Solving Polynomial Systems Using Linear Algebra

Martin Kreuzer

Universität Passau

martin.kreuzer@uni-passau.de

Introduction to Computer Algebra and Applications

Douala, Oct. 9, 2017

The following is joint work with **Lorenzo Robbiano** (Genova, Italy) and contained in the new book (which appeared in 2016):

Computational Linear and
Commutative **A**lgebra

The following is joint work with **Lorenzo Robbiano** (Genova, Italy) and contained in the new book (which appeared in 2016):

Computational Linear and
Commutative **A**lgebra

Contents

1. Endomorphisms

The following is joint work with **Lorenzo Robbiano** (Genova, Italy) and contained in the new book (which appeared in 2016):

Computational Linear and
Commutative **A**lgebra

Contents

1. **Endomorphisms**
2. **Commuting Families**

The following is joint work with **Lorenzo Robbiano** (Genova, Italy) and contained in the new book (which appeared in 2016):

Computational Linear and
Commutative **A**lgebra

Contents

1. **Endomorphisms**
2. **Commuting Families**
3. **The Eigenvalue Method**

The following is joint work with **Lorenzo Robbiano** (Genova, Italy) and contained in the new book (which appeared in 2016):

Computational Linear and
Commutative **A**lgebra

Contents

1 – Endomorphisms

Proofs involving matrices
can be shortened by 50%

1 – Endomorphisms

Proofs involving matrices
can be shortened by 50%
if one throws the matrices out.
(Emil Artin)

1 – Endomorphisms

Proofs involving matrices
can be shortened by 50%
if one throws the matrices out.
(Emil Artin)

Setting: K field

V finite dimensional K-vector space, $d := \dim_K(V)$

$\varphi :\ V \longrightarrow V$ endomorphism of V

1 – Endomorphisms

Proofs involving matrices
can be shortened by 50%
if one throws the matrices out.
(Emil Artin)

Setting: K field

V finite dimensional K-vector space, $d := \dim_K(V)$

$\varphi : \; V \longrightarrow V$ endomorphism of V

After choosing a K-basis B of V, we can represent φ by a matrix A in $\mathrm{Mat}_d(K)$.

The Minimal Polynomial

Definition 1.1 The polynomial
$\chi_\varphi(z) = \det(z \cdot \mathrm{id}_V - \varphi) = \det(z \cdot I_n - A)$ is called the **characteristic polynomial** of φ.

The characteristic polynomial has degree d. Its zeros are called the **eigenvalues** of φ.

The Minimal Polynomial

Definition 1.1 The polynomial
$\chi_\varphi(z) = \det(z \cdot \mathrm{id}_V - \varphi) = \det(z \cdot I_n - A)$ is called the **characteristic polynomial** of φ.

The characteristic polynomial has degree d. Its zeros are called the **eigenvalues** of φ.

Definition 1.2 The monic polynomial $\mu_\varphi(z)$ in $K[z]$ of smallest degree such that $\mu_\varphi(\varphi) = 0$ is called the **minimal polynomial** of φ.

The Minimal Polynomial

Definition 1.1 The polynomial $\chi_\varphi(z) = \det(z \cdot \mathrm{id}_V - \varphi) = \det(z \cdot I_n - A)$ is called the **characteristic polynomial** of φ.

The characteristic polynomial has degree d. Its zeros are called the **eigenvalues** of φ.

Definition 1.2 The monic polynomial $\mu_\varphi(z)$ in $K[z]$ of smallest degree such that $\mu_\varphi(\varphi) = 0$ is called the **minimal polynomial** of φ.

The set of all polynomials $f \in K[z]$ such that $f(\varphi) = 0$ is a principal ideal. Its unique monic generator is $\mu_\varphi(z)$.

Thus $\mu_\varphi(z)$ is the unique monic generator of the kernel of the K-algebra homomorphism $K[z] \longrightarrow \mathrm{Mat}_d(K)$ given by $z \mapsto \varphi$.

Theorem 1.3 **(Cayley-Hamilton Theorem)**

The characteristic polynomial of φ *satisfies* $\chi_\varphi(\varphi) = 0$.

In particular, it is a multiple of $\mu_\varphi(z)$.

Theorem 1.3 **(Cayley-Hamilton Theorem)**
The characteristic polynomial of φ *satisfies* $\chi_\varphi(\varphi) = 0$*.*

In particular, it is a multiple of $\mu_\varphi(z)$*.*

Even more is true: the polynomials $\chi_\varphi(z)$ and $\mu_\varphi(z)$ have the same irreducible factors. So, if we write

$$\mu_\varphi(z) \;=\; p_1(z)^{m_1} \cdots p_s(z)^{m_s}$$

with irreducible monic polynomials $p_1(z), \ldots, p_s(z)$ and with $m_i \geq 1$, then these polynomials are also the irreducible factors of $\chi_\varphi(z)$. They are called the **eigenfactors** of φ.

Theorem 1.3 (Cayley-Hamilton Theorem)
The characteristic polynomial of φ satisfies $\chi_\varphi(\varphi) = 0$.

In particular, it is a multiple of $\mu_\varphi(z)$.

Even more is true: the polynomials $\chi_\varphi(z)$ and $\mu_\varphi(z)$ have the same irreducible factors. So, if we write

$$\mu_\varphi(z) \;=\; p_1(z)^{m_1} \cdots p_s(z)^{m_s}$$

with irreducible monic polynomials $p_1(z), \ldots, p_s(z)$ and with $m_i \geq 1$, then these polynomials are also the irreducible factors of $\chi_\varphi(z)$. They are called the **eigenfactors** of φ.

Remark 1.4 An **eigenvalue** $\lambda \in K$ of φ corresponds to an eigenfactor $p_i(z) = z - \lambda$.

