$(a+1)b$	$(a+1)b+a+1$
5	$(a+1)b+1$	$(a+1)b$	$ab+a$	ab	b	$b+1$
6	$(a+1)b$	$(a+1)b+1$	$ab+a+1$	$ab+1$	$b+1$	b

Actually, I'm pretty sure each square in the table can take two different values: in rows 1, 2 we can add 1 to each square. In rows $3, 4$ we can add a to each square. In rows $5, 6$ we can add $a+1$ to each square. (In short, in a row corresponding to irreducible polynomial $p_s(x) = x^2 + Xx + Y$, we may add X to each square).

Here's a bit of discussion on how we got to the above expressions. e.g. to define an isomorphism $f\colon \mathbb{F}_4[x]/(p_3(x)) \to \mathbb{F}_4[x]/(p_1(x))$, we have $p_1(b) = b^2 + b + a = 0$ and would like to define $f(c)$ to be some element of $\mathbb{F}_4[x]/(p_1(x))$ such that $p_3(f(c)) = 0$, i.e. $f(c)^2 + af(c) + 1 = 0$. Now, we can let $f(c) = mb + n$ (all quadratic and higher terms get "modded" out). So, we'd like

$$\begin{aligned} &(mb+n)^2 + a(mb+n) + 1 = 0 \\ \implies\ &m^2b^2 + n^2 + amb + an + 1 = 0 \\ \implies\ &m^2(b+a) + n^2 + amb + an + 1 = 0 \end{aligned}$$

Equating coefficients of b^1 and b^0, we want

$$m^2 + am = 0 \text{ and } m^2 a + n^2 + an + 1 = 0.$$

A simple bash (there are only $3 \times 4 = 12$ possibilities for (m, n), since $m \neq 0$ otherwise we'd just get an element of $\mathbb{F}_4$) shows that the only possible values for (m, n) are (a, a) and $(a, 0)$.

Notice also that we didn't really need to fill out the whole table, since just filling in the first column is enough to work out at least some isomorphism between each pair of constructed fields. e.g. if we had a map $\mathbb{F}_4[x]/(p_3(x)) \to \mathbb{F}_4[x]/(p_1(x))$given by $c \mapsto ab + a$, then we see $(a + 1)c + 1 \mapsto b$, which we can use to define an inverse function $\mathbb{F}_4[x]/(p_1(x)) \to \mathbb{F}_4[x]/(p_3(x))$. It's then easy to see how we can compose our functions to get the whole table using just the first column.

(b)

Again, we look for monic irreducible polynomials, but over $\mathbb{F}_3$ and with degree 3, since we'd like to construct a field with $27 = 3^3$ elements. We'll do this by eliminating all non-irreducible polynomials of degree 3, which are exactly the ones that have a linear factor (of x, $x + 1$, or $x + 2$) and so are zero when x is taken to be 0, 1 or 2. Using this process, we find that there are eight monic polynomials of degree 3 which are irreducible over $\mathbb{F}_3$:

$$p_1(x) = x^3 + 2x + 1, \qquad p_2(x) = x^3 + 2x + 2, \qquad p_3(x) = x^3 + x^2 + 2, \qquad p_4(x) = x^3 + x^2 + x + 2,$$

$$p_5(x) = x^3 + x^2 + 2x + 1, \qquad p_6(x) = x^3 + 2x^2 + 1, \qquad p_7(x) = x^3 + 2x^2 + x + 1, \qquad p_8(x) = x^3 + 2x^2 + 2x + 2$$

Just like in part (a), we can construct $\mathbb{F}_{27}$ by taking $\mathbb{F}_3[x]/(p(x))$, where $p(x)$ can be any of the eight monic irreducible polynomials listed above.

Now we construct isomorphisms between these. This time, we'll let $F_i := \mathbb{F}_3[x]/(p_i(x))$ so that we can avoid having to repeatedly write out that long expression. Now, let F_s and F_t be the source and target fields, and let c and b be the cosets of x in F_s and F_t, respectively.

Here's a table that shows what c could be mapped to, in terms of b:

source field \ target field	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
F_1	b	$2b$	$2b^2 + 2b$	$2b^2 + b$	$2b^2$	$2b^2 + b$	$2b^2 + 2b$	$2b^2$
F_2	$2b$	b	$b^2 + b$	$b^2 + 2b$	b^2	$b^2 + 2b$	$b^2 + b$	b^2
F_3		$b^2 + 2$						
F_4								
F_5								
F_6								
F_7								
F_8								

Actually, each square in the table can take three different values, e.g. in the F_1 and F_2 row, we may add 0, 1, or 2 to the entry in each square. In general, we can see that there will be three different isomorphisms from F_s to F_t since we can first fix a way of sending $F_s \to F_1$ (take the inverse of some map specified by the above table), and after that there are three ways of "completing the map" by choosing an isomorphism $F_1 \to F_j$.

