MAST30005 Assignment 1

Chengjing Zhang

May 6, 2019

1 Algebras

Let k be a field. Then a k-algebra consists of a vector space V over k along with a multiplication $m : V \times V \longrightarrow V$ satisfying a list of properties. Find this list of properties (either by figuring it out or from the literature) and translate this definition, line by line, into the definition from class (more precisely, the special case of the definition from class where $R = k$ is a field).

Solution:

For all elements $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V$ and all elements $a, b \in k$, m satisfies the following three properties:

1. Right distributivity: $m(\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z}) = m(\boldsymbol{x}, \boldsymbol{z}) + m(\boldsymbol{y}, \boldsymbol{z})$,
2. Left distributivity: $m(\boldsymbol{x}, \boldsymbol{y} + \boldsymbol{z}) = m(\boldsymbol{x}, \boldsymbol{y}) + m(\boldsymbol{x}, \boldsymbol{z})$
3. Compativity with scalars: $m(a\boldsymbol{x}, b\boldsymbol{y}) = (a \cdot b)m(\boldsymbol{x}, \boldsymbol{y})$

An algebra is *associative* if the multiplication of elements of an algebra is associative. An algebra is *unitary* if it has an identity element with respect to the multiplication. The algebra defined in class is actually unitary associative algebra. Therefore, we assume m is associative, and there exists $\boldsymbol{e} \in V$ such that for all elements $\boldsymbol{x} \in V$, $m(\boldsymbol{e}, \boldsymbol{x}) = m(\boldsymbol{x}, \boldsymbol{e}) = \boldsymbol{e}$.

First, we show that we can get the definition in class from this definiton.

V is a vector space, hence V forms a group with respect to vector addition $+$. m is associative and there exists identity with respect to multiplication m, therefore, (V, m) forms a monoid. Combining right distributivity and left distributivity, $(V, +, m)$ forms a ring.

Define a map

$$\begin{aligned} \varphi : k &\longrightarrow V \\ r &\longmapsto r\boldsymbol{e} \end{aligned}$$

where $r \in R$ and $\boldsymbol{e} \in V$ is the identity element with respect to multiplication m, and $r\boldsymbol{e}$ is the scalar product in V. For all elements $a, b \in k$, $\varphi(a+b) = (a+b)\boldsymbol{e} = a\boldsymbol{e} + b\boldsymbol{e} = \varphi(a) + \varphi(b)$, thus φ is a group homomorphism with respect to vector addition. For all elements $a, b \in k$, by compativity with scalars, $\varphi(a \cdot b) = (a \cdot b)\boldsymbol{e} = m(a\boldsymbol{e}, b\boldsymbol{e}) = m(\varphi(a), \varphi(b))$, hence φ is a monoid homomorphism with respect to multiplication m. Therefore, φ is a ring homomorphism.

For all elements $\boldsymbol{x} \in V$, $a \in k$, $m(\boldsymbol{x}, \varphi(a)) = m(\boldsymbol{x}, a\boldsymbol{e}) = am(\boldsymbol{x}, \boldsymbol{e}) = a\boldsymbol{x} = am(\boldsymbol{e}, \boldsymbol{x}) = m(a\boldsymbol{e}, \boldsymbol{x}) = m(\varphi(a), \boldsymbol{x})$, hence $\varphi(a) \in Z(V)$, therefore $\varphi(k) \subseteq Z(V)$.

So far we have shown that k-algebra defined by these properties is a ring $(V, +, m)$ together with a ring homomorphism φ such that the image of φ is contained in the centre of V.

Next, we show that from the definition in class, we are able to get all these properties.

Since any k-algebra V equipped with a ring homomorphism φ is a k-module with canonical multiplication:

$$\begin{aligned} m : k \times V &\longrightarrow V \\ (a, \boldsymbol{v}) &\longmapsto \varphi(a) \cdot (\boldsymbol{v}) \end{aligned}$$

where $a \in k$ and $\boldsymbol{v} \in V$. Since we have any k-module is a vector space, V forms a vector space with multiplication m.

By definition of ring, $(V, +, m)$ satisfies left and right distributive law, hence the first and the second properties hold. In addition, V should also be associative and unitary with respect to m.

We use "$\boldsymbol{x} \cdot \boldsymbol{y}$" to denote "$m(\boldsymbol{x}, \boldsymbol{y})$" here for convienience. For any $a, b \in k$ and $\boldsymbol{x}, \boldsymbol{y} \in V$,

$$\begin{aligned} a\boldsymbol{x} \cdot b\boldsymbol{y} &= (\varphi(a) \cdot \boldsymbol{x}) \cdot (\varphi(b) \cdot \boldsymbol{y}) \\ &= \varphi(a) \cdot \boldsymbol{x} \cdot \varphi(b) \cdot \boldsymbol{y} \\ &= \varphi(a) \cdot \varphi(b) \cdot \boldsymbol{x} \cdot \boldsymbol{y} \\ &= (\varphi(a) \cdot \varphi(b)) \cdot (\boldsymbol{x} \cdot \boldsymbol{y}) \\ &= (a \cdot b) \cdot (\boldsymbol{x} \cdot \boldsymbol{y}) \,. \end{aligned}$$

Hence, compativity with scalars holds.