Algorithm 1.5 **(Minimal Polynomials via Reduction)**
Let $\varphi \in \mathrm{End}_K(V)$*, and let* $A \in \mathrm{Mat}_d(K)$ *be a matrix representing* φ *with respect to a* K*-basis of* V*. Then the following algorithm computes the minimal polynomial* $\mu_\varphi(z)$ *in* $K[z]$*.*

Algorithm 1.5 **(Minimal Polynomials via Reduction)**
Let $\varphi \in \mathrm{End}_K(V)$*, and let* $A \in \mathrm{Mat}_d(K)$ *be a matrix representing* φ *with respect to a* K*-basis of* V*. Then the following algorithm computes the minimal polynomial* $\mu_\varphi(z)$ *in* $K[z]$*.*

(1) *Let* $L = \{I_d\}$*.*

Algorithm 1.5 **(Minimal Polynomials via Reduction)**
Let $\varphi \in \mathrm{End}_K(V)$, and let $A \in \mathrm{Mat}_d(K)$ be a matrix representing φ with respect to a K-basis of V. Then the following algorithm computes the minimal polynomial $\mu_\varphi(z)$ in $K[z]$.

(1) *Let $L = \{I_d\}$.*

(2) *For $i = 1, 2, \ldots,$ compute the matrix A^i and check whether it is K-linearly dependent on the matrices in L. If this is not the case, append A^i to L and continue with the next number i.*

Algorithm 1.5 **(Minimal Polynomials via Reduction)**
Let $\varphi \in \mathrm{End}_K(V)$, *and let* $A \in \mathrm{Mat}_d(K)$ *be a matrix representing* φ *with respect to a* K*-basis of* V. *Then the following algorithm computes the minimal polynomial* $\mu_\varphi(z)$ *in* $K[z]$.

(1) *Let* $L = \{I_d\}$.

(2) *For* $i = 1, 2, \ldots,$ *compute the matrix* A^i *and check whether it is* K*-linearly dependent on the matrices in* L. *If this is not the case, append* A^i *to* L *and continue with the next number* i.

(3) *If there exist* $c_0, \ldots, c_{i-1} \in K$ *such that* $A^i = c_{i-1}A^{i-1} + \cdots + c_1 A + c_0 I_d$ *then return the polynomial* $\mu_\varphi(z) = z^i - c_{i-1}z^{i-1} - \cdots - c_0$ *and stop.*

Algorithm 1.6 **(Minimal Polynomials via Elimination)**
Let $\varphi \in \mathrm{End}_K(V)$, *let* $f \in K[z]$, *and let* $\psi = f(\varphi)$. *Given the minimal polynomial of* φ, *the following algorithm computes the minimal polynomial of* ψ.

Algorithm 1.6 **(Minimal Polynomials via Elimination)**
Let $\varphi \in \mathrm{End}_K(V)$, *let* $f \in K[z]$, *and let* $\psi = f(\varphi)$. *Given the minimal polynomial of* φ, *the following algorithm computes the minimal polynomial of* ψ.

(1) *Form the polynomial ring* $K[u, z]$ *and the ideal* $I_\psi = \langle \mu_\varphi(u),\, z - f(u) \rangle$ *in* $K[u, z]$.

Algorithm 1.6 (Minimal Polynomials via Elimination)
Let $\varphi \in \mathrm{End}_K(V)$*, let* $f \in K[z]$*, and let* $\psi = f(\varphi)$*. Given the minimal polynomial of* φ*, the following algorithm computes the minimal polynomial of* ψ*.*

(1) *Form the polynomial ring* $K[u, z]$ *and the ideal* $I_\psi = \langle \mu_\varphi(u),\, z - f(u) \rangle$ *in* $K[u, z]$*.*

(2) *Compute the elimination ideal* $J_\psi = I_\psi \cap K[z]$*.*

Algorithm 1.6 **(Minimal Polynomials via Elimination)**
Let $\varphi \in \mathrm{End}_K(V)$*, let* $f \in K[z]$*, and let* $\psi = f(\varphi)$*. Given the minimal polynomial of* φ*, the following algorithm computes the minimal polynomial of* ψ*.*

(1) *Form the polynomial ring* $K[u, z]$ *and the ideal* $I_\psi = \langle \mu_\varphi(u),\, z - f(u) \rangle$ *in* $K[u, z]$*.*

(2) *Compute the elimination ideal* $J_\psi = I_\psi \cap K[z]$*.*

(3) *Return the monic generator of* J_ψ*.*

Example 1.7 Let $K = \mathbb{Q}$, and let φ be the endomorphism of $V = K^4$ defined by the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

(a) First we use Algorithm 1.5 to compute $\mu_\varphi(z)$ via reduction. During the first three iterations of the algorithm it turns out that $\{I_4, A, A^2, A^3\}$ is K-linearly independent. Then, in the fourth iteration, we discover the relation $A^4 = -A^3 + A^2 - I_4$, and therefore we get $\mu_\varphi(z) = z^4 + z^3 - z^2 + 1$.

Example 1.7 Let $K = \mathbb{Q}$, and let φ be the endomorphism of $V = K^4$ defined by the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

(a) First we use Algorithm 1.5 to compute $\mu_\varphi(z)$ via reduction. During the first three iterations of the algorithm it turns out that $\{I_4, A, A^2, A^3\}$ is K-linearly independent. Then, in the fourth iteration, we discover the relation $A^4 = -A^3 + A^2 - I_4$, and therefore we get $\mu_\varphi(z) = z^4 + z^3 - z^2 + 1$.

(b) Now let $\psi = \varphi^2 - \varphi$. To compute $\mu_\psi(z)$ using Algorithm 1.6, we form the ideal $I_\psi = \langle u^4 + u^3 - u^2 + 1,\ z - (u^2 - u)\rangle$ in $K[u, z]$ and compute the monic generator of $J_\psi = I_\psi \cap K[z]$. The result is $\mu_\psi(z) \ = \ z^4 - 4\,z^3 + z^2 + 5\,z + 2 \ = \ (z-2)(z^3 - 2z^2 - 3z - 1)$.

