Multiplication map

As before, let K be a field, let $P = K[x_1, \dots, x_n]$, and let $f_1, \dots, f_s \in P$, let $\overline{K}$ be the algebraic closure of K , and let $\overline{P} = \overline{K}[x_1, \dots, x_n]$. By $\mathcal{S}$ we denote the system of polynomial equations

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \qquad \vdots \\ f_s(x_1, \dots, x_n) = 0 \end{cases}$$

By I we denote the ideal $(f_1, \dots, f_s)$, by A the quotient ring P/I , and by $\overline{A}$ the quotient ring $\overline{P}/I\overline{P}$. As usual we assume that I is zero-dimensional so that A is a finite dimensional K -vector space by the Finiteness Criterion.

Definition

Given a polynomial $f \in P$ we consider the following K -linear map $m_f : A \longrightarrow A$ defined by $m_f(g \mod I) = fg \mod I$, and call it the multiplication map defined by f. We also consider the induced K -linear map on the dual spaces $m_f^* : A^* \longrightarrow A^*$ defined by $m_f^*(\varphi) = \varphi \circ m_f$.

A first example

Example

- Let $P = \mathbb{R}[x]$, $f = x^2 + 1$, I the ideal generated by the polynomial $x^3 - x^2 + x - 1 = (x-1)(x^2+1)$, and $A = P/I$.
- We consider the multiplication map $m_f : A \longrightarrow A$ and describe it via its representation with respect to the $\mathbb{R}$ -basis of A given by $(1,\, x,\, x^2)$.
- Using the relations $x^3 + x = x^2 + 1 \mod I$, $x^4 + x^2 = x^2 + 1 \mod I$, we deduce that the matrix which represents m_f is

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

- It is singular, hence 0 is an eigenvalue. Moreover, $\mathcal{Z}(I) = \{1,\, i, -i\}$, and we see that $0 = f(i) = f(-i)$, but $\mathcal{Z}_{\mathbb{R}}(I) = \{1\}$ and $0 \neq f(1)$.

- Next theorem makes an important link between $\mathcal{Z}(I)$ and eigenvalues, and the example motivates the reason why we need the assumption that $\mathcal{Z}_K(I) = \mathcal{Z}(I)$.

Eigenvalues

Theorem

Let I be a zero-dimensional ideal in P such that $\mathcal{Z}_K(I) = \mathcal{Z}(I)$, let $f \in P$, and let $\lambda \in K$. The following conditions are equivalent

1. *The element λ is an eigenvalue of m_f.*
2. *There exists a point $p \in \mathcal{Z}(I)$ such that $\lambda = f(p)$.*

Proof.

Let $\mathrm{id}: A \longrightarrow A$ denote the identity map.

We know that λ is an eigenvalue of m_f if and only if $m_f - \lambda\,\mathrm{id}$ is not invertible.

Let us prove $(1) \implies (2)$.

If λ does not coincide with any of the values of f at the points $p \in \mathcal{Z}(I)$, then the ideal $J = I + (f - \lambda)$ has the property that $\mathcal{Z}(J) = \emptyset$.

On the other hand the ideal J is defined over K, hence the Weak Nullstellenzatz implies that $1 \in J$.

It means that there exists $g \in P$ such that $1 = g(f - \lambda) + h$ with $h \in I$. Then $1 = g(f - \lambda) \mod I$, so that $m_f - \lambda\,\mathrm{id}$ is invertible with inverse m_g, and hence λ is not an eigenvalue of m_f. This finishes the proof of $a) \implies b)$,

Let us prove $(2) \implies (1)$.

If λ is not an eigenvalue of m_f, then $m_f - \lambda\,\mathrm{id}$ is an invertible map, in particular it is surjective. So, there exists $g \in P$ such that $g(f - \lambda) = 1 \mod I$. Clearly this implies that there cannot exist $p \in \mathcal{Z}(I)$ such that $f(p) - \lambda = 0$

□

The matrix M_{fE}^{E}

- If $E = (t_1, \dots, t_\mu)$ is a row of polynomials whose residue classes form a K-basis of $A = P/I$, then we use the short form fE to mean the row of vectors $(ft_1, \dots, ft_\mu)$.
- A way of describing m_f explicitly is to fix such a K-basis E of A and represent m_f via the matrix M_{fE}^{E} where the j-column of M_{fE}^{E} is given by the coefficients of ft_j when written in terms of E. In other words, if

$$ft_j = \sum_{k=1}^{\mu} a_{kj} t_k \mod I$$

then the j^{th} column of M_{fE}^{E} is $(a_{1j}, a_{2j}, \dots, a_{\mu j})^{\text{tr}}$. A more compact way of expressing this fact is the following formula

$$fE = E\, M_{fE}^{E} \mod I$$

- Usually a K-basis E is an order ideal of monomials and hence we may assume that $t_1 = 1$. We may as well assume that the residue classes of some of the indeterminates (most of the times all) are among the entries of E.

