# Chapter 2

# Linear Systems of Equations

## 2.1 One equation in multiple unknowns

We start by considering one linear equation in $n$ unknowns:

***Definition 2.1*** *A linear equation in $n$ unknowns $X^1, \ldots, X^n$ with coefficients $a^1, \ldots, a^n, b \in \mathbb{F}$ is an equation of the form*

$$a_1 X^1 + a_2 X^2 + \cdots + a_n X^n = b. \tag{2.1}$$

*The scalar $a_i$ is called the **coefficient** (מקדם) of the $i$-th unknown. We write the coefficients of the $X^i$'s in the form*

$$[a_1, a_2, \ldots, a_n] \in \mathbb{F}^n_{row}.$$

*We also refer to the **extended** list of coefficients, which includes the right-hand side*

$$[a_1, a_2, \ldots, a_n, b] \in \mathbb{F}^{n+1}_{row}.$$

**Example**: Consider the following equation in two unknowns,

$$2(X^1 + X^2 - 6) = 3X^2 + 4(8 - X^1).$$

This is a linear equation in two unknowns albeit not of the form (2.1). By algebraic manipulations (based on the axioms of field) we can rewrite it as

$$6X^1 - X^2 = 44,$$

which in the above notation corresponds to the extended list of coefficients $[a_1, a_2, b] = [6, -1, 44]$. ▲▲▲

***Definition 2.2*** *A solution to* (2.1) *is an n-tuple of field elements,*

$$\begin{bmatrix} x^1 \\ \vdots \\ x^n \end{bmatrix} \in \mathbb{F}^n_{col},$$

*such that*

$$a_1 x^1 + \cdots + a_n x^n = b. \tag{2.2}$$

*The* ***set of all solutions*** *(which could be an empty set) is a subset of* $\mathbb{F}^n$*,*

$$S_{[a_1,\ldots,a_n|b]} = \left\{ \begin{bmatrix} x^1 \\ \vdots \\ x^n \end{bmatrix} \in \mathbb{F}^n_{col} \ : \ \sum_{i=1}^{n} a_i x^i = b \right\}.$$

*In words, the set of solutions of the linear equation defined by the coefficients* $[a_1, \ldots, a_n, b]$ *is the set of all* $[x^1, \ldots, x^n]^T \in \mathbb{F}^n_{col}$ *satisfying* (2.2)*.*

Generally, an equation may have one solution, many solutions, or no solution at all. What do we mean then by *solving* an equation? We mean that we obtain a "constructive recipe" for generating all of its solutions.

**Example**: Consider the linear equation in two unknowns,

$$X^1 + X^2 = 1. \tag{2.3}$$

We are looking for pairs of scalars $[x^1, x^2]^T \in \mathbb{F}^2_{\text{col}}$ satisfying this equation. We may see right away that

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

are both solutions to (2.3), but do there exist more solutions? Take any $t \in \mathbb{F}$ and substitute it for $X^2$. Then, we are left with the equation

$$X^1 + t = 1,$$

which is solvable, and this solution is unique, $x^1 = 1 - t$. Thus, for *every* choice of $t \in \mathbb{F}$, the pair $[1-t, t]^T$ is a solution to (2.3). Namely,

$$\left\{ \begin{bmatrix} 1-t \\ t \end{bmatrix} \ : \ t \in \mathbb{F} \right\} \subseteq S_{[1,1|1]}.$$

In words, for every $t \in \mathbb{F}$, the pair $[1-t, t]^T \in \mathbb{F}^2_{\text{col}}$ is a solution to the linear equation with two unknowns and coefficients $a_1 = 1$, $a_2 = 1$ and $b = 1$.

In fact, this inclusion between sets turns out to be an equality, as every solution to (2.3) must be of the form $[1-t, t]^T$. Note how we broke the symmetry between the two unknowns: we treated the second unknown as a "free" parameter, which may assume any value, whereas the value of the first unknown was "dependent" on the choice of the second unknown. Note also that the choice of the second unknown as "free" is arbitrary; we could have done it the other way around. ▲▲▲

***Definition 2.3*** *A linear equation of the form* (2.1) *is called* ***homogeneous*** *(הומוגנית) if* $b = 0$. *It is called* ***consistent*** *(עקבית) if its set of solutions is not empty.*

**Example**: Suppose that all the coefficients $a_i$ are zero, namely

$$0_{\mathbb{F}} \cdot X^1 + \cdots + 0_{\mathbb{F}} \cdot X^n = b.$$

If $b \neq 0_{\mathbb{F}}$ then no $[x^1, \ldots, x^n]^T \in \mathbb{F}^n_{\text{col}}$ satisfies the equation, i.e., the equation is not consistent, namely,

$$S_{[0,\ldots,0|b]} = \varnothing.$$

If on the other hand $b = 0_{\mathbb{F}}$, then *every* $n$-tuple is a solution, i.e., the set of all solutions is $\mathbb{F}^n$. In other words,

$$\left\{ \begin{bmatrix} x^1 \\ \vdots \\ x^n \end{bmatrix} \in \mathbb{F}^n_{\text{col}} \ : \ \sum_{i=1}^{n} 0_{\mathbb{F}} \cdot x^i = 0_{\mathbb{F}} \right\} = \mathbb{F}^n_{\text{col}}.$$

▲▲▲

We now show how an equation can be modified without changing its set of solutions. Take an equation of the form (2.1), and let $\mathbb{F} \ni c \neq 0_{\mathbb{F}}$. Consider the equation

$$(ca_1)X^1 + \cdots + (ca_n)X^n = cb, \tag{2.4}$$

obtained by multiplying all the coefficients in (2.1) by $c$.

***Proposition 2.4*** *Every solution of* (2.1) *is a solution of* (2.4)*, and vice-versa, every solution of* (2.4) *is a solution of* (2.1)*. That is, both equations have the same set of solutions,*

$$S_{[a_1,\ldots,a_n|b]} = S_{[ca_1,\ldots,ca_n|cb]}.$$

*Proof*: If $[x^1,\ldots,x^n]^T$ is a solution of (2.1), then by definition

$$a_1x^1 + \cdots + a_nx^n = b.$$

Multiplying both sides by $c$, using the distributive law and the associativity of products,

$$\begin{aligned} cb &= c\left(a_1x^1 + \cdots + a_nx^n\right) \\ &= c(a_1x^1) + \cdots + c(a_nx^n) \\ &= (ca_1)x^1 + \cdots + (ca_n)x^n, \end{aligned}$$

i.e., $[x^1,\ldots,x^n]^T$ is also a solution of (2.4). The reverse implication follows by multiplying (2.4) by $c^{-1}$. ■

Proposition 2.4 implies that we have a means of changing an equation without changing its set of solutions. This is the idea behind the procedure of simplifying equations. Suppose that there exists at least one $a_i$ different from zero. Let $k \in \{1,\ldots,n\}$ be the smallest index for which $a_i \neq 0$, i.e., $a_k \neq 0$ and $a_i = 0$ for all $i < k$. That is, we can write the equation as

$$a_kX^k + a_{k+1}X^{k+1} + \cdots + a_nX^n = b.$$

(We call $X^k$ the **leading variable** (**המשתנה המוביל**) of the equation.) Multiplying this equation by $a_k^{-1}$ we obtain an equation having the same set of solutions, whose first non-zero coefficient is one,

$$X^k + (a_{k+1}/a_k)X^{k+1} + \cdots + (a_n/a_k)X^n = b/a_k.$$

We say that this equation is in **standard form** (**הצנה מתוקנת**). By Theorem 1.1, no matter which values we substitute for $X^1,\ldots,X^{k-1}$ and $X^{k+1},\ldots,X^n$,

there exists a unique value of $X^k$ for which this equation holds. That is, the set of solutions can be written as

$$S_{[a_1,\ldots,a_n|b]} = \left\{ \begin{bmatrix} t^1 \\ \vdots \\ t^{k-1} \\ b/a_k - \sum_{i=k+1}^{n} (a_i/a_k) t^i \\ t^{k+1} \\ \vdots \\ t^n \end{bmatrix} \;:\; t^1, \ldots, t^n \in \mathbb{F} \right\}.$$

This is what we mean by a solutions which is constructive, or explicit (**מפורש**). The full set of solutions can be generated by selecting all possible values for $(t^1, \ldots, t^{k-1}, t^{k+1}, \ldots t^n)$. In this representation we say that the variables $X^i$ for $i \neq k$ are **free variables** (**משתנים חופשיים**) (because we can generate all solutions by selecting their values "freely") whereas $X^k$ is a **dependent variable** (**משתנה קשור**) (because once the free variables have been assigned, the value of $X^k$ depends on those assigned values).

We may formulate the following corollary:

***Corollary 2.5*** *Every linear equation in $n$ unknowns having at least one non-zero coefficient $a_i$ is consistent, and its set of solutions can be represented by means of $n-1$ free variables.*

**Exercises**

**(easy) 2.1** Write the set of solutions to the linear equation in two unknowns over $\mathbb{R}$,

$$3X^1 - 4X^2 = 7.$$

**(easy) 2.2** Write the equation over $\mathbb{R}$

$$0\,X^1 + 0\,X^2 - 4X^3 + 0\,X^4 + 7X^5 = 3$$

in normalized form and write its set of solutions in explicit form.

**(intermediate) 2.3** Find the set of solutions to the equation

$$X^1 + X^2 + X^3 = 1$$

over the field $\mathbb{F}_2$. Solve the same equation over the field $\mathbb{F}_3$.

**(intermediate) 2.4** Find the set of solutions to the equation

$$a_1X^1 + a_2X^2 + a_3X^3 = b$$

over the field $\mathbb{R}$ for the following sets of coefficients:

(a) $[a_1, a_2, a_3|b] = [1, 1, 2|1]$.
(b) $[a_1, a_2, a_3|b] = [0, 1, 6|3]$.
(c) $[a_1, a_2, a_3|b] = [0, 3, 6|3]$.

**(intermediate) 2.5** Suppose that $[x^1, \ldots, x^n]^T$ is a solution to both equations,

$$a_1X^1 + \cdots + a_nX^n = b \qquad \text{and} \qquad c_1X^1 + \cdots + c_nX^n = d.$$

Prove that for every $\alpha \in \mathbb{F}$ it is also a solution to the equation

$$(\alpha\, a_1 + c_1)X^1 + \cdots + (\alpha\, a_n + c_n)X^n = \alpha\, b + d.$$

## 2.2 Systems of equations

We introduce next the notion of a system of $m$ **linear equations in** $n$ **unknowns** (**מערכת משוואות ליניאריות**). For this we need $m$ sets of coefficients $a_i$ and $b$. Rather than using new symbols for each equation, we denote the coefficients for the $i$-th equation by an upper index $i$. That is, we consider a system of $m$ equations of the form

$$\begin{array}{ccccc} a_1^1X^1 & +a_2^1X^2 & +\ldots & +a_n^1X^n & = b^1 \\ a_1^2X^1 & +a_2^2X^2 & +\ldots & +a_n^2X^n & = b^2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_1^mX^1 & +a_2^mX^2 & +\ldots & +a_n^mX^n & = b^m \end{array}, \tag{2.5}$$

where

$$a_j^i \in \mathbb{F} \qquad i = 1, \ldots, m \quad \text{and} \quad j = 1, \ldots, n$$

is the **coefficient** (**מקדם**) of the $j$-th variable in the $i$-th equation, and

$$b^i \in \mathbb{F} \qquad i = 1, \ldots, m$$

is the right-hand side of the $i$-th equation. Please note: the upper indexes in $a^i_j$ and in $b^i$ enumerate the equation, whereas the lower index in $a^i_j$ enumerates the variable.

A **solution** (**פתרון**) to the system is any $n$-tuple $[x^1, x^2, \ldots, x^n]^T \in \mathbb{F}^n_{\text{col}}$, such that

$$\begin{array}{cccccc} a^1_1 x^1 & +a^1_2 x^2 & + \ldots & +a^1_n x^n & = b^1 \\ a^2_1 x^1 & +a^2_2 x^2 & + \ldots & +a^2_n x^n & = b^2 \\ \vdots & \vdots & & \vdots & \vdots \\ a^m_1 x^1 & +a^m_2 x^2 & + \ldots & +a^m_n x^n & = b^m \end{array} . \tag{2.6}$$

Given a system of equations (2.5) (which is uniquely determined by $n$, $m$ and the scalars $a^i_j$ and $b^i$), we would like to find the set of **all** of its solutions,

$$S = \left\{ \begin{bmatrix} x^1 \\ \vdots \\ x^n \end{bmatrix} \in \mathbb{F}^n \ : \ \sum_{j=1}^{n} a^i_j x^j = b^i \text{ for all } i = 1, \ldots, m \right\}.$$

As in the case of a single equation, solving the system of equations means obtaining a constructive way of generating all of its solutions.

Like for a single equation:

***Definition 2.6*** *A system of linear equations* (2.5) *is called* ***homogeneous*** *(**מערכת משוואות הומוגנית**) if the right-hand side is zero, namely, $b^i = 0$ for all $i = 1, \ldots, m$. It is called* ***consistent*** *(**עקבית**) if its set of solutions is not empty.*

**Example**: Consider the inhomogeneous system of two equations in two unknowns over $\mathbb{R}$,

$$\begin{array}{ccc} X^1 & +X^2 & = 0 \\ X^1 & +X^2 & = 1. \end{array}$$

Each equation separately has a solution, however this system is not consistent as if $[x^1, x^2]^T$ was a solution, it would imply that

$$0 = x^1 + x^2 = 1,$$

which violates the axioms of field. ▲ ▲ ▲

**Example**: Consider the inhomogenous system of $m = 2$ linear equations in $n = 4$ unknowns over $\mathbb{R}$,

$$\begin{array}{cccc} X^1 & +2X^2 & -X^4 & = 1 \\ & & X^3 & +4X^4 & = 3. \end{array}$$

This is a quite special form of a system as we will immediately see. First, it is not very difficult to "guess" a solution

$$[1, 0, 3, 0]^T \in \mathbb{F}^4_{\text{col}}.$$

In fact, we may observe that the variable $X^1$ only appears in the first equation, whereas the variable $X^3$ only appears in the second equation. As a result, suppose that we substitute $s \in \mathbb{F}$ for $X^2$ and $t \in \mathbb{F}$ for $X^4$. Then, we obtain two *decoupled* linear equations for $X^1$ and $X^3$, whose solutions are

$$\begin{aligned} x^1 &= 1 - 2s + t \\ x^3 &= 3 - 4t. \end{aligned}$$

As we did in the previous section, we may treat $X^2$ and $X^4$ as free variables, so that the set of solutions is generated by all possible choices of those variables, yielding,

$$S = \left\{ \begin{bmatrix} 1 - 2s + t \\ s \\ 3 - 4t \\ t \end{bmatrix} \in \mathbb{F}^4_{\text{col}} \ : \ s, t \in \mathbb{F} \right\}.$$

If, for example, $\mathbb{F}$ is a finite field, then we can enumerate the set of solutions, which is a finite set. ▲ ▲ ▲

Not every system of equations is as "transparent" as in the above example. What do we do when the system is more complicated? We transform it into a "transparent" one having the *same* set of solutions, and we then solve the easier one.