Ok, the table is incomplete but I'll just demonstrate how you could complete it. Say we wanted to construct some isomorphisms $F_3 \to F_2$. Split this map into two bits, $f\colon F_3 \to F_1$ and then $g\colon F_1 \to F_2$. First fix one possible f. Take the current map (in above table) sending $F_1 \to F_3$, we'll try to find its inverse. We have

$$\begin{aligned} c &\mapsto 2b^2 + 2b \\ \implies c^2 &\mapsto (2b^2 + 2b)^2 = b^4 + 2b^3 + b^2. \end{aligned}$$

Now, using $b^3 + b^2 + 2 = 0$ we get $b^4 + b^3 + 2b = 0$. Adding these two equations up get us $b^4 + 2b^3 + b^2 + 2b + 2 = 0$, so that we have

$$\begin{aligned} c^2 &\mapsto b + 1 \\ \implies c^2 + 2 &\mapsto b. \end{aligned}$$

So, we'll take the fixed map $f\colon F_3 \to F_1$ to be the one specified by $x \mapsto x^2 + 2$, where x represents the coset of x in each field. We then have three options for $g\colon F_1 \to F_2$, where we can send $x \mapsto 2x$, $2x + 1$ or $2x + 2$. Composing:

1. $x \mapsto x^2 + 2 \mapsto (2x)^2 + 2 = x^2 + 2$, or
2. $x \mapsto x^2 + 2 \mapsto (2x + 1)^2 + 2 = x^2 + x$, or
3. $x \mapsto x^2 + 2 \mapsto (2x + 2)^2 + 2 = x^2 + 2x$

are the three ways we can define an isomorphism $F_3 \to F_2$.

Question 3

(a)

Let $\phi\colon G \to M$ be a monoid homomorphism, where G is a group. Then for all $g \in G$,

$$1 = \phi(1) = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$$

and

$$1 = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}).$$

(noting that g^{-1} does exist since G is a group). Hence $\phi(g)$ has an inverse, $\phi(g^{-1})$, so $\phi(g) \in M^\times$ for all $g \in G$. Hence $\phi(G) \subseteq M^\times$, so we can identify $\phi\colon G \to M$ with the group homomorphism $\varphi\colon G \to M^\times$ defined by

$$\varphi(g) = \phi(g)$$

for all $g \in G$. This process is clearly reversible.

(b)

In class, the monoid algebra RM was defined to be the free R-module (RM, i), equipped with a particular multiplication. Let A be an R-algebra and $\phi\colon M \to (A, \cdot)$ be a monoid map. There is a canonical structure of an R-module on A, and any monoid map can also be thought of as a set map, so we may use the universal property of the free R-module to conclude that there exists a unique R-module homomorphism $f\colon RM \to A$ satisfying $f \circ i = \phi$. What we need to do is show that f is actually an R-algebra homomorphism. Now, since f is an R-module homomorphism, we have

$$\begin{aligned} f(x + y) &= f(x) + f(y), \text{ and} \\ f(r \cdot x) &= r \cdot f(x) \end{aligned}$$

for any $x, y \in RM$ and $r \in R$. Note that the second condition implies $f(r \cdot 1_{RM}) = r \cdot f(1_{RM}) = r \cdot 1_A$, so that the canonical ring homomorphisms $\phi_1\colon R \to RM$ and $\phi_2\colon R \to A$, given by $\phi_1(r) = r \cdot 1_{RM}$ and $\phi_2(r) = r \cdot 1_A$ $\forall\, r \in R$, satisfy $f \circ \phi_1 = \phi_2$. So, all that's left to do to show that f is an R-algebra homomorphism is to prove that $f(xy) = f(x)f(y)$ for all $x, y \in RM$. Indeed, from class we know that every element in the free R-module RM can be expressed uniquely as a linear combination of elements of $\{i(m) \mid m \in M\}$. So, if we let x, y be arbitrary elements of RM, then we can write

