Linear Algebra 2

Lecture #20

Cramer's rule. The adjugate matrix. Roots of polynomials

Irena Penev

April 9, 2025

- This lecture has four parts:
    1. Cramer's rule

- This lecture has four parts:
    1. Cramer's rule
    2. The adjugate matrix

- This lecture has four parts:
    1. Cramer's rule
    2. The adjugate matrix
    3. Algebraically closed fields

- This lecture has four parts:
  1. Cramer's rule
  2. The adjugate matrix
  3. Algebraically closed fields
  4. Common roots of polynomials via determinants

1. Cramer's rule

1. Cramer's rule

- Before stating Cramer's rule, we set up some notation.

1. Cramer's rule

- Before stating Cramer's rule, we set up some notation.
- For a matrix $A \in \mathbb{F}^{n\times n}$, a vector $\mathbf{b} \in \mathbb{F}^n$, and an index $j \in \{1, \dots, n\}$, we denote by $A_j(\mathbf{b})$ the matrix obtained from A by replacing the j-th column of A with $\mathbf{b}$.
  - For example, for

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix},$$

we have that

$$A_1(\mathbf{b}) = \begin{bmatrix} 4 & 1 & 1 \\ 5 & 2 & 2 \\ 6 & 0 & 3 \end{bmatrix}, \quad A_2(\mathbf{b}) = \begin{bmatrix} 1 & 4 & 1 \\ 0 & 5 & 2 \\ 0 & 6 & 3 \end{bmatrix}, \quad A_3(\mathbf{b}) = \begin{bmatrix} 1 & 1 & 4 \\ 0 & 2 & 5 \\ 0 & 0 & 6 \end{bmatrix}.$$

1. Cramer's rule

- Before stating Cramer's rule, we set up some notation.
- For a matrix $A \in \mathbb{F}^{n \times n}$, a vector $\mathbf{b} \in \mathbb{F}^n$, and an index $j \in \{1, \dots, n\}$, we denote by $A_j(\mathbf{b})$ the matrix obtained from A by replacing the j-th column of A with $\mathbf{b}$.
  - For example, for

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix},$$

we have that

$$A_1(\mathbf{b}) = \begin{bmatrix} 4 & 1 & 1 \\ 5 & 2 & 2 \\ 6 & 0 & 3 \end{bmatrix}, \quad A_2(\mathbf{b}) = \begin{bmatrix} 1 & 4 & 1 \\ 0 & 5 & 2 \\ 0 & 6 & 3 \end{bmatrix}, \quad A_3(\mathbf{b}) = \begin{bmatrix} 1 & 1 & 4 \\ 0 & 2 & 5 \\ 0 & 0 & 6 \end{bmatrix}.$$

- In what follows, it will be convenient to use the fraction notation in fields.

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} \;=\; \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \ldots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

- First an example, then a proof.

Example 7.7.1

Let

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix},$$

with entries understood to be in $\mathbb{Z}_3$. Solve the matrix-vector equation $A\mathbf{x} = \mathbf{b}$.

Solution.

Example 7.7.1

Let

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix},$$

with entries understood to be in $\mathbb{Z}_3$. Solve the matrix-vector equation $A\mathbf{x} = \mathbf{b}$.

Solution. Note that $\det(A) = 2$, and in particular, A is invertible (by Theorem 7.4.1). So, Cramer's rule applies. We compute:

- $\det\big(A_1(\mathbf{b})\big) = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 2 & 2 \\ 0 & 1 & 1 \end{vmatrix} = 2;$
- $\det\big(A_2(\mathbf{b})\big) = \begin{vmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{vmatrix} = 1;$
- $\det\big(A_3(\mathbf{b})\big) = \begin{vmatrix} 2 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 0.$

Example 7.7.1

Let

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix},$$

with entries understood to be in $\mathbb{Z}_3$. Solve the matrix-vector equation $A\mathbf{x} = \mathbf{b}$.

Solution (continued). By Cramer's rule, $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\begin{aligned} \mathbf{x} &= \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_3(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T \\ &= \begin{bmatrix} \frac{2}{2} & \frac{1}{2} & \frac{0}{2} \end{bmatrix}^T \\ &= \begin{bmatrix} 1 & 2 & 0 \end{bmatrix}^T. \end{aligned}$$

□

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} \quad = \quad \begin{bmatrix} \frac{\det\big(A_1(\mathbf{b})\big)}{\det(A)} & \frac{\det\big(A_2(\mathbf{b})\big)}{\det(A)} & \ldots & \frac{\det\big(A_n(\mathbf{b})\big)}{\det(A)} \end{bmatrix}^T.$$

Proof.

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} \quad = \quad \left[\begin{array}{cccc} \frac{\det\big(A_1(\mathbf{b})\big)}{\det(A)} & \frac{\det\big(A_2(\mathbf{b})\big)}{\det(A)} & \dots & \frac{\det\big(A_n(\mathbf{b})\big)}{\det(A)} \end{array} \right]^T.$$

Proof. Since A is invertible, we know that the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely, $\mathbf{x} = A^{-1}\mathbf{b}$.

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} = \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \dots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

Proof. Since A is invertible, we know that the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely, $\mathbf{x} = A^{-1}\mathbf{b}$. Now, for this solution $\mathbf{x}$, we set $\mathbf{x} = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix}^T$.

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} \;=\; \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \dots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

Proof. Since A is invertible, we know that the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely, $\mathbf{x} = A^{-1}\mathbf{b}$. Now, for this solution $\mathbf{x}$, we set $\mathbf{x} = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix}^T$. WTS

$$\mathbf{x} \;=\; \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \dots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} \quad = \quad \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \dots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

Proof. Since A is invertible, we know that the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely, $\mathbf{x} = A^{-1}\mathbf{b}$. Now, for this solution $\mathbf{x}$, we set $\mathbf{x} = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix}^T$. WTS

$$\mathbf{x} \quad = \quad \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \dots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

Fix an index $j \in \{1, \dots, n\}$. WTS

$$x_j \quad = \quad \frac{\det\left(A_j(\mathbf{b})\right)}{\det(A)}.$$

Proof (continued). Set $A = \begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_n \end{bmatrix}$. Then:

$$\begin{aligned}
\det(A_j(\mathbf{b})) &= \det\Big(\begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{j-1} & \mathbf{b} & \mathbf{a}_{j+1} & \dots \mathbf{a}_n \end{bmatrix}\Big) \\
&= \det\Big(\begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{j-1} & A\mathbf{x} & \mathbf{a}_{j+1} & \dots \mathbf{a}_n \end{bmatrix}\Big) \\
&= \det\Big(\begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{j-1} & \sum_{i=1}^{n} x_i \mathbf{a}_i & \mathbf{a}_{j+1} & \dots \mathbf{a}_n \end{bmatrix}\Big) \\
&\overset{(*)}{=} \sum_{i=1}^{n} x_i \det\Big(\begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{j-1} & \mathbf{a}_i & \mathbf{a}_{j+1} & \dots \mathbf{a}_n \end{bmatrix}\Big) \\
&\overset{(**)}{=} x_j \det\Big(\begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{j-1} & \mathbf{a}_j & \mathbf{a}_{j+1} & \dots \mathbf{a}_n \end{bmatrix}\Big) \\
&= x_j \det(A),
\end{aligned}$$

where (*) follows from Proposition 7.2.1(a), and (**) follows from the fact that any matrix with two identical columns has determinant zero (by Proposition 7.1.5).