**Example**: Consider the inhomogeneous system of $m = 2$ linear equations in $n = 4$ unknowns over $\mathbb{R}$,

$$\begin{array}{cccccc} X^1 & +2X^2 & +X^3 & +3X^4 & = 4 \\ 3X^1 & +6X^2 & +2X^3 & +5X^4 & = 9. \end{array}$$

This system is not "transparent" as the previous one. In secondary school you learned how to solve such equations by **eliminating variables** (**חילוץ משתנים**). Take the first equation and multiply it by 3,

$$3X^1 \quad +6X^2 \quad +3X^3 \quad +9X^4 \quad = 12.$$

We proved (Proposition 2.4) that this does not alter its set of solutions. Take now this equation and subtract it from the second equation in the original system, yielding

$$-X^3 \quad -4X^4 \quad = -3.$$

Then, add this equation to the first equation in the original system, yielding

$$X^1 \quad +2X^2 \qquad -X^4 \quad = 1.$$

Finally, multiply the penultimate equation by $(-1)$ yielding

$$X^3 \quad +4X^4 \quad = 3.$$

Look at the last two equations. This is the system of the previous example—the "transparent" system, whose solution we've already found. As we will prove in the next section, the solutions of both sets of equations are the same. ▲▲▲

## 2.3 Equivalent systems of equations

Our goal is to now formalize the process we have just done in a specific example. Given a linear system (2.5) of $m$ equations in $n$ unknowns, we may form a new equation, which is a **linear combination** (**צירוף ליניארי**) of the $m$ equations by multiplying each equation by a number $c_i$, $i = 1, \ldots, m$, and add up the resulting $m$ equations, Multiplying the $i$-th equation by $c_i$ and summing over the $m$ equations yields the equation

$$\sum_{i=1}^{m} c_i \left( \sum_{j=1}^{n} a_j^i X^j \right) = \sum_{i=1}^{m} c_i b^i,$$

which we can rearrange by interchanging the order of summation (see Exercise 1.20 ) into

$$\sum_{j=1}^{n} \underbrace{\left( \sum_{i=1}^{m} c_i a_j^i \right)}_{\text{coefficient of } X^j} X^j = \underbrace{\sum_{i=1}^{m} c_i b^i}_{\text{right-hand side}} .$$

In more explicit notation, if for every $i = 1, \ldots, m$,

$$a_1^i X^1 + \cdots + a_n^i X^n = b^i,$$

then multiplying this equation by $c_i$ and summing over all $i = 1, \ldots, m$,

$$c_1(a_1^1 X^1 + \cdots + a_n^1 X^n) + \cdots + c_m(a_1^m X^1 + \cdots + a_n^m X^n) = c_1 b^1 + \cdots + c_m b^m,$$

which we further reorganize as

$$(c_1 a_1^1 + \ldots c_m a_1^m) X^1 + \cdots + (c_1 a_n^1 + \ldots c_m a_n^m) X^n = c_1 b^1 + \cdots + c_m b^m. \quad (2.7)$$

Note that we applied here both the extended associativity and commutativity of addition and the distributive law. We conclude that a linear combination of linear equations is again a linear equation.

***Proposition 2.7 ((משפט הירושה))*** *Every solution* $[x^1, \ldots, x^n]^T \in \mathbb{F}^n_{col}$ *of* (2.5) *is also a solution of* (2.7).

*Proof*: Let $[x^1, \ldots, x^n]^T$ be a solution to (2.5), i.e.,

$$a_1^i x^1 + \cdots + a_j^n x^n = b^i \qquad \text{for all } i = 1, \ldots, m.$$

Multiplying the $i$-th equation by $c_i$, summing over $i$ and applying the distributive law, we recover the desired result after exchanging the order of summation. Note that we used here the consistency of equality and addition: if $s_1 = t_1$, $s_2 = t_2$ up to $t_m = s_m$, then

$$s_1 + s_2 + \cdots + s_m = t_1 + t_2 + \cdots + t_m.$$

■

Note, however, that the reverse is not necessarily true. Not every solution to (2.7) is necessarily a solution of (2.5) ("information may have been lost").

More generally, consider a linear system of $k$ equations in $n$ unknowns,

$$\begin{array}{cccccc} g_1^1 X^1 & +g_2^1 X^2 & +\ldots & +g_n^1 X^n & = z^1 \\ g_1^2 X^1 & +g_2^2 X^2 & +\ldots & +g_n^2 X^n & = z^2 \\ \vdots & \vdots & & \vdots & \vdots \\ g_1^k X^1 & +g_2^k X^2 & +\ldots & +g_n^k X^n & = z^k \end{array} . \quad (2.8)$$

If each of the $k$ equations in (2.8) is a linear combination of the $m$ equations in (2.5), then, by Proposition 2.7, every solution of (2.5) is also a solution to (2.8) (but not necessarily the other way around).

This observation brings us to the following definition:

***Definition 2.8*** *Two linear systems of equations are called* ***equivalent*** *(שקולות) if every equation in one system is a linear combination of the equations in the other system.*

**Example**: Back to our first example, the systems

$$\begin{array}{rrrl} 2X^1 & -X^2 & +X^3 & = 0 \\ X^1 & +3X^2 & +4X^3 & = 0 \end{array}$$

and

$$\begin{array}{rrrl} & X^2 & +X^3 & = 0 \\ X^1 & & +X^3 & = 0 \end{array}$$

are equivalent. The first equation in the second system is obtained by a linear combination of the first system with coefficients $[-1/7, 2/7]$ and the second equation in the second system is obtained by a linear combination of the first system with coefficients $[3/7, 1/7]$. Conversely, the first equation in the first system is obtained by a linear combination of the second system with coefficients $[-1, 2]$, and the second equation in the first system is obtained by a linear combination of the second system with coefficients $[3, 1]$. ▲▲▲

The importance of equivalent systems stems from the following fact:

***Proposition 2.9*** *Equivalent systems have the same set of solutions.*

*Proof*: By Proposition 2.7, every solution of a linear system is also a solution of an equation obtained by a linear combination of that system. Since each equation in one system is a linear combination of the equation in the other system, every solution of System A is a solution of System B, and conversely, every solution of System B is a solution of System A, ■

This notion of two systems being equivalent has a very important property:

***Lemma 2.10*** *If a linear system of equations B is obtained by linear combinations of a linear system of equations A, and a linear system of equations C is obtained by linear combinations of a linear system of equations B, then System C is obtained by linear combinations of the equations in System A.*

*Proof*: Suppose that System A has $m$ equations, System B has $k$ equations and System C has $p$ equations, all in $n$ unknowns. If System B is obtained by linear combinations of System A, then the $\ell$-th equation in System B is obtained by taking linear combinations of the $m$ equations in System A, with coefficients $c_1^\ell, \ldots, c_m^\ell$, namely, the $\ell$-th equation of system B is of the form

$$\sum_{s=1}^{m} c_s^\ell \sum_{j=1}^{n} a_j^s X^j = \sum_{s=1}^{m} c_s^\ell b^s.$$

Likewise, if System C is is obtained by linear combinations of System B, then the $i$-th equation in System C is obtained by taking linear combinations of the $k$ equations in System B, with coefficients $d_1^i, \ldots, d_k^i$, namely, the $i$-th equation of system C is of the form

$$\sum_{\ell=1}^{k} d_\ell^i \sum_{s=1}^{m} c_s^\ell \sum_{j=1}^{n} a_j^s X^j = \sum_{\ell=1}^{k} d_\ell^i \sum_{s=1}^{m} c_s^\ell b^s.$$

Reorganizing this equation as

$$\sum_{s=1}^{m} \underbrace{\left( \sum_{\ell=1}^{k} d_\ell^i c_s^\ell \right)}_{e_s^i} \sum_{j=1}^{n} a_j^s X^j = \sum_{s=1}^{m} \underbrace{\left( \sum_{\ell=1}^{k} d_\ell^i c_s^\ell \right)}_{e_s^i} b^s,$$

proves that System C is obtained by a linear combinations of System A. ■

***Corollary 2.11*** *If a linear system of equations B is equivalent to a linear system of equations A, and a linear system of equations C is equivalent to a linear system of equations B, then System C is equivalent to System A.*

*Proof*: Apply the previous lemma both ways. ■

These observations are key to the solution of linear systems of equations. What we actually do is to replace the original system by equivalent systems through a chain of transformations which ensure that we always remain with a system that is equivalent to the original one, so that the set of solutions never changes. The key is to end up with a system equations which is "transparent".

**Comment:** Note that in all summations, the index we sum upon always appears once as an upper index and once as a lower index. If you come across a summation in which this is not the case, look for an error.

We end this section by observing that while we have a well-defined notion of equivalence between systems of equations, we don't yet have a means for verifying wether two systems of equations are equivalent, nor a systematic way of generating equivalent systems to a given system.

### Exercises

**(easy) 2.6** Consider the following linear system of two equations in three unknowns over $\mathbb{R}$,

$$\begin{array}{rrrr} 2X^1 & +X^2 & +X^3 & = 2 \\ X^1 & +2X^2 & -X^3 & = -1. \end{array}$$

(a) Is this a homogeneous system?

(b) Is $[1,0,0]^T$ a solution?

(c) Write an equation which is a linear combination of this system with coefficients $[2,-3]$.

(d) Is $X^1 + X^2 = 1/3$ a linear combination of this system? If it is, what are the coefficients?

(e) Is $2X^1 + X^2 + X^3 = 1$ a linear combination of this system? If it is, what are the coefficients?

**(easy) 2.7** Write the set of solutions of the linear system over $\mathbb{R}$ in the unknowns $(X,Y)$:

$$\begin{array}{rrr} X & +Y & = 5 \\ 2X & -Y & = 3. \end{array}$$

**(easy) 2.8** Write the set of solutions of the linear system over $\mathbb{R}$ in the unknowns $(X, Y, Z)$:

$$\begin{array}{rrrl} X & +Y & -Z & = -1 \\ X & -Y & -Z & = -1. \end{array}$$

**(intermediate) 2.9** Show that the following two homogeneous systems of equations are equivalent,

$$\left\{ \begin{array}{rrl} X^1 & -X^2 & = 0 \\ 2X^1 & +X^2 & = 0 \end{array} \right. \quad \text{and} \quad \left\{ \begin{array}{rrl} 3X^1 & +X^2 & = 0 \\ X^1 & +X^2 & = 0. \end{array} \right.$$

**(intermediate) 2.10** Show that the following two homogeneous systems of equations over $\mathbb{R}$ are equivalent,

$$\left\{ \begin{array}{rrrl} -X^1 & +X^2 & +4X^3 & = 0 \\ X^1 & +3X^2 & +8X^3 & = 0 \\ \frac{1}{2}X^1 & +X^2 & +\frac{5}{2}X^3 & = 0 \end{array} \right. \quad \text{and} \quad \left\{ \begin{array}{rrrl} X^1 & & -X^3 & = 0 \\ & X^2 & +3X^3 & = 0. \end{array} \right.$$

**(intermediate) 2.11** Consider the following two homogeneous systems of equations over $\mathbb{R}$

$$\left\{ \begin{array}{rrl} X^1 & -X^2 & = 0 \\ 2X^1 & +X^2 & = 0 \end{array} \right. \quad \text{and} \quad \left\{ \begin{array}{rrl} X^1 & +2X^2 & = 0 \\ -2X^1 & -4X^2 & = 0. \end{array} \right.$$

Are they equivalent? If they are, write each system as a linear combination of the other.

**(harder) 2.12** We showed that if two systems of equations are equivalent, then they have the same sets of solutions. What about the converse? Show that if two homogeneous systems of linear equations in two unknowns have the same solutions, then they are equivalent.

**(harder) 2.13** Does there exists a linear system of $m$ equations in $n$ unknowns having a *unique* solution when

(a) $m = 4$ and $n = 3$.

(b) $m = 3$ and $n = 4$.

If the answer is positive provide an example; if it is negative explain why.

# 2.4 Matrix notation

## 2.4.1 Definitions

An important practice in mathematics is the adoption of convenient notations. In the present case, since a linear system of equations (hence also its solutions) is fully determined by the coefficients $a^i_j$ and the $b^i$, there is no need to carry around also the variables $X^j$. We organize the coefficients $a^i_j$ in a rectangular array

$$A = \begin{bmatrix} a^1_1 & a^1_2 & \cdots & a^1_n \\ a^2_1 & a^2_2 & \cdots & a^2_n \\ \vdots & \vdots & \cdots & \vdots \\ a^m_1 & a^m_2 & \cdots & a^m_n \end{bmatrix}$$

which we call the $m \times n$ **matrix of coefficients** (**מטריצת המקדמים**). The entry at the $i$-th row and the $j$-th column is the coefficient of the $j$-th unknown in the $i$-th equation. Likewise, we organize the $b^i$'s as an $m \times 1$ matrix

$$\mathbf{b} = \begin{bmatrix} b^1 \\ b^2 \\ \vdots \\ b^m \end{bmatrix},$$

which is an element of $\mathbb{F}^m_{\text{col}}$. If we further organize the unknowns as an $n \times 1$ matrix,

$$\mathbf{X} = \begin{bmatrix} X^1 \\ X^2 \\ \vdots \\ X^n \end{bmatrix},$$

then we may symbolically represent the system of equations as $A\mathbf{X} = \mathbf{b}$. At this stage this is just a symbolic notation, but it will acquire a meaning shortly.

**Comments:**

(a) Note that in $a^i_j$, the upper index $i$ designates the row and the lower index $j$ designates the column. It will sometimes be convenient to write the $(i, j)$-th element of a matrix $A$ also by $(A)^i_j$.

(b) Formally, an $m \times n$ matrix $A$ is a function from the set $\{1, \ldots, m\} \times \{1, \ldots, n\}$ to the field $\mathbb{F}$. For every pair of indexes $(i, j)$ it returns the field element which we denote by $a_j^i$.

(c) We denote the set of $m \times n$ matrices with values in the field $\mathbb{F}$ by

$$M_{m\times n}(\mathbb{F}).$$

(d) $M_{1\times n}(\mathbb{F})$ coincides with $\mathbb{F}^n_{\text{row}}$, whereas $M_{m\times 1}(\mathbb{F})$ coincides with $\mathbb{F}^m_{\text{col}}$.