Eigenvalues and coordinates of zeros

Corollary

Let x_i be such that its class is among the entries of E. Then the x_i coordinates of the points in $\mathcal{Z}_K(I)$ are the eigenvalues of m_{x_i}.

Proof.

It follows immediately from the theorem, since $x_i(p)$ is exactly the x_i coordinate of p. □

We observe that, as in the case of the `Lex`*-method, we need the zeros of a polynomial (in this case the characteristic polynomial), and hence we hit again an intrinsic obstacle: we need approximation.*

The above corollary gives a first method for computing $\mathcal{Z}_K(I)$, however what we get is only a grid of points which is usually a much larger set than $\mathcal{Z}_K(I)$. Sometimes we can do better, but we need a description of eigenvectors. In the sequel we use the following terminology.

Eigenvectors and coordinates of zeros

Definition

Let $\varphi : V \longrightarrow V$ be a linear map of K-vector spaces, let $\lambda \in K$ be an eigenvalue of φ, and let $W_\lambda = \text{Ker}(\varphi - \lambda\,\mathrm{id})$ be the corresponding eigenspace. Then the non-zero vectors in W_λ are called λ-eigenvectors, or simply eigenvectors, if the context is clear.

Corollary (Eigenvectors)

Let $p \in \mathcal{Z}_K(I)$, and let $E = (t_1, \dots, t_\mu)$ be a row of power products whose classes form a K-basis of A. Then the vector $E(p) = (t_1(p), \dots, t_\mu(p))$ is an $f(p)$-eigenvector of m_f^*.

Proof.

We use the formula $fE = E\, M_{fE}^E \mod I$ and evaluate both sides at p. We get

$$f(p)E(p) = E(p)\, M_{fE}^E$$

By transposing both sides we get

$$f(p)(E(p))^{\mathrm{tr}} = (M_{fE}^E)^{\mathrm{tr}}\, (E(p))^{\mathrm{tr}}$$

This formula means that $E(p)$ is an $f(p)$-eigenvector of the matrix $(M_{fE}^E)^{\mathrm{tr}}$, hence of m_f^*.

□

Non-derogatory matrices I

Definition

A square matrix $M \in \mathrm{Mat}_\mu(\mathbb{C})$ is said to be non-derogatory if the following equivalent conditions are satisfied.

1. All eigenspaces of M are 1-dimensional.
2. The Jordan canonical form of M has one Jordan block per eigenvalue.
3. $\mathrm{MinPoly}_M = \mathrm{CharPoly}_M$.

Next corollary is one of the many variations which can be played around the above result. It highlights the importance of non-derogatory matrices.

Non-derogatory matrices II

Corollary

Let $1, x_1, \dots, x_n$ *be the first* $n+1$ *-entries of* E *, assume that the matrix* $(M_{fE}^{E})^{\mathrm{tr}}$ *is non-derogatory, let* $\mathcal{Z}_K(I) = \mathcal{Z}(I) = \{p_1, \dots, p_r\}$ *, and let* $W_1, \dots, W_r$ *be the* 1 *-dimensional eigenspaces corresponding to* $f(p_1), \dots f(p_r)$ *respectively. If we choose* $v_j = (a_{1j}, a_{2j}, \dots, a_{r+1,j}, \dots) \in W_j \setminus 0$ *, for* $j = 1, \dots, r$ *, then we have the equalities* $p_j = (a_{2j}/a_{1j}, \dots, a_{r+1,j}/a_{1j})$ *for* $j = 1, \dots, r$*.*

Proof.

We use the above corollary about eigenvectors to deduce that the vector $E(p_j) = (t_1(p_j), \dots, t_\mu(p_j))$ is an $f(p_j)$-eigenvector of f, hence it is a non-zero vector in W_j for $j = 1, \dots, r$.