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} = \begin{bmatrix} \frac{\det\big(A_1(\mathbf{b})\big)}{\det(A)} & \frac{\det\big(A_2(\mathbf{b})\big)}{\det(A)} & \dots & \frac{\det\big(A_n(\mathbf{b})\big)}{\det(A)} \end{bmatrix}^T.$$

Proof (continued). We have now shown that

$$\det\big(A_j(\mathbf{b})\big) = x_j \det(A).$$

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} = \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \dots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T .$$

Proof (continued). We have now shown that

$$\det\left(A_j(\mathbf{b})\right) = x_j \det(A).$$

Since A is invertible, Theorem 7.4.1 guarantees that $\det(A) \neq 0$.

Cramer's rule

Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$, and let $\mathbf{b} \in \mathbb{F}^n$. Then the matrix-vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution, namely

$$\mathbf{x} = \begin{bmatrix} \frac{\det\left(A_1(\mathbf{b})\right)}{\det(A)} & \frac{\det\left(A_2(\mathbf{b})\right)}{\det(A)} & \cdots & \frac{\det\left(A_n(\mathbf{b})\right)}{\det(A)} \end{bmatrix}^T.$$

Proof (continued). We have now shown that

$$\det(A_j(\mathbf{b})) = x_j \det(A).$$

Since A is invertible, Theorem 7.4.1 guarantees that $\det(A) \neq 0$. So, we can divide both sides of the equality above by $\det(A)$ to obtain

$$x_j = \frac{\det\left(A_j(\mathbf{b})\right)}{\det(A)}.$$

This completes the argument. □

2. The adjugate matrix

Definition

Given a field $\mathbb{F}$ and a matrix $A \in \mathbb{F}^{n\times n}$ ($n \geq 2$), with cofactors $C_{i,j} = (-1)^{i+j}\det(A_{i,j})$ (for $i, j \in \{1, \ldots, n\}$), the *cofactor matrix* of A is the matrix $\left[\ C_{i,j}\ \right]_{n\times n}$. The *adjugate matrix* (also called the *classical adjoint*) of A, denoted by adj(A), is the transpose of the cofactor matrix of A, i.e.

$$\mathrm{adj}(A) \quad := \quad \left(\left[\ C_{i,j}\ \right]_{n\times n} \right)^T.$$

So, the i, j-th entry of adj(A) is the cofactor $C_{j,i}$ (note the swapping of the indices).

Example 7.8.1

Consider the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

with entries understood to be in $\mathbb{R}$. Compute the cofactor and adjugate matrices of the matrix A.

Solution.

Example 7.8.1

Consider the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

with entries understood to be in $\mathbb{R}$. Compute the cofactor and adjugate matrices of the matrix A.

Solution. For all $i, j \in \{1, 2, 3\}$, we let $C_{i,j} = (-1)^{i+j}\det(A_{i,j})$. We compute (next slide):

Solution (continued). Reminder: $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix}$.

- $C_{1,1} = (-1)^{1+1} \begin{vmatrix} 2 & 2 \\ 0 & 3 \end{vmatrix} = 6$;
- $C_{1,2} = (-1)^{1+2} \begin{vmatrix} 0 & 2 \\ 0 & 3 \end{vmatrix} = 0$;
- $C_{1,3} = (-1)^{1+3} \begin{vmatrix} 0 & 2 \\ 0 & 0 \end{vmatrix} = 0$;
- $C_{2,1} = (-1)^{2+1} \begin{vmatrix} 1 & 1 \\ 0 & 3 \end{vmatrix} = -3$;
- $C_{2,2} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 0 & 3 \end{vmatrix} = 3$;
- $C_{2,3} = (-1)^{2+3} \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} = 0$;
- $C_{3,1} = (-1)^{3+1} \begin{vmatrix} 1 & 1 \\ 2 & 2 \end{vmatrix} = 0$;
- $C_{3,2} = (-1)^{3+2} \begin{vmatrix} 1 & 1 \\ 0 & 2 \end{vmatrix} = -2$;
- $C_{3,3} = (-1)^{3+3} \begin{vmatrix} 1 & 1 \\ 0 & 2 \end{vmatrix} = 2$.

Example 7.8.1

Consider the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

with entries understood to be in $\mathbb{R}$. Compute the cofactor and adjugate matrices of the matrix A.

Solution (continued). So, the cofactor matrix of A is

$$\begin{bmatrix} C_{1,1} & C_{1,2} & C_{1,3} \\ C_{2,1} & C_{2,2} & C_{2,3} \\ C_{3,1} & C_{3,2} & C_{3,3} \end{bmatrix} = \begin{bmatrix} 6 & 0 & 0 \\ -3 & 3 & 0 \\ 0 & -2 & 2 \end{bmatrix}.$$

Example 7.8.1

Consider the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

with entries understood to be in $\mathbb{R}$. Compute the cofactor and adjugate matrices of the matrix A.

Solution (continued). So, the cofactor matrix of A is

$$\begin{bmatrix} C_{1,1} & C_{1,2} & C_{1,3} \\ C_{2,1} & C_{2,2} & C_{2,3} \\ C_{3,1} & C_{3,2} & C_{3,3} \end{bmatrix} = \begin{bmatrix} 6 & 0 & 0 \\ -3 & 3 & 0 \\ 0 & -2 & 2 \end{bmatrix}.$$

The adjugate matrix of A is the transpose of the cofactor matrix, i.e.

$$\operatorname{adj}(A) = \begin{bmatrix} 6 & -3 & 0 \\ 0 & 3 & -2 \\ 0 & 0 & 2 \end{bmatrix}.$$

□

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ ($n \geq 2$). Then

$$\text{adj}(A)\,A \;=\; A\,\text{adj}(A) \;=\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)}\text{adj}(A)$.

Proof.

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ ($n \geq 2$). Then

$$\operatorname{adj}(A)\, A \;=\; A \operatorname{adj}(A) \;=\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$.

Proof. Let us first show that the first statement implies the second.

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ $(n \geq 2)$. Then

$$\text{adj}(A)\, A \;\;=\;\; A\, \text{adj}(A) \;\;=\;\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$.

Proof. Let us first show that the first statement implies the second. Indeed, if A is invertible, then $\det(A) \neq 0$, and so if the first statement holds, then we get that

$$\left(\tfrac{1}{\det(A)} \text{adj}(A)\right) A \;\;=\;\; A \left(\tfrac{1}{\det(A)} \text{adj}(A)\right) \;\;=\;\; I_n,$$

and consequently, $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$.

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ $(n \geq 2)$. Then

$$\text{adj}(A)\, A \;=\; A\, \text{adj}(A) \;=\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)}\text{adj}(A)$.

Proof. Let us first show that the first statement implies the second. Indeed, if A is invertible, then $\det(A) \neq 0$, and so if the first statement holds, then we get that

$$\left(\frac{1}{\det(A)}\text{adj}(A)\right) A \;=\; A \left(\frac{1}{\det(A)}\text{adj}(A)\right) \;=\; I_n,$$

and consequently, $A^{-1} = \frac{1}{\det(A)}\text{adj}(A)$.

It remains to prove the first statement, i.e. that $\text{adj}(A)\, A = A\, \text{adj}(A) = \det(A) I_n$.

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ ($n \geq 2$). Then

$$\text{adj}(A)\,A \;=\; A\,\text{adj}(A) \;=\; \det(A)I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)}\text{adj}(A)$.