We denote the $i$-th row of the matrix $A$ by

$$\text{Row}^i(A) = \begin{bmatrix} a_1^i & a_2^i & \ldots & a_n^i \end{bmatrix}.$$

Likewise, we denote the $j$-th column of $A$ by

$$\text{Col}_j(A) = \begin{bmatrix} a_j^1 \\ a_j^2 \\ \vdots \\ a_j^m \end{bmatrix}.$$

In fact, we may present the matrix $A$ either as a column of $m$ rows, each of size $n$ or as a row of $n$ columns, each of size $m$,

$$A = \begin{bmatrix} \text{Row}^1(A) \\ \text{Row}^2(A) \\ \vdots \\ \text{Row}^m(A) \end{bmatrix} = \begin{bmatrix} \text{Col}_1(A) & \text{Col}_2(A) & \cdots & \text{Col}_n(A) \end{bmatrix}$$

We may also write the coefficients and the right-hand side of the equations as a unified $m \times (n+1)$ matrix,

$$\begin{bmatrix} A|\mathbf{b} \end{bmatrix} = \left[\begin{array}{cccc|c} a_1^1 & a_2^1 & \cdots & a_n^1 & b^1 \\ a_1^2 & a_2^2 & \cdots & a_n^2 & b^2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_1^m & a_2^m & \cdots & a_n^m & b^m \end{array}\right].$$

It is called the **augmented matrix** (**המטריצה המורחבת**) of the system $A\mathbf{X} = \mathbf{b}$. Finally, we denote the set of solutions to $A\mathbf{X} = \mathbf{b}$ by $S_{[A|\mathbf{b}]}$.

**Exercises**

**(easy) 2.14** Consider the matrix

$$A = \begin{bmatrix} 0 & 0 & 1 & 4 \\ 2 & 4 & 2 & 6 \\ 3 & 6 & 2 & 5 \end{bmatrix}$$

What are $a_3^2$, $\mathrm{Row}^2(A)$ and $\mathrm{Col}_3(A)$?

**(easy) 2.15** Write the system of equations represented by the extended matrix

$$\left[\begin{array}{cccc|c} 0 & 0 & 1 & 4 & 3 \\ 2 & 4 & 2 & 6 & 7 \\ 3 & 6 & 2 & 5 & 8 \end{array}\right].$$

### 2.4.2 Elementary row-operations and row-equivalence

Next, we consider operations on matrices that correspond to forming linear combinations of equations. We define the following **elementary row-operations** (**פעולות שורה יסודיות**):

1. Multiplication of the $k$-th row by a non-zero scalar $\mathbb{F} \ni c \neq 0$.
2. Replacement of the $r$-th row with row $r$ plus $c$ times row $s$, where $c \in \mathbb{F}$.

These operations are in fact functions taking an element in $M_{m\times n}(\mathbb{F})$ and returning an element in $M_{m\times n}(\mathbb{F})$.

Formally, if $A$ is a matrix, and $e$ is the operation (the function) taking a matrix and returning a matrix having all rows the same, except that the $r$-th row has been multiplied by $\mathbb{F} \ni c \neq 0$, then for every pair of indexes $i, j$,

$$(e(A))_j^i = \begin{cases} c\,a_j^i & i = r \\ a_j^i & i \neq r, \end{cases}$$

i.e.,

$$e : \begin{bmatrix} a_1^1 & \cdots & a_n^1 \\ \vdots & \vdots & \vdots \\ a_1^r & \cdots & a_n^r \\ \vdots & \vdots & \vdots \\ a_1^m & \cdots & a_n^m \end{bmatrix} \mapsto \begin{bmatrix} a_1^1 & \cdots & a_n^1 \\ \vdots & \vdots & \vdots \\ c\,a_1^r & \cdots & c\,a_n^r \\ \vdots & \vdots & \vdots \\ a_1^m & \cdots & a_n^m \end{bmatrix}$$

If $e$ is the operation taking a matrix and returning a matrix having all rows the same, except for the $r$-th row being the sum of the $r$-th row and $c$ times the $s$-th row of $A$, then for every pair of indexes $i, j$,

$$(e(A))^i_j = \begin{cases} a^i_j + c\,a^s_j & i = r \\ a^i_j & i \neq r, \end{cases}$$

i.e.,

$$e : \begin{bmatrix} a^1_1 & \cdots & a^1_n \\ \vdots & \vdots & \vdots \\ a^r_1 & \cdots & a^r_n \\ \vdots & \vdots & \vdots \\ a^m_1 & \cdots & a^m_n \end{bmatrix} \mapsto \begin{bmatrix} a^1_1 & \cdots & a^1_n \\ \vdots & \vdots & \vdots \\ a^r_1 + c\,a^s_1 & \cdots & a^r_n + c\,a^s_n \\ \vdots & \vdots & \vdots \\ a^m_1 & \cdots & a^m_n \end{bmatrix}$$

***Lemma 2.12*** *Every elementary row-operation $e$ has in inverse operation $e^{-1}$, which is also an elementary row-operation, such that for every matrix $A$,*

$$e^{-1}(e(A)) = A.$$

*Proof*: The operation of multiplying the $r$-th row by $c \neq 0$ can be reversed by multiplying that same row by $1/c$ (which is why we required $c \neq 0$), which is also an elementary row-operation. The operation of replacing the $r$-th row by the sum of row $r$ and $c$ times row $s$ can be reversed by the elementary row-operation of replacing the $r$-th row by the sum of row $r$ and $(-c)$ times row $s$. ■

***Definition 2.13*** *An $m \times n$ matrix $A$ is row-equivalent (**שקולה לפי שורה**) to an $m \times n$ matrix $B$ if it can be obtained from $B$ by a finite sequence of elementary row-operations. That is, if there exists a sequence $e_1, e_2, \ldots, e_s$ of elementary row-operations, such that*

$$A = e_s(e_{s-1}(\ldots e_1(B))).$$

**Example**: Since

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \overset{r_2 \leftarrow r_2 + 2r_1}{\longrightarrow} \begin{bmatrix} 1 & 2 & 3 \\ 6 & 9 & 12 \end{bmatrix} \overset{r_1 \leftarrow -4r_1}{\longrightarrow} \begin{bmatrix} -4 & -8 & -12 \\ 6 & 9 & 12 \end{bmatrix},$$

it follows by definition that all three matrices are row-equivalent. ▲▲▲

***Proposition 2.14*** *Row-equivalence is an* ***equivalence relation*** *(יחס שקילות): that is, (i) every matrix is row-equivalent to itself, (ii) if $A$ is row-equivalent to $B$ then $B$ is row-equivalent to $A$, and (iii) if $A$ is row-equivalent to $B$ and $B$ is row-equivalent to $C$, then $A$ is row-equivalent to $C$. (In particular, we have a well-defined notion of two matrices being row-equivalent to each other.)*

*Proof*: Every matrix $A$ is equivalent to itself, for example, because if $e$ is the elementary row-operation of multiplying the first row by 1, then

$$A = e(A).$$

If $A$ is row-equivalent to $B$, then by definition, there exists a sequence of elementary row-operations $e_1, e_2, \ldots, e_k$, such that

$$A = e_k(e_{k-1}(\cdots e_2(e_1(B)))).$$

Since every $e_j$ has an inverse $e_j^{-1}$, it follows that

$$e_k^{-1}(A) = e_k^{-1}(e_k(e_{k-1}(\cdots e_2(e_1(B))))) = e_{k-1}(\cdots e_2(e_1(B))),$$

and proceeding inductively,

$$B = e_1^{-1}(e_2^{-1}(\cdots e_{k-1}^{-1}(e_k^{-1}(A))),$$

proving that $B$ is row-equivalent to $A$. Finally, if $B$ is also row-equivalent to $C$, then by definition, there exists a sequence of elementary row-operations $f_1, f_2, \ldots, f_s$, such that

$$B = f_s(f_{s-1}(\cdots f_2(f_1(C)))).$$

Hence,

$$A = e_k(e_{k-1}(\cdots e_2(e_1(f_s(f_{s-1}(\cdots f_2(f_1(C)))))))),$$

proving that $A$ is row-equivalent to $C$. ■

Note that we have two notions of equivalence: equivalence between systems of equations and row-equivalence between matrices. We will shortly claim that these two notions are related, namely, if two matrices are row-equivalent, then they represent equivalent systems of equations.

***Proposition 2.15*** *If $A$ and $B$ are row-equivalent $m \times n$ matrices, then the homogeneous linear systems $A\mathbf{X} = 0$ and $B\mathbf{X} = 0$ have the same solutions,*

$$S_{[A|0]} = S_{[B|0]}.$$

*Proof*: By definition, there exists a sequence of elementary row-operations $e_1, e_2, \ldots, e_k$, such that

$$A = e_k(e_{k-1}(\cdots e_2(e_1(B)))).$$

It suffices to show that if $e$ is any elementary row-operation, then the homogenous linear systems $e(A)\mathbf{X} = 0$ and $A\mathbf{X} = 0$ have the same set of solutions.

Let $e$ be an elementary row-operation. Since every row in $e(A)$ is a linear combination of the rows in $A$, then every solution of $A\mathbf{X} = 0$ is also a solution of $e(A)\mathbf{X} = 0$ (see Proposition 2.9). Conversely, since every row in $A$ is a linear combination of the rows in $e(A)$ (since $A = e^{-1}(e(A))$), then every solution of $e(A)\mathbf{X} = 0$ is also a solution of $A\mathbf{X} = 0$. ■

In fact, an analogous statement holds for inhomogeneous systems by considering the extended matrices:

***Proposition 2.16*** *If $[A|\mathbf{c}]$ and $[B|\mathbf{d}]$ are row-equivalent $m \times (n+1)$ matrices, then the linear systems $A\mathbf{X} = \mathbf{c}$ and $B\mathbf{X} = \mathbf{d}$ have the same solutions,*

$$S_{[A|\mathbf{c}]} = S_{[B|\mathbf{d}]}.$$

**Exercises**

**(easy) 2.16** Let $e$ be an elementary row-operation. Show that for every matrix $A$, every row of $e(A)$ is a linear combination of the rows in $A$.

**(easy) 2.17** Explain *explicitly* why in the proof of Proposition 2.15 it suffices to show that the solutions of a homogeneous linear system do not change under a single elementary row-operation.

**(easy) 2.18** Can a matrix $A \in M_{2\times 4}$ and a matrix $B \in M_{4\times 3}$ be row-equivalent? If yes, give an example and if not explain why.

**(easy) 2.19** Consider the following row-operations:

$e_1$ : multiplying the first row by $-2$.
$e_2$ : exchanging the first and the second rows.
$e_3$ : adding the third row 3 times the first row.

(a) What are the inverse operations $e_1^{-1}$, $e_2^{-1}$ and $e_3^{-1}$.

(b) Perform the three operations sequentially on the matrix

$$\begin{bmatrix} 2 & 1 & -1 & 3 \\ 1 & -2 & 0 & 1 \\ 0 & 0 & 2 & 1 \end{bmatrix} \in M_{3\times 4}(\mathbb{F}).$$

**(intermediate) 2.20** Let $e_1$ and $e_2$ be two elementary row-operations. Is it always the case that

$$e_1(e_2(A)) = e_2(e_1(A))\,?$$

If yes, explain why. If not, give an example.

**(intermediate) 2.21** Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{F}).$$

(a) Show that if $ad - bc = 0$ then $A$ is row-equivalent to a matrix having a row with all entries zero. Hint: separate the cases $c = 0$ and $c \neq 0$.

(b) Show that if $ad - bc \neq 0$ then $A$ is row-equivalent to the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

**(intermediate) 2.22** Show that two matrices in which two rows have been interchanged are row-equivalent.

### 2.4.3 Row-reduced echelon matrices

We next show how a sequence of elementary row-operations can be used to "simplify" a matrix, which means that its set of solutions can be obtained easily.

**Example**: By performing a sequence of eight elementary row-operations, the matrix

$$A = \begin{bmatrix} 2 & -1 & 3 & 2 \\ 1 & 4 & 0 & -1 \\ 2 & 6 & -1 & 5 \end{bmatrix}$$

can be brought to the form

$$B = \begin{bmatrix} 1 & 0 & 0 & 17/3 \\ 0 & 1 & 0 & -5/3 \\ 0 & 0 & 1 & -11/3 \end{bmatrix}.$$

What did we gain? The homogeneous linear system $B\mathbf{X} = 0$, whose solutions coincide by Proposition 2.15 with those of $A\mathbf{X} = 0$, takes the form

$$\begin{array}{rrrl} X^1 & & +17/3\,X^4 & = 0 \\ & X^2 & -5/3\,X^4 & = 0 \\ & & X^3 \quad -11/3\,X^4 & = 0. \end{array}$$

We can let $X^4$ assume any value, say $s$, and then

$$\mathbf{x} = [-17/3s, 5/3s, 11/3s, s]^T$$

is a solution. In fact, there are no other solutions, as any other solution would fail to satisfy the equation $BX = 0$. That is,

$$S_{[A|0]} = S_{[B|0]} = \left\{ \begin{bmatrix} -17/3s \\ 5/3s \\ 11/3s \\ s \end{bmatrix} \in \mathbb{F}^4_{\text{col}} \ : \ s \in \mathbb{F} \right\}.$$

▲▲▲

**Comment:** It is sometimes notationally convenient to write a blank instead of zero in a matrix. Thus, the above matrix $B$ is written as

$$B = \begin{bmatrix} 1 & & & 17/3 \\ & 1 & & -5/3 \\ & & 1 & -11/3 \end{bmatrix}.$$

**Example**: Consider the non-homogeneous linear system represented by the augmented matrix

$$A = \left[\begin{array}{cccc|c} 1 & -2 & 8 & 5 & 2 \\ 2 & 3 & 1 & 4 & 1 \\ 4 & -1 & 17 & 14 & 3 \end{array}\right].$$

By performing a sequence of elementary row-operations, we obtain the augmented matrix

$$B = \left[\begin{array}{cccc|c} 1 & -2 & 8 & 5 & 2 \\ & 7 & -17 & -6 & -3 \\ & & & & -2 \end{array}\right].$$

This system is not consistent because the third equation has all coefficients of the $X^i$'s zero but the right-hand side is not zero. ▲▲▲

In both example, we manipulated the system through the matrix of coefficients until reaching an equivalent system which is explicit, from which we could determine the solution (in the first example) or determine that there are no solutions (in the second example). This brings us to the following definition:

***Definition 2.17*** *An $m \times n$ matrix $A$ is said to be a* ***row-reduced echelon matrix*** *(**מטריצה בצורת מדרגות מצומצמת**) if*

*(a) There exists a number $r \leq m$, such that the rows $r+1, \ldots, m$ are identically zero (if $r = m$ then there are no rows that are identically zero).*

*(b) For each $i = 1, \ldots, r$ (i.e., for each non-zero row), let $a^i_{k_i}$ be the first non-zero entry; then $a^i_{k_i} = 1$ and $k_1 < k_2 < \cdots < k_r$ (the $k_i$'s are the columns of the leading coefficients in the non-zero rows).*

*(c) For each $i$, $a^i_{k_i}$ is the only nonzero element in the $k_i$-th column.*

**Example**: A **zero matrix** (**מטריצת אפסים**) is a matrix having all entries zero; if $A \in M_{m\times n}$ is a zero matrix, we write $A = 0$, or $A = 0_{m\times n}$. A zero matrix is an example of a row-reduced echelon matrix (with $r = 0$). ▲▲▲

**Example**: The matrix $B$ in the first example is a row-reduced echelon matrix (with $r = m = 3$). The matrix

$$\begin{bmatrix} 1 & -3 & & & 17/3 \\ & & 1 & & -5/3 \\ & & & 1 & -11/3 \\ & & & & \\ & & & & \end{bmatrix} \tag{2.9}$$

also satisfies all three conditions with $m = 5$, $r = 3$ and $k_1 = 1$, $k_2 = 3$ and $k_3 = 4$. ▲▲▲

**Example**: A very important row-reduced echelon matrix is the **identity matrix** (**מטריצת הזהות**) $I$, which is a square matrix (i.e., $m = n$) of the form

$$I^i_j = \delta^j_i = \begin{cases} 1 & i = j \\ 0 & i \neq j, \end{cases}$$

i.e.,

$$I = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

The symbol $\delta^j_i$ is called **Kronecker's delta**. ▲▲▲

Row-reduced echelon matrices are useful, because we can read off the solution to the associated linear system right away. For every $i = 1, \ldots, r$, we call the variable $X^{k_i}$ a **dependent variable**; a variable $X^j$ which is not a dependent variable, i.e., $j \notin \{k_1, \ldots, k_r\}$, is called a **free variable**. The general solution of a linear system $A\mathbf{X} = \mathbf{b}$, where $A$ is a row-reduced echelon matrix is constructed as follows: assign arbitrary values to the free variables, and then, express the dependent variables in terms of the free variables: that is, for each $i = 1, \ldots, r$,

$$x^{k_i} = b^i - \sum_{j \notin \{k_1, \ldots, k_r\}} a^i_j x^j.$$

Note that the summation is only on the indexes of the free variables.