$$x = \sum_{m \in M} a_m \cdot i(m), \qquad y = \sum_{n \in M} b_n \cdot i(n)$$

where each a_i, $b_i \in R$, for $i \in M$. Then we have

$$\begin{aligned}
f(xy) &= f\left(\sum_{m\in M} a_m \cdot i(m) \sum_{n\in M} b_n \cdot i(n)\right) \\
&= f\left(\sum_{(m,n)\in M\times M} a_m \cdot b_n \cdot (i(m)i(n))\right) \\
&= \sum_{(m,n)\in M\times M} a_m \cdot b_n \cdot f\left((i(m)i(n))\right) && \text{(since } f \text{ is an } R\text{-module homomorphism)} \\
&= \sum_{(m,n)\in M\times M} a_m \cdot b_n \cdot f\left(i(mn)\right) && \text{(since } i \text{ is a monoid homomorphism)} \\
&= \sum_{(m,n)\in M\times M} a_m \cdot b_n \cdot \phi(mn) \\
&= \sum_{(m,n)\in M\times M} a_m \cdot b_n \cdot [\phi(m)\phi(n)] && \text{(since } \phi \text{ is a monoid homomorphism)} \\
&= \sum_{(m,n)\in M\times M} a_m \cdot b_n \cdot [f(i(m))f(i(n))] \\
&= \sum_{m\in M} a_m \cdot f\left(i(m)\right) \sum_{n\in M} b_n \cdot f\left(i(n)\right) \\
&= f\left(\sum_{m\in M} a_m \cdot i(m)\right) f\left(\sum_{n\in M} b_n \cdot i(n)\right) \\
&= f(x)f(y)
\end{aligned}$$

which is what we wanted to show. (Note that I've assumed i is a monoid homomorphism from M to $(RM, \times)$ because I'm pretty sure that's supposed to be true.)

(c)

Let k be a field and G be a group. The universal property of the group algebra kG along with the map i defined in class is: for any k-algebra A and any group homomophism ϕ from G to $A^\times$ (i.e. the group of invertible elements in $(A, \cdot)$), there exists exactly one k-algebra homomorphism $f\colon kG \to A$ satisfying $f \circ i = \phi$.

To prove this universal property, note that by part (a) any group homomorphism ϕ from G to $A^\times$ can be identified with a monoid homomorphism φ from G to A. So, if we define the monoid homomorphism $\varphi\colon G \to A$ by $g \mapsto \phi(g)$ then proving that there exists exactly one k-algebra homomorphism $f\colon kG \to A$ satisfying $f \circ i = \phi$ is equivalent to proving that there exists exactly one k-algebra homomorphism satisfying $f \circ i = \varphi$.

But by part (b), there is a unique k-algebra homomphism $f\colon kG \to A$ satisfying $f \circ i = \varphi$ (we take (kG, i) to be our monoid ring and A and $\varphi\colon G \to A$ to be an R-algebra and monoid map respectively), so we are done.

Question 4

(a)

Given a representation of G on a k-vector space V

$$\begin{aligned}
G \times V &\to V \\
(g, v) &\mapsto \varrho(g)(v)
\end{aligned}$$

where $\varrho(g)(v)$ is k-linear for each g, we can form the k-algebra kG with the ring homomorphism $k \to kG$ given by $\alpha \mapsto \alpha \cdot 1$. Now, take the map $G \to End_k(V)$ defined by

$$\begin{aligned}
G &\to End_k(V) \\
g &\mapsto \varrho(g).
\end{aligned}$$

Since G was acting on V, this is really just a group homomorphism $G \to End_k(V)^\times$ (bijective endomorphisms). Also, we can think of $End_k(V)$ as a k-algebra since it has a multiplication. So, by the universal property from problem 3(c), I think we can say that there is then a unique canonical k-algebra homomorphism $kG \to End_k(V)$. I'm pretty sure this k-algebra homomorphism ends up being something like

$$kG \to End_k(V)$$
$$\sum \alpha_g g \mapsto \sum \alpha_g \varrho(g)$$

where $\sum \alpha_g \varrho(g)$ denotes the endomorphism sending $v \mapsto \sum \alpha_g \varrho(g)(v)$.

We can also go the other way. Given a k-algebra homomorphism $f\colon kG \to End_k(V)$, we can define a representation of G on V by taking $\varrho(g)$ to be $f(1 \cdot g)$. Now, notice that the map $G \to kG$ given by $g \to 1 \cdot g$ is a monoid homomorphism, so composing it with the k-algebra homomorphism f gives a monoid homomorphism $G \to End_k(V)$. But by problem 3(a), this can be identified with a group homomorphism $G \to End_k(V)^\times$, so that taking $g \mapsto 1 \cdot g \mapsto f(1 \cdot g) =: \varrho(g)$ does describe a group action on V.