Eigenspaces

Recall: For an eigenvalue $\lambda \in K$ of φ, the corresponding eigenspace is defined by

$$\mathrm{Eig}(\varphi, \lambda) = \mathrm{Ker}(\varphi - \lambda\, \mathrm{id}_V)$$

Eigenspaces

Recall: For an eigenvalue $\lambda \in K$ of φ, the corresponding eigenspace is defined by

$$\mathrm{Eig}(\varphi, \lambda) = \mathrm{Ker}(\varphi - \lambda\ \mathrm{id}_V)$$

Example 1.8 The 90^o rotation $\varphi : \mathbb{Q}^2 \longrightarrow \mathbb{Q}^2$ given by $M(\varphi) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ satisfies $\mu_\varphi(z) = \chi_\varphi(z) = z^2 + 1$.

Eigenspaces

Recall: For an eigenvalue $\lambda \in K$ of φ, the corresponding eigenspace is defined by

$$\mathrm{Eig}(\varphi, \lambda) = \mathrm{Ker}(\varphi - \lambda\, \mathrm{id}_V)$$

Example 1.8 The 90^o rotation $\varphi : \mathbb{Q}^2 \longrightarrow \mathbb{Q}^2$ given by $M(\varphi) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ satisfies $\mu_\varphi(z) = \chi_\varphi(z) = z^2 + 1$.

Question: How can we define eigenspaces when the eigenfactors $p_i(z)$ are not linear?

Eigenspaces

Recall: For an eigenvalue $\lambda \in K$ of φ, the corresponding eigenspace is defined by

$$\mathrm{Eig}(\varphi, \lambda) = \mathrm{Ker}(\varphi - \lambda \, \mathrm{id}_V)$$

Example 1.8 The 90^o rotation $\varphi : \mathbb{Q}^2 \longrightarrow \mathbb{Q}^2$ given by $M(\varphi) = \binom{0\ -1}{1\ \ \ 0}$ satisfies $\mu_\varphi(z) = \chi_\varphi(z) = z^2 + 1$.

Question: How can we define eigenspaces when the eigenfactors $p_i(z)$ are not linear?

Definition 1.9 $\mathrm{Eig}(\varphi, p_i(z)) = \mathrm{Ker}(p_i(\varphi))$ is called the **eigenspace** of φ associated to the eigenfactor $p_i(z)$.

Generalized Eigenspaces

Recall: Given an eigenvalue $\lambda \in K$ of φ,

$$\mathrm{Gen}(\varphi, \lambda) = \bigcup_{i \geq 1} \mathrm{Ker}(\varphi - \lambda\, \mathrm{id}_V)^i$$

is called the **generalized eigenspace** or the **principal space** associated to λ.

Generalized Eigenspaces

Recall: Given an eigenvalue $\lambda \in K$ of φ,

$$\mathrm{Gen}(\varphi, \lambda) = \bigcup_{i \geq 1} \mathrm{Ker}(\varphi - \lambda \, \mathrm{id}_V)^i$$

is called the **generalized eigenspace** or the **principal space** associated to λ.

Recall: If $\chi_\varphi(z)$ is a product of linear factors, then the vector space V is the direct sum of the generalized eigenspaces.

Generalized Eigenspaces

Recall: Given an eigenvalue $\lambda \in K$ of φ,

$$\mathrm{Gen}(\varphi, \lambda) = \bigcup_{i \geq 1} \mathrm{Ker}(\varphi - \lambda \,\mathrm{id}_V)^i$$

is called the **generalized eigenspace** or the **principal space** associated to λ.

Recall: If $\chi_\varphi(z)$ is a product of linear factors, then the vector space V is the direct sum of the generalized eigenspaces.

Definition 1.10 **(a)** $\mathrm{BigKer}(\varphi) = \bigcup_{i \geq 1} \mathrm{Ker}(\varphi^i)$ is called the **big kernel** of φ.

(b) $\mathrm{SmIm}(\varphi) = \bigcap_{i \geq 1} \mathrm{Im}(\varphi^i)$ is called the **small image** of φ.

Recall: The vector space V is in general **not** the direct sum of $\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$.

Recall: The vector space V is in general **not** the direct sum of $\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$.

Proposition 1.11 **(Fittings Lemma)**

(a) $\mathrm{Ker}(\varphi) \subset \mathrm{Ker}(\varphi^2) \subset \cdots \subset \mathrm{Ker}(\varphi^s) = \mathrm{Ker}(\varphi^{s+1}) = \cdots$
$\cdots = \mathrm{BigKer}(\varphi)$

(b) $\mathrm{Im}(\varphi) \supset \mathrm{Im}(\varphi^2) \supset \cdots \supset \mathrm{Im}(\varphi^s) = \mathrm{Im}(\varphi^{s+1}) = \cdots$
$\cdots = \mathrm{SmIm}(\varphi)$

(c) $V = \mathrm{BigKer}(\varphi) \oplus \mathrm{SmIm}(\varphi)$

Let $\mu_\varphi(z) = p_1^{m_1} \cdots p_s^{m_s}$ be the factorization of $\mu_\varphi(z)$.

Let $\mu_\varphi(z) = p_1^{m_1} \cdots p_s^{m_s}$ be the factorization of $\mu_\varphi(z)$.

Definition 1.12 For every eigenfactor $p_i(z)$, the space $\mathrm{Gen}(\varphi, p_i(z)) = \mathrm{BigKer}(p_i(\varphi))$ is called the **generalized eigenspace** of φ associated to $p_i(z)$.

Let $\mu_\varphi(z) = p_1^{m_1} \cdots p_s^{m_s}$ be the factorization of $\mu_\varphi(z)$.