So far, We have shown that the definition in class is equivalent to the definition here.

2 Finite fields

Part A

Find all the ways to construct $\mathbb{F}_{16}$ as the quotient of a polynomial ring over $\mathbb{F}_4$ and construct the isomorphisms between them.

Solution:

First, we use 0, 1, a, $a+1$ to denote the elements in $\mathbb{F}_4$. Since the polynomial ring $\mathbb{F}_4[x]$ is PID, the irreducible polynomials are prime. Hence, the ideals generated by irreducible polynomials are prime therefore maximal. So $\mathbb{F}_{16}$ can be constructed as quotient of the polymonial ring over $\mathbb{F}_4$ by an irreducible polynomial of degree 2, since the quotient of the polynomial ring by an maximal ideal is a field.

To find irreducible polynomials, we just need to consider monic polynomials, since all polynomials can be simplified to a monic form. There are 16 monic polynomials of degree 2 in $\mathbb{F}_4[x]$. Only 6 polynomials in these polynomials are irreducible, which are x^2+ax+1, $x^2+(a+1)x+1$, x^2+x+a, x^2+ax+a, $x^2+x+(a+1)$ and $x^2+(a+1)x+(a+1)$.

Therefore, there are 6 ways to construct $\mathbb{F}_{16}$, which are $\mathbb{F}_4[x]/(x^2+ax+1)$, $\mathbb{F}_4[x]/(x^2+(a+1)x+1)$, $\mathbb{F}_4[x]/(x^2+x+a)$, $\mathbb{F}_4[x]/(x^2+ax+a)$, $\mathbb{F}_4[x]/(x^2+x+(a+1))$, $\mathbb{F}_4[x]/(x^2+(a+1)x+(a+1))$.

Since $\mathbb{F}_{16}\backslash\{0\}$ forms a cyclic group with respect to multiplication, we just need to find a primitive element in each construction, then we will get isomorphisms between every two constructions, which send the primitive element in one construction to the primitive element in the other constuction. Primitive elements in each consturction are $ax+(x^2+ax+1)$ in $\mathbb{F}_4[x]/(x^2+ax+1)$, $x+a+(x^2+(a+1)x+1)$ in $\mathbb{F}_4[x]/(x^2+(a+1)x+1)$, $x+(x^2+x+a)$ in $\mathbb{F}_4[x]/(x^2+x+a)$, $x+(x^2+ax+a)$ in $\mathbb{F}_4[x]/(x^2+ax+a)$, $x+(x^2+x+(a+1))$ in $\mathbb{F}_4[x]/(x^2+x+(a+1))$ and $x+(x^2+(a+1)x+(a+1))$ in $\mathbb{F}_4[x]/(x^2+(a+1)x+(a+1))$.

So far, we have got isomorphisms from any construction to another construction, which send the primitive element in one construction to the primitive element in the other construction.

Part B

Find all the ways to construct $\mathbb{F}_{27}$ as the quotient of a polynomial ring over $\mathbb{F}_3$ and construct the isomorphisms between them.

Solution:

Similarly, $\mathbb{F}_{27}$ can be constructed as quotient of the polynomial ring over $\mathbb{F}_{16}$ by an polynomial ring over $\mathbb{F}_3$ by an irreducible polynomial of degree 3.

There are 27 monic polynomials of degree 3 in $\mathbb{F}_3[x]$. Only 8 of them are irreducible, which are x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+x^2+x+2,

x^3+x^2+2x+1, x^3+2x^2+1, x^3+2x^2+x+1 and x^3+2x^2+2x+2. Hence, there are 8 ways to construct $\mathbb{F}_{27}$, which are $\mathbb{F}_3[x]/(x^3+2x+1)$, $\mathbb{F}_3[x]/(x^3+2x+2)$, $\mathbb{F}_3[x]/(x^3+x^2+2)$, $\mathbb{F}_3[x]/(x^3+x^2+x+2)$, $\mathbb{F}_3[x]/(x^3+x^2+2x+1)$, $\mathbb{F}_3[x]/(x^3+2x^2+1)$, $\mathbb{F}_3[x]/x^3+2x^2+x+1$ and $\mathbb{F}_3[x]/(x^3+2x^2+2x+2)$.