(b)

Given a representation of G on V as in the problem statement, we can think of a kG-module structure on V with our abelian group being $(V, +)$, and our scalar multiplication defined by:

$$kG \times V \to V$$
$$\left(\sum \alpha_g g, v\right) \mapsto \sum \alpha_g \varrho(g)(v).$$

We can reverse this: given a scalar multiplcation $kG \times V \to V$, we can make g act by letting $\varrho(g)(v) := (1 \cdot g) \cdot v$ for each $v \in V$.

We should show all the structure stuff is preserved. Basically, $\varrho(g)$ being an endomorphism translates to our scalar multiplication being linear, i.e. if we write g, h to mean either the elements $1 \cdot g, 1 \cdot h \in kG$ or the actual elements of G, and take $\alpha \in k$, then we have

$$\varrho(g)(u+v) = \varrho(g)(u) + \varrho(g)(v) \text{ for all } u, v \in V \iff g \cdot (u+v) = g \cdot u + g \cdot v \text{ for all } u, v \in V.$$
$$\varrho(g)(\alpha v) = \alpha \varrho(g)(v) \text{ for all } v \in V \iff g \cdot (\alpha v) = \alpha g \cdot v \text{ for all } v \in V$$

Actually, the second condition is not an axiom of modules. It comes from V being both a k-module and a kG-module thus having a scalar multiplication for both, and it's nice to have $g \cdot (\alpha \cdot v) = \alpha g \cdot v$ so that the two scalar multiplications behave well with each other. Anyway, we can see there is then a canonical k-algebra homomorphism $kG \to End_k(V)$ by letting $\varrho\left(\sum \alpha_g g\right)(v) := \left(\sum \alpha_g g\right) \cdot v$, because the properties of a k-algebra homomorphism translate to the properties of the scalar multiplication on our module. That is, where $a, b \in kG$:

$$\varrho(a+b) = \varrho(a) + \varrho(b) \iff (a+b) \cdot v = a \cdot v + b \cdot b \text{ for all } v \in V$$
$$\varrho(ab) = \varrho(a)\varrho(b) \iff (ab) \cdot (v) = a \cdot (b \cdot v) \text{ for all } v \in V$$
$$\varrho(1_{kG})(v) = v \text{ for all } v \in V \iff 1_{kg} \cdot v = v \text{ for all } v \in V$$

(and "nice properties of scalar multiplications" tells us $\varrho(\alpha \cdot 1_G) = \alpha \varrho(1_{kG})$ translates to $(\alpha \cdot 1_G) \cdot v = \alpha \cdot v$ for all $v \in V$, so we do have a k-algebra homomorphism, not just a ring homomorphism). Finally, using part (a), we get a representation of G on V from this k-algebra homomorphism $kG \to End_k(V)$.

(c)

Let D_n denote the dihedral group of size $2n$, i.e. the symmetries of a regular n-gon. Let $r \in D_n$ be the element corresponding to an anticlockwise rotation of $\frac{2\pi}{n}$, and let $s \in D_n$ be the element corresponding to a horizontal reflection (i.e. reflection about the x-axis). Then the defining representations of D_n could be described using the algebra homomorphism $\mathbb{R}D_n \to End(\mathbb{R}^2)$ specified by

$$r \mapsto \begin{bmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{bmatrix}$$
$$s \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

where the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in \mathbb{R}$ is supposed to denote the endomorphism sending elements $(x, y) \in \mathbb{R}^2$ to $(ax + by, cx + dy) \in \mathbb{R}^2$. Note: the reason this specifies an $\mathbb{R}$-algebra homomorphism is that specifying the image of r and s is enough to define a group homomorphism $f\colon D_n \to (\mathbb{R}^2)^\times$ since r and s are generators, and one can check that we do end up with a valid homomorphism with our choice of $f(r)$ and $f(s)$ (expand to see $f(r)^n = f(s)^2 = f(s)f(r)f(s)f(r) = I_2$). Then, we use the universal property of the group algebra to get the unique $\mathbb{R}$-algebra homomorphism we want.