Definition 1.12 For every eigenfactor $p_i(z)$, the space $\mathrm{Gen}(\varphi, p_i(z)) = \mathrm{BigKer}(p_i(\varphi))$ is called the **generalized eigenspace** of φ associated to $p_i(z)$.

Theorem 1.13 **(Primary Decomposition Theorem)**
In the above setting we have

$$V \;=\; \mathrm{Gen}(\varphi, p_1(z)) \oplus \cdots \oplus \mathrm{Gen}(\varphi, p_s(z))$$

where $\mathrm{Gen}(\varphi, p_i(z)) = \mathrm{Ker}(p_i(\varphi)^{m_i})$.

Example 1.14 Let $V = \mathbb{Q}^6$, and let $\varphi \in \mathrm{End}_{\mathbb{Q}}(V)$ be defined by

$$A = \begin{pmatrix} -12 & -16 & 3 & -4 & -8 & -20 \\ 78 & 104 & 18 & 26 & 52 & 130 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -237 & -316 & -72 & -79 & -158 & -395 \\ 78 & 104 & 18 & 26 & 52 & 130 \\ 36 & 48 & -9 & 12 & 24 & 60 \end{pmatrix}$$

with respect to the canonical basis.

Example 1.14 Let $V = \mathbb{Q}^6$, and let $\varphi \in \mathrm{End}_{\mathbb{Q}}(V)$ be defined by

$$A = \begin{pmatrix} -12 & -16 & 3 & -4 & -8 & -20 \\ 78 & 104 & 18 & 26 & 52 & 130 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -237 & -316 & -72 & -79 & -158 & -395 \\ 78 & 104 & 18 & 26 & 52 & 130 \\ 36 & 48 & -9 & 12 & 24 & 60 \end{pmatrix}$$

with respect to the canonical basis.

Then we have $\mu_\varphi(z) = z^3 - 125\,z^2 = (z - 125)\,z^2$.

(a) $\mathrm{Ker}(\varphi - 125\ \mathrm{id}_V) = \langle v_1 \rangle$, where $v_1 = (4, -26,\ 0, 79, -26, -12)$.

(a) $\operatorname{Ker}(\varphi - 125\ \mathrm{id}_V) = \langle v_1 \rangle$, where $v_1 = (4, -26,\ 0, 79, -26, -12)$.

(b) A $\mathbb{Q}$-basis of $\operatorname{Ker}(\varphi^2)$ is $(v_2, v_3, v_4, v_5, v_6)$, where

$$v_2 = (4, -3, 0, 0, 0, 0), \quad v_3 = (1, 0, 0, -3, 0, 0), \quad v_4 = e_3$$
$$v_5 = (2, 0, 0, 0, -3, 0), \quad v_6 = (5, 0, 0, 0, 0, -3)$$

(a) $\mathrm{Ker}(\varphi - 125\ \mathrm{id}_V) = \langle v_1 \rangle$, where $v_1 = (4, -26,\ 0, 79, -26, -12)$.

(b) A $\mathbb{Q}$-basis of $\mathrm{Ker}(\varphi^2)$ is $(v_2, v_3, v_4, v_5, v_6)$, where

$$v_2 = (4, -3, 0, 0, 0, 0), \quad v_3 = (1, 0, 0, -3, 0, 0), \quad v_4 = e_3$$
$$v_5 = (2, 0, 0, 0, -3, 0), \quad v_6 = (5, 0, 0, 0, 0, -3)$$

According to the theorem, the tuple $(v_1, v_2, v_3, v_4, v_5, v_6)$ is a $\mathbb{Q}$-basis of V.

2 – Commuting Families

I read that you can make chocolate fondue from chocolate leftovers. I am confused.

2 – Commuting Families

I read that you can make chocolate fondue from chocolate leftovers. I am confused.

What are chocolate leftovers?

2 – Commuting Families

I read that you can make chocolate fondue from chocolate leftovers. I am confused. What are chocolate leftovers?

Recall: If a set of diagonalizable endomorphisms commutes, then there exists a **simultaneous diagonalization**.

Question: Is there also a simultaneous decomposition into generalized eigenspaces?

2 – Commuting Families

I read that you can make chocolate fondue from chocolate leftovers. I am confused. What are chocolate leftovers?

Recall: If a set of diagonalizable endomorphisms commutes, then there exists a **simultaneous diagonalization**.

Question: Is there also a simultaneous decomposition into generalized eigenspaces?

Definition 2.1 Given a tuple $\Phi = (\varphi_1, \ldots, \varphi_n)$ of pairwise commuting endomorphisms of V, the K-algebra $\mathcal{F} = K[\Phi] = K[\varphi_1, \ldots, \varphi_n]$ is called a **commuting family**.

Joint Eigenspaces

Question: How do we define "simultaneous" eigenspaces for a commuting family?

Joint Eigenspaces

Question: How do we define "simultaneous" eigenspaces for a commuting family?

Definition 2.2 **(a)** A set $\mathcal{C} = \{p_\varphi(z) \mid \varphi \in \mathcal{F}\}$ is called a **coherent family of eigenfactors** of $\mathcal{F}$ if $\bigcap_{\varphi \in \mathcal{F}} \mathrm{Eig}(\varphi, p_\varphi(z)) \neq \{0\}$.

Joint Eigenspaces

Question: How do we define "simultaneous" eigenspaces for a commuting family?

Definition 2.2 **(a)** A set $\mathcal{C} = \{p_\varphi(z) \mid \varphi \in \mathcal{F}\}$ is called a **coherent family of eigenfactors** of $\mathcal{F}$ if $\bigcap_{\varphi\in\mathcal{F}} \mathrm{Eig}(\varphi, p_\varphi(z)) \neq \{0\}$.

(b) In this case, the intersection is called a **joint eigenspace** of $\mathcal{F}$

Joint Eigenspaces

Question: How do we define "simultaneous" eigenspaces for a commuting family?