**Example**: In the matrix (2.9), $X^1$, $X^3$ and $X^4$ are dependent variables, whereas $X^2$ and $X^5$ are free variables. Setting $X^2 = s$ and $X^5 = t$, the general solution of $A\mathbf{X} = 0$ is

$$\mathbf{x} = [3s - \tfrac{17}{3}t, s, \tfrac{5}{3}t, \tfrac{11}{3}t, t]^T.$$

▲ ▲ ▲

When is a non-homogeneous system consistent? Let $A\mathbf{X} = \mathbf{b}$ with $A$ being a row-reduced echelon matrix. There are two possibilities: if $A$ has a row with all its entries zero, and the corresponding row of $\mathbf{b}$ is non-zero, then the system does not have any solution. Otherwise, the zero rows can be ignored, and the system is consistent.

**Exercises**

**(easy) 2.23** Construct three matrices, each of which fails to satisfy exactly *one* condition in the definition of a row-reduced echelon matrix.

**(easy) 2.24** Let $A$ be a row-reduced echelon matrix having $r$ non-zero rows. Explain why it must hold that $r \leq m$ and $r \leq n$.

**(easy) 2.25** Characterize all $1 \times n$ and all $m \times 1$ row-reduced echelon matrices.

**(easy) 2.26** Explain why the $n \times n$ identity matrix is the unique $n \times n$ row-reduced echelon matrix having no zero row.

**(easy) 2.27** Characterize *all* the $2 \times 2$ row-reduced echelon matrices.

### 2.4.4 The Gauss-Jordan algorithm

The key theorem for a systematic solution of linear systems is the following:

***Theorem 2.18*** *Every $m \times n$ matrix $A$ is row-equivalent to a row-reduced echelon matrix.*

*Proof*: The proof follows a procedure called the **Gauss-Jordan algorithm**. If all the entries of $A$ are zero, then $A$ is already a row-reduced echelon matrix (hence it is row-equivalent to one). Otherwise, if needed, take any row whose first nonzero entry is the least, and bring it to be the first row (this is an operation preserving row-equivalence, see Exercise 2.22); in the new matrix, $k_1$ is the column of the first non-zero entry of the first row. Divide the first row by $a^1_{k_1}$ such that after this change $a^1_{k_1} = 1$. Then, subtract from the $i$-th row, $i \neq 1$, $a^i_{k_1}$ times the first row. These are elementary row-operations which eliminate all entries in the $k_1$-st column except in the first row.

Next, ignore the first row and bring to the second row the row whose first nonzero entry is the least. Denote by $k_2$ the column of the first non-zero entry of the second row; by construction, $k_2 > k_1$. Divide the second row by $a^2_{k_2}$ such that after this change $a^2_{k_2} = 1$. Then, subtract from the $i$-th row, $i \neq 2$, $a^i_{k_2}$ times the second row. These are elementary row-operations which eliminate all entries in the $k_2$-nd column except in the second row. Note also that this did not destroy the fact that up to the $k_2$-th column, the only nonzero entries are $a^1_{k_1} = 1$ and possibly $a^1_j$ for $k_1 < j < k_2$.

We proceed this way, until reaching the $m$-th row, or until the remaining rows are identically zero. ■

**Example**: Apply the Gauss-Jordan algorithm on

$$A = \begin{bmatrix} 2 & 1 & 2 & 10 \\ 1 & 2 & 1 & 8 \\ 3 & 1 & -1 & 2 \end{bmatrix}.$$

We follows the procedure,

$$\begin{bmatrix} 2 & 1 & 2 & 10 \\ 1 & 2 & 1 & 8 \\ 3 & 1 & -1 & 2 \end{bmatrix} \overset{r_1 \leftarrow r_1/2}{\longrightarrow} \begin{bmatrix} 1 & 1/2 & 1 & 5 \\ 1 & 2 & 1 & 8 \\ 3 & 1 & -1 & 2 \end{bmatrix} \overset{r_2 \leftarrow r_2 - r_1}{\longrightarrow} \begin{bmatrix} 1 & 1/2 & 1 & 5 \\ 0 & 3/2 & 0 & 3 \\ 3 & 1 & -1 & 2 \end{bmatrix}$$

$$\overset{r_3 \leftarrow r_3 - 3r_1}{\longrightarrow} \begin{bmatrix} 1 & 1/2 & 1 & 5 \\ 0 & 3/2 & 0 & 3 \\ 0 & -1/2 & -4 & -13 \end{bmatrix} \overset{r_2 \leftarrow 2r_2/3}{\longrightarrow} \begin{bmatrix} 1 & 1/2 & 1 & 5 \\ 0 & 1 & 0 & 2 \\ 0 & -1/2 & -4 & -13 \end{bmatrix}$$

$$\overset{r_1 \leftarrow r_1 - r_2/2}{\longrightarrow} \begin{bmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & -1/2 & -4 & -13 \end{bmatrix} \overset{r_3 \leftarrow r_3 + r_2/2}{\longrightarrow} \begin{bmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & -4 & -12 \end{bmatrix}$$

$$\overset{r_3 \leftarrow -r_3/4}{\longrightarrow} \begin{bmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix} \overset{r_1 \leftarrow r_1 - r_3}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

▲ ▲ ▲

**Example**: With $A$ as in the previous example, solve the linear system

$$A\mathbf{X} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

using the augmented matrix of this system. ▲ ▲ ▲

**Solution of linear systems using the Gauss-Jordan algorithm** Let $[A|\mathbf{b}]$ be the augmented matrix representing a linear system of $m$ equations in $n$ unknowns. We now have a systematic way of determining whether it is consistent, and if it is, finding its set of solutions. Let $R \in M_{m\times n}(\mathbb{F})$ be a row-reduced echelon matrix which is row-equivalent to $A$ and let $[R|\mathbf{d}]$ be the augmented matrix obtained by applying on $[A|\mathbf{b}]$ the elementary row-operations bringing $A$ into $R$. That is, the system represented by $[R|\mathbf{d}]$ has the same set of solutions as the system represented by $[A|\mathbf{b}]$.

Let $r \leq m$ be the number of non-zero rows in $R$ and let $k_1 < k_2 < \cdots < k_r$ be the columns of the leading non-zero elements in each of these rows. Thus, the variables

$$X^{k_1}, X^{k_2}, \ldots, X^{k_r}$$

are the dependent variables, whereas the rest, which we denote by

$$X^{\ell_1}, X^{\ell_2}, \ldots, X^{\ell_{n-r}}$$

are the free variables.

By the structure of the row-reduced echelon matrix, the first $r$ equations read

$$\begin{aligned} X^{k_1} + \sum_{j=1}^{n-r} r^1_{\ell_j} X^{\ell_j} &= d^1 \\ &\vdots \\ X^{k_r} + \sum_{j=1}^{n-r} r^r_{\ell_j} X^{\ell_j} &= d^r, \end{aligned}$$

whereas the next $m-r$ equations read

$$\begin{aligned} 0 &= d^{r+1} \\ &\vdots \\ 0 &= d^{m}. \end{aligned}$$

Evidently, if $d^{r+1}, \ldots, d^m$ are not all zero, then the system is not consistent. If however,

$$d^{r+1} = d^{r+2} = \cdots = d^m = 0,$$

then we can replace the free variables $X^{\ell_1}, \ldots, X^{\ell_{n-r}}$ by any sequence of scalars $t^1, \ldots, t^{n-r}$, obtaining a solvable equation for each of the dependent variables $X^{k_1}, \ldots, X^{k_r}$ (a linear equation in one unknown!), whose solution is

$$x^{k_i} = d^i - \sum_{j=1}^{n-r} r^1_{\ell_j} t^j.$$

We should have perhaps noted long ago, that any homogeneous linear system has at least one solution, $[0, 0, \ldots, 0]^T$, which we simply denote by $0 \in \mathbb{F}^n_{\text{col}}$. This solution is called the **trivial solution** (**הפתרון הטריוויאלי**). For any matrix that has free variables, there also exist non-trivial solutions to the homogeneous problem (as they may assume any value). In particular,

***Proposition 2.19*** *If $A$ is an $m \times n$ matrix with $m < n$ (i.e., less equations than unknowns), then the homogeneous system $A\mathbf{X} = 0$ has non-trivial solutions.*

*Proof*: Reduce $A$ to a row-reduced echelon matrix. Then, there are at most $m$ nonzero rows, hence there are at least $m - n$ free variables. ■

The question of whether there exist non-trivial solutions is central to linear algebra. Naively, we would expect solutions to be unique when the number of equations is equal to the number of unknown, i.e., when $m = n$. This is not sufficient. The following theorem characterizes the square matrices for which the trivial solution is the only solution:

***Theorem 2.20*** *Let $A$ be an $n \times n$ matrix. Then, the homogeneous system $A\mathbf{X} = 0$ has only a trivial solution if and only if $A$ is row-equivalent to the $n \times n$ identity matrix.*

*Proof*: There are two directions to prove. Assume first that $A$ is row-equivalent to the identity matrix. Since row-equivalent matrices have the same associated solutions, the solutions to $A\mathbf{X} = 0$ coincide with the solutions of $I\mathbf{X} = 0$, i.e,

$$X^1 = 0 \qquad X^2 = 0 \qquad \cdots \qquad X^n = 0,$$

and those only include the trivial solution.

Conversely, suppose that $x = 0$ is the only solution to $A\mathbf{X} = 0$. Let $R$ denote a row-reduced echelon matrix which is row-equivalent to $A$. Then, $R\mathbf{X} = 0$ doesn't have non-trivial solutions, which means that all of its $n$ rows are non-zero. This is only possible if $k_1 = 1$, $k_2 = 2$, etc, and the only row-reduced echelon matrix satisfying these conditions is the identity matrix. ■

**Exercises**

**(intermediate) 2.28** Suppose that $A$ is a square matrix which is row-equivalent to the identity matrix. Show that the inhomogeneous system $A\mathbf{X} = \mathbf{b}$ is consistent and has a unique solution.

**(intermediate) 2.29** Let $\mathbb{F} = \mathbb{Q}$. Find all the solutions to the homogeneous linear system

$$\begin{array}{rrrl} \frac{1}{3}X^1 & +2X^2 & -6X^3 & = 0 \\ -4X^1 & & +5X^3 & = 0 \\ -3X^1 & +6X^2 & -13X^3 & = 0 \\ -\frac{7}{3}X^1 & +2X^2 & -\frac{8}{3}X^3 & = 0 \end{array}$$

by first writing it in matrix form, and then transforming the matrix of coefficients into a row-reduced echelon matrix.

**(intermediate) 2.30** What are all the solutions (if any) of the system

$$\begin{array}{rrrl} X^1 & -X^2 & +2X^3 & = 1 \\ 2X^1 & & +2X^3 & = 1 \\ X^1 & -3X^2 & +4X^3 & = 2. \end{array}$$

Use the augmented matrix representation to solve this system.

**(intermediate) 2.31** Show using the Gauss-Jordan algorithm that the non-homogeneous system

$$\begin{array}{cccc} X^1 & -2X^2 & +X^3 & +2X^4 & = 1 \\ X^1 & +X^2 & -X^3 & +X^4 & = 2 \\ X^1 & +7X^2 & -5X^3 & -X^4 & = 3. \end{array}$$

has no solutions.

**(intermediate) 2.32** Let

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

For which $\mathbf{b} \in \mathbb{F}^3_{\text{col}}$ does the system $A\mathbf{X} = \mathbf{b}$ have a solution?

**(intermediate) 2.33** Let

$$A = \begin{bmatrix} 3 & -6 & 2 & -1 \\ -2 & 4 & 1 & 3 \\ 0 & 0 & 1 & 1 \\ 1 & -2 & 1 & 0 \end{bmatrix}.$$

For which $\mathbf{b} \in \mathbb{F}^4_{\text{col}}$ does the system $A\mathbf{X} = \mathbf{b}$ have a solution?

**(harder) 2.34** Let $A$ and $B$ be two $2 \times 3$ row-reduced echelon matrices. Suppose that the homogeneous systems $A\mathbf{X} = 0$ and $B\mathbf{X} = 0$ have the same set of solutions. Prove that $A = B$.

## 2.5 Operations with matrices

### 2.5.1 Addition of matrices

Given two matrices $A, B \in M_{m\times n}(\mathbb{F})$ we define their sum

$$S = A + B$$

to be a matrix $S \in M_{m\times n}(\mathbb{F})$, whose entries $s^i_j$ are given by

$$s^i_j = a^i_j + b^i_j.$$

Note that the "+" sign in both relations has a totally different meaning: the first is addition in $M_{m\times n}(\mathbb{F})$, whereas the second is addition in $\mathbb{F}$. Another way to write the definition of the addition of matrices (of the same size!) is

$$(A+B)^i_j = a^i_j + b^i_j.$$

**Example**:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 7 & 8 & 9 \\ 10 & 11 & 12 \end{bmatrix} = \begin{bmatrix} 8 & 10 & 12 \\ 14 & 16 & 18 \end{bmatrix}.$$

▲ ▲ ▲

If we denote by $0_{m\times n}$ (or just 0 in short) the $m \times n$-matrix whose entries are all zero, then

$$A + 0 = A$$

for every $A \in M_{m\times n}(\mathbb{F})$. Likewise, given $A \in M_{m\times n}(\mathbb{F})$, we denote by $(-A)$ the $m \times n$ matrix given by

$$(-A)^i_j = -a^i_j.$$

For every $A \in M_{m\times n}(\mathbb{F})$,

$$A + (-A) = 0.$$

It is easy to see that matrix addition is associative, namely, for every $A, B, C \in M_{m\times n}(\mathbb{F})$ we have

$$(A + B) + C = A + (B + C),$$

and commutative. namely,

$$A + B = B + A.$$

Note that the addition of matrices satisfies the four axioms of addition in a field. This doesn't make $M_{m\times n}(\mathbb{F})$ into a field!