By observing that elements in $\mathbb{F}_{27}\backslash\{0\}$ must have order 1, 2, 13 or 26, and order of cosets of x and $2x$ are not 1 and 2, one of x and $2x$ must be primitive since $2^{13} \neq 1 (\mathrm{mod}\, 26)$. We can easily find an primitive element in each construction, which are $x+(x^3+2x+1)$ in $\mathbb{F}_3[x]/(x^3+2x+1)$, $x+(x^3+2x+1)$ in $\mathbb{F}_3[x]/(x^3+2x+2)$, $2x+(x^3+x^2+2)$ in $\mathbb{F}_3[x]/(x^3+x^2+2)$,$2x+(x^3+x^2+x+2)$ in $\mathbb{F}_3[x]/(x^3+x^2+x+2)$, $x+(x^3+x^2+2x+1)$ in $\mathbb{F}_3[x]/(x^3+x^2+2x+1)$, $x+(x^3+2x^2+1)$ in $\mathbb{F}_3[x]/(x^3+2x^2+1)$, $x+(x^3+2x^2+x+1)$ in $\mathbb{F}_3[x]/(x^3+2x^2+x+1)$ and $2x+(x^3+2x^2+2x+2)$ in $\mathbb{F}_3[x]/(x^3+2x^2+2x+2)$.

So far, we have got isomorphisms from any construction to another construction, which send the primitive element in one construction to the primitive element in the other construction.

3 Group algebras

Let G be a finite group, and let k be a field. You will show the universal property of the group algebra kG in several steps.

3.1 Part A

Given a monoid M, we will use the notation $M^\times$ for the group of invertible elements in M. Given a group G and a monoid M, show that the set of monoid homomorphisms from G to M can be identified with the set of group homomorphisms from G to $M^\times$.

Proof. First, all group homomorphisms $\varphi : G \longrightarrow M^\times$ are also monoid homomorphisms from G to M, hence $\mathrm{Hom}_{group}(G, M^\times) \subseteq \mathrm{Hom}_{monoid}(G, M)$.

We prove that all monoid homorphisms from G to M are also group homomorphisms from G to $M^\times$ by contradiction. If there exists a monoid homomorphism $\psi \in \mathrm{Hom}_{monoid}(G, M)$ such that $\psi \notin \mathrm{Hom}_{group}(G, M^\times)$, then there exists an element $g \in G$ such that $\psi(g) \in M\backslash M^\times$. Since G is a group, g has an inverse $g^{-1} \in G$. Since ψ is a monoid homomorphism, $\psi(g) \cdot \psi(g^{-1}) = \psi(gg^{-1}) = \psi(1_G) = 1_M$. Therefore, $\psi(g)$ has an inverse $\psi(g^{-1}) \in M$, which contradicts to the assumption that $\psi(g) \notin M^\times$.

Therefore, $\mathrm{Hom}_{group}((G, M^\times) \cong \mathrm{Hom}_{monoid}(G, M))$. □

3.2 Part B

Let R be a commutative ring, and let M be a monoid. Show that the monoid algebra RM along with the map $i : M \longrightarrow RM$ defined in class satisfies the

following universal property: for any R-algebra a and any monoid map ϕ from M to $(A, \cdot)$, there exists exactly one R-algebra homomorphism $f : RM \longrightarrow A$ satisfying $f \circ i = \phi$.

Proof. In class, we defined i by letting it send any element $m \in M$ to $\beta_m \in RM$, where β_m send m to $1_R \in R$, and all the other elements to 0. We also have shown that the set $\{\beta_m\}_{m\in M}$ is a linearly independent sappning basis of RM. For any $\psi \in RM$, ψ can be uniquely represented as $\psi = \sum_{m\in M} \psi(m)\beta_m$. In addition, we have also shown that RM forms a R-module. Therefore, we can define a canonical map

$$\begin{aligned} f : RM &\longrightarrow A \\ \psi = \sum_{m\in M} \psi(m)\beta_m &\longmapsto \sum_{m\in M} \psi(m)\phi(m). \end{aligned}$$

For any element $m \in M$, $(f \circ i)(m) = f(i(m)) = f\left(\sum_{n\in M} \beta_m(n)\beta_m\right) = \sum_{n\in M} \beta_m(n)\phi(n) = \phi(m)$. Hence, $f \circ i = \phi$.

