

HOMEWORK / PRACTICAL SESSION 1

In what follows the polynomial denoted $f(x)$ is assume to be squarefree.

Exercise 1. Let $f(x) = x^d + \sum_{i=0}^{d-1} f_i x^i$ and $g(x)$ be two polynomials. We denote $\mathbb{A} = \mathbb{K}[x]/(f)$.

1. Show that $\mathcal{M}_g : \begin{cases} \mathbb{A} \longrightarrow \mathbb{A} \\ h \longmapsto g * h \end{cases}$ is a \mathbb{K} -linear map.
2. Find (the entries of) the matrix associated to \mathcal{M}_g in the monomial basis.
3. Write the matrix of \mathcal{M}_g in the Lagrange basis.
4. Give an polynomial condition depending only on the coefficients of the polynomials f and g vanishing if and only if the two polynomial share a root.

Exercise 2. Using the Lagrange basis, show that if a polynômial $f(x)$ divides a polynomial $g(x)$ then all the roots of $f(x)$ are also roots of $g(x)$.

Exercise 3. Let $f(x) = f_d * \prod_{i=1}^d (x - \zeta_i) \in \mathbb{C}[x]$ and let $\mathbb{A} = \mathbb{C}[x]/(f)$. We consider $g(x) \in \mathbb{A}$ and the following map:

$$\mathcal{P} : \begin{cases} \mathbb{A} \longrightarrow \mathbb{A} \\ h \longmapsto \frac{h * h}{\|h * h\|_2} \end{cases}$$

where $\|h\|_2 = \sqrt{\sum_{i=0}^{d-1} |h_i|^2}$ if $h(x) = \sum_{i=0}^{d-1} h_i x^i$. We consider the sequence defined by $H_i = \mathcal{P}(H_{i-1})$ and $H_0 = h$. We assume that $|h(\zeta_1)| > |h(\zeta_i)|$ for all $i \in \{2, \dots, d\}$.

1. Show that there exists a sequence of complex numbers (a_i) such that $|a_i| = 1$ and such that the sequence $(a_i * H_i)$ convergences.
2. Show that the $H = \lim_{i \rightarrow \infty} a_i * H_i$ is an eigenvector of the map $\mathcal{M}_h : g \in \mathbb{A} \longmapsto h * g \in \mathbb{A}$.
3. What is the eigenvalue associated to this eigenvector.
4. We now assume that the roots of $f(x)$ are such that $|\zeta_1| > |\zeta_i|$ for all $i \in \{2, \dots, d\}$. Give an iterative procedure to approximate ζ_1 .

This method is called “power iteration” in numerical linear algebra.

Exercise 4. Let $f(x) = f_d * \prod_{i=1}^d (x - \zeta_i) \in \mathbb{C}[x]$, $\mathbb{A} = \mathbb{C}[x]/(f)$ and $g \in \mathbb{A}$.

1. Show that if $\mathcal{M}_g : \mathbb{A} \longrightarrow \mathbb{A}$ has maximal rank d then $f(x)$ and $g(x)$ have no common root.
2. Assume \mathcal{M}_g invertible. Express the inverse element $g^{-1} \in \mathbb{A}$ in the monomial basis in terms of its expression in the Lagrangian basis and the Vandermonde matrix.
3. Assume now that $f_0 \neq 0$ and that $|\zeta_1| < |\zeta_i|$ for all $i \in \{2, \dots, d\}$. Using the previous exercise, give an algorithm to compute ζ_1 .

In linear numerical algebra, this is the inverse power iteration.