Proof. Let us first show that the first statement implies the second. Indeed, if A is invertible, then $\det(A) \neq 0$, and so if the first statement holds, then we get that

$$\left(\frac{1}{\det(A)}\text{adj}(A)\right) A \;=\; A\left(\frac{1}{\det(A)}\text{adj}(A)\right) \;=\; I_n,$$

and consequently, $A^{-1} = \frac{1}{\det(A)}\text{adj}(A)$.

It remains to prove the first statement, i.e. that $\text{adj}(A)\,A = A\,\text{adj}(A) = \det(A)I_n$. We will prove that $\text{adj}(A)\,A = \det(A)I_n$; the proof of $A\,\text{adj}(A) = \det(A)I_n$ is in the Lecture Notes.

Proof (continued). Reminder: WTS $\mathrm{adj}(A)\, A = \det(A) I_n$.

Proof (continued). Reminder: WTS $\mathrm{adj}(A)\, A = \det(A) I_n$.

We will prove this by showing that the matrices $\mathrm{adj}(A)\, A$ and $\det(A) I_n$ have the same corresponding entries.

Proof (continued). Reminder: WTS $\mathrm{adj}(A)\,A = \det(A) I_n$.

We will prove this by showing that the matrices $\mathrm{adj}(A)\,A$ and $\det(A) I_n$ have the same corresponding entries. Fix indices $i, j \in \{1, \ldots, n\}$.

Proof (continued). Reminder: WTS $\operatorname{adj}(A)\,A = \det(A) I_n$.

We will prove this by showing that the matrices $\operatorname{adj}(A)\,A$ and $\det(A) I_n$ have the same corresponding entries. Fix indices $i, j \in \{1, \ldots, n\}$. The i, j-th entry of the matrix $\det(A) I_n$ is $\det(A)$ if $i = j$, and is zero if $i \neq j$.

Proof (continued). Reminder: WTS $\mathrm{adj}(A)\,A = \det(A)I_n$.

We will prove this by showing that the matrices $\mathrm{adj}(A)\,A$ and $\det(A)I_n$ have the same corresponding entries. Fix indices $i, j \in \{1, \ldots, n\}$. The i, j-th entry of the matrix $\det(A)I_n$ is $\det(A)$ if $i = j$, and is zero if $i \neq j$. We must show this holds for the i, j-th entry of the matrices $\mathrm{adj}(A)\,A$ as well.

Proof (continued). Reminder: WTS $\mathrm{adj}(A)\,A = \det(A)I_n$.

We will prove this by showing that the matrices $\mathrm{adj}(A)\,A$ and $\det(A)I_n$ have the same corresponding entries. Fix indices $i, j \in \{1, \ldots, n\}$. The i,j-th entry of the matrix $\det(A)I_n$ is $\det(A)$ if $i = j$, and is zero if $i \neq j$. We must show this holds for the i,j-th entry of the matrices $\mathrm{adj}(A)\,A$ as well.

The i-th row of $\mathrm{adj}(A)$ is $\begin{bmatrix} C_{1,i} & \ldots & C_{n,i} \end{bmatrix}$, and the j-th column of A is $\begin{bmatrix} a_{1,j} & \ldots & a_{n,j} \end{bmatrix}^T$.

Proof (continued). Reminder: WTS $\text{adj}(A)\,A = \det(A)I_n$.

We will prove this by showing that the matrices $\text{adj}(A)\,A$ and $\det(A)I_n$ have the same corresponding entries. Fix indices $i, j \in \{1, \ldots, n\}$. The i, j-th entry of the matrix $\det(A)I_n$ is $\det(A)$ if $i = j$, and is zero if $i \neq j$. We must show this holds for the i, j-th entry of the matrices $\text{adj}(A)\,A$ as well.

The i-th row of $\text{adj}(A)$ is $\begin{bmatrix} C_{1,i} & \ldots & C_{n,i} \end{bmatrix}$, and the j-th column of A is $\begin{bmatrix} a_{1,j} & \ldots & a_{n,j} \end{bmatrix}^T$. So, the i, j-th entry of $\text{adj}(A)\,A$ is $\sum_{k=1}^{n} a_{k,j} C_{k,i}$.

Proof (continued). Reminder: WTS $\mathrm{adj}(A)\,A = \det(A) I_n$.

We will prove this by showing that the matrices $\mathrm{adj}(A)\,A$ and $\det(A) I_n$ have the same corresponding entries. Fix indices $i, j \in \{1, \ldots, n\}$. The i, j-th entry of the matrix $\det(A) I_n$ is $\det(A)$ if $i = j$, and is zero if $i \neq j$. We must show this holds for the i, j-th entry of the matrices $\mathrm{adj}(A)\,A$ as well.

The i-th row of $\mathrm{adj}(A)$ is $\begin{bmatrix} C_{1,i} & \ldots & C_{n,i} \end{bmatrix}$, and the j-th column of A is $\begin{bmatrix} a_{1,j} & \ldots & a_{n,j} \end{bmatrix}^T$. So, the i, j-th entry of $\mathrm{adj}(A)\,A$ is $\sum_{k=1}^{n} a_{k,j} C_{k,i}$. We need to show that this number is equal to $\det(A)$ if $i = j$ and is zero if $i \neq j$.

Now, let B_1 be the matrix obtained by replacing the i-th column of A by the j-th column of A. Then $\det(B_1) = \sum_{k=1}^{n} a_{k,j} C_{k,i}$ (via Laplace expansion along the i-th column of B_1). But if $i = j$, then $\det(B_1) = \det(A)$ (because $B_1 = A$), and if $i \neq j$, then $\det(B_1) = 0$ (because B_1 has two identical columns, namely, the i-th and j-th column). $\square$

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ ($n \geq 2$). Then

$$\operatorname{adj}(A)\, A \;=\; A \operatorname{adj}(A) \;=\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$.

Example 7.8.3

Show that the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

(with entries understood to be in $\mathbb{R}$) is invertible, and using Theorem 7.8.2, find its inverse A^{-1}.

Solution.

Example 7.8.3

Show that the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

(with entries understood to be in $\mathbb{R}$) is invertible, and using Theorem 7.8.2, find its inverse A^{-1}.

Solution. The matrix A is upper triangular, and so its determinant can be computed by multiplying the entries along the main diagonal. So, $\det(A) = 1 \cdot 2 \cdot 3 = 6$.

Example 7.8.3

Show that the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix},$$

(with entries understood to be in $\mathbb{R}$) is invertible, and using Theorem 7.8.2, find its inverse A^{-1}.

Solution. The matrix A is upper triangular, and so its determinant can be computed by multiplying the entries along the main diagonal. So, $\det(A) = 1 \cdot 2 \cdot 3 = 6$. Since $\det(A) \neq 0$, Theorem 7.4.1 guarantees that A is invertible.

Solution (continued). Reminder: $\det(A) = 6$, A is invertible.

Solution (continued). Reminder: $\det(A) = 6$, A is invertible.

In Example 7.8.1, we compute the adjugate matrix of A:

$$\text{adj}(A) = \begin{bmatrix} 6 & -3 & 0 \\ 0 & 3 & -2 \\ 0 & 0 & 2 \end{bmatrix}.$$

So, by Theorem 7.8.5, we have that

$$\begin{aligned} A^{-1} &= \tfrac{1}{\det(A)}\text{adj}(A) = \tfrac{1}{6}\begin{bmatrix} 6 & -3 & 0 \\ 0 & 3 & -2 \\ 0 & 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -1/2 & 0 \\ 0 & 1/2 & -1/3 \\ 0 & 0 & 1/3 \end{bmatrix}. \end{aligned}$$

□

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ ($n \geq 2$). Then

$$\text{adj}(A)\, A \;=\; A\, \text{adj}(A) \;=\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$.