For any two elements $\psi, \psi' \in RM$,

$$\begin{aligned} f(\psi) + f(\psi') &= \sum_{m\in M} \psi(m)\phi(m) + \sum_{m\in M} \psi'(m)\phi(m) \\ &= \sum_{m\in M} \left(\psi(m) + \psi'(m)\right)\phi(m) \\ &= f(\psi + \psi'). \end{aligned}$$

Hence f preserves addition from RM and A. We also have

$$\begin{aligned} f(\psi) \cdot f(\psi') &= \left(\sum_{m\in M} \psi(m)\phi(m)\right) \cdot \left(\sum_{n\in M} \psi'(n)\phi(n)\right) \\ &= \sum_{m,n\in M} \left(\psi(m)\phi(m)\right) \cdot \left(\psi(n)\phi(n)\right) \\ &= \sum_{m,n\in M} (\psi(m) \cdot \psi'(n))(\phi(m) \cdot \phi(n)) \\ &= \sum_{m'\in M} \left(\sum_{\substack{(m,n)\in M \\ m\cdot n = m'}} \psi(n) \cdot \psi'(m) \right) \phi(m') \\ &= f(\psi \cdot \psi'). \end{aligned}$$

Thus f preserve multiplication from RM to A. Therefore, f is a ring homomorphism.

Then we show that f is unique. If $f : RM \longrightarrow A$ and $g : RM \longrightarrow A$ satisfy $f \circ i = \phi$ and $g \circ i = \phi$, then for any element $m \in M$, $f(\beta_m) =$

$(f \circ i)(m) = \phi(m)$ and $g(\beta_m) = (g \circ i)(m) = \phi(m)$, thus $f(\beta_m) = g(\beta_m)$. Let $\mathcal{B} = \{\beta_m\} \subseteq RM$, ι be the inclusion from $\mathcal{B}$ to RM, then we have $f \circ \iota = g \circ \iota$, call it $\tilde{\phi}$. Since $\tilde{\phi}$ is a set map from $\mathcal{B}$ to A, and $\mathcal{B}$ is a basis of RM, by universal property of basis in linear algebra, there is only one map $\tilde{f}$ from RM to A such that $\tilde{f} \circ \iota = \tilde{\phi}$. Therefore, $f = \tilde{f} = g$, hence f is unique. □

3.3 Part C

Combine the two previous points to formulate and prove the universal property of of kG.

First, we conclude the univeral property from the previous two statements:

Theorem 1. *For any k-algebra A and any group homomorphism ϕ from G to $(A^\times, \cdot)$, there exists a unique k-algebra homomorphism $f : kG \longrightarrow A$ satisfying $f \circ i = \phi$, where i is the map*

$$\begin{aligned} i : G &\longrightarrow kG \\ g &\longmapsto \beta_g \end{aligned}$$

Proof. The set of group homomorphisms from G to $(A^\times, \cdot)$ can be identified with the set of monoid homomorphisms from G to $(A, \cdot)$. Hence, ϕ is also a monoid homomorphism. By universal property of monoid algebra, there exists a unique k-algebra homomorphism f such that $f \circ i = \phi$.

□

4 Representations

A representation of G on a k-vector space V is an action of G on V via k-linear maps. In other words, a representation of G on V is a G-action

$$\begin{aligned} \rho : G \times V &\longrightarrow V \\ (g, v) &\longmapsto \rho(g)(v) \end{aligned}$$

such that for each $g \in G$ the map $\rho(g)$ is k-linear.

4.1 Part A

Prove that a representation of G on V consists of the same data as k-algebra homomorphism $kG \longrightarrow \mathrm{End}_k(V)$.

Proof. First, we show that we can construct a k-algebra homomorphism from kG to $\mathrm{End}_k(V)$ with the G-action ρ.

Define the canonical map from G to kG

$$\begin{aligned} i : G &\longrightarrow kG \\ g &\longmapsto \beta_g \end{aligned}$$

where $g \in G$ and β_g is the element of kG which sends g to 1 and all the other elements to 0.

From lecture, we know that $\mathrm{End}_k(V)$ forms a k-algebra. Since $\rho(g) \in \mathrm{End}_k(V)$, by univeral property of k-algebra, there exists a unique k-algebra homomorphism f from kG to $\mathrm{End}_k V$ such that $f \circ i = \rho$.

Therefore, given a G-action ρ, we can get a k-algebra homomorphism.

Then we prove that given a k-algebra homomophism f, we can construct a G-action ρ such that for every $g \in G$ the map $\rho(g)$ is k-linear.

Let $\rho(g) = (f \circ i)(g) = f(\beta_g)$, then for any $g, h \in G$ and $\boldsymbol{v} \in V$, $\rho(g \cdot h)(\boldsymbol{v}) = f(\beta_{gh})(\boldsymbol{v}) = f(\beta_g \cdot \beta_h)(\boldsymbol{v}) = (f(\beta_g) \circ f(\beta_h))(\boldsymbol{v}) = f(\beta_g)\,(f(\beta_h)(\boldsymbol{v})) = \rho(g)(\rho(h)(\boldsymbol{v}))$. Since $\{\beta_g | g \in G\}$ forms a subgroup in the group of invertible elements in kG, and it is isomorphic to G, therefore, i forms a group homomorphism, so $\beta_{1_G} = 1_{kG}$. Since f is a k-algebra homomorphism, we have $f(1_{kG}) = 1_{\mathrm{End}_k(V)}$, where $1_{\mathrm{End}_k(V)}$ is the identity endomorphism on V. Thus, for any $\boldsymbol{v} \in V$, $\rho(1_G)(\boldsymbol{v}) = f(1_{kG})(\boldsymbol{v}) = \boldsymbol{v}$.