Question 5

(a)

We have, for all $\theta \in \mathbb{R}$,

$$\cos(2\theta) = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1.$$

So, for all $\theta \in \mathbb{R}$,

$$\begin{aligned} \cos(4\theta) &= \cos^2(2\theta) - 1 \\ &= 2(2\cos^2\theta - 1)^2 - 1 \\ &= 8\cos^4\theta - 8\cos^2\theta + 2 - 1. \end{aligned}$$

By setting $\theta = 15^\circ$ (and $\alpha = \cos(15^\circ)$), we get

$$\begin{aligned} 8\alpha^4 - 8\alpha^2 + 1 &= \frac{1}{2} \\ \implies 16\alpha^4 - 16\alpha^2 + 1 &= 0 \\ \implies \alpha^4 - \alpha^2 + \frac{1}{16} &= 0 \end{aligned}$$

We'll now show that the polynomial $p(x) = x^4 - x^2 + \frac{1}{16}$ is irreducible over $\mathbb{Q}$.

Suppose $p(x)$ is not irreducible over $\mathbb{Q}$. Then it must have at least one factor which is a quadratic or a linear polynomial. Let's first look at the case where we can factor $p(x)$ into two (WLOG monic) quadratics:

$$x^4 - x^2 + \frac{1}{16} = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$$

where $a, b, c, d \in \mathbb{Q}$. Comparing coefficients of x^3, we find $a + c = 0$, so $c = -a$. Then, comparing coefficients of x, we have $ad - ba = 0$, so $a = 0$ or $b = d$. If $a = 0$:

$$x^4 - x^2 + \frac{1}{16} = x^4 + (b + d)x^2 + bd$$

so $b + d = -1$ and $bd = \frac{1}{16}$. But then $b(1 - b) = \frac{1}{16}$, so that $16b^2 - 16b + 1 = 0$, but the two solutions to this equation are irrational since the discriminant is $256 - 64 = 192$ is not a perfect square.

Therefore $a \neq 0$, so we must have $b = d$. Then since $bd = \frac{1}{16}$, we must have $b = d = \pm\frac{1}{4}$. Our equation is now the following

$$x^4 - x^2 + \frac{1}{16} = x^4 + (2b - a^2)x^2 + \frac{1}{16}.$$

Comparing coefficients of x^2, we get $-1 = 2b - a^2$, where $b = \pm\frac{1}{4}$. So, $a^2 = 2b + 1 = \pm\frac{1}{2} + 1 = \frac{1}{2}$ or $\frac{3}{2}$, but neither is a square of a rational number so we have a contradiction.

The other case is that $p(x)$ has a linear factor with rational coefficients. However, this would imply that $p(x)$ has a rational root, but

$$\begin{aligned} x^4 - x^2 + \frac{1}{16} &= 0 \\ \implies 16x^4 - 16x^2 + 1 &= 0 \\ \implies x^2 &= \frac{16 \pm \sqrt{192}}{32} \end{aligned}$$

so the square of any root of $p(x)$ is not rational, so $p(x)$ does not have any rational roots.

Putting this together, we see that $p(x)$ is the irreducible polynomial we are looking for.

(b)

Letting $\beta = \alpha^2$, the equation $\alpha^4 - \alpha^2 + \frac{1}{16} = 0$ becomes

$$\beta^2 - \beta + \frac{1}{16} = 0.$$

Clearly the polynomial $x^2 - x + \frac{1}{16}$ is irreducible (as otherwise $x^4 - x^2 + \frac{1}{16}$ would not be irreducible, which would contradict our findings in part (a)), so it must be the irreducible polynomial for $\beta = \alpha^2$ over $\mathbb{Q}$. Hence, the irreducible polynomial for α^2 over $\mathbb{Q}$ has degree two.

(c)

Recall some useful facts from class:

- The constructible numbers form a subfield of $\mathbb{R}$. So, the sum or product of any two constructible numbers is also constructible, and the multiplicative inverse of any (non-zero) constructible number is also constructible.
- $45°$ is constructible, i.e. $\cos(45°) = \frac{1}{\sqrt{2}}$ is constructible
- $60°$ is constructible, i.e. $\cos(60°) = \frac{1}{2}$ is constructible. Actually, remember that when we constructed $60°$ in class, part of it involved constructing a 30-60-90 triangle with hypotenuse length 2, so that one of the sides must have had length $\sqrt{3}/2$. So $\sqrt{3}/2$ is also constructible.