Theorem 7.8.2

Let $\mathbb{F}$ be a field, and let $A \in \mathbb{F}^{n \times n}$ $(n \geq 2)$. Then

$$\text{adj}(A)\, A \;=\; A\, \text{adj}(A) \;=\; \det(A) I_n.$$

Consequently, if A is invertible, then $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$.

Corollary 7.8.4

Let $\mathbb{F}$ be a field, and let $a, b, c, d \in \mathbb{F}$. Then the matrix

$$A \;=\; \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible if and only if $ad \neq bc$, and in this case, the inverse of A is given by the formula

$$A^{-1} \;=\; \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Corollary 7.8.4

Let $\mathbb{F}$ be a field, and let $a, b, c, d \in \mathbb{F}$. Then the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible if and only if $ad \neq bc$, and in this case, the inverse of A is given by the formula

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Proof (outline).

Corollary 7.8.4

Let $\mathbb{F}$ be a field, and let $a, b, c, d \in \mathbb{F}$. Then the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible if and only if $ad \neq bc$, and in this case, the inverse of A is given by the formula

$$A^{-1} = \tfrac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Proof (outline). It is easy to see that

$$\det(A) = ad - bc \qquad \text{and} \qquad \text{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Corollary 7.8.4

Let $\mathbb{F}$ be a field, and let $a, b, c, d \in \mathbb{F}$. Then the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible if and only if $ad \neq bc$, and in this case, the inverse of A is given by the formula

$$A^{-1} = \tfrac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Proof (outline). It is easy to see that

$$\det(A) = ad - bc \qquad \text{and} \qquad \operatorname{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

We know that A is invertible iff $\det(A) \neq 0$, which happens precisely when $ad \neq bc$.

Corollary 7.8.4

Let $\mathbb{F}$ be a field, and let $a, b, c, d \in \mathbb{F}$. Then the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible if and only if $ad \neq bc$, and in this case, the inverse of A is given by the formula

$$A^{-1} = \tfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Proof (outline). It is easy to see that

$$\det(A) = ad - bc \qquad \text{and} \qquad \operatorname{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

We know that A is invertible iff $\det(A) \neq 0$, which happens precisely when $ad \neq bc$. In this case, Theorem 7.8.2 guarantees that

$$A^{-1} = \tfrac{1}{\det(A)}\operatorname{adj}(A) = \tfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

which is what we needed to show. □

3. Algebraically closed fields (subsec. 2.4.5 of the Lecture Notes)

3. Algebraically closed fields (subsec. 2.4.5 of the Lecture Notes)

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

3. Algebraically closed fields (subsec. 2.4.5 of the Lecture Notes)

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

The Fundamental Theorem of Algebra

Any non-constant polynomial with complex coefficients has a complex root.

- By the Fundamental Theorem of Algebra, the field $\mathbb{C}$ is algebraically closed.

3. Algebraically closed fields (subsec. 2.4.5 of the Lecture Notes)

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

The Fundamental Theorem of Algebra

Any non-constant polynomial with complex coefficients has a complex root.

- By the Fundamental Theorem of Algebra, the field $\mathbb{C}$ is algebraically closed.
- On the other hand, $\mathbb{R}$ is not algebraically closed, and similarly, neither is $\mathbb{Q}$.
  - For example, the polynomial $x^2 + 1$ has no roots in $\mathbb{R}$ (and in particular, it has no roots in $\mathbb{Q}$).
  - It does, however, have two complex roots, namely, i and $-i$.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- No finite field is algebraically closed.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- No finite field is algebraically closed.
  - To see this, consider any finite field $\mathbb{F} = \{f_1, \ldots, f_t\}$ ($t \geq 2$), and consider the polynomial

$$p(x) = (x - f_1) \ldots (x - f_t) + 1,$$

which is a polynomial of degree t with coefficients in $\mathbb{F}$.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- No finite field is algebraically closed.
  - To see this, consider any finite field $\mathbb{F} = \{f_1, \dots, f_t\}$ ($t \geq 2$), and consider the polynomial

$$p(x) = (x - f_1) \dots (x - f_t) + 1,$$

    which is a polynomial of degree t with coefficients in $\mathbb{F}$.
  - Then for each $i \in \{1, \dots, t\}$, we have that $p(f_i) = 1$, and consequently, f_i is not a root of $p(x)$.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- No finite field is algebraically closed.
  - To see this, consider any finite field $\mathbb{F} = \{f_1, \dots, f_t\}$ $(t \geq 2)$, and consider the polynomial

$$p(x) \quad = \quad (x - f_1) \dots (x - f_t) + 1,$$

    which is a polynomial of degree t with coefficients in $\mathbb{F}$.
  - Then for each $i \in \{1, \dots, t\}$, we have that $p(f_i) = 1$, and consequently, f_i is not a root of $p(x)$.
  - Since $\mathbb{F} = \{f_1, \dots, f_t\}$, we see that $p(x)$ has no roots in $\mathbb{F}$.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- No finite field is algebraically closed.
  - To see this, consider any finite field $\mathbb{F} = \{f_1, \dots, f_t\}$ ($t \geq 2$), and consider the polynomial

    $$p(x) \quad = \quad (x - f_1) \dots (x - f_t) + 1,$$

    which is a polynomial of degree t with coefficients in $\mathbb{F}$.
  - Then for each $i \in \{1, \dots, t\}$, we have that $p(f_i) = 1$, and consequently, f_i is not a root of $p(x)$.
  - Since $\mathbb{F} = \{f_1, \dots, f_t\}$, we see that $p(x)$ has no roots in $\mathbb{F}$.
- Thus, of the fields that we have seen so far, namely, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$ (where p is a prime number), only the field $\mathbb{C}$ is algebraically closed.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- No finite field is algebraically closed.
  - To see this, consider any finite field $\mathbb{F} = \{f_1, \dots, f_t\}$ ($t \geq 2$), and consider the polynomial

    $$p(x) \quad = \quad (x - f_1) \dots (x - f_t) + 1,$$

    which is a polynomial of degree t with coefficients in $\mathbb{F}$.
  - Then for each $i \in \{1, \dots, t\}$, we have that $p(f_i) = 1$, and consequently, f_i is not a root of $p(x)$.
  - Since $\mathbb{F} = \{f_1, \dots, f_t\}$, we see that $p(x)$ has no roots in $\mathbb{F}$.
- Thus, of the fields that we have seen so far, namely, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$ (where p is a prime number), only the field $\mathbb{C}$ is algebraically closed.
- Other algebraically closed fields do exist, but we will not study them in this course.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- It can be shown (though we will not give a formal proof) that any non-constant polynomial with coefficients in an algebraically closed field $\mathbb{F}$ can be factored into linear terms in a unique way.

- More precisely, if $p(x)$ is a polynomial of degree $n \geq 1$, and with coefficients in an algebraically closed field $\mathbb{F}$, then there exist numbers $a, \alpha_1, \dots, \alpha_\ell$ in $\mathbb{F}$ s.t. $a \neq 0$ and s.t. $\alpha_1, \dots, \alpha_\ell$ are pairwise distinct, and positive integers $n_1, \dots, n_\ell$ satisfying $n_1 + \cdots + n_\ell = n$, s.t.

$$p(x) = a(x - \alpha_1)^{n_1} \dots (x - \alpha_\ell)^{n_\ell}.$$

  Moreover, $a, \alpha_1, \dots, \alpha_\ell, n_1, \dots, n_\ell$ are uniquely determined by the polynomial $p(x)$, up to a permutation of the α_i's and the corresponding n_i's.

