Abstract Linear Algebra

Contents

1 Linear Systems

A **linear equation** in the variables $x_1, x_2, \ldots, x_n$ is an equation of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, where b and a coefficients are complex numbers.

A **linear system** is a collection of one or more linear equations involving the same variables.

A **solution** of the linear system is a list of numbers that satisfy each of the equations in the linear system. The **solution set** of the linear system is the set of all possible solutions. We can solve the linear system algebraically (finding solutions for the equations) or geometrically (such as, do these hyperplanes intersect).

A linear system has:

1. Exactly one solution
2. No solution
3. Infinitely many solutions

A linear system is **inconsistent** if it has no solution. Otherwise, it is **consistent**.

Given $m \geq 1$ equations in $n \geq 1$ variables:

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots + a_{1n}x_n & = & b_1 \\ \vdots & & & & & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots + a_{mn}x_n & = & b_m \end{array}$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \qquad \left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right]$$

Coefficient matrix
Size: $m \times n$

Augmented matrix
Size: $m \times (n+1)$

Elementary Row Operations (does not change the solution set):

1. **Interchange**: Interchange two rows.
2. **Scaling**: Multiply all entries in a row by a non-zero constant.
3. **Replacement**: Replace one row by the sum of itself and a multiple of another row.

A matrix is in **Row-Echelon Form (REF)** if following properties hold:

1. All non-zero rows are above all zero rows (every entry is zero).
2. The leading entry (first nonzero entry) of each row is to the right of the leading entry of the row above.
3. All entries in a column below a leading entry are zero.

Furthermore, a matrix in REF is also in **Reduced Row-Echelon Form (RREF)** if following properties hold:

1. The leading entry in each non-zero row is 1.

2. Each leading 1 is the only non-zero entry in its column.

Any non-zero matrix can be converted to infinite different REFs (with elementary row operations) and one unique RREF.

A linear system:

1. has no solution if RREF has a leading entry in the last column
2. has a unique solution if RREF has a leading entry in every column except the last column
3. has infinite solutions if the last column and at least one more column in RREF do not have leading entries.

Pivot: the leading entry of a row in REF or RREF.

Pivot position: the position of a leading entry in REF or RREF.

Pivot column: a column that contains a pivot position.

Gaussian Elimination:

1. Begin with the leftmost non-zero column. In this pivot column, we choose a non-zero entry as pivot and swap rows to move it to the top.
2. Use row replacement operations to create zeros in all positions below the pivot.
3. Cover the row containing the pivot position and the pivot column along with all rows above it and all columns left to it. Apply step 1-2 to the sub matrix that remains. Repeat until there are no more non-zero rows to modify.
4. Now we have REF. If there is a pivot in the rightmost column, the system is inconsistent and we stop.
5. Make the rightmost pivot 1 by scaling, and create zeros above it with replacement. Repeat for the next rightmost pivot until finishing all rows. Now we have RREF.
6. Let variables corresponding to columns without pivots be free variables (parameters), and parameterize other variables with them. The dimension of a solution set is the number of its free variables.

2 Fields

A field $(\mathbb{F}, 0, 1, +, \cdot)$ is a set $\mathbb{F}$ with two unique distinct elements $0, 1 \in \mathbb{F}$ and two operations

$$\begin{cases} + : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} \\ \cdot \ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} \end{cases}$$

satisfying the following properties:

- *Commutativity:* $\forall\ a, b \in \mathbb{F}$,
$$a + b = b + a, \qquad a \cdot b = b \cdot a.$$
- *Associativity:* $\forall\ a, b, c \in \mathbb{F}$,
$$(a + b) + c = a + (b + c), \qquad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$
- *Identities:* $\forall\ a \in \mathbb{F}$,
$$a + 0 = a \qquad \text{and} \qquad a \cdot 1 = a.$$
- *Additive inverse:* $\forall\ a \in \mathbb{F}$, $\exists\ b \in \mathbb{F}$ s.t.
$$a + b = 0.$$
- *Multiplicative inverse:* $\forall\ a \in \mathbb{F}$ with $a \neq 0$, $\exists\ b \in \mathbb{F}$ s.t.
$$a \cdot b = 1.$$
- *Distributive property:* $\forall\ a, b, c \in \mathbb{F}$,
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

To prove the uniqueness of 0 and 1: Suppose there exists two distinct 0s, namely $0 \neq 0', 0 + 0' = 0 = 0'$, which forms contradiction. Suppose there exists two distinct 1s, namely $1 \neq 1', 1 \cdot 1' = 1 = 1'$, which forms contradiction.

Examples:

1. $\mathbb{R}$ with standard operations is a field.
2. $\mathbb{Q}$: numbers $\dfrac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$. Here
$$0_{\mathbb{Q}} = \frac{0}{1}, \qquad 1_{\mathbb{Q}} = \frac{1}{1},$$
with standard operations is a field.
3. Irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ with standard operations is *not* a field:
   - Take $a = \sqrt{2}$ and $b = 1 - \sqrt{2}$. Then
$$a + b = \sqrt{2} + 1 - \sqrt{2} = 1 \in \mathbb{Q} \qquad \left(= \tfrac{1}{1}\right).$$
   - $\nexists\, 0$.