Now, where $\alpha = \cos(15°)$, recall from part (a):

$$\alpha^4 - \alpha^2 + \frac{1}{16} = 0 \implies 16\alpha^4 - 16\alpha + 1 = 0$$

$$\implies \alpha^2 = \frac{16 \pm \sqrt{192}}{32} = \frac{2 \pm \sqrt{3}}{4} = \frac{1 + 3 \pm 2\sqrt{3}}{8} = \frac{(1 \pm \sqrt{3})^2}{8}$$

$$\implies \alpha = \pm\frac{1 \pm \sqrt{3}}{2\sqrt{2}}$$

We'll show that all four of the possible values for α are constructible, so that α must be constructible. Indeed, from our dot points at the start of part (c), we have that 1, $\frac{1}{\sqrt{2}}$, $\frac{\sqrt{3}}{2}$ constructible. Also, $2 = 1+1$ is constructible, so $\sqrt{3} = \frac{\sqrt{3}}{2} \times 2$ and $\frac{1}{2} = 2^{-1}$ are constructible.

Since we can make each of $\pm\frac{1\pm\sqrt{3}}{2\sqrt{2}}$ by taking sums, differences and products of 1, $\frac{1}{2}$, $\sqrt{3}$ and $\frac{1}{\sqrt{2}}$, we conclude that α (which must be one of these four values) is constructible.

(d)

The irreducible polynomial of $\cos(45°) = \frac{1}{\sqrt{2}}$ over $\mathbb{Q}$ is $x^2 - \frac{1}{2}$ which has degree 2, so $\dim_{\mathbb{Q}} \mathbb{Q}[\cos(45°)] = 2$. Also, from part (a), the degree of the irreducible polynomial of $\alpha = \cos(15°)$ over $\mathbb{Q}$ has degree $4 > 2$, so $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = 4$. Therefore $\alpha \notin \mathbb{Q}[\cos(45°)]$, so the degree of irreducible polynomial of α over $\mathbb{Q}[\cos(45°)]$ must be at least 2. We'll find a quadratic $q(x)$ with coefficients in $\mathbb{Q}[\cos(45°)]$ such that $q(\alpha) = 0$.

To find $q(x)$, remember that the irreducible polynomial of α over $\mathbb{Q}$ had four roots, $\pm\frac{1\pm\sqrt{3}}{2\sqrt{2}}$, as calculated in part (c). So, we want to choose two and multiply the corresponding linear factors together and hopefully end up with all coefficients in $\mathbb{Q}[\cos(45°)]$. One of these roots should be α, which we calculate to be

$$\alpha = \cos(15°)4 = \cos(60° - 45°) = \cos(60°)\cos(45°) + \sin(60°)\sin(45°) = \frac{1 + \sqrt{3}}{2\sqrt{2}}.$$

Then we can take

$$q(x) = \left(x - \frac{1 + \sqrt{3}}{2\sqrt{2}}\right)\left(x - \frac{1 - \sqrt{3}}{2\sqrt{2}}\right) = \left(x - \frac{1}{2\sqrt{2}} - \frac{\sqrt{3}}{2\sqrt{2}}\right)\left(x - \frac{1}{2\sqrt{2}} + \frac{\sqrt{3}}{2\sqrt{2}}\right)$$

$$= \left(x - \frac{1}{2\sqrt{2}}\right)^2 - \left(\frac{\sqrt{3}}{2\sqrt{2}}\right)^2 = x^2 - \frac{1}{\sqrt{2}}x + \frac{1}{8} - \frac{3}{8} = x^2 - \cos(45°)x - \frac{1}{4}.$$

Since $\alpha \notin \mathbb{Q}[\cos(45°)]$, and $q(x) = x^2 - \cos(45°)x - \frac{1}{4}$ is a degree 2 polynomial with all coefficients in $\mathbb{Q}[\cos(45°)]$ such that $q(\alpha) = 0$, it must be the irreducible polynomial of α over $\mathbb{Q}[\cos(45°)]$.

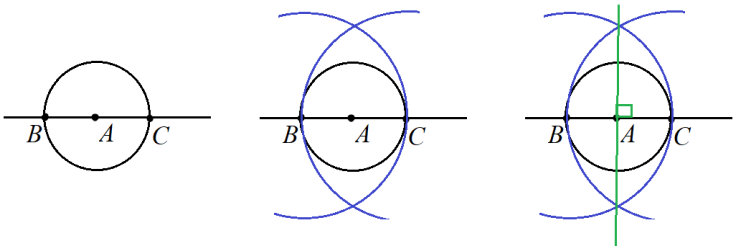
(e)

We begin with some lemmas:

Lemma 1. *Given a line l and a point A (not necessarily on l), we can construct a line though A perpendicular to l.*

Proof. Here are the steps required to construct the perpendicular:

1. Draw a circle centred at A, intersecting l at distinct points B and C.
2. Draw circles centred at B and C with radius BC.
3. Draw a line through the intersection points of the circles drawn in step 2. This line is the perpendicular we want.