Since $\rho(g) \in \mathrm{End}_k(V)$, it is a k-linear map. Hence ρ is a G-action such that for each $g \in G$ the map $\rho(g)$ is k-linear.

Therefore, we can construct a G-action from a k-algebra homomorphism. □

4.2 Part B

Prove that a representation of G on V consists of the same data as the structure of a kG-module on V.

Proof. First, we show that we are able to construct a kG-module from G-action ρ.

Define a multiplication between kG and V as

$$\begin{aligned} \text{“}\cdot\text{”} : kG \times V &\longrightarrow V \\ (\psi = \sum_{g \in G} \psi(g)\beta_g, \boldsymbol{v}) &\longmapsto \sum_{g \in G} \psi(g)\rho(g)(\boldsymbol{v}). \end{aligned}$$

For any $a, b \in k$, $\varphi, \psi \in kG$, $\boldsymbol{v} \in V$,

$$\begin{aligned} (a\varphi + b\psi) \cdot \boldsymbol{v} &= \sum_{g \in G} (a\varphi(g) + b\psi(g))\rho(g)(\boldsymbol{v}) \\ &= a \sum_{g \in G} \varphi(g)\rho(g)(\boldsymbol{v}) + b \sum_{g \in G} \psi(g)\rho(g)(\boldsymbol{v}) \\ &= a(\varphi \cdot \boldsymbol{v}) + b(\psi \cdot \boldsymbol{v}). \end{aligned}$$

And for any $a, b \in k$, $\psi \in kG$ and $\boldsymbol{v}, \boldsymbol{u} \in V$,

$$\begin{aligned}\psi \cdot (a\boldsymbol{v} + b\boldsymbol{u}) &= \sum_{g\in G} \psi(g)(a\rho(g)(\boldsymbol{v}) + b\rho(g)(\boldsymbol{u})) \\ &= a\sum_{g\in G} \psi(g)\rho(g)(\boldsymbol{v}) + b\sum_{g\in G} \psi(g)\rho(g)(\boldsymbol{u}) \\ &= \psi \cdot \boldsymbol{v} + \psi \cdot \boldsymbol{u}.\end{aligned}$$

Hence, "$\cdot$" is bilinear.

For any $\varphi, \psi \in kG$, $\boldsymbol{v} \in V$,

$$\begin{aligned}(\varphi \cdot \psi) \cdot \boldsymbol{v} &= \sum_{g\in G} (\varphi \cdot \psi)(g)\rho(g)(\boldsymbol{v}) \\ &= \sum_{g\in G} \left(\sum_{\substack{hk=g \\ h,k\in G}} (\varphi(h) \cdot \psi(k))\rho(h \cdot k)(\boldsymbol{v}) \right) \\ &= \sum_{g\in G} \left(\sum_{\substack{hk=G \\ h,k\in G}} \Big(\varphi(h)\Big(\psi(k)\rho(h)(\rho(k)(\boldsymbol{v}))\Big)\Big) \right) \\ &= \sum_{h\in G} \varphi(h)\rho(h) \left(\sum_{k\in G} \psi(k)\rho(k)(\boldsymbol{v}) \right) \\ &= \sum_{h\in G} \varphi(h)\rho(h)(\psi \cdot \boldsymbol{v}) \\ &= \varphi \cdot (\psi \cdot \boldsymbol{v}).\end{aligned}$$

Sicne $\beta_{1_G} = 1_{kG}$, for any $v \in V$, we have $1_{kG} \cdot \boldsymbol{v} = \beta_{1_G} \cdot \boldsymbol{v} = \rho(1_G)(\boldsymbol{v}) = \boldsymbol{v}$. Therefore, V forms a kG-module together the scalar multiplication "$\cdot$".

Hence, from a G-action ρ, we can construct a kG-module over V.

Next, we show that from a kG-module over V, we can get a G-action.

Define a map

$$\begin{aligned}\rho : G \times V &\longrightarrow V \\ (g, v) &\longmapsto \beta_g \boldsymbol{v}.\end{aligned}$$

Clearly, for any $a, b \in k$, $g \in G$ and $\boldsymbol{v}, \boldsymbol{u} \in V$, $\rho(g)(a\boldsymbol{v}+b\boldsymbol{u}) = \beta_g(a\boldsymbol{v}+b\boldsymbol{u}) = a\beta_g\boldsymbol{v} + b\beta_g\boldsymbol{u} = a\rho(g)(\boldsymbol{v}) + b\rho(g)(\boldsymbol{u})$, hence $\rho(g)$ is k-linear.