Definition 2.2 **(a)** A set $\mathcal{C} = \{p_\varphi(z) \mid \varphi \in \mathcal{F}\}$ is called a **coherent family of eigenfactors** of $\mathcal{F}$ if $\bigcap_{\varphi \in \mathcal{F}} \mathrm{Eig}(\varphi, p_\varphi(z)) \neq \{0\}$.

(b) In this case, the intersection is called a **joint eigenspace** of $\mathcal{F}$

(c) and the intersection $\bigcap_{\varphi \in \mathcal{F}} \mathrm{Gen}(\varphi, p_\varphi(z))$ is called a **joint generalized eigenspace** of $\mathcal{F}$.

Definition 2.3 Given an ideal I in a commuting family $\mathcal{F}$,
$\mathrm{Ker}(I) = \bigcap_{\varphi \in I} \mathrm{Ker}(\varphi)$ is called the **kernel** of I and
$\mathrm{BigKer}(I) = \bigcap_{\varphi \in I} \mathrm{BigKer}(\varphi)$ is called the **big kernel** of I.

Definition 2.3 Given an ideal I in a commuting family $\mathcal{F}$, $\operatorname{Ker}(I) = \bigcap_{\varphi \in I} \operatorname{Ker}(\varphi)$ is called the **kernel** of I and $\operatorname{BigKer}(I) = \bigcap_{\varphi \in I} \operatorname{BigKer}(\varphi)$ is called the **big kernel** of I.

Theorem 2.4 **(Joint Generalized Eigenspace Decomposition)** *Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the maximal ideals of $\mathcal{F}$.*

(a) $V = \operatorname{BigKer}(\mathfrak{m}_1) \oplus \cdots \oplus \operatorname{BigKer}(\mathfrak{m}_s)$

(b) *The joint eigenspaces of $\mathcal{F}$ are* $\operatorname{Ker}(\mathfrak{m}_1), \ldots, \operatorname{Ker}(\mathfrak{m}_s)$.

(c) *The joint generalized eigenspaces of $\mathcal{F}$ are* $\operatorname{BigKer}(\mathfrak{m}_1), \ldots, \operatorname{BigKer}(\mathfrak{m}_s)$.

Algorithm 2.5 (Computing the Kernel of an Ideal)
Let $I = \langle \psi_1, \ldots, \psi_s \rangle$ be an ideal of $\mathcal{F}$, and for $i \in \{1, \ldots, s\}$ let $A_i \in \mathrm{Mat}_d(V)$ be the matrix representing ψ_i with respect to a fixed K-basis of V. Then the following algorithm computes the kernel of I.

Algorithm 2.5 **(Computing the Kernel of an Ideal)**

Let $I = \langle \psi_1, \ldots, \psi_s \rangle$ *be an ideal of* $\mathcal{F}$*, and for* $i \in \{1, \ldots, s\}$ *let* $A_i \in \mathrm{Mat}_d(V)$ *be the matrix representing* ψ_i *with respect to a fixed* K*-basis of* V*. Then the following algorithm computes the kernel of* I*.*

(1) *Form the block column matrix* $C = \mathrm{Col}(A_1, \ldots, A_s)$ *by putting* $A_1, \ldots, A_s$ *into a column of matrices.*

Algorithm 2.5 (Computing the Kernel of an Ideal)
Let $I = \langle \psi_1, \ldots, \psi_s \rangle$ *be an ideal of* $\mathcal{F}$, *and for* $i \in \{1, \ldots, s\}$ *let* $A_i \in \mathrm{Mat}_d(V)$ *be the matrix representing* ψ_i *with respect to a fixed* K*-basis of* V. *Then the following algorithm computes the kernel of* I.

(1) *Form the block column matrix* $C = \mathrm{Col}(A_1, \ldots, A_s)$ *by putting* $A_1, \ldots, A_s$ *into a column of matrices.*

(2) *Compute a system of generators of* $\mathrm{Ker}(C)$ *and return the corresponding vectors of* V.

Algorithm 2.5 **(Computing the Kernel of an Ideal)**
Let $I = \langle \psi_1, \ldots, \psi_s \rangle$ *be an ideal of* $\mathcal{F}$*, and for* $i \in \{1, \ldots, s\}$ *let* $A_i \in \mathrm{Mat}_d(V)$ *be the matrix representing* ψ_i *with respect to a fixed* K*-basis of* V*. Then the following algorithm computes the kernel of* I*.*

(1) *Form the block column matrix* $C = \mathrm{Col}(A_1, \ldots, A_s)$ *by putting* $A_1, \ldots, A_s$ *into a column of matrices.*

(2) *Compute a system of generators of* $\mathrm{Ker}(C)$ *and return the corresponding vectors of* V*.*

Example 2.6 Let $K = \mathbb{Q}$, let $V = K^4$ and let φ_1, φ_2 be the endomorphisms of V represented by the matrices

$$A_1 = \begin{pmatrix} 0 & \frac{5}{2} & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & \frac{5}{2} & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

From $A_1 A_2 = A_2 A_1$ it follows that $\mathcal{F} = K[\varphi_1, \varphi_2]$ is a commuting family.

$$A_1 = \begin{pmatrix} 0 & \frac{5}{2} & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & \frac{5}{2} & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

From $A_1 A_2 = A_2 A_1$ it follows that $\mathcal{F} = K[\varphi_1, \varphi_2]$ is a commuting family. Let I be the ideal of $\mathcal{F}$ generated by $\{\varphi_1^2 - 5\,\mathrm{id}_V,\ \varphi_2 - \mathrm{id}_V\}$. The matrices representing the generators of I are

$$M_1 = \begin{pmatrix} -\frac{5}{2} & 0 & \frac{5}{2} & \frac{5}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -5 & 0 \\ \frac{5}{2} & 0 & \frac{5}{2} & -\frac{5}{2} \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

We form the block column matrix $C = \mathrm{Col}(M_1, M_2)$. This is a matrix of size 8×4 whose rank is 2. Hence we get $\mathrm{Ker}(I) = \mathrm{Ker}(C) = \langle e_2,\ e_1 + e_4 \rangle$.