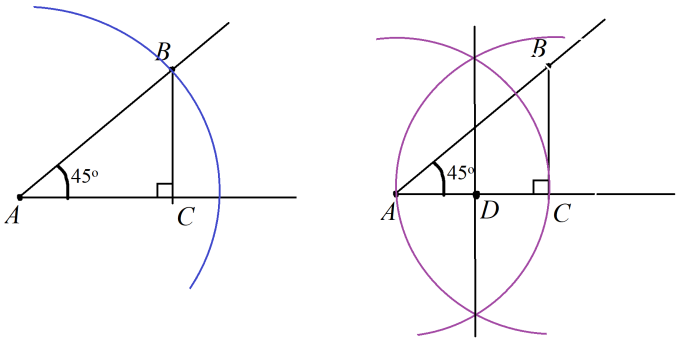
(Note that these steps work even if A is not on l). □

Also, from part (d),

$$\cos(15°) = \frac{1+\sqrt{3}}{2\sqrt{2}} = (1+\sqrt{3}) \times \frac{\cos(45°)}{2}.$$

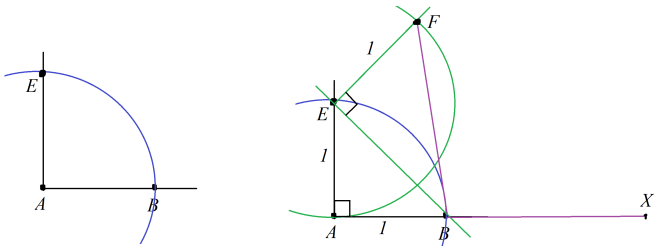
Now for the actual steps:

1. We have an already constructed 45° angle. Label the vertex of this angle A. Draw a circle centred at A with radius 1 (if we can't do this, draw a circle with radius k and multiply all subsequent lengths in our proof by k) and let it intersect one leg of the 45° angle at B. Draw a perpendicular from B to the other leg of the angle, and say it intersects the leg at C. Then, since $AB = 1$ and $\angle ACB = 90°$, we have $AC = \cos(45°)$.
2. Draw the circles centred at A and C with radius AC. These two circles intersect at two points. Draw the line connecting these two points, and let it intersect AC at D. Then, D is the midpoint of AC so $AD = \frac{\cos(45°)}{2}$.

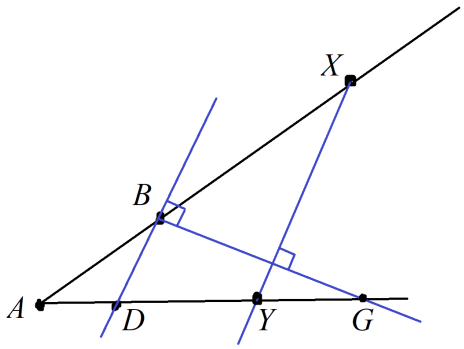


3. Now we construct a point X on line AB such that $BX = \sqrt{3}$ (so $AX = 1+\sqrt{3}$). Draw the circle centred at A with radius $AB = 1$. Let the perpendicular to AB through A intersect this circle at E. Then, $AE = 1$. Draw in line EB.

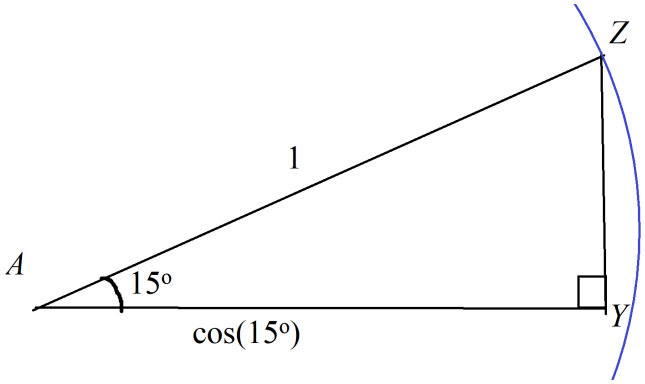
4. Next, draw a circle centred at E with radius $EA = 1$. Let the perpendicular to BE through E intersect this circle at F, so that $EF = 1$. Then, we have $BF^2 = BE^2 + FE^2 = AB^2 + AE^2 + FE^2 = 3$, so $BF = \sqrt{3}$. Then, draw a circle centred at B with radius $BF = \sqrt{3}$ and let this circle intersect line AB at X, so that A, B, X lie on the line in that order.