For any $g, h \in G$, $\boldsymbol{v} \in V$,

$$\begin{aligned}\rho(g \cdot h)(\boldsymbol{v}) &= \beta_{gh}\boldsymbol{v} \\ &= (\beta_g \cdot \beta_h)\boldsymbol{v} \\ &= \beta_g(\beta_h\boldsymbol{v}) \\ &= \rho(g)(\rho(h)(\boldsymbol{v})).\end{aligned}$$

Since $\beta_{1_G} = 1_{kG}$, for any $\boldsymbol{v} \in V$, $\rho(1_G)(\boldsymbol{v}) = \beta_{1_G}\boldsymbol{v} = 1_{kG}\boldsymbol{v} = \boldsymbol{v}$. Hence ρ is a G-action.

Therefore, we can also construct a G-action from a kG-module.

□

4.3 Part C

Descibe the defining representation of the dihedral groups as algebra homomorphisms from the group algebra to the Endomorphism ring of $\mathbb{R}^2$.

Solution:

Let the rotations in dihedral group D_n be r_i where $1 \leq i < n-1$, the reflections in D_n be S_j where $1 \leq j \leq n$, we can define a canonical map:

$$\begin{aligned} f : kG &\longrightarrow \operatorname{End}_k \mathbb{R}^2 \\ \beta_{r_i} &\longmapsto \begin{pmatrix} \cos(\frac{2\pi i}{n}) & -\sin(\frac{2\pi i}{n}) \\ \sin(\frac{2\pi i}{n}) & \cos(\frac{2\pi i}{n}) \end{pmatrix} \\ \beta_{s_j} &\longmapsto \begin{pmatrix} \cos(\frac{2\pi j}{n}) & \sin(\frac{2\pi j}{n}) \\ \sin(\frac{2\pi j}{n}) & -\cos(\frac{2\pi j}{n}) \end{pmatrix}. \\ &test \end{aligned}$$

This maps forms a k-algebra homomorphism. Since $f(r_i)$ and $f(s_j)$ are all matrices, thus they are linear maps from $\mathbb{R}^2$ to $\mathbb{R}^2$. This also defines a representation since $f(r_i)$ and $f(s_i)$ are G-action.

5 Constructions with straight edge and compass

Let $\alpha = \cos(15^\circ)$.

5.1 Part A

Using the addition formulas for sine and cosine, find the irreducible polynomial of α over Q.

Solution:

$$\begin{aligned} cos(30^\circ) &= cos^2(15^\circ) - sin^2(15^\circ) \\ &= cos^2(15^\circ) - (1 - cos^2(15^\circ)) \\ &= 2\alpha^2 - 1. \end{aligned}$$

Hence, $\frac{\sqrt{3}}{2} = 2\alpha^2 - 1$, therefore, $\left(\frac{\sqrt{3}}{2}\right)^2 = \left(2\alpha^2 - 1\right)^2$. Simplify the equation and we get $16\alpha^4 - 16\alpha^2 + 1 = 0$. This is irreducible since it does not have rational root.

5.2 Part B

Show that the irreducible polynomial for α^2 over $\mathbb{Q}$ has degree 2.

Solution:

From the previous question, we know that $16(\alpha^2)^2 - 16\alpha^2 + 1$ is an irreducible polynomial for α^2 over $\mathbb{Q}$. Therefore, the irreducible polynomial for α^2 over $\mathbb{Q}$ has degree 2.

5.3 Part C

From here, argue that $\cos(15°)$ is constructible.

Solution:

Since the irreducible polynomial of α^2 over $\mathbb{Q}$ has degree 2, and it is algebraic over $\mathbb{Q}$, α^2 satisfies all the necessary conditions of a constructible number. We will construct α^2 in (f), hence it is constructible. Since α^2 is constructible, we can construct a right-angled triangle whose hypotenuse is of length $\frac{1+\alpha^2}{2}$ and one of the leg is of length $\frac{|1-\alpha^2|}{2}$. By Pythagorean theorem, the other leg in this right-angled triangle is of length α, hence α is constructible.

5.4 Part D

Assume now that $\cos(45°)$ has already been constructed. (How?) Find the irreducible polynomial of $\cos(45°)$ over $\mathbb{Q}[\cos(45°)]$.

Solution:

Fisrt, we show how to construct $\cos(45°)$ from segment AB of length 1 in Figure 1:

1. Draw the circle with center A through B and the circle with center B through A.
2. Draw a line perpendicular to AB through B, intersecting the circle with center B through A at point C and D.
3. Draw the segments AD and AC, intersecting the circle with center A through B at point E and F.
4. Draw the segment EF. Label the intersection point of AB and EF as H.
5. Then we have got $\cos(45°)$, which is the length of AH.