We could define in a similar way products of matrices of the same size. We could. But we won't do so. We will rather have a different definition for products of matrices, not necessarily of the same size, which will relate to linear combinations of systems of equations.

You may ask yourself what is the purpose of adding up matrices, and whether it relates to the solution of linear systems of equations. The meaning of matrix addition will be clarified later in this course, in the context of linear transformations.

**Exercises**

**(easy) 2.35** Show that matrix addition is both associative and commutative.

### 2.5.2 Multiplication by a scalar

For a matrix $A \in M_{m\times n}(\mathbb{F})$ and a scalar $c \in \mathbb{F}$ we define their product, $cA \in M_{m\times n}(\mathbb{F})$, whose entries are defined by

$$(cA)^i_j = c\,a^i_j.$$

That is, the scalar $c$ multiplies every entry of $A$ to yield the matrix $cA$. We could think of the elements of $\mathbb{F}$ as "acting" on elements in $M_{m\times n}(\mathbb{F})$ resulting in an element in $M_{m\times n}(\mathbb{F})$.

**Example**:

$$4 \cdot \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 4 & 8 & 12 \\ 16 & 20 & 24 \end{bmatrix}.$$

▲ ▲ ▲

It is easy to see that multiplication by a scalar satisfies

$$1_{\mathbb{F}} \cdot A = A$$

for every $A \in M_{m\times n}(\mathbb{F})$, and

$$c(dA) = (cd)A$$

for every $c, d \in \mathbb{F}$ and $A \in M_{m\times n}(\mathbb{F})$; this is a kind-of associativity up to the fact that the product between scalars differs from the product between a scalar and a matrix. Also, for every $A \in M_{m\times n}(\mathbb{F})$,

$$0_{\mathbb{F}} \cdot A = 0_{m\times n}$$

and for every $c \in \mathbb{F}$,

$$c\,0_{m\times n} = 0_{m\times n}.$$

Finally, for every $A \in M_{m\times n}(\mathbb{F})$,

$$(-1_{\mathbb{F}})A = (-A).$$

The product of a scalar and a matrix satisfies also distributive properties: on the one hand, for every $A, B \in M_{m\times n}(\mathbb{F})$ and $c \in \mathbb{F}$,

$$c\,(A + B) = c\,A + c\,B. \tag{2.10}$$

On the other hand, for every $A \in M_{m\times n}(\mathbb{F})$ and $c, d \in \mathbb{F}$,

$$(c + d)\,A = c\,A + d\,A. \tag{2.11}$$

**Exercises**

**(easy) 2.36** Show that the multiplication of a matrix by a scalar satisfies $1_{\mathbb{F}} \cdot A = A$ for every $A \in M_{m\times n}(\mathbb{F})$, and $c(dA)) = (cd)A$ for every $c, d \in \mathbb{F}$ and $A \in M_{m\times n}(\mathbb{F})$.

**(easy) 2.37** Show that for every $A \in M_{m\times n}(\mathbb{F})$,

$$(-1_{\mathbb{F}})A = (-A),$$

and more generally that for every $A \in M_{m\times n}(\mathbb{F})$ and $c \in \mathbb{F}$

$$(-c)\,A = -(c\,A).$$

**(easy) 2.38** Prove the two distributive properties (2.10), (2.11) of the product of a scalar and a matrix.

### 2.5.3 Products of matrices

We started this chapter by considering linear systems in which each equation is a linear combination of the equations of another system, before focusing on the particular case of elementary row-operations. We now return to the procedure of forming linear combinations of equations in a more systematic way, leaning upon our new notational system of matrices.

Let $A \in M_{m\times n}(\mathbb{F})$ be a matrix representing a system of $m$ equations in $n$ unknowns. Suppose that we want to create from it a system of $p$ equations in the same $n$ unknowns by taking linear combinations of the equations of the first system. Think of the $i$-th equation in the new system. It is formed by multiplying the first equation by a scalar $b_1^i$, the second equation by a scalar $b_2^i$ up to the $m$-th equation by a scalar $b_m^i$, and adding up the $m$ equations.

What is the coefficient of $X^1$ in the new equation? It is

$$b_1^i a_1^1 + b_2^i a_1^2 + \cdots + b_m^i a_1^m = \sum_{k=1}^{m} b_k^i a_1^k.$$

Note that the index $i$ remains fixed—it represents the index of the equation in the new system—and so does the index 1—which represents the variable whose coefficient we calculate.

Likewise, the coefficient of $X^2$ in the new $i$-th equation is

$$b_1^i a_2^1 + b_2^i a_2^2 + \cdots + b_m^i a_2^m = \sum_{k=1}^{m} b_k^i a_2^k,$$

and more generally, the coefficient of $X^j$ in the new $i$-th equation is

$$b_1^i a_j^1 + b_2^i a_j^2 + \cdots + b_m^i a_j^m = \sum_{k=1}^{m} b_k^i a_j^k.$$

Thus, to form $p$ equations by linear combinations of $m$ equations we need $p \times m$ scalars

$$\{b_j^i \ : \ i = 1, \ldots, p, \ \ j = 1, \ldots, m\},$$

such that the coefficient of the $j$-th variable in the new $i$-th equation is given by

$$\sum_{k=1}^{m} b_k^i a_j^k.$$

This operation of forming linear combinations of equations can be represented using matrices.

***Definition 2.21*** *Let $B \in M_{p\times m}(\mathbb{F})$ and let $A \in M_{m\times n}(\mathbb{F})$. Their product (**מכפלה של מטריצות**) $BA$ is a $p \times n$ matrix whose $(i, j)$-th entry is given by*

$$(BA)_j^i = \sum_{k=1}^{m} b_k^i a_j^k = b_1^i a_j^1 + \cdots + b_m^i a_j^m.$$

Note: for the product $BA$ to be defined, the number of columns in $B$ has to be equal to the number of rows in $A$.

**Example**: Consider a linear system of 2 equations in 3 unknowns represented by the matrix

$$A = \begin{bmatrix} 5 & -1 & 2 \\ 15 & 4 & 8 \end{bmatrix}.$$

We form a new system of 2 equations in 3 unknowns by multiplying it by the matrix

$$B = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}.$$

The first equation in the new system is obtained by multiplying the first equation in the original system by 1 and the second equation by zero and adding the two—in other words, the first equation remains the same. The second equation in the new system is obtained be multiplying the first equation in the original system by $(-3)$ and the second equation by 1 and adding the two. The corresponding matrix product is

$$\begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 5 & -1 & 2 \\ 15 & 4 & 8 \end{bmatrix} = \begin{bmatrix} 5 & -1 & 2 \\ 0 & 7 & 2 \end{bmatrix}.$$

▲ ▲ ▲

Note that when we wrote the unknowns as an $n \times 1$ matrix, and the right-hand side of the equation as an $m \times 1$ matrix,

$$\mathbf{X} = \begin{bmatrix} X^1 \\ X^2 \\ \vdots \\ X^n \end{bmatrix} \qquad \text{and} \qquad \mathbf{b} = \begin{bmatrix} b^1 \\ b^2 \\ \vdots \\ b^m \end{bmatrix},$$

the equation $A\mathbf{X} = \mathbf{b}$ can be interpreted in terms of matrix multiplication: the product of an $m \times n$ matrix and an $n \times 1$ matrix is an $m \times 1$ matrix.

**Example**: Let $A$ be an $m \times n$ matrix and let $I_m$ (or in short $I$) be the $m \times m$ identity matrix, which we recall is given by

$$I^j_i = \delta^j_i = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

Then,

$$(I_m A)^i_j = \sum_{k=1}^{m} \delta^i_k A^k_j = A^i_j,$$

namely $I_m A = A$ for every $A$. Likewise,

$$(AI_n)^i_j = \sum_{k=1}^{n} A^i_k \delta^k_j = A^i_j,$$

namely, $AI_n = A$. ▲▲▲

**Example**: Let's see what happens when we multiply a matrix by a matrix which has all entries zero except for one entry, which is 1. For example, suppose that the $(2,3)$ entry equals one,

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a^1_1 & a^1_2 & a^1_3 & a^1_4 \\ a^2_1 & a^2_2 & a^2_3 & a^2_4 \\ a^3_1 & a^3_2 & a^3_3 & a^3_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ a^3_1 & a^3_2 & a^3_3 & a^3_4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Thus, the third row was copied into the second row of the product.

For the other way around

$$\begin{bmatrix} a^1_1 & a^1_2 & a^1_3 & a^1_4 \\ a^2_1 & a^2_2 & a^2_3 & a^2_4 \\ a^3_1 & a^3_2 & a^3_3 & a^3_4 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & a^1_2 \\ 0 & 0 & a^2_2 \\ 0 & 0 & a^3_2 \end{bmatrix},$$

i.e., the second column was copied into the third column of the product. ▲▲▲

Here is another way to define the product of two matrices. Let $B \in M_{1\times m}(\mathbb{F}) = \mathbb{F}^m_{\text{row}}$ and $A \in M_{m\times 1}(\mathbb{F}) = \mathbb{F}^n_{\text{col}}$. We define their product by

$$BA = \begin{bmatrix} b_1 & b_2 & \cdots & b^m \end{bmatrix} \begin{bmatrix} a^1 \\ a^2 \\ \vdots \\ a^m \end{bmatrix} = \sum_{j=1}^{m} b_j a^j.$$

Then, for $B \in M_{p\times m}(\mathbb{F})$ and $A \in M_{m\times n}(\mathbb{F})$, their product $BA \in M_{p\times n}(\mathbb{F})$ is defined by

$$(BA)^i_j = \text{Row}^i(B) \cdot \text{Col}_j(A).$$

The following relations are useful to remember,

$$\begin{aligned} \text{Row}^i(AB) &= \text{Row}^i(A) \cdot B \\ \text{Col}_j(AB) &= A \cdot \text{Col}_j(B). \end{aligned} \tag{2.12}$$

**Exercises**

**(easy) 2.39** Let

$$A = \begin{bmatrix} 2 & -1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 3 \\ 1 \\ -1 \end{bmatrix} \qquad \text{and} \qquad C = \begin{bmatrix} 1 & -1 \end{bmatrix}.$$

Calculate $ABC$ and $CAB$ (advice: before starting to calculate, determine the size of the matrices in each case).

**(easy) 2.40** Let

$$A = \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix} \qquad B = \begin{bmatrix} & & 1 \\ 1 & & \\ & 1 & \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}.$$

Calculate $AB$, $BA$, $ABC$ and $CBA$.

**(intermediate) 2.41** Let

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Calculate $A^2$, $A^3$, $A^4$, $A^5$ and $A^6$.

**(intermediate) 2.42** Find a non-zero matrix $A \in M_{2\times 2}(\mathbb{F})$ satisfying $A^2 = 0_{2\times 2}$.

**(intermediate) 2.43** Let

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Calculate $A^{2020}$.

**(intermediate) 2.44** Let $A \in M_{m\times n}(\mathbb{F})$ and $B \in B_{k\times m}(\mathbb{F})$. Which of the following statements is true? If it is, prove it, otherwise provide a counter example.

(a) If the first row of $A$ is zero, then the first row of $BA$ is zero.

(b) If the first column of $A$ is zero, then the first column of $BA$ is zero.

(c) If the first two rows of $B$ are zero, then the first two rows of $BA$ are zero.

(d) If the first two columns of $B$ are zero, then the first two columns of $BA$ are zero.

(e) If the $i$-th and the $j$-th rows of $A$ are equal then the $i$-th and the $j$-th rows of $BA$ are equal.

(f) If the $i$-th and the $j$-th columns of $A$ are equal then the $i$-th and the $j$-th columns of $BA$ are equal.

(g) If the $i$-th and the $j$-th rows of $B$ are equal then the $i$-th and the $j$-th rows of $BA$ are equal.

(h) If the $i$-th and the $j$-th columns of $B$ are equal then the $i$-th and the $j$-th columns of $BA$ are equal.

**(harder) 2.45** Prove or disprove the following statements:

(a) If $A, B \in M_{n\times n}(\mathbb{F})$ satisfy $AB = B$ and $B \neq 0$, then $A = I_2$.

(b) There exists a matrix $A \in M_{2\times 2}(\mathbb{F})$ satisfying $A^2 = -I_2$.

### 2.5.4 Algebraic properties of matrix multiplication

Since we have introduced a new operation—a product of matrices—there are natural questions to raise: (i) is it commutative? (ii) is it associative? (iii) does this product have a unit element? (iii) is it distributive? (iv) How does it relate to multiplication by a scalar?

For commutativity, for $AB$ and $BA$ to be defined, it must be that if $A \in M_{m\times n}(\mathbb{F})$, then $B \in M_{n\times m}(\mathbb{F})$. Take for example, $m = n = 2$, and consider the matrices

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix}.$$

Then,

$$AB = \begin{bmatrix} 2 & 7 \\ 6 & 15 \end{bmatrix} \qquad \text{and} \qquad BA = \begin{bmatrix} 5 & 8 \\ 9 & 12 \end{bmatrix},$$

i.e., matrix multiplication is not commutative.

For associativity, we first note that if $A$ is an $m \times n$ matrix, $B$ is an $n \times p$ matrix and $C$ is a $p \times q$ matrix, then both $(AB)C$ and $A(BC)$ are well-defined $m \times q$ matrices.

***Proposition 2.22*** *Matrix multiplication is associative: for all* $A \in M_{m\times n}(\mathbb{F})$, $B \in M_{n\times p}(\mathbb{F})$ *and* $C \in M_{p\times q}(\mathbb{F})$,

$$(AB)C = A(BC).$$

*Proof*: Just follow the definition, using the associative properties of both addition and multiplication in $\mathbb{F}$.

$$((AB)C)^i_j = \sum_{k=1}^{p} (AB)^i_k c^k_j = \sum_{k=1}^{p} \left( \sum_{s=1}^{n} a^i_s b^s_k \right) c^k_j = \sum_{k=1}^{p} \sum_{s=1}^{n} a^i_s b^s_k c^k_j,$$

and

$$(A(BC))^i_j = \sum_{s=1}^{n} a^i_s (BC)^s_j = \sum_{s=1}^{n} a^i_s \left( \sum_{k=1}^{p} b^s_k c^k_j \right) = \sum_{s=1}^{n} \sum_{k=1}^{p} a^i_s b^s_k c^k_j.$$

Since the order of summation can be interchanged (commutativity of addition), both expressions are equal. ■

**Comment:** Since $(AB)C = A(BC)$, we may write products $ABC$ unambiguously. The same holds for the product of four of more matrices (as long as they are of compatible size).

**Comment:** if $A$ is a square matrix, then $AA$ is well-defined. By associativity, $AAA$, $AAAA$ are well-defined, hence we may write $A^k$, $k \in \mathbb{N}$ unambiguously.

Regarding unit elements, we saw that an $m \times n$ matrix has a unit element $I_m$ for left-multiplication and a unit element $I_n$ for right-multiplication.