Example 2.7 Let us consider the two matrices

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

For $i = 1, 2$, let φ_i be the endomorphism of $V = \mathbb{Q}^6$ represented by A_i with respect to the canonical basis, and let $\Phi = (\varphi_1, \varphi_2)$.

Example 2.7 Let us consider the two matrices

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

For $i = 1, 2$, let φ_i be the endomorphism of $V = \mathbb{Q}^6$ represented by A_i with respect to the canonical basis, and let $\Phi = (\varphi_1, \varphi_2)$.

The family $K[\varphi_1, \varphi_2]$ is a commuting family. It has two maximal ideals, namely $\mathfrak{m}_1 = \langle \varphi_1 \rangle$ and $\mathfrak{m}_2 = \langle \varphi_1 - \mathrm{id}_V \rangle$. By the theorem, it follows that V is the direct sum of the two joint generalized eigenspaces $\mathrm{BigKer}(\mathfrak{m}_1)$ and $\mathrm{BigKer}(\mathfrak{m}_2)$.

First we calculate $\mathrm{BigKer}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1^2)$. This is the 4-dimensional vector subspace of V given by

$$\mathrm{BigKer}(\mathfrak{m}_1) = \langle (1,0,0,-1,0,0),(0,1,0,-1,0,0),\\ (0,0,1,0,0,-1),(0,0,0,0,1,-1)\rangle$$

First we calculate $\mathrm{BigKer}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1^2)$. This is the 4-dimensional vector subspace of V given by

$$\mathrm{BigKer}(\mathfrak{m}_1) = \langle (1,0,0,-1,0,0), (0,1,0,-1,0,0), (0,0,1,0,0,-1), (0,0,0,0,1,-1) \rangle$$

The corresponding joint eigenspace is $\mathrm{Ker}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1)$ which is the 2-dimensional vector subspace of V given by

$$\mathrm{Ker}(\mathfrak{m}_1) \;=\; \langle (0,1,0,-1,0,0),\ (0,0,0,0,1,-1) \rangle$$

First we calculate $\mathrm{BigKer}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1^2)$. This is the 4-dimensional vector subspace of V given by

$$\mathrm{BigKer}(\mathfrak{m}_1) = \langle (1,0,0,-1,0,0), (0,1,0,-1,0,0), (0,0,1,0,0,-1), (0,0,0,0,1,-1) \rangle$$

The corresponding joint eigenspace is $\mathrm{Ker}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1)$ which is the 2-dimensional vector subspace of V given by

$$\mathrm{Ker}(\mathfrak{m}_1) \;=\; \langle (0,1,0,-1,0,0),\; (0,0,0,0,1,-1) \rangle$$

Next we compute the second joint generalized eigenspace $\mathrm{BigKer}(\mathfrak{m}_2)$ and find that

$$\mathrm{BigKer}(\mathfrak{m}_2) \;=\; \mathrm{Ker}(\mathfrak{m}_2) \;=\; \langle (0,0,0,1,0,0),\; (0,0,0,0,0,1) \rangle$$

First we calculate $\mathrm{BigKer}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1^2)$. This is the 4-dimensional vector subspace of V given by

$$\mathrm{BigKer}(\mathfrak{m}_1) = \langle (1,0,0,-1,0,0), (0,1,0,-1,0,0), \\ (0,0,1,0,0,-1), (0,0,0,0,1,-1) \rangle$$

The corresponding joint eigenspace is $\mathrm{Ker}(\mathfrak{m}_1) = \mathrm{Ker}(\varphi_1)$ which is the 2-dimensional vector subspace of V given by

$$\mathrm{Ker}(\mathfrak{m}_1) \;=\; \langle (0,1,0,-1,0,0),\; (0,0,0,0,1,-1) \rangle$$

Next we compute the second joint generalized eigenspace $\mathrm{BigKer}(\mathfrak{m}_2)$ and find that

$$\mathrm{BigKer}(\mathfrak{m}_2) \;=\; \mathrm{Ker}(\mathfrak{m}_2) \;=\; \langle (0,0,0,1,0,0),\; (0,0,0,0,0,1) \rangle$$

At this point it is easy to see that, indeed, the vector space V has a direct sum decomposition $V = \mathrm{BigKer}(\mathfrak{m}_1) \oplus \mathrm{BigKer}(\mathfrak{m}_2)$.

$\mathfrak{m}$-Eigenfactors

Let $\varphi \in \mathcal{F}$ and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{F}$.

Definition 2.8 Consider the K-algebra homomorphism $K[z] \longrightarrow \mathcal{F}/\mathfrak{m}$ given by $z \mapsto \varphi$. If it is not injective, its kernel is a principal ideal generated by an irreducible monic polynomial $p_{\mathfrak{m},\varphi}(z)$. This polynomial is called the **$\mathfrak{m}$-eigenfactor** of φ.

$\mathfrak{m}$-Eigenfactors

Let $\varphi \in \mathcal{F}$ and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{F}$.

Definition 2.8 Consider the K-algebra homomorphism $K[z] \longrightarrow \mathcal{F}/\mathfrak{m}$ given by $z \mapsto \varphi$. If it is not injective, its kernel is a principal ideal generated by an irreducible monic polynomial $p_{\mathfrak{m},\varphi}(z)$. This polynomial is called the **$\mathfrak{m}$-eigenfactor** of φ.

(a) Every eigenfactor of φ is of the form $p_{\mathfrak{m},\varphi}(z)$ for some maximal ideal $\mathfrak{m}$ of $\mathcal{F}$.