- More precisely, if $p(x)$ is a polynomial of degree $n \geq 1$, and with coefficients in an algebraically closed field $\mathbb{F}$, then there exist numbers $a, \alpha_1, \dots, \alpha_\ell$ in $\mathbb{F}$ s.t. $a \neq 0$ and s.t. $\alpha_1, \dots, \alpha_\ell$ are pairwise distinct, and positive integers $n_1, \dots, n_\ell$ satisfying $n_1 + \dots + n_\ell = n$, s.t.

$$p(x) = a(x - \alpha_1)^{n_1} \dots (x - \alpha_\ell)^{n_\ell}.$$

  Moreover, $a, \alpha_1, \dots, \alpha_\ell, n_1, \dots, n_\ell$ are uniquely determined by the polynomial $p(x)$, up to a permutation of the α_i's and the corresponding n_i's.
- Here, a is the leading coefficient of $p(x)$, i.e. the coefficient in front of x^n. Numbers $\alpha_1, \dots, \alpha_\ell$ are the roots of $p(x)$ with *multiplicities* $n_1, \dots, n_\ell$, respectively.

- More precisely, if $p(x)$ is a polynomial of degree $n \geq 1$, and with coefficients in an algebraically closed field $\mathbb{F}$, then there exist numbers $a, \alpha_1, \dots, \alpha_\ell$ in $\mathbb{F}$ s.t. $a \neq 0$ and s.t. $\alpha_1, \dots, \alpha_\ell$ are pairwise distinct, and positive integers $n_1, \dots, n_\ell$ satisfying $n_1 + \dots + n_\ell = n$, s.t.

$$p(x) = a(x - \alpha_1)^{n_1} \dots (x - \alpha_\ell)^{n_\ell}.$$

  Moreover, $a, \alpha_1, \dots, \alpha_\ell, n_1, \dots, n_\ell$ are uniquely determined by the polynomial $p(x)$, up to a permutation of the α_i's and the corresponding n_i's.
- Here, a is the leading coefficient of $p(x)$, i.e. the coefficient in front of x^n. Numbers $\alpha_1, \dots, \alpha_\ell$ are the roots of $p(x)$ with *multiplicities* $n_1, \dots, n_\ell$, respectively.
- If we think of each α_i as being a root "n_i times" (due to its multiplicity), then we see that the n-th degree polynomial $p(x)$ has exactly n roots in $\mathbb{F}$.

Definition

An *algebraically closed field* is a field $\mathbb{F}$ that has the property that every non-constant polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$.

- The discussion from the previous slide is often summarized as follows:

  Every n-th degree polynomial (with $n \geq 1$) with coefficients in an algebraically closed field has exactly n roots in that field, when multiplicities are taken into account.

4. Common roots of polynomials via determinants

4. Common roots of polynomials via determinants

- Any non-constant polynomial with coefficients in an algebraically closed field $\mathbb{F}$ has a root in $\mathbb{F}$. However, there is no general formula for computing such a root.

4. Common roots of polynomials via determinants

- Any non-constant polynomial with coefficients in an algebraically closed field $\mathbb{F}$ has a root in $\mathbb{F}$. However, there is no general formula for computing such a root.
- So, it may be surprising that, given arbitrary polynomials $p(x)$ and $q(x)$ with coefficients in an algebraically closed field $\mathbb{F}$, we can use determinants to determine whether $p(x)$ and $q(x)$ have a common root, i.e. whether there exists a number $x_0 \in \mathbb{F}$ for which we have $p(x_0) = 0$ and $q(x_0) = 0$ (next slide).

4. Common roots of polynomials via determinants

- Any non-constant polynomial with coefficients in an algebraically closed field $\mathbb{F}$ has a root in $\mathbb{F}$. However, there is no general formula for computing such a root.
- So, it may be surprising that, given arbitrary polynomials $p(x)$ and $q(x)$ with coefficients in an algebraically closed field $\mathbb{F}$, we can use determinants to determine whether $p(x)$ and $q(x)$ have a common root, i.e. whether there exists a number $x_0 \in \mathbb{F}$ for which we have $p(x_0) = 0$ and $q(x_0) = 0$ (next slide).
- However, the determinant in question will only tell us whether such a common root exists; it provides no information on how one might actually compute such a root.

Theorem 7.11.1

Let $\mathbb{F}$ be an **algebraically closed field**. Let m and n be positive integers, and let $p(x) = \sum_{i=0}^{m} a_i x^i$ ($a_m \neq 0$) and $q(x) = \sum_{i=0}^{n} b_i x^i$ ($b_n \neq 0$) be polynomials with coefficients in $\mathbb{F}$. Let P be the $n \times (n+m)$ matrix whose j-th row (for $j \in \{1, \ldots, n\}$) is

$$\left[\quad \underbrace{0 \quad \ldots \quad 0}_{j-1} \quad a_m \quad a_{m-1} \quad \ldots \quad a_0 \quad \underbrace{0 \quad \ldots \quad 0}_{n-j} \quad \right],$$

and let Q be the $m \times (n+m)$ matrix whose j-th row (for $j \in \{1, \ldots, m\}$) is

$$\left[\quad \underbrace{0 \quad \ldots \quad 0}_{j-1} \quad b_n \quad b_{n-1} \quad \ldots \quad b_0 \quad \underbrace{0 \quad \ldots \quad 0}_{m-j} \quad \right].$$

Then $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$ iff

$$\det\left(\left[\frac{P}{Q} \right] \right) = 0.$$

- First a more detailed explanation of how out matrix is formed, then an example, then a proof.

- For example, if $m = 3$ and $n = 5$, so that
  - $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0$,
  - $q(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$,

  then we have

$$\left[\begin{array}{c} P \\ \hdashline Q \end{array}\right] = \left[\begin{array}{cccccccc} a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 \\ 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & 0 & 0 & a_3 & a_2 & a_1 & a_0 \\ \hdashline b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \end{array}\right]_{8\times 8}.$$

Example 7.11.2

Determine whether the polynomials $p(x) = 5x^3 - 2x^2 + x - 4$ and $q(x) = 7x^2 - 6x - 1$ have a common complex root.

Proof.

Example 7.11.2

Determine whether the polynomials $p(x) = 5x^3 - 2x^2 + x - 4$ and $q(x) = 7x^2 - 6x - 1$ have a common complex root.

Proof. In this case, it is easy to see that $p(1) = 0$ and $q(1) = 0$, and so 1 is a common root of $p(x)$ and $q(x)$. However, let us use Theorem 7.11.1, in order to illustrate how this theorem can be applied.

Using the notation of Theorem 7.11.1, we have that $m = 3$, $n = 2$, and the matrices P and Q are given by

- $P = \begin{bmatrix} 5 & -2 & 1 & -4 & 0 \\ 0 & 5 & -2 & 1 & -4 \end{bmatrix}$;
- $Q = \begin{bmatrix} 7 & -6 & -1 & 0 & 0 \\ 0 & 7 & -6 & -1 & 0 \\ 0 & 0 & 7 & -6 & -1 \end{bmatrix}$.

Example 7.11.2

Determine whether the polynomials $p(x) = 5x^3 - 2x^2 + x - 4$ and $q(x) = 7x^2 - 6x - 1$ have a common complex root.