5. Now, we have points A, B, X, D (see diagram below) such that $AB = 1$, $AX = 1 + \sqrt{3}$ and $AD = \frac{\cos(45^\circ)}{2}$. Construct the perpendicular to BD through B and let it intersect line AD at G. Construct the perpendicular to BG through X and let it intersect AD at Y. Then, we have BD parallel to XY (since both are perpendicular to BG), so triangles ABD and AXY are similar. Then, $AB/AX = AD/AY$, so $AY = \frac{AD \cdot AX}{AB} = (1 + \sqrt{3}) \times \frac{\cos(45^\circ)}{2} = \cos(15^\circ)$.



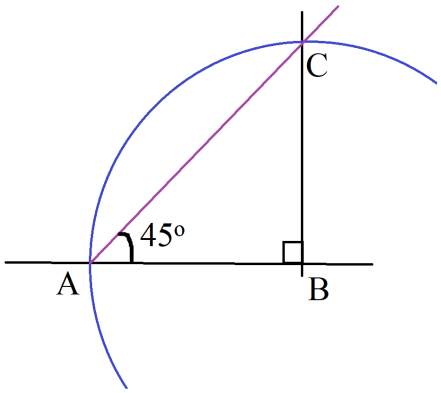
6. Finally, draw the perpendicular to AY through Y, and let it intersect the circle with radius 1 centred at A at Z. Then, since $AZ = 1$, $AY = \cos(15^\circ)$ and $\angle AYZ = 90^\circ$, $\angle ZAY = 15^\circ$, which is the angle we wanted.



(f)

From part (c), we knew that $\cos(15^\circ)$ is one of $\pm\frac{1\pm\sqrt{3}}{2\sqrt{2}}$. Actually, from (d) we know that $\cos(15^\circ) = \frac{1+\sqrt{3}}{2\sqrt{2}}$. So, all we need to do is show how to construct a 45° angle from scratch, and from there we can do the same as in

part (e). But this is simple: label the two given points A and B. Draw the perpendicular to AB passing through B, and let it intersect the circle centred at B with radius BA at a point C. Then, $BA = BC$ and $\angle ABC = 90°$, so $\triangle ABC$ is right isosceles, so $\angle CAB = 45°$.



(g)

In each case, where $F \subset F[\beta]$ is the field extension, we just want to write $F[\beta] \cong F[x]/(p(x))$, where $p(x) \in F[X]$ is the irreducible polynomial of β over F. Using part (a), (b) and (c):

1. $\mathbb{Q}[\cos(45°)] = \mathbb{Q}\left[\frac{1}{\sqrt{2}}\right] \cong \mathbb{Q}[x]/(x^2 - \frac{1}{2})$
2. $\mathbb{Q}[\cos(15°)] \cong \mathbb{Q}[x]/\left(x^4 - x^2 + \frac{1}{16}\right)$
3. $\mathbb{Q}[\cos^2(15°)] \cong \mathbb{Q}[x]/\left(x^2 - x + \frac{1}{16}\right)$
4. $\mathbb{Q}[\cos(15°)] \cong \mathbb{Q}[\cos(45°)][x]/\left(x^2 - \cos(45°)x - \frac{1}{4}\right)$
5. For this one, we first notice the irreducible polynomial of $\cos^2(15°)$ over $\mathbb{Q}$ has degree 2 (see part (b)), while the irreducible polynomial of $\cos(15°)$ over $\mathbb{Q}$ has degree 4 (see part (a)), hence $\cos(15°) \notin \mathbb{Q}[\cos^2(15°)]$. So, the irreducible polynomial of $\cos(15°)$ over $\mathbb{Q}[\cos^2(15°)]$ must have degree at least 2, and from this we can see that the required irreducible polynomial is $x^2 - \cos^2(15°)$. So, $\mathbb{Q}[\cos(15°)] \cong \mathbb{Q}[\cos^2(15°)][x]/\left(x^2 - \cos^2(15°)\right)$.