$\mathfrak{m}$-Eigenfactors

Let $\varphi \in \mathcal{F}$ and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{F}$.

Definition 2.8 Consider the K-algebra homomorphism $K[z] \longrightarrow \mathcal{F}/\mathfrak{m}$ given by $z \mapsto \varphi$. If it is not injective, its kernel is a principal ideal generated by an irreducible monic polynomial $p_{\mathfrak{m},\varphi}(z)$. This polynomial is called the **$\mathfrak{m}$-eigenfactor** of φ.

(a) Every eigenfactor of φ is of the form $p_{\mathfrak{m},\varphi}(z)$ for some maximal ideal $\mathfrak{m}$ of $\mathcal{F}$.

(b) A maximal ideal $\mathfrak{m}$ of $\mathcal{F} = K[\varphi_1, \ldots, \varphi_s]$ is **linear**, i.e. we have $\mathfrak{m} = \langle \varphi_1 - \lambda_1 \operatorname{id}_V, \ldots, \varphi_s - \lambda_s \operatorname{id}_V \rangle$, if and only if the $\mathfrak{m}$-eigenfactor of φ_i is linear $p_{\mathfrak{m},\varphi_i}(z) = z - \lambda_i$ for $i = 1, \ldots, s$.

$\mathfrak{m}$-Eigenfactors

Let $\varphi \in \mathcal{F}$ and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{F}$.

Definition 2.8 Consider the K-algebra homomorphism $K[z] \longrightarrow \mathcal{F}/\mathfrak{m}$ given by $z \mapsto \varphi$. If it is not injective, its kernel is a principal ideal generated by an irreducible monic polynomial $p_{\mathfrak{m},\varphi}(z)$. This polynomial is called the **$\mathfrak{m}$-eigenfactor** of φ.

(a) Every eigenfactor of φ is of the form $p_{\mathfrak{m},\varphi}(z)$ for some maximal ideal $\mathfrak{m}$ of $\mathcal{F}$.

(b) A maximal ideal $\mathfrak{m}$ of $\mathcal{F} = K[\varphi_1, \ldots, \varphi_s]$ is **linear**, i.e. we have $\mathfrak{m} = \langle \varphi_1 - \lambda_1 \operatorname{id}_V, \ldots, \varphi_s - \lambda_s \operatorname{id}_V \rangle$, if and only if the $\mathfrak{m}$-eigenfactor of φ_i is linear $p_{\mathfrak{m},\varphi_i}(z) = z - \lambda_i$ for $i = 1, \ldots, s$.

(c) If $\mathfrak{m}$ is linear and $\psi = f(\varphi_1, \ldots, \varphi_s)$ then $p_{\mathfrak{m},\psi}(z) = z - f(\lambda_1, \ldots, \lambda_s)$.

Algorithm 2.9 **(Computing $\mathfrak{m}$-Eigenfactors)**

Let $\Phi = (\varphi_1, \ldots, \varphi_n)$ *be a system of* K*-algebra generators of the family* $\mathcal{F}$*, let* $P = K[x_1, \ldots, x_n]$*, let* $f(x_1, \ldots, x_n) \in P$*, let* $\psi = f(\varphi_1, \ldots, \varphi_n) \in \mathcal{F}$*, and let* $\mathfrak{m}$ *be a maximal ideal of* $\mathcal{F}$ *given by an explicit set of generators of the preimage* $\mathfrak{M}$ *of* $\mathfrak{m}$ *in* P*. The following algorithm computes the* $\mathfrak{m}$*-eigenfactor of* ψ*.*

Algorithm 2.9 **(Computing $\mathfrak{m}$-Eigenfactors)**

Let $\Phi = (\varphi_1, \ldots, \varphi_n)$ be a system of K-algebra generators of the family $\mathcal{F}$, let $P = K[x_1, \ldots, x_n]$, let $f(x_1, \ldots, x_n) \in P$, let $\psi = f(\varphi_1, \ldots, \varphi_n) \in \mathcal{F}$, and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{F}$ given by an explicit set of generators of the preimage $\mathfrak{M}$ of $\mathfrak{m}$ in P. The following algorithm computes the $\mathfrak{m}$-eigenfactor of ψ.

(1) *In ring $P[z]$ form the ideal $I_{\mathfrak{m},\psi} = \langle z - f(x_1, \ldots, x_n) \rangle + \mathfrak{M} \cdot P[z]$ and compute the elimination ideal $J_{\mathfrak{m},\psi} = I_{\mathfrak{m},\psi} \cap K[z]$.*

Algorithm 2.9 **(Computing $\mathfrak{m}$-Eigenfactors)**
Let $\Phi = (\varphi_1, \ldots, \varphi_n)$ be a system of K-algebra generators of the family $\mathcal{F}$, let $P = K[x_1, \ldots, x_n]$, let $f(x_1, \ldots, x_n) \in P$, let $\psi = f(\varphi_1, \ldots, \varphi_n) \in \mathcal{F}$, and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{F}$ given by an explicit set of generators of the preimage $\mathfrak{M}$ of $\mathfrak{m}$ in P. The following algorithm computes the $\mathfrak{m}$-eigenfactor of ψ.

(1) *In ring $P[z]$ form the ideal $I_{\mathfrak{m},\psi} = \langle z - f(x_1, \ldots, x_n)\rangle + \mathfrak{M} \cdot P[z]$ and compute the elimination ideal $J_{\mathfrak{m},\psi} = I_{\mathfrak{m},\psi} \cap K[z]$.*

(2) *Return the monic generator of $J_{\mathfrak{m},\psi}$.*

Example 2.10 Let $K = \mathbb{Q}$, let $V = K^4$, and let φ be the K-endomorphism of V defined by the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Example 2.10 Let $K = \mathbb{Q}$, let $V = K^4$, and let φ be the K-endomorphism of V defined by the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

(a) Notice that A is the companion matrix of the polynomial $z^4 + z^3 - z^2 + 1 = (z+1)(z^3 - z + 1)$. Hence we have $\mu_\varphi(z) = \chi_\varphi(z) = z^4 + z^3 - z^2 + 1$.