The assumption about $(M_{fE}^{E})^{\mathrm{tr}}$ means that all the W_j 's are 1-dimensional vector spaces, hence the vectors $E(p_j)$ and v_j are proportional.

On the other hand, we know that $t_1 = 1$, hence $t_1(p_j) = 1$, hence $a_{1j} \neq 0$. We divide the coordinates of v_j by a_{1j} and conclude. □

We observe that the computation of eigenspaces creates a new difficulty. Since the eigenvalues are in general given up to a certain degree of accuracy, the eigenspaces are not computable as kernels of linear maps.

Example I

Example

- Let I be the ideal in $P = \mathbb{R}[x, y]$ generated by the set of polynomials $\{x^2 + 4/3xy + 1/3y^2 - 7/3x - 5/3y + 4/3,\ y^3 + 10/3xy + 7/3y^2 - 4/3x - 20/3y + 4/3,\ xy^2 - 7/3xy - 7/3y^2 - 2/3x + 11/3y + 2/3\}$.
- We can check that this set is a `DegRevLex`-Gröbner basis, hence $E = [1, x, y, xy, y^2]$ is a basis modulo I .
- By computing $\mathrm{NF}(x^2, I)$, $\mathrm{NF}(x^2y, I)$, $\mathrm{NF}(xy^2, I)$, we get

$$M_{xE}^{E} = \begin{pmatrix} 0 & -4/3 & 0 & 4/3 & -2/3 \\ 1 & 7/3 & 0 & -4/3 & 2/3 \\ 0 & 5/3 & 0 & 4/3 & -11/3 \\ 0 & -4/3 & 1 & 1/3 & 7/3 \\ 0 & -1/3 & 0 & -2/3 & 7/3 \end{pmatrix}$$

$$(M_{xE}^{E})^{\mathrm{tr}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -4/3 & 7/3 & 5/3 & -4/3 & -1/3 \\ 0 & 0 & 0 & 1 & 0 \\ 4/3 & -4/3 & 4/3 & 1/3 & -2/3 \\ -2/3 & 2/3 & -11/3 & 7/3 & 7/3 \end{pmatrix}$$

- Its characteristic polynomial is $x^5 - 5x^4 + 7x^3 + x^2 - 8x + 4$ which factorizes as follows $(x+1)(x-1)^2(x-2)^2$. Since we can check (with CoCoA) that $\dim(W_1) = 2$, we deduce that $(M_{xE}^{E})^{\mathrm{tr}}$ is derogatory.

Example II

Example (continued)

- By computing $\mathrm{NF}(xy^2, I)$, $\mathrm{NF}(y^3, I)$, we get the multiplication matrix

$$M_{yE}^{E} = \begin{pmatrix} 0 & 0 & 0 & -2/3 & -4/3 \\ 0 & 0 & 0 & 2/3 & 4/3 \\ 1 & 0 & 0 & -11/3 & 20/3 \\ 0 & 1 & 0 & 7/3 & -10/3 \\ 0 & 0 & 1 & 7/3 & -7/3 \end{pmatrix}$$

whose transposed is

$$(M_{yE}^{E})^{\mathrm{tr}} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -2/3 & 2/3 & -11/3 & 7/3 & 7/3 \\ -4/3 & 4/3 & 20/3 & -10/3 & -7/3 \end{pmatrix}$$

- Its characteristic polynomial is $y^5 - 5y^3 + 4y$ which factorizes in the following way $y(y-1)(y+1)(y-2)(y+2)$.
- We check that all the eigenspaces are 1-dimensional, hence the matrix $(M_{yE}^{E})^{\mathrm{tr}}$ is non-derogatory.
- We may choose one non-zero vector inside each of them, for instance the vectors $v_1 = (1, 1, 0, 0, 0)$, $v_2 = (1, 1, 1, 1, 1)$, $v_3 = (1, 2, -1, -2, 1)$, $v_4 = (1, -1, 2, -2, 4)$, $v_5 = (1, 2, -2, -4, 4)$.
- Therefore, five points in $\mathcal{Z}(I)$ are $(1, 0)$, $(1, 1)$, $(2, -1)$, $(-1, 2)$, $(2, -2)$. But $\dim_{\mathbb{R}}(P/I) = 5$, hence $\mathcal{Z}_{\mathbb{R}}(I) = \mathcal{Z}(I) = \{(1, 0), (1, 1), (2, -1), (-1, 2), (2, -2)\}$.