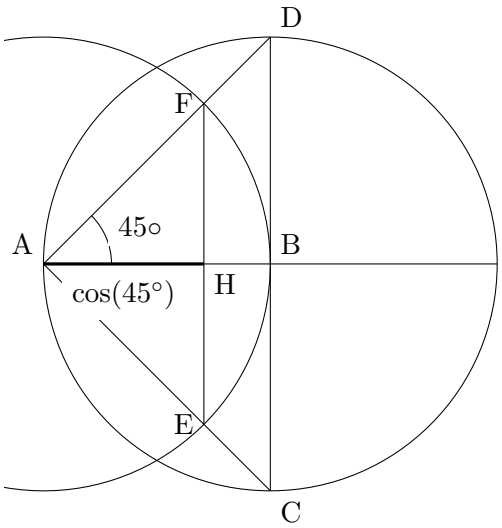

Figure 1: Construction of $\cos(45^\circ)$

Use the relation $15^\circ = 45^\circ - 30^\circ$, by the addition formula for sine and cosine, we have

$$\begin{aligned}\cos(15^\circ) &= \cos(45^\circ)\cos(30^\circ) + \sin(45^\circ)\sin(30^\circ) \\ &= \cos(45^\circ)\left(2\cos^2(15^\circ) - 1\right) + \cos(45^\circ)\frac{1}{2} \\ &= 2\cos(45^\circ)\cos^2(15^\circ) - \frac{1}{2}\cos(45^\circ).\end{aligned}$$

Simplify this euqation, we get

$$4\cos(45^\circ)\alpha^2 - 2\alpha - \cos(45^\circ) = 0.$$

The roots of this equation are not contained in $\mathbb{Q}[\cos(45^\circ)]$, hence it is irreducible over $\mathbb{Q}[\cos(45^\circ)]$.

5.5 Part E

Translate (d) in to a step by step construction, using straight-edge and compass, of a 15° angle from an already constructed 45° angle.

Solution:

Multiplying both sides of Equation 5.4 by $\cos(45^\circ)$, we have

$$\begin{aligned}4\cos^2(45^\circ)\alpha^2 - 2\cos(45^\circ)\alpha - \cos^2(45^\circ) &= 0 \\ 2\alpha^2 - 2cos(45^\circ)\alpha - \cos^2(45^\circ) &= 0 \\ \alpha^2 + \left(\alpha^2 - 2\cos(45^\circ) + \cos(45^\circ)\right) - 2\cos^2(45^\circ) &= 0 \\ \alpha^2 + \left(\alpha - \cos(45^\circ)\right)^2 &= 1.\end{aligned}$$

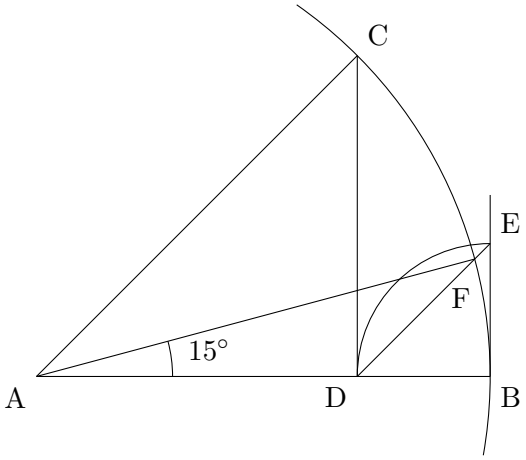

Figure 2: Construction of 15° from an already constructed 45°

This can be seen as the intersection of the circle $x^2 + y^2 = 1$ and the line $y = x - \cos(45°)$. Therefore, we get a way to construct 15° from 45°, which is shown in Figure 2.

Assume we have AB which is an segment of length 1, C which is a point on the circle with center A through B such that $\angle CAB = 45°$, then:

1. Draw a line CD perpendicular to AB, intersecting AB at D.
2. Draw a line perpendicular to AB through B.
3. Draw a circle with center B through D, intersecting the line perpendicular to AB through B at E.
4. Draw the segment DE, this is the line $y = x - \cos(45°)$. Label the intersection point of this segment and the circle with the center A as F.
5. Connect A and F. $\angle FAB = 15°$.

5.6 Part F

Translate (a) - (c) into a construction of a 15° angle from scratch (starting with two arbitrary distince points in the plane).

Solution:

Let $\beta = \alpha^2$. From (b), $16\beta^2 - 16\beta + 1 = 0$. Simplify this equation and we get $(2\beta - 1)^2 + \left(\frac{1}{2}\right)^2 = 1$. From this equation, we can conclude the construction of β, which is shown in Figure 3.