Proof (continued). We now have that

$$\det\left(\begin{bmatrix} P \\ \hdashline Q \end{bmatrix}\right) = \begin{vmatrix} 5 & -2 & 1 & -4 & 0 \\ 0 & 5 & -2 & 1 & -4 \\ \hdashline 7 & -6 & -1 & 0 & 0 \\ 0 & 7 & -6 & -1 & 0 \\ 0 & 0 & 7 & -6 & -1 \end{vmatrix} = 0.$$

Theorem 7.11.2 now guarantees that $p(x)$ and $q(x)$ have a common complex root. $\square$

Theorem 7.11.1

Let $\mathbb{F}$ be an **algebraically closed field**. Let m and n be positive integers, and let $p(x) = \sum_{i=0}^{m} a_i x^i$ ($a_m \neq 0$) and $q(x) = \sum_{i=0}^{n} b_i x^i$ ($b_n \neq 0$) be polynomials with coefficients in $\mathbb{F}$. Let P be the $n \times (n+m)$ matrix whose j-th row (for $j \in \{1, \dots, n\}$) is

$$\left[\begin{array}{ccccccc} \underbrace{0 \quad \dots \quad 0}_{j-1} & a_m & a_{m-1} & \dots & a_0 & \underbrace{0 \quad \dots \quad 0}_{n-j} \end{array} \right],$$

and let Q be the $m \times (n+m)$ matrix whose j-th row (for $j \in \{1, \dots, m\}$) is

$$\left[\begin{array}{ccccccc} \underbrace{0 \quad \dots \quad 0}_{j-1} & b_n & b_{n-1} & \dots & b_0 & \underbrace{0 \quad \dots \quad 0}_{m-j} \end{array} \right].$$

Then $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$ iff

$$\det\left(\left[\begin{array}{c} P \\ \hline Q \end{array} \right] \right) = 0.$$

- Let's prove the theorem!

Proof.

Claim. *Polynomials $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$ iff there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ that satisfy the following:*

- $deg(r(x)) \leq n - 1$;
- $deg(s(x)) \leq m - 1$;
- $r(x)p(x) + s(x)q(x) = 0$.

Proof of the Claim.

Proof.

Claim. *Polynomials $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$ iff there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ that satisfy the following:*

- $deg(r(x)) \leq n-1$;
- $deg(s(x)) \leq m-1$;
- $r(x)p(x) + s(x)q(x) = 0$.

Proof of the Claim. Suppose first that $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$, say α.

Proof.

Claim. *Polynomials $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$ iff there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ that satisfy the following:*

- $deg(r(x)) \leq n - 1$;
- $deg(s(x)) \leq m - 1$;
- $r(x)p(x) + s(x)q(x) = 0$.

Proof of the Claim. Suppose first that $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$, say α. Then we set

$$r(x) := \tfrac{q(x)}{x-\alpha} \qquad \text{and} \qquad s(x) := -\tfrac{p(x)}{x-\alpha},$$

and we observe that $\deg(r(x)) = \deg(q(x)) - 1 = n - 1$, $\deg(s(x)) = \deg(p(x)) - 1 = m - 1$, and

$$r(x)p(x) + s(x)q(x) \;=\; \tfrac{q(x)p(x)}{x-\alpha} - \tfrac{p(x)q(x)}{x-\alpha} \;=\; 0.$$

Proof of the Claim (continued). Suppose conversely there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ s.t.

- $\deg(r(x)) \leq n - 1$;
- $\deg(s(x)) \leq m - 1$;
- $r(x)p(x) + s(x)q(x) = 0$.

WTS $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$.

Proof of the Claim (continued). Suppose conversely there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ s.t.

- $\deg(r(x)) \leq n - 1$;
- $\deg(s(x)) \leq m - 1$;
- $r(x)p(x) + s(x)q(x) = 0$.

WTS $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$.

Then $r(x)p(x)$ and $s(x)q(x)$ are non-constant polynomials with coefficients in $\mathbb{F}$, and they have exactly the same roots with the same corresponding multiplicities.

Proof of the Claim (continued). Suppose conversely there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ s.t.

- $\deg(r(x)) \leq n-1$;
- $\deg(s(x)) \leq m-1$;
- $r(x)p(x) + s(x)q(x) = 0$.

WTS $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$.

Then $r(x)p(x)$ and $s(x)q(x)$ are non-constant polynomials with coefficients in $\mathbb{F}$, and they have exactly the same roots with the same corresponding multiplicities.

Since $\deg(p(x)) = m$, we know that $p(x)$ has exactly m roots in $\mathbb{F}$ (when multiplicities are taken into account).

- Here, we are using the fact that $\mathbb{F}$ is algebraically closed.

Proof of the Claim (continued). Suppose conversely there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ s.t.

- $\deg(r(x)) \leq n - 1$;
- $\deg(s(x)) \leq m - 1$;
- $r(x)p(x) + s(x)q(x) = 0$.

WTS $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$.

Then $r(x)p(x)$ and $s(x)q(x)$ are non-constant polynomials with coefficients in $\mathbb{F}$, and they have exactly the same roots with the same corresponding multiplicities.

Since $\deg(p(x)) = m$, we know that $p(x)$ has exactly m roots in $\mathbb{F}$ (when multiplicities are taken into account).

- Here, we are using the fact that $\mathbb{F}$ is algebraically closed.

But $\deg(s(x)) \leq m - 1$, and so at least one of the roots of $p(x)$ either fails to be a root of $s(x)$, or is a root of $s(x)$ but has smaller multiplicity in $s(x)$ than in $p(x)$.

Proof of the Claim (continued). Suppose conversely there exist non-zero polynomials $r(x)$ and $s(x)$ with coefficients in $\mathbb{F}$ s.t.

- $\deg(r(x)) \leq n-1$;
- $\deg(s(x)) \leq m-1$;
- $r(x)p(x) + s(x)q(x) = 0$.

WTS $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$.

Then $r(x)p(x)$ and $s(x)q(x)$ are non-constant polynomials with coefficients in $\mathbb{F}$, and they have exactly the same roots with the same corresponding multiplicities.

Since $\deg(p(x)) = m$, we know that $p(x)$ has exactly m roots in $\mathbb{F}$ (when multiplicities are taken into account).

- Here, we are using the fact that $\mathbb{F}$ is algebraically closed.

But $\deg(s(x)) \leq m-1$, and so at least one of the roots of $p(x)$ either fails to be a root of $s(x)$, or is a root of $s(x)$ but has smaller multiplicity in $s(x)$ than in $p(x)$. This root of $p(x)$ must therefore be a root of $q(x)$. ♦

Proof (continued). *We have now proven the Claim below:*

Claim. *Polynomials* $p(x)$ *and* $q(x)$ *have a common root in* $\mathbb{F}$ *iff there exist non-zero polynomials* $r(x)$ *and* $s(x)$ *with coefficients in* $\mathbb{F}$ *that satisfy the following:*

- $deg(r(x)) \leq n - 1$;
- $deg(s(x)) \leq m - 1$;
- $r(x)p(x) + s(x)q(x) = 0$.

Proof (continued). In view of the Claim, it now suffices to determine if there exist non-zero polynomials $r(x) = \sum_{i=0}^{n-1} c_i x^i$ and $s(x) = \sum_{i=0}^{m-1} d_i x^i$ s.t. $r(x)p(x) + s(x)q(x) = 0$.

Proof (continued). In view of the Claim, it now suffices to determine if there exist non-zero polynomials $r(x) = \sum_{i=0}^{n-1} c_i x^i$ and $s(x) = \sum_{i=0}^{m-1} d_i x^i$ s.t. $r(x)p(x) + s(x)q(x) = 0$.