Next,

***Proposition 2.23*** *Matrix multiplication and matrix addition are distributive. If $A$ and $B$ are $m \times n$ matrices and $C$ and $D$ are $n \times p$ matrices, then*

$$(A+B)C = AC + BC \qquad \text{and} \qquad A(C+D) = AC + AD.$$

*Proof*: This is left as an exercise. ■

Finally, we also have the following form of associativity:

***Proposition 2.24*** *Let $A \in M_{m\times n}(\mathbb{F})$ and $B \in M_{n\times p}(\mathbb{F})$. Let $\lambda \in \mathbb{F}$. Then,*

$$\lambda(AB) = (\lambda A)B.$$

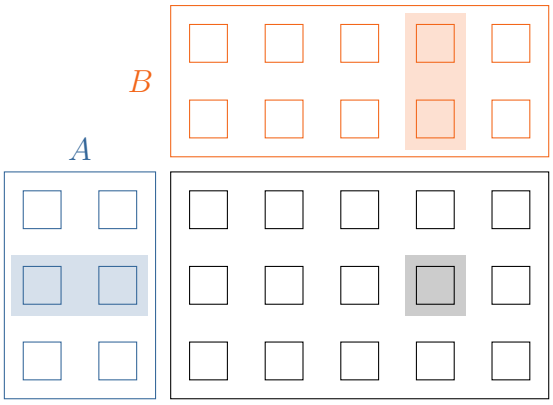
*Proof*: This is left as an exercise. ■

**Exercises**

**(intermediate) 2.46** Prove Propositions 2.23 and 2.24.

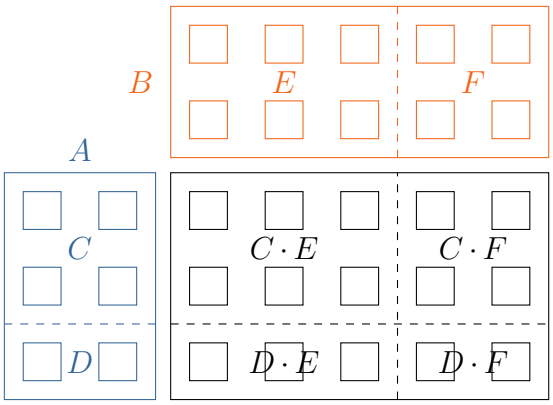
### 2.5.5 Matrix multiplication and block patterns

Consider as an example a product of a $3 \times 2$ matrix $A$ and a $2 \times 5$ matrix $B$. We may look at this product as follows:



In this illustration, $(AB)_4^2$ is determined by multiplying the second row of $A$ and the fourth column of $B$.

Think now of $A$ and $B$ as matrices which are internally divided into sub-matrices as follows:




Here, we partition the rows of $A$ into two groups so that we represent the matrix $A \in M_{3\times 2}(\mathbb{F})$ as

$$A = \begin{bmatrix} C \\ D \end{bmatrix},$$

where $C \in M_{2\times 2}(\mathbb{F})$ and $D \in M_{1\times 2}(\mathbb{F})$. Likewise, we partition the columns of $B$ into two groups so that we represent the matrix $B \in M_{3\times 2}(\mathbb{F})$ as

$$B = \begin{bmatrix} E & F \end{bmatrix},$$

where $E \in M_{2\times 3}(\mathbb{F})$ and $F \in M_{2\times 2}(\mathbb{F})$. Then, the product $AB \in M_{3\times 5}(\mathbb{F})$ can be represented as a **block matrix**

$$AB = \begin{bmatrix} CE & CF \\ DE & DF \end{bmatrix},$$

with $CE \in M_{2\times 3}(\mathbb{F})$, $CF \in M_{2\times 2}(\mathbb{F})$, $DE \in M_{1\times 3}(\mathbb{F})$ and $DF \in M_{1\times 2}(\mathbb{F})$.

### 2.5.6 Invertible matrices

In this section we consider the algebra of $n\times n$ matrices with values in $\mathbb{F}$, which we denote by $M_n(\mathbb{F})$ (as short-hand notation for $M_{n\times n}(\mathbb{F})$). Such matrices

are called **square matrices** (**מטריצות ריבועיות**); they have the property that their product yields once again a matrix of the same type. Note that in the context of linear systems, square matrices represent systems of equations in which the number of equations equals the number of variables.

***Definition 2.25*** *A matrix $A \in M_n(\mathbb{F})$ is called* ***invertible*** *(**הפיכה**) if there exists a matrix $B \in M_n(\mathbb{F})$ such that*

$$BA = AB = I_n.$$

*The matrix $B$ is called an* ***inverse*** *(**הפכית**) of the matrix $A$. The set of $n \times n$ invertible matrices is denoted by $\mathrm{GL}_n(\mathbb{F})$.*

**Comments:**

(a) By definition, if $A$ is invertible and $B$ is an inverse of $A$, then $B$ is invertible and $A$ is an inverse of $B$.

(b) At this stage, we are referring to *an* inverse rather than *the* inverse because we don't (yet) know whether there exists a unique inverse.

**Example**: The matrix $I_n$ is invertible as

$$I_n I_n = I_n,$$

i.e., $I_n$ is its own inverse. ▲▲▲

**Comment:** If a matrix $A \in M_n(\mathbb{F})$ has a row whose entries are all zero or a column whose entries are all zero, then it is not invertible. Why? Suppose that the $i$-th row of $A$ is zero. Then, for every matrix $B \in M_n(\mathbb{F})$,

$$(AB)^i_i = \mathrm{Row}^i(A) \cdot \mathrm{Col}_i(B) = 0 \neq (I_n)^i_i,$$

i.e., $AB$ cannot be equal $I_n$. Similarly, if the $i$-th column of $A$ is zero, then for every matrix $B \in M_n(\mathbb{F})$,

$$(BA)^i_i = \mathrm{Row}^i(B) \cdot \mathrm{Col}_i(A) = 0_{\mathbb{F}} \neq 1_{\mathbb{F}} = (I_n)^i_i,$$

and $BA$ product cannot be equal $I_n$.

In fact, there are many more matrices that are not invertible:

***Proposition 2.26*** *Let $A \in M_n(\mathbb{F})$. If there exists a non-zero matrix $C \in M_n(\mathbb{F})$ such that $AC = 0$, then $A$ in not invertible.*

*Proof*: Suppose by contradiction that $A$ is invertible. That it, there exists a matrix $B \in M_n(\mathbb{F})$ such that $BA = I_n$. Using the associativity of matrix multiplication,

$$C = I_n C = (BA)C = B(AC) = B \cdot 0_{n\times n} = 0_{n\times n},$$

which is a contradiction, because we assumed that $C$ was not a zero matrix. ■

**Example**: In the case of $2 \times 2$ matrices we can find "by hand" a complete characterization of all the invertible matrices. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0_{2\times 2}.$$

A direct calculation shows that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ad-bc & \\ & ad-bc \end{bmatrix} = (ad-bc)I.$$

There are now two possibilities: if $ad - bc = 0_{\mathbb{F}}$ then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = 0_{2\times 2},$$

and by Proposition 2.26, $A$ is not invertible. If, however, $ad - bc \neq 0_{\mathbb{F}}$, then $A$ is invertible with

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

being an inverse. ▲▲▲

**Comment:** The scalar $ad - bc$ is known as the **determinant** (דטרמיננטה) of the matrix $A$, denoted

$$\det A = ad - bc.$$

We will study determinants of general square matrices later on in this course.

***Lemma 2.27*** *Let $A, L, R \in M_n(\mathbb{F})$ be such that*

$$LA = I_n \qquad \text{and} \qquad AR = I_n.$$

*(The matrix $L$ is called a **left-inverse** (**הפכית שמאלית**) of $A$ and the matrix $R$ is called a **right-inverse** (**הפכית ימנית**) of $A$.) Then*

$$L = R,$$

*and $A$ is invertible.*

*Proof*: Using the associativity of matrix multiplication,

$$L = LI_n = L(AR) = (LA)R = I_nR = R,$$

i.e., $L = R$. By definition $L(= R)$ is an inverse of $A$. ■

***Corollary 2.28*** *If $A \in M_n(\mathbb{F})$ is invertible, then its inverse is unique.*

*Proof*: Suppose that $L, R \in M_n(\mathbb{F})$ are both inverses of $A$. By defintiion,

$$LA = I_n \qquad \text{and} \qquad AR = I_n.$$

By Lemma 2.27, $L = R$, proving the uniqueness of $A$. ■

Since an invertible matrix $A$ has a unique inverse, we can introduced a notation for its inverse: $A^{-1}$.

We now further characterize the set $\mathrm{GL}_n(\mathbb{F})$ of invertible $n \times n$ matrices with entries in $\mathbb{F}$.

***Proposition 2.29*** *Let $A, B \in M_n(\mathbb{F})$. Then,*

*(a) If $A$ is invertible, so is $A^{-1}$ and $(A^{-1})^{-1} = A$*

*(b) If $A$ and $B$ are both invertible, then so is $AB$ and*

$$(AB)^{-1} = B^{-1}A^{-1}.$$

*(Note the inversion in the order of $B^{-1}$ and $A^{-1}$ relative to $A$ and $B$, and recall that matrix multiplication is not commutative.)*

*Proof*: By definition of the inverse,

$$AA^{-1} = A^{-1}A = I_n,$$

which proves, by definition, that $A^{-1}$ is invertible and $A$ is its inverse. For the second statement, using the associativity of matrix multiplication,

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$$
$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n,$$

proving that $B^{-1}A^{-1}$ is the inverse of $AB$. ■

***Corollary 2.30*** *Any (finite) product of invertible matrices is invertible.*

*Proof*: This is left as an exercise. ■

**Comment:** We have just seen that the set $\mathrm{GL}_n(\mathbb{F})$ satisfies the following properties:

(a) It is not empty.

(b) It is endowed with a product that takes two elements of $\mathrm{GL}_n(\mathbb{F})$ and returns an element in $\mathrm{GL}_n(\mathbb{F})$.

(c) It has a unit element $I_n$ satisfying $AI_n = I_nA = A$ for every $A \in \mathrm{GL}_n(\mathbb{F})$.

(d) Every $A \in \mathrm{GL}_n(\mathbb{F})$ has a $B \in \mathrm{GL}_n(\mathbb{F})$ satisfying $AB = BA = I_n$.

Such a structure is called a **group** (חבורה); it is the main subject of a second-year course in algebra. Note that a group, unlike a field, is endowed with only one algebraic operation, which does not need to be commutative. The notation $\mathrm{GL}_n$ stands for the **general linear group**.

### Exercises

**(easy) 2.47** Let $A \in M_n(\mathbb{F})$. Show that if there exists a non-zero matrix $C \in M_n(\mathbb{F})$ such that $CA = 0$, then $A$ in not invertible.

**(easy) 2.48** Is the matrix

$$\begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix}$$

invertible? If it is, what is its inverse?

**(easy) 2.49** Is the matrix

$$\begin{bmatrix} 1 & & \\ & 3 & \\ & & 6 \end{bmatrix}$$

invertible? If it is, what is its inverse?

**(intermediate) 2.50** Prove that for every $k \in \mathbb{N}$, a product of $k$ invertible matrices is invertible.

**(intermediate) 2.51** Prove or disprove the following statements:

(a) If $A, B, C \in M_n(\mathbb{F})$ satisfy that $A$ is invertible and $AB = AC$, then $B = C$.

(b) If $A, B \in \mathrm{GL}_n(\mathbb{F})$, then $A + B \in \mathrm{GL}_n(\mathbb{F})$.

(c) If $A, B \in M_n(\mathbb{F})$ are not invertible, then $A + B$ is not invertible.

(d) If $A \in \mathrm{GL}_n(\mathbb{F})$, then $A^3 \in \mathrm{GL}_n(\mathbb{F})$.

### 2.5.7 Elementary matrices

Next, we relate matrix multiplication to elementary row-operations. When we start with an $m \times n$ matrix, an elementary row-operation yields a new matrix of the same size, with each row being a linear combination of the rows of the original matrix. In other words, an elementary row-operation can be represented by a left-multiplication by an $m \times m$ matrix.

***Definition 2.31*** *An $m \times m$ matrix $E$ is called an **elementary matrix** (**מטריצה יסודית**) if there exists an elementary row-operation $e$ such that for every matrix $A$ (having $m$ rows) $EA = e(A)$.*

**Example**: Let $m = 2$. Then, the elementary matrices obtained by multiplying the first and second rows by $0 \neq c \in \mathbb{F}$ are

$$\begin{bmatrix} c & \\ & 1 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 1 & \\ & c \end{bmatrix}.$$

The elementary matrices corresponding to adding $s$ times the first row to the second row, and $s$ times the second row to the first row are

$$\begin{bmatrix} 1 & \\ s & 1 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 1 & s \\ & 1 \end{bmatrix}.$$

▲▲▲

More generally, we denote by $D_k(a)$ the elementary matrix multiplying the $k$-th row by $a$. It is easy to verify that since

$$(e(A))^i_j = \begin{cases} c\,A^k_j & i = k \\ A^i_j & i \neq k, \end{cases}$$

it follows that

$$(D_k(a))^i_j = \begin{cases} 1 & i = j \neq k \\ a & i = j = k \\ 0 & \text{otherwise} \end{cases}.$$

**Example**: The elementary matrix corresponding to multiplying the second row by $c \neq 0$ is

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & c & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

▲▲▲

We denote by $T^\ell_k(c)$ the elementary matrix adding $c$ times the $\ell$-th row to the $k$-th row. It is easy to verify that since

$$(e(A))^i_j = \begin{cases} A^i_j & i \neq k \\ A^r_j + c\,A^k_j & i = r, \end{cases}$$

it follows that

$$(T_k^\ell(c))_j^i = \begin{cases} 1 & i = j \\ c & i = k,\ j = \ell \\ 0 & \text{otherwise} \end{cases}.$$

***Proposition 2.32*** *An elementary matrix is invertible and its inverse is again an elementary matrix; hence a product of elementary matrices is invertible.*

*Proof*: We show first that

$$(D_k(a))^{-1} = D_k(a^{-1}).$$

Indeed,

$$(D_k(a) \cdot D_k(a^{-1}))_j^i = \sum_{p=1}^{m} (D_k(a))_p^i (D_k(a^{-1}))_j^p = \begin{cases} 0 & i \neq j \\ 1 \cdot 1 & i = j \neq k \\ a \cdot a^{-1} & i = j = k. \end{cases}$$

In a similar way, we show that

$$(T_k^\ell(a))^{-1} = T_k^\ell(-a).$$

Finally, since any product of invertible matrices is invertible, it follows that any product of elementary matrices is invertible (see Exercise 2.50). ■

***Corollary 2.33*** *Two matrices $A, B \in M_{m\times n}(\mathbb{F})$ are row-equivalent if and only if there exists an $m \times m$ matrix $P$, which is a product of elementary matrices (hence in $GL_m(\mathbb{F})$), such that*

$$B = PA.$$

*Proof*: By definition, $A$ and $B$ are row-equivalent if and only if there exists a sequence of elementary row-operations $e_1, \ldots, e_k$, such that

$$B = e_k(e_{k-1}\cdots(e_1(A))).$$

We have just seen that every elementary row-operation is realized by a left-multiplication by an elementary matrix. That is, there exists a sequence $E_1, \ldots, E_k$ of elementary matrices such that

$$B = E_k(E_{k-1} \ldots (E_1(A))).$$

Since matrix multiplication is associative, we obtain the desired result with

$$P = E_k E_{k-1} \ldots E_1.$$

■

***Corollary 2.34*** *To every matrix $A \in M_{m\times n}(\mathbb{F})$ there exists a matrix $P \in \mathrm{GL}_m(\mathbb{F})$, which is a product of elementary matrices, such that*

$$R = PA$$

*is a row-reduced echelon matrix.*

*Proof*: By the Gauss-Jordan algorithm, $A$ is row-equivalent to a row-reduced echelon matrix $R$. By Corollary 2.33, there exists a matrix $P \in \mathrm{GL}_m(\mathbb{F})$, which is a product of elementary matrices, such that $R = PA$. ■

**Exercises**

**(easy) 2.52** Show by a direct calculation that the elementary $2 \times 2$ matrix

$$T_1^2(c) = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}$$

is invertible.