Example 2.10 Let $K = \mathbb{Q}$, let $V = K^4$, and let φ be the K-endomorphism of V defined by the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

(a) Notice that A is the companion matrix of the polynomial $z^4 + z^3 - z^2 + 1 = (z+1)(z^3 - z + 1)$. Hence we have $\mu_\varphi(z) = \chi_\varphi(z) = z^4 + z^3 - z^2 + 1$.

(b) Consequently, there are two maximal ideals $\mathfrak{m}_1 = \langle \varphi + 1 \rangle$ and $\mathfrak{m}_2 = \langle \varphi^3 - \varphi + 1 \rangle$ in the family $\mathcal{F} = K[\varphi]$.

Example 2.10 Let $K = \mathbb{Q}$, let $V = K^4$, and let φ be the K-endomorphism of V defined by the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

(a) Notice that A is the companion matrix of the polynomial $z^4 + z^3 - z^2 + 1 = (z+1)(z^3 - z + 1)$. Hence we have $\mu_\varphi(z) = \chi_\varphi(z) = z^4 + z^3 - z^2 + 1$.

(b) Consequently, there are two maximal ideals $\mathfrak{m}_1 = \langle \varphi + 1 \rangle$ and $\mathfrak{m}_2 = \langle \varphi^3 - \varphi + 1 \rangle$ in the family $\mathcal{F} = K[\varphi]$.

(c) Let us consider the endomorphism $\psi = \varphi^2 - \varphi$ of K^4. We compute its minimal polynomial and obtain

$$\mu_\psi(z) \;=\; z^4 - 4\,z^3 + z^2 + 5\,z + 2 \;=\; (z-2)(z^3 - 2z^2 - 3z - 1)$$

Thus we have $\dim_K(K[\psi]) = \dim_K(K[\varphi]) = 4$.

(d) This implies that the inclusion $K[\psi] \subseteq K[\varphi]$ is an equality and hence that ψ is a K-algebra generator of $\mathcal{F}$. We express φ explicitly as an element of $K[\psi]$ and get $\varphi = \frac{3}{7}\psi^3 - \frac{13}{7}\psi^2 + \frac{5}{7}\psi + \frac{11}{7}\,\mathrm{id}_V$.

(d) This implies that the inclusion $K[\psi] \subseteq K[\varphi]$ is an equality and hence that ψ is a K-algebra generator of $\mathcal{F}$. We express φ explicitly as an element of $K[\psi]$ and get $\varphi = \frac{3}{7}\psi^3 - \frac{13}{7}\psi^2 + \frac{5}{7}\psi + \frac{11}{7}\,\mathrm{id}_V$.

(e) Starting with $\mathfrak{m}_1 = \langle \varphi + 1 \rangle$ and the $\mathfrak{m}_1$-eigenfactor $p_{\mathfrak{m}_1,\varphi}(z) = z + 1$ of φ, we can use Algorithm 2.9 to compute $p_{\mathfrak{m}_1,\psi}(z)$. The result is $p_{\mathfrak{m}_1,\psi}(z) = z - 2$, and we find that $p_{\mathfrak{m}_1,\varphi}(z) = z + 1$ divides $p_{\mathfrak{m}_1,\psi}(z^2 - z) = z^2 - z - 2 = (z + 1)(z - 2)$.

(d) This implies that the inclusion $K[\psi] \subseteq K[\varphi]$ is an equality and hence that ψ is a K-algebra generator of $\mathcal{F}$. We express φ explicitly as an element of $K[\psi]$ and get $\varphi = \frac{3}{7}\psi^3 - \frac{13}{7}\psi^2 + \frac{5}{7}\psi + \frac{11}{7}\,\mathrm{id}_V$.

(e) Starting with $\mathfrak{m}_1 = \langle \varphi + 1 \rangle$ and the $\mathfrak{m}_1$-eigenfactor $p_{\mathfrak{m}_1,\varphi}(z) = z + 1$ of φ, we can use Algorithm 2.9 to compute $p_{\mathfrak{m}_1,\psi}(z)$. The result is $p_{\mathfrak{m}_1,\psi}(z) = z - 2$, and we find that $p_{\mathfrak{m}_1,\varphi}(z) = z + 1$ divides $p_{\mathfrak{m}_1,\psi}(z^2 - z) = z^2 - z - 2 = (z+1)(z-2)$.

(f) Next we compute the polynomial $p_{\mathfrak{m}_2,\psi}(z)$ using Algorithm 2.9. For this we form the polynomial ring $K[x,z]$ and the ideal $I_{\mathfrak{m},\psi} = \langle x^3 - x + 1,\, z - (x^2 - x) \rangle$ in $K[x,z]$. Then we compute the monic generator of $I_{\mathfrak{m}_2,\psi} \cap K[z]$ and get the eigenfactor $p_{\mathfrak{m}_2,\psi}(z) = z^3 - 2\,z^2 - 3\,z - 1$ of ψ. Again, we note that the polynomial $p_{\mathfrak{m}_2,\varphi}(z) = z^3 - z + 1$ divides $p_{\mathfrak{m}_2,\psi}(z^2 - z)$ here. This follows from $p_{m_2,\psi}(z^2 - z) = (z^2 - z)^3 - 2(z^2 - z)^2 - 3(z^2 - z) - 1 = (z^3 - z + 1)(z^3 - 3z^2 + 2z - 1)$.

THE END

THE END

Thank you for your attention!

THE END

Thank you for your attention!

In the end, everything is a gag.

(Charlie Chaplin)