So, we need to determine if there exist $c_0, \dots, c_{n-1}, d_0, \dots, d_{m-1} \in \mathbb{F}$ s.t. at least one of $c_0, \dots, c_{n-1}$ is non-zero and at least one of $d_0, \dots, d_{m-1}$ is non-zero, and s.t.

$$\underbrace{\Big(\sum_{i=0}^{n-1} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{m} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{m-1} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{n} b_i x^i\Big)}_{=q(x)} = 0.$$

Proof (continued). In view of the Claim, it now suffices to determine if there exist non-zero polynomials $r(x) = \sum_{i=0}^{n-1} c_i x^i$ and $s(x) = \sum_{i=0}^{m-1} d_i x^i$ s.t. $r(x)p(x) + s(x)q(x) = 0$.

So, we need to determine if there exist $c_0, \dots, c_{n-1}, d_0, \dots, d_{m-1} \in \mathbb{F}$ s.t. at least one of $c_0, \dots, c_{n-1}$ is non-zero and at least one of $d_0, \dots, d_{m-1}$ is non-zero, and s.t.

$$\underbrace{\Big(\sum_{i=0}^{n-1} c_i x^i\Big)}_{=r(x)} \underbrace{\Big(\sum_{i=0}^{m} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{m-1} d_i x^i\Big)}_{=s(x)} \underbrace{\Big(\sum_{i=0}^{n} b_i x^i\Big)}_{=q(x)} \quad = \quad 0.$$

But obviously, if $c_0, \dots, c_{n-1}$ are all zero, then $d_0, \dots, d_{m-1}$ are all zero, and vice versa.

Proof (continued). In view of the Claim, it now suffices to determine if there exist non-zero polynomials $r(x) = \sum_{i=0}^{n-1} c_i x^i$ and $s(x) = \sum_{i=0}^{m-1} d_i x^i$ s.t. $r(x)p(x) + s(x)q(x) = 0$.

So, we need to determine if there exist $c_0, \dots, c_{n-1}, d_0, \dots, d_{m-1} \in \mathbb{F}$ s.t. at least one of $c_0, \dots, c_{n-1}$ is non-zero and at least one of $d_0, \dots, d_{m-1}$ is non-zero, and s.t.

$$\underbrace{\Big(\sum_{i=0}^{n-1} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{m} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{m-1} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{n} b_i x^i\Big)}_{=q(x)} = 0.$$

But obviously, if $c_0, \dots, c_{n-1}$ are all zero, then $d_0, \dots, d_{m-1}$ are all zero, and vice versa. So, we in fact need to determine if the above equality holds for some numbers $c_0, \dots, c_{n-1}, d_0, \dots, d_{m-1} \in \mathbb{F}$, at least one of which is non-zero.

Proof (continued). Reminder:

$$\underbrace{\Big(\sum_{i=0}^{n-1} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{m} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{m-1} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{n} b_i x^i\Big)}_{=q(x)} \quad = \quad 0.$$

We now write the polynomial on the left-hand-side in the standard form, and we set all the coefficients that we obtain equal to zero.

- We can do this since our polynomial is identically zero, i.e. it is zero as a polynomial. This means precisely that all its coefficients are zero.

Proof (continued). Reminder:

$$\underbrace{\Big(\sum_{i=0}^{n-1} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{m} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{m-1} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{n} b_i x^i\Big)}_{=q(x)} \quad = \quad 0.$$

This yields a system of $n + m$ linear equations in the variables $c_{n-1}, \ldots, c_0, d_{m-1}, \ldots, d_0$ (we treat $a_m, \ldots, a_0, b_n, \ldots, b_0$ as constants).

Proof (continued). Reminder:

$$\underbrace{\Big(\sum_{i=0}^{n-1} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{m} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{m-1} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{n} b_i x^i\Big)}_{=q(x)} \quad = \quad 0.$$

This yields a system of $n+m$ linear equations in the variables $c_{n-1}, \ldots, c_0, d_{m-1}, \ldots, d_0$ (we treat $a_m, \ldots, a_0, b_n, \ldots, b_0$ as constants).

In each equation, we arrange the variables $c_{n-1}, \ldots, c_0, d_{m-1}, \ldots, d_0$ in this order from left to right. We arrange the equations for the coefficients in front of $x^{n+m-1}, \ldots, x^1, x^0$ from top to bottom.

Proof (continued). Reminder:

$$\underbrace{\left(\sum_{i=0}^{n-1} c_i x^i\right)}_{=r(x)} \underbrace{\left(\sum_{i=0}^{m} a_i x^i\right)}_{=p(x)} + \underbrace{\left(\sum_{i=0}^{m-1} d_i x^i\right)}_{=s(x)} \underbrace{\left(\sum_{i=0}^{n} b_i x^i\right)}_{=q(x)} = 0.$$

This yields a system of $n+m$ linear equations in the variables $c_{n-1}, \ldots, c_0, d_{m-1}, \ldots, d_0$ (we treat $a_m, \ldots, a_0, b_n, \ldots, b_0$ as constants).

In each equation, we arrange the variables $c_{n-1}, \ldots, c_0, d_{m-1}, \ldots, d_0$ in this order from left to right. We arrange the equations for the coefficients in front of $x^{n+m-1}, \ldots, x^1, x^0$ from top to bottom. We then rewrite this linear system as a matrix-vector equation

$$A \left[\begin{array}{ccc:ccc} c_{n-1} & \ldots & c_0 & d_{m-1} & \ldots & d_0 \end{array}\right]^T = \mathbf{0},$$

and we observe that the coefficient matrix A satisfies $A^T = \left[\begin{array}{c} P \\ \hdashline Q \end{array}\right]$.

- Intermission: Let's look at an example with $m = 3$ and $n = 5$.

Intermission: Example with $m = 3$ and $n = 5$. Then

- $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0$,
- $q(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$,
- $r(x) = c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$,
- $s(t) = d_2x^2 + d_1x + d_0$,

then our equation becomes

$$\underbrace{\Big(\sum_{i=0}^{4} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{3} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{2} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{5} b_i x^i\Big)}_{=q(x)} \quad = \quad 0$$

which yields the system of linear equations on the next slide (we consider the coefficients in front of $x^7, x^6, x^5, x^4, x^3, x^2, x^1, x^0$ from top to bottom, and we arrange the variables $c_4, c_3, c_2, c_1, c_0, d_2, d_1, d_0$ from left to right).

Intermission (continued): Example with $m = 3$ and $n = 5$.

Reminder: our equation was

$$\underbrace{\left(\sum_{i=0}^{4} c_i x^i\right)}_{=r(x)} \underbrace{\left(\sum_{i=0}^{3} a_i x^i\right)}_{=p(x)} + \underbrace{\left(\sum_{i=0}^{2} d_i x^i\right)}_{=s(x)} \underbrace{\left(\sum_{i=0}^{5} b_i x^i\right)}_{=q(x)} \quad = \quad 0$$

	c_4		c_3		c_2		c_1		c_0		d_2		d_1		d_0		
x^7	$a_3 c_4$									$+$	$b_5 d_2$					$=$	0
x^6	$a_2 c_4$	$+$	$a_3 c_3$							$+$	$b_4 d_2$	$+$	$b_5 d_1$			$=$	0
x^5	$a_1 c_4$	$+$	$a_2 c_3$	$+$	$a_3 c_2$					$+$	$b_3 d_2$	$+$	$b_4 d_1$	$+$	$b_5 d_0$	$=$	0
x^4	$a_0 c_4$	$+$	$a_1 c_3$	$+$	$a_2 c_2$	$+$	$a_3 c_1$			$+$	$b_2 d_2$	$+$	$b_3 d_1$	$+$	$b_4 d_0$	$=$	0
x^3			$a_0 c_3$	$+$	$a_1 c_2$	$+$	$a_2 c_1$	$+$	$a_3 c_0$	$+$	$b_1 d_2$	$+$	$b_2 d_1$	$+$	$b_3 d_0$	$=$	0
x^2					$a_0 c_2$	$+$	$a_1 c_1$	$+$	$a_2 c_0$	$+$	$b_0 d_2$	$+$	$b_1 d_1$	$+$	$b_2 d_0$	$=$	0
x^1							$a_0 c_1$	$+$	$a_1 c_0$			$+$	$b_0 d_1$	$+$	$b_1 d_0$	$=$	0
x^0									$a_0 c_0$					$+$	$b_0 d_0$	$=$	0