**(easy) 2.53** Write down explicitly the elementary matrix corresponding to the elementary row-operation of adding $c$ times row 4 to row 2 for $m = 5$.

**(intermediate) 2.54** For each of the following matrices, determine whether it is a product of elementary matrices; if it is find its inverse:

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad C = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & 1 \end{bmatrix} \quad E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

### 2.5.8 Elementary matrices and invertibility

We will now use the last results to state conditions under which a square matrix is invertible.

***Theorem 2.35*** *Let $A \in M_m(\mathbb{F})$. Then the following statements are equivalent:*

*(a) $A$ is invertible.*

*(b) $A$ is row-equivalent to $I_m$.*

*(c) $A$ is a product of elementary matrices.*

**Comment:** When we say that three (or more) statements are equivalent, it means that if one of them is true, then all of them are true, and equivalently, if one of them is false, then all are false. To prove it, it suffices to prove that the first statement implies the second, that the second implies the third, and so on, and finally that the last implies the first.

*Proof*: Statement (b) implies statement (c) as if $A$ is row-equivalent to $I_m$, then there exist elementary matrices $E_1, \ldots, E_s$ such that

$$A = E_s E_{s-1} \ldots E_1 I_m = E_s E_{s-1} \ldots E_1.$$

Statement (c) implies statement (a) by Proposition 2.32. Thus, it only remains to prove that an invertible matrix is row-equivalent to $I_m$.

Let $R$ be a row-reduced echelon matrix which is row-equivalent to $A$. Since $R$ and $A$ are row-equivalent, there exists a matrix $P$, which is a product of elementary matrices, such that $R = PA$, hence $R$ is invertible. It follows that $R$ does not have a row that is zero, but a square row-reduced echelon matrix which has no zero rows can only be the identity matrix. ■

In fact, the inverse of an invertible matrix can be calculated as follows:

***Proposition 2.36*** *Let $A \in \mathrm{GL}_m(\mathbb{F})$ and let $P$ be a product of elementary matrices such that $PA = I_m$. Then,*

$$PI_m = A^{-1}.$$

*That is, the sequence of operations reducing $A$ to $I_m$ is the same sequence bringing $I_m$ to $A^{-1}$.*

*Proof*: We have

$$(PI_m)A = P(I_mA) = PA = I_m,$$

which, by the uniqueness of the matrix inverse proves that $PI_m = A^{-1}$. ■

We finally relate the property of being invertible to the existence of solution to linear systems of equations:

***Theorem 2.37*** *Let $A \in M_m(\mathbb{F})$. The following statements are equivalent:*

*(a) $A$ is invertible.*

*(b) The homogeneous system $A\mathbf{X} = 0$ only has the trivial solution.*

*(c) For every $m \times 1$ matrix $\mathbf{b}$, the system $A\mathbf{X} = \mathbf{b}$ is consistent and its solution is unique.*

*Proof*: Suppose that Statement (a) holds, i.e., $A$ is invertible. On the one hand, $\mathbf{x} = A^{-1}\mathbf{b}$ is a solution; on the other hand, if $A\mathbf{x} = \mathbf{b}$, then

$$\mathbf{x} = I\mathbf{x} = A^{-1}A\mathbf{x} = A^{-1}\mathbf{b},$$

i.e., a solution exists and it is unique (because we actually determined what it must be), so that Statement (c) holds. Statement (b) is a particular example of Statement (c), so that (c) implies (b). It remains to prove that Statement (b) implies Statement (a).

Suppose, by contradiction, that Statement (b) holds and that $A$ is not invertible. Let $R$ be the row-reduced echelon matrix which is row-equivalent to $A$. Since $A$ is not invertible, $R$ is not the identity matrix, hence it has at

least one row identically zero. It follows that it has at least one free variable, contradicting the fact that $A\mathbf{X} = 0$ has a unique solution (since its solutions are the same as the solutions of $R\mathbf{X} = 0$). ■

With that we finally have:

***Corollary 2.38*** *A square matrix having either a left- or a right-inverse is invertible. That is, let $A \in M_n(\mathbb{F})$. If there exists an $L \in M_n(\mathbb{F})$ such that $LA = I_n$, or if there exists an $R \in M_n(\mathbb{F})$ such that $AR = I_n$, then $A$ is invertible.*

*Proof*: Suppose for example that $A$ has a left-inverse $L$. Let $\mathbf{x}$ be a solution to $A\mathbf{X} = 0$, then

$$\mathbf{x} = I_n\mathbf{x} = LA\mathbf{x} = L(A\mathbf{x}) = 0,$$

i.e., 0 is the unique solution to $A\mathbf{X} = 0$ implying by Theorem 2.37 that $A$ is invertible. On the other hand, if $R$ is a right-inverse of $A$, then $A$ is a left-inverse for $R$, hence $R$ is invertible, and $AR = I_n$ implies that $A$ is invertible as well. ■

***Corollary 2.39*** *A product of square matrices is invertible if and only if every matrix in this product is invertible.*

*Proof*: We will show it for a product of two matrices; the general case can be shown inductively. We already know that a product of invertible matrices is invertible—we will now show that if $AB$ is invertible then both $A$ and $B$ are invertible. Let $C$ be the inverse of $AB$, then

$$(AB)C = A(BC) = I,$$

i.e., $A$ has a right-inverse, and by Corollary 2.38 it is invertible. Likewise,

$$C(AB) = (CA)B = I,$$

i.e., $B$ has a left-inverse, and by Corollary 2.38 it is invertible. ■

As a final note, if $A \in \mathrm{GL}_n(\mathbb{F})$, then the linear system (whether homogeneous or not)

$$A\mathbf{X} = \mathbf{b}$$

has a unique solution,

$$\mathbf{x} = A^{-1}\mathbf{b}.$$

In this section we obtained an algorithm (using the Gauss-Jordan procedure) for calculating $A^{-1}$. Note however, that this chapter has a much wider scope, encompassing linear systems of arbitrary $m, n$, whether consistent or not.

### Exercises

**(easy) 2.55** Let $A$ be an $m \times m$ matrix. Prove that if $A$ is invertible and $AB = 0$ for some $m \times m$ matrix $B$, then $B = 0$.

**(intermediate) 2.56** For each of the two matrices

$$\begin{bmatrix} 2 & 5 & -1 \\ 4 & -1 & 2 \\ 6 & 4 & 1 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 1 & -1 & 2 \\ 3 & 2 & 4 \\ 0 & 1 & -2 \end{bmatrix}$$

find using elementary row-operations whether they are invertible and find their inverses if they are (this is quite tedious, but one has to do it at some point...).

**(intermediate) 2.57** Is the matrix

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

invertible? If it is, what is its inverse?

**(intermediate) 2.58** Let $A$ be a $2 \times 1$ matrix and let $B$ be a $1 \times 2$ matrix. Show that the $2 \times 2$ matrix $AB$ is not invertible.

**(intermediate) 2.59** The following matrices are over $\mathbb{R}$. Determine whether they are invertible, and if they are, find their inverses:

$$U_1 = \begin{bmatrix} 2 & 1 & 2 \\ 4 & 0 & 3 \\ 0 & 3 & 5 \end{bmatrix} \qquad U_2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad U_3 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$U_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \qquad U_5 = \begin{bmatrix} 2 & 3 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \end{bmatrix} \qquad U_6 = \begin{bmatrix} 1 & 3 & 4 \\ 2 & 4 & 0 \\ 3 & 1 & 1 \end{bmatrix}$$

**(intermediate) 2.60** Consider the matrix

$$A = \begin{bmatrix} 1 & 0 & 3 \\ 3/2 & 1/2 & 3 \\ -5 & 4 & -9 \end{bmatrix}.$$

If possible, express it as a product of elementary matrices. If not, explain why.

**(intermediate) 2.61** Let $A \in M_n(\mathbb{F})$ satisfy the equation

$$A^2 - A + I = 0.$$

Show that $A$ is invertible and express its inverse in terms of $A$.

**(intermediate) 2.62** Let $A \in M_n(\mathbb{F})$ satisfy the equation

$$A^3 - 2A + I = 0.$$

Show that $A$ is invertible and express its inverse in terms of $A$.

**(intermediate) 2.63** Show that if $A, B \in M_n(\mathbb{F})$ satisfy that $AB^2 - A$ is invertible, then $BA - A$ is invertible.

**(intermediate) 2.64** Let $A \in M_n(\mathbb{F})$, $B \in M_k(\mathbb{F})$ and $D \in M_{n\times k}(F)$. Consider the block matrix $C \in M_{n+k}(\mathbb{F})$ given by

$$C = \begin{bmatrix} A & D \\ & B \end{bmatrix}.$$

Show that if $A$ and $B$ are invertible, then so is $C$. What about the converse?

**(harder) 2.65** Show that if $A, B, A + B \in \mathrm{GL}_n(\mathbb{F})$, then

$$A^{-1} + B^{-1} \in \mathrm{GL}_n(\mathbb{F}).$$

**(harder) 2.66** Let $A$ be an $m \times m$ matrix. Prove that if $A$ is *not* invertible then there exists a non-zero $m \times m$ matrix $B$ such that $AB = 0$.

**(harder) 2.67** Let $A$ be an $m \times n$ matrix with $n < m$, and let $B$ be an $n \times m$ matrix. Show that $AB$ is not invertible. Hint: what can you say about the homogeneous system $B\mathbf{X} = 0$?

# 2.6 The structure of the set of solutions

## 2.6.1 The homogeneous case

Let $A \in M_{m\times n}(\mathbb{F})$. Consider the set $S_{[A|0]}$ of all solutions $\mathbf{x} \in M_{n\times 1}(\mathbb{F}) = \mathbb{F}^n_{\text{col}}$ to the homogeneous system

$$A\mathbf{X} = 0.$$

This set turns out to have interesting properties, which will play a central role throughout this course:

***Theorem 2.40*** *Let $A \in M_{m\times n}(\mathbb{F})$. Then,*

*(a) If $\mathbf{u}, \mathbf{v} \in S_{[A|0]}$, then $\mathbf{u} + \mathbf{v} \in S_{[A|0]}$.*

*(b) If $\mathbf{u} \in S_{[A|0]}$ and $\lambda \in \mathbb{F}$, then $\lambda\,\mathbf{u} \in S_{[A|0]}$.*

*(In other words, the set of solutions of a homogeneous system is closed under addition and under scalar multiplication.)*

*Proof*: For the first statement, if $\mathbf{u}, \mathbf{v} \in S_{[A|0]}$, then

$$A\mathbf{u} = 0 \qquad \text{and} \qquad A\mathbf{v} = 0,$$

from which follows from distributivity that

$$A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = 0,$$

namely $\mathbf{u} + \mathbf{v} \in S_{[A|0]}$. For the second statement, if $A\mathbf{u} = 0$, then

$$A(\lambda\mathbf{u}) = \lambda(A\mathbf{u}) = 0,$$

namely $\lambda u \in S_{[A|0]}$. Note that we used here the fact that for every $i = 1, \ldots, m$,

$$(A(\lambda\mathbf{u}))^i = \sum_{k=1}^{n} a^i_k(\lambda\mathbf{u})^k = \sum_{k=1}^{n} \lambda a^i_k u^k = \lambda \sum_{k=1}^{n} a^i_k u^k = (\lambda(A\mathbf{u}))^i.$$

■

**Example**: Consider the case of $m = 1$ and $n = 2$,

$$X^1 + X^2 = 0.$$

The set of solutions of this "system" of equations is

$$S_{[1,1|0]} = \left\{ \begin{bmatrix} t \\ -t \end{bmatrix} \ : \ t \in \mathbb{F} \right\}.$$

Take any two elements,

$$\begin{bmatrix} t \\ -t \end{bmatrix}, \begin{bmatrix} s \\ -s \end{bmatrix} \in S_{[1,1|0]},$$

their sum

$$\begin{bmatrix} t \\ -t \end{bmatrix} + \begin{bmatrix} s \\ -s \end{bmatrix} = \begin{bmatrix} t+s \\ -(t+s) \end{bmatrix}$$

is also an element of $S_{[1,1|0]}$. Likewise, for every $\lambda \in \mathbb{F}$,

$$\lambda \begin{bmatrix} t \\ -t \end{bmatrix} = \begin{bmatrix} \lambda t \\ -\lambda t \end{bmatrix}$$

is an element of $S_{[1,1|0]}$. ▲▲▲

### 2.6.2 The inhomogeneous case

Consider next an inhomogeneous system,

$$A\mathbf{X} = \mathbf{b},$$

where $A \in M_{m\times n}(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^m_{\text{col}}$. Do we get here the same phenomenon? Is it true that $\mathbf{u}, \mathbf{v} \in S_{[A|\mathbf{b}]}$ implies that $\mathbf{u} + \mathbf{v} \in S_{[A|\mathbf{b}]}$. Let's verify it. If $\mathbf{u}, \mathbf{v} \in S_{[A|\mathbf{b}]}$, then

$$A\mathbf{u} = \mathbf{b} \qquad \text{and} \qquad A\mathbf{v} = \mathbf{b},$$

and

$$A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{b} + \mathbf{b}$$

which differs from $\mathbf{b}$ unless $\mathbf{b} = 0$ (note that we don't write $\mathbf{b} + \mathbf{b} = 2\mathbf{b}$ as we are in a general field). Thus, unless the system is homogeneous, $\mathbf{u}+\mathbf{v} \notin S_{[A|\mathbf{b}]}$.

The following theorem shows that the set of solution of an inhomogeneous system has its own algebraic structure:

***Theorem 2.41*** *Let $A \in M_{m\times n}(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^m_{col}$. If $\mathbf{u} \in S_{[A|\mathbf{b}]}$ and $\mathbf{v} \in S_{[A|0]}$, then $\mathbf{u}+\mathbf{v} \in S_{[A|\mathbf{b}]}$.*

*Proof*: Let $\mathbf{u} \in S_{[A|\mathbf{b}]}$ and $\mathbf{v} \in S_{[A|0]}$, namely,

$$A\mathbf{u} = \mathbf{b} \qquad \text{and} \qquad A\mathbf{v} = 0.$$

Then,

$$A(\mathbf{u}+\mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{b} + 0 = \mathbf{b},$$

which means that $\mathbf{u}+\mathbf{v} \in S_{[A|\mathbf{b}]}$. ■

In fact, we can prove something even stronger.