For any segment AB, we can draw a circle with the center A through B and another circle with the center B through A. Connecting two intersection

points, we will get a bisection of the sengment AB. By this method, we are able to get the midpoint of a segment, and we will skip this detail later.

Assume we have two points A and B on a plane, set the length of AB as 1, then:

1. Draw a circle with center A through B.
2. Draw the bisection of AB. Label the midpoint C and the intersection of the circle and the bisection as D. In $\triangle ACD$, the length of AC is $\frac{1}{2}$, the length of AD is 1, by the equation for β, the length of CD is $2\beta - 1$.
3. Get the midpoint of CD, denoted E. The length of CE is $\beta - \frac{1}{2}$
4. Draw a circle with center C through F. Then the length of EF is β.

Since the relation between α and β is $\alpha^2 = \beta$, we can transform this equation to $\left(\frac{1-\beta}{2}\right)^2 + \left(\frac{1+\beta}{2}\right)^2 = \alpha^2$. Hence, we can construct a right-angled triangle to get α, which is also shown in Figure 3.

1. Extend CF and draw a circle with the center F through C to get the intersection point of this circle and straight line CF. Call this intersection point H. The length of CF and FH are both $\frac{1}{2}$.
2. Find the midpoint of EF, call it I. Hence, the length of IF is $\frac{\beta}{2}$.
3. Draw a circle with center I through H, the radius of this circle is $\frac{\beta+1}{2}$. Extend AB and call the intersection point of the extending line and the circle with center I as J. The length of CI is $\frac{1-\beta}{2}$. The length of IJ is equal to the length of IH, which is $\frac{\beta+1}{2}$. Since this is a right-angled triangle, by Pythagorean theorem, the length of CJ is α.
4. Then find a point G on the extended AB such that the length of CG is 1. (Use the length of BC is $\frac{1}{2}$.)
5. Draw a circle with center C through G and draw a line perpendicular to CK through K. Call the intersection point K. $\angle KCG = 15°$.

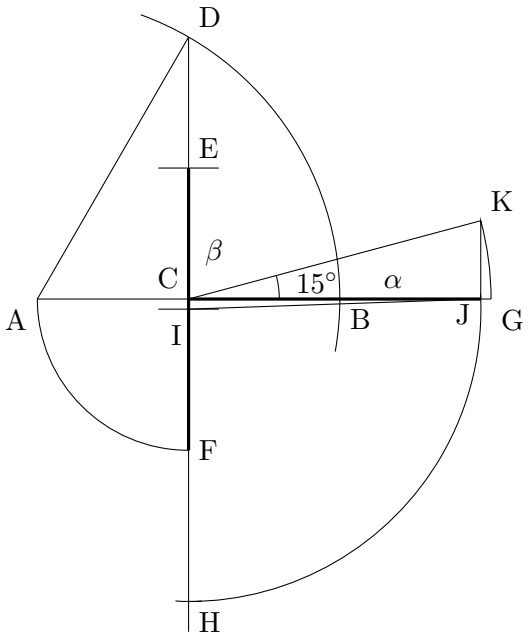

Figure 3: Construction of β and α

5.7 Part G

Write each of the above field extensions

$$\mathbb{Q} \subset \mathbb{Q}[\cos(45°)] \tag{1}$$
$$\mathbb{Q} \subset \mathbb{Q}[\cos(15°)] \tag{2}$$
$$\mathbb{Q} \subset \mathbb{Q}[\cos(15°)] \tag{3}$$
$$\mathbb{Q}[\cos(45°)] \subset \mathbb{Q}[\cos(15°)] \tag{4}$$
$$\mathbb{Q}[\cos(15°)] \subset \mathbb{Q}[\cos^2(15°)] \tag{5}$$

as quotient of the polynomial ring over the smaller field.

Solution:

The field extensions as quotient of the polynomial rings over the smaller

fields are the following:

$$\begin{aligned}
\mathbb{Q}[\cos(45^\circ)] &\cong \mathbb{Q}[x]/\left(x^2 - \frac{1}{2}\right) \\
\mathbb{Q}[\cos(15^\circ)] &\cong \mathbb{Q}[x]/\left(x^4 - x^2 + \frac{1}{16}\right) \\
\mathbb{Q}[\cos^2(15^\circ)] &\cong \mathbb{Q}[x]/\left(x^2 - x + \frac{1}{16}\right) \\
\mathbb{Q}[\cos(15\circ)] &\cong \mathbb{Q}[\cos(45^\circ)][x]/\left(x^2 - \frac{1}{2\cos(45^\circ)}x - \frac{1}{4}\right) \\
\mathbb{Q}[\cos(15^\circ)] &\cong \mathbb{Q}[\cos^2(15^\circ)][x]/\left(x^2 - \cos^2(15^\circ)\right).
\end{aligned}$$