Intermission (continued): Example with $m = 3$ and $n = 5$.
Reminder: our equation was

$$\underbrace{\Big(\sum_{i=0}^{4} c_i x^i\Big)}_{=r(x)}\underbrace{\Big(\sum_{i=0}^{3} a_i x^i\Big)}_{=p(x)} + \underbrace{\Big(\sum_{i=0}^{2} d_i x^i\Big)}_{=s(x)}\underbrace{\Big(\sum_{i=0}^{5} b_i x^i\Big)}_{=q(x)} \quad = \quad 0$$

	c_4		c_3		c_2		c_1		c_0		d_2		d_1		d_0		
x^7	$a_3 c_4$									$+$	$b_5 d_2$					$=$	0
x^6	$a_2 c_4$	$+$	$a_3 c_3$							$+$	$b_4 d_2$	$+$	$b_5 d_1$			$=$	0
x^5	$a_1 c_4$	$+$	$a_2 c_3$	$+$	$a_3 c_2$					$+$	$b_3 d_2$	$+$	$b_4 d_1$	$+$	$b_5 d_0$	$=$	0
x^4	$a_0 c_4$	$+$	$a_1 c_3$	$+$	$a_2 c_2$	$+$	$a_3 c_1$			$+$	$b_2 d_2$	$+$	$b_3 d_1$	$+$	$b_4 d_0$	$=$	0
x^3			$a_0 c_3$	$+$	$a_1 c_2$	$+$	$a_2 c_1$	$+$	$a_3 c_0$	$+$	$b_1 d_2$	$+$	$b_2 d_1$	$+$	$b_3 d_0$	$=$	0
x^2					$a_0 c_2$	$+$	$a_1 c_1$	$+$	$a_2 c_0$	$+$	$b_0 d_2$	$+$	$b_1 d_1$	$+$	$b_2 d_0$	$=$	0
x^1							$a_0 c_1$	$+$	$a_1 c_0$			$+$	$b_0 d_1$	$+$	$b_1 d_0$	$=$	0
x^0									$a_0 c_0$					$+$	$b_0 d_0$	$=$	0

This linear system, in turn, translates into the following matrix-vector equation (next slide):

Intermission (continued): Example with $m = 3$ and $n = 5$.

$$\left[\begin{array}{ccccc:ccc} a_3 & 0 & 0 & 0 & 0 & b_5 & 0 & 0 \\ a_2 & a_3 & 0 & 0 & 0 & b_4 & b_5 & 0 \\ a_1 & a_2 & a_3 & 0 & 0 & b_3 & b_4 & b_5 \\ a_0 & a_1 & a_2 & a_3 & 0 & b_2 & b_3 & b_4 \\ 0 & a_0 & a_1 & a_2 & a_3 & b_1 & b_2 & b_3 \\ 0 & 0 & a_0 & a_1 & a_2 & b_0 & b_1 & b_2 \\ 0 & 0 & 0 & a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & 0 & 0 & 0 & a_0 & 0 & 0 & b_0 \end{array}\right] \left[\begin{array}{c} c_4 \\ c_3 \\ c_2 \\ c_1 \\ c_0 \\ \hdashline d_2 \\ d_1 \\ d_0 \end{array}\right] = \mathbf{0}.$$

Intermission (continued): Example with $m = 3$ and $n = 5$.

$$\left[\begin{array}{ccccc|ccc} a_3 & 0 & 0 & 0 & 0 & b_5 & 0 & 0 \\ a_2 & a_3 & 0 & 0 & 0 & b_4 & b_5 & 0 \\ a_1 & a_2 & a_3 & 0 & 0 & b_3 & b_4 & b_5 \\ a_0 & a_1 & a_2 & a_3 & 0 & b_2 & b_3 & b_4 \\ 0 & a_0 & a_1 & a_2 & a_3 & b_1 & b_2 & b_3 \\ 0 & 0 & a_0 & a_1 & a_2 & b_0 & b_1 & b_2 \\ 0 & 0 & 0 & a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & 0 & 0 & 0 & a_0 & 0 & 0 & b_0 \end{array}\right] \left[\begin{array}{c} c_4 \\ c_3 \\ c_2 \\ c_1 \\ c_0 \\ \hline d_2 \\ d_1 \\ d_0 \end{array}\right] = \mathbf{0}.$$

The transpose of the coefficient matrix that we obtained is precisely the matrix

$$\left[\begin{array}{c} P \\ \hline Q \end{array}\right] = \left[\begin{array}{cccccccc} a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 \\ 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & 0 & 0 & a_3 & a_2 & a_1 & a_0 \\ \hline b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \end{array}\right]_{8\times 8}.$$

Proof (continued). We now have the following sequence of equivalent statements:

$$p(x) \text{ and } q(x) \text{ have a common root in } \mathbb{F} \iff A \left[\begin{array}{ccc|ccc} c_{n-1} & \dots & c_0 & d_{m-1} & \dots & d_0 \end{array}\right]^T = \mathbf{0} \text{ has a non-zero solution}$$

$$\stackrel{(*)}{\iff} A \text{ is non-invertible}$$

$$\stackrel{(*)}{\iff} A^T = \left[\begin{array}{c} P \\ \hline Q \end{array}\right] \text{ is non-invertible}$$

$$\stackrel{(*)}{\iff} \det\left(\left[\begin{array}{c} P \\ \hline Q \end{array}\right]\right) = 0,$$

where all three instances of (*) follow from the Invertible Matrix Theorem. □

Theorem 7.11.1

Let $\mathbb{F}$ be an **algebraically closed field**. Let m and n be positive integers, and let $p(x) = \sum_{i=0}^{m} a_i x^i$ ($a_m \neq 0$) and $q(x) = \sum_{i=0}^{n} b_i x^i$ ($b_n \neq 0$) be polynomials with coefficients in $\mathbb{F}$. Let P be the $n \times (n+m)$ matrix whose j-th row (for $j \in \{1, \dots, n\}$) is

$$\left[\quad \underbrace{0 \quad \dots \quad 0}_{j-1} \quad a_m \quad a_{m-1} \quad \dots \quad a_0 \quad \underbrace{0 \quad \dots \quad 0}_{n-j} \quad \right],$$

and let Q be the $m \times (n+m)$ matrix whose j-th row (for $j \in \{1, \dots, m\}$) is

$$\left[\quad \underbrace{0 \quad \dots \quad 0}_{j-1} \quad b_n \quad b_{n-1} \quad \dots \quad b_0 \quad \underbrace{0 \quad \dots \quad 0}_{m-j} \quad \right].$$

Then $p(x)$ and $q(x)$ have a common root in $\mathbb{F}$ iff

$$\det\left(\left[\begin{array}{c} P \\ \hline Q \end{array} \right] \right) = 0.$$