***Theorem 2.42*** *Let $A \in M_{m\times n}(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^m_{col}$. Suppose that the inhomogeneous system is consistent, namely, that there exists $\mathbf{x} \in \mathbb{F}^n_{col}$ satisfying*

$$A\mathbf{x} = \mathbf{b}.$$

*Then,* every $\mathbf{u} \in S_{[A|\mathbf{b}]}$ *can be represented as*

$$\mathbf{u} = \mathbf{x} + \mathbf{v},$$

*for some $\mathbf{v} \in S_{[A|0]}$.*

*Proof*: Let $\mathbf{u} \in S_{[A|\mathbf{b}]}$, and write

$$\mathbf{u} = \mathbf{x} + \underbrace{(\mathbf{u}-\mathbf{x})}_{=\mathbf{v}}.$$

Now,

$$A\mathbf{v} = A(\mathbf{u}-\mathbf{x}) = A\mathbf{u} - A\mathbf{x} = \mathbf{b} - \mathbf{b} = 0,$$

i.e., $\mathbf{v} \in S_{[A|0]}$. ■

In other words, if an inhomogeneous system is consistent, every solution can be represented as the sum of one particular solution and a solution of the corresponding homogeneous system.

**Example**: Consider the inhomogeneous system with $m = 1$ and $n = 2$,

$$X^1 + X^2 = 5.$$

The set of solutions of this "system" of equations is

$$S_{[1,1|5]} = \left\{ \begin{bmatrix} t \\ 5 - t \end{bmatrix} \ : \ t \in \mathbb{F} \right\}.$$

Note that

$$\mathbf{x} = \begin{bmatrix} 0 \\ 5 \end{bmatrix}$$

is a particular solution of this system, and that the set of solutions can be written as

$$S_{[1,1|5]} = \left\{ \begin{bmatrix} 0 \\ 5 \end{bmatrix} + \begin{bmatrix} t \\ -t \end{bmatrix} \ : \ t \in \mathbb{F} \right\}.$$

That is, every solution can be represented as the sum of one particular solution and a solution of the homogeneous system. ▲▲▲

## 2.7 The geometry of solutions

### 2.7.1 Affine spaces

We end this chapter on linear systems of equations by presenting a geometric interpretation of the set of solutions of systems $A\mathbf{X} = \mathbf{b}$. To this end we introduce an algebraic construct called an **affine space** (**מרחב אפיני**) over a field $\mathbb{F}$. The introduction will be somewhat less formal than the standard of this course, because the goal here is mainly to develop some intuition.

An affine space over a field $\mathbb{F}$ encompasses two (non-empty) sets: a set of so-called **points** (**נקודות**) and a set of so-called **translations** (**הזזות**). To distinguish between the two, we denote the points by uppercase roman characters, e.g., $P, Q, \ldots$, and we denote the translations by lowercase roman characters, e.g., $\mathbf{u}, \mathbf{v}, \ldots$.

It is useful to think of the points as actual points (say on a plane) and of the translations as arrows on that same plane. Translations *act* on points by

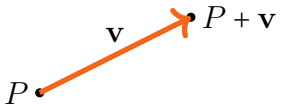
translating them into other points. We denote this action using the addition sign: a translation $\mathbf{v}$ acting on a point $P$ yields a point which we denote by

$$P + \mathbf{v}.$$

In other words there exists a function of the type

$$+ : \text{points} \times \text{translations} \to \text{points}.$$

This is the image one should have in mind:



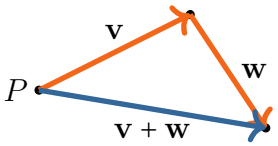

The rule is that for every two points $P, Q$ there exists a unique translation $\mathbf{v}$ such that $Q = P + \mathbf{v}$; we denote this unique translation by $Q - P$, which is sometimes also denoted by $\vec{PQ}$.

**Comments:**

(a) There is no meaning to adding two points! Thus far, the addition operation represents only the action of a translation on a point.

(b) An affine space does not come equipped with a special point, such as an origin.

Translations can be composed. One can act on a point $P$ by a translation $\mathbf{v}$ and then act on the resulting point by a translation $\mathbf{w}$, as depicted below:




In an affine space, an addition of translations is defined, satisfying the rule that $\mathbf{v} + \mathbf{w}$ is the translation equivalent to a translation by $\mathbf{v}$ followed by a translation by $\mathbf{w}$, that is,

$$P + (\mathbf{v} + \mathbf{w}) = (P + \mathbf{v}) + \mathbf{w}.$$

Note the difference between the types of addition on both sides of the equation. The addition on the left-hand side is a function

$$+ : \text{translations} \times \text{translations} \to \text{translations}.$$

The addition of translations is assumed to be associative and commutative. Also, there exists a zero translation, which we denote by 0, satisfying for every point $P$,

$$P + 0 = P.$$

This last point merits some elaboration. By assumption, there exists for a point $P$ a unique translation $\mathbf{v}$ satisfying

$$P + \mathbf{v} = P,$$

and there exists for a point $Q$ a unique translation $\mathbf{w}$ satisfying

$$Q + \mathbf{w} = Q,$$

The claim is that $\mathbf{v} = \mathbf{w}$, so that there exists a single translation which leaves all points unaffected. Why this? Because if $Q - P = \mathbf{u}$, i.e., $Q = P + \mathbf{u}$, then

$$Q + \mathbf{v} = (P + \mathbf{u}) + \mathbf{v} = P + (\mathbf{u} + \mathbf{v}) = P + (\mathbf{v} + \mathbf{u}) = (P + \mathbf{v}) + \mathbf{u} = P + \mathbf{u} = Q,$$

i.e., both $Q + \mathbf{w} = Q$ and $Q + \mathbf{v} = Q$, and by the uniqueness assumption, $\mathbf{v} = \mathbf{w}$.

Also, given a point $P$ and a translation $\mathbf{v}$, there exists a unique translation $\mathbf{w}$, such that

$$(P + \mathbf{v}) + \mathbf{w} = P,$$

i.e.,

$$P + (\mathbf{v} + \mathbf{w}) = P,$$

from which we deduce that $\mathbf{v} + \mathbf{w} = 0$, i.e., every translation has an additive inverse.

Thus far, the field $\mathbb{F}$ has played no role. An affine space is endowed with an additional operation, which is the scalar multiplication of a translation by a scalar (think of it as a *scaling* of the translation): for a translation $\mathbf{v}$ and a scalar $\lambda \in \mathbb{F}$, one forms a product $\lambda\mathbf{v}$, which is a translation. That is,

$$\cdot : \text{scalars} \times \text{translations} \to \text{translations}.$$

Scalar multiplication is associative, in the sense that

$$\alpha(\beta\mathbf{v}) = (\alpha\beta)\mathbf{v},$$

has a neutral element,

$$1_{\mathbb{F}} \cdot \mathbf{v} = \mathbf{v},$$

and is distributive both over scalar addition,

$$(\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta v$$

and over the addition of translations,

$$\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}.$$

### 2.7.2 The affine space $\mathcal{A}^n(\mathbb{F})$

Thus far, the discussion was completely general. We now consider a particular instance of an affine space. Let $n \in \mathbb{N}$ be any natural number. The affine space $\mathcal{A}^n(\mathbb{F})$ is defined as follows: the points belong to the set

$$\mathcal{A}^n(\mathbb{F}) = \left\{ \begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix} \ : \ p^1, \ldots, p^n \in \mathbb{F} \right\},$$

whereas the translation belong to the set,

$$V^n(\mathbb{F}) = \left\{ \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \ : \ v^1, \ldots, v^n \in \mathbb{F} \right\}.$$

Note that these two sets are essentially "the same", and we use different parentheses to distinguish between the two.

The action of a translation on a point is defined by

$$\begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix} + \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \begin{pmatrix} p^1 + v^1 \\ \vdots \\ p^n + v^n \end{pmatrix}.$$

For the operations on translations, we exploit the fact that we use a matrix notation so that addition and scalar multiplication have already been defined.

And now we connect this geometric construct to the set of solutions to linear system. Let $A \in M_{m\times n}(\mathbb{F})$. We interpret the solutions of the system $A\mathbf{X} = \mathbf{b}$ (which are $n$-tuples of field elements) as points in the affine space $\mathcal{A}^n(\mathbb{F})$. In contrast, we interpret the set of solutions of the homogeneous system $A\mathbf{X} = 0$ (which are also $n$-tuples of field elements) as the space of translations $V^n(\mathbb{F})$.

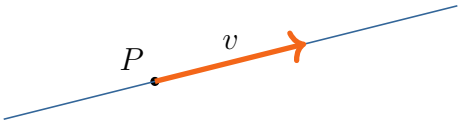
Theorem 2.42 can then be interpreted as follows. Suppose that the system $A\mathbf{X} = \mathbf{b}$ is consistent, i.e., it has at least one solution $P$ (a point in the affine space). Then, its set of solutions is all the points $Q$ obtained by translating $P$ by a solution of the homogeneous equation (which is indeed a translation).

### 2.7.3 Lines in affine spaces

Let $\mathcal{A}$ be the set of points in an affine space over $\mathbb{F}$ and let $V$ be the set of translations. A set of points $L \subset A$ is called a **line** (ישר), if there exists a point $P \in \mathcal{A}$ and a translation $0 \neq \mathbf{v} \in V$, such that

$$L = \{P + t\mathbf{v} \ : \ t \in \mathbb{F}\}.$$

That is, a line is a set of points obtained by translating a point $P \in \mathcal{A}$ by all translations which are multiples of a translation $\mathbf{v} \in V$.




***Proposition 2.43*** *Let $a, b \in \mathbb{F}$, which are not both zero and let $c \in \mathbb{F}$. Then, the set of solutions to the equation*

$$aX + bY = c$$

*is a line in the affine space $\mathcal{A}^2(\mathbb{F})$.*

*Proof*: We already have a technique for finding the space of solutions $S_{[a,b|c]}$. Suppose first that $a \neq 0_{\mathbb{F}}$. Then, the extended matrix $[a, b|c]$ is row-equivalent

to a matrix of the form $[1, d|e]$; the corresponding linear systems have the same solutions. The set of solutions is the set of points

$$S_{[1,d|e]} = \left\{ \begin{pmatrix} e - dt \\ t \end{pmatrix} \ : \ t \in \mathbb{F} \right\},$$

which we can rewrite as

$$S_{[1,d|e]} = \left\{ \begin{pmatrix} e \\ 0 \end{pmatrix} + t \begin{bmatrix} -d \\ 1 \end{bmatrix} \ : \ t \in \mathbb{F} \right\}.$$

If $a = 0$ and $b \neq 0$, then

$$S_{[0,b|c]} = \left\{ \begin{pmatrix} t \\ c/b \end{pmatrix} \ : \ t \in \mathbb{F} \right\},$$

which we can rewrite as

$$S_{[0,b|c]} = \left\{ \begin{pmatrix} 0 \\ c/b \end{pmatrix} + t \begin{bmatrix} 1 \\ 0 \end{bmatrix} \ : \ t \in \mathbb{F} \right\},$$

which is also a line. ■

In fact the converse is also true:

***Proposition 2.44*** *Let $L \subset \mathcal{A}^2(\mathbb{F})$ be a line. Then, there exist $a, b \in \mathbb{F}$, which are not both zero and a $c \in \mathbb{F}$, such that $L$ is the set of solutions to the linear equation*

$$aX + bY = c.$$

*Proof*: Let

$$L = \left\{ \begin{pmatrix} p^1 \\ p^2 \end{pmatrix} + t \begin{bmatrix} v^1 \\ v^2 \end{bmatrix} \ : \ t \in \mathbb{F} \right\}$$

be a line in $\mathcal{A}^2(\mathbb{F})$. Let $[x^1, x^2]^T \in L$. Then, there exists a $t \in \mathbb{F}$, such that

$$x^1 = p^1 + tv^1 \qquad \text{and} \qquad x^2 = p^2 + t\,v^2.$$

Since the translation is non-zero, either $v^1 \neq 0$ or $v^2 \neq 0$. If $v^1 \neq 0$, then

$$t = (x^1 - p^1)/v^1,$$

so that

$$x^2 = p^2 + v^2(x^1 - p^1)/v^1,$$

which we may rewrite as

$$v^2x^1 - v^1x^2 = v^2p^1 - v^1p^2.$$

That is, all points in $L$ are solution of the equation

$$v^2X^1 - v^1X^2 = v^2p^1 - v^1p^2.$$

We can also think of it differently: we are trying to solve a system of two equations in one unknown,

$$v^1t = x^1 - p^1$$
$$v^2t = x^2 - p^2.$$

The extended matrix is

$$\left[\begin{array}{c|c} v^1 & x^1 - p^1 \\ v^2 & x^2 - p^2 \end{array}\right].$$

Suppose that $v^1 \neq 0$. Then, the corresponding row-reduced echelon matrix is

$$\left[\begin{array}{c|c} 1 & (x^1 - p^1)/v^1 \\ 0 & (x^2 - p^2) - v^2(x^1 - p^1)/v^1 \end{array}\right].$$

This equation is consistent if and only if

$$(x^2 - p^2) - v^2(x^1 - p^1)/v^1 = 0,$$

which is the same as we obtained before. ■

### 2.7.4 Planes in affine spaces

Let $\mathcal{A}$ be the set of points in an affine space over $\mathbb{F}$ and let $V$ be the set of translations. A set of points $M \subset A$ is called a **plane** (**מישור**), if there exists a point $P \in \mathcal{A}$ and two translation $0 \neq \mathbf{u}, \mathbf{v} \in V$, such that none is a multiple of the other, such that

$$M = \{P + s\mathbf{u} + t\mathbf{v} \ : \ s, t \in \mathbb{F}\}.$$

That is, a plane is a set of points obtained by translating a point $P \in \mathcal{A}$ by all translations which are linear combinations of two translation $\mathbf{u}, \mathbf{v} \in V$.

***Proposition 2.45*** *Let $a, b, c \in \mathbb{F}$, which are not all zero and let $d \in \mathbb{F}$. Then, the set of solutions to the equation*

$$aX + bY + cZ = d$$

*is a plane in the affine space $\mathcal{A}^3(\mathbb{F})$.*

*Proof*: We leave this as an exercise. Separate the cases $a \neq 0$, $a = 0$ by $b \neq 0$, and $a = b = 0$. ■

And conversely,

***Proposition 2.46*** *Let $M \subset \mathcal{A}^3(\mathbb{F})$ be a plane. Then, there exist $a, b, c \in \mathbb{F}$, which are not all zero and a $d \in \mathbb{F}$, such that $M$ is the set of solutions to the linear equation*

$$aX + bY + cZ = d.$$