3 Complex Numbers

$$\mathbb{C} = \{\, a + bi \;:\; a, b \in \mathbb{R} \,\},$$

where a is the real part and b is the imaginary part.

Convention: $i^2 = -1$. Then

$$0 \equiv 0 + 0i, \qquad 1 \equiv 1 + 0i.$$

Addition and multiplication ($\forall\ a, b, c, d \in \mathbb{R}$):

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$\begin{aligned}(a + bi)(c + di) &= ac + adi + cbi + bd\, i^2 \\ &= (ac - bd) + (ad + bc)\, i.\end{aligned}$$

With these operations, the complex numbers form a field.

Additive inverse of $a + bi$

Let $c + di$ be an additive inverse with $c, d \in \mathbb{R}$, s.t.

$$\begin{aligned}(c + di) + (a + bi) &= 0 + 0i \\ (c + a) + (d + b)\, i &= 0 + 0i.\end{aligned}$$

Hence

$$\begin{aligned} c + a &= 0 & \qquad d + b &= 0 \\ c &= -a & \qquad d &= -b \end{aligned}$$

so that

$$c + di = -a - bi.$$

Multiplicative inverse of $a + bi \neq 0 + 0i$

Here $a \neq 0$ or $b \neq 0$. Let $c + di$ be the multiplicative inverse of $a + bi$, with $c, d \in \mathbb{R}$:

$$\begin{aligned}(a + bi)\,(c + di) &= 1 + 0i \\ (a + bi)(a - bi)\,(c + di) &= (a - bi) \\ (a^2 + b^2)\,(c + di) &= (a - bi) \\ \beta &= \frac{a - bi}{a^2 + b^2} \\ &= \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i.\end{aligned}$$

Since $a \neq 0$ or $b \neq 0$, $a^2 + b^2 \neq 0$.

4 $\mathbb{F}^n$

A list allows duplications and may be written as a row or as a column:

$$(x_1, \ldots, x_n), \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

$\mathbb{F}^n$ is the set of all lists of length n of elements of $\mathbb{F}$:

$$\mathbb{F}^n = \{\, (x_1, \ldots, x_n) \ : \ x_k \in \mathbb{F} \text{ for } k \in \{1, \ldots, n\}\,\}.$$

Addition, $\forall\ x_i, y_i \in \mathbb{F}$:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1,\ \ldots,\ x_n + y_n).$$

Scalar multiplication, $\forall \lambda \in \mathbb{F}, x_i \in \mathbb{F}$:

$$\lambda\, (x_1, \ldots, x_n) = (\lambda \cdot x_1,\ \ldots,\ \lambda \cdot x_n)$$

Is $\mathbb{F}^n$ a field under piecewise multiplication:

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1,\ \ldots,\ x_n y_n),$$

with piecewise addition above?

For $n = 1$ we get $\mathbb{F}^n = \mathbb{F}$. ✓

For $n > 1$, take $\mathbb{F} = \mathbb{R}$, so $\mathbb{F}^2 = \mathbb{R}^2$. Then

$$0 \equiv (0, 0), \qquad 1 \equiv (1, 1)$$

I claim that $\mathbb{R}^2$ is not a field under piecewise operations.

Proof. Assume $\mathbb{R}^2$ is a field. Choose $e_1 = (a, 0)$ with $a \neq 0$. Assume $e_2 = (c, d)$ is its multiplicative inverse):

$$\begin{aligned} e_1 e_2 &= (1, 1) \\ (a, 0) \cdot (c, d) &= (1, 1) \\ (a \cdot c,\ 0 \cdot d) &= (1, 1) \\ 0 \cdot d &= 1. \end{aligned}$$

But $d \in \mathbb{R}$ gives $0 \cdot d = 0$, so there is a contradiction since $0 \neq 1$. □

We can use the same proof structure for larger n. This goes the same for other $\mathbb{F}$. Since 0 is unique in a field, and $\forall a \in \mathbb{F}, 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, so $0 \cdot a = 0$. Since $0 \neq 1, 0 \cdot a \neq 1$. Hence any $\mathbb{F}^n$ for $n > 1$ is not a field under piecewise addition and multiplication operations.

5 Vector Spaces

A vector space $(V, +, \cdot)$ over a field $\mathbb{F}$ is a set V with a vector addition

$$+ : V \times V \longrightarrow V$$

and a scalar multiplication

$$\cdot\ : \mathbb{F} \times V \longrightarrow V,$$

satisfying the following properties:

- *Commutativity:* $\forall\ u_1, u_2 \in V$,
$$u_1 + u_2 = u_2 + u_1.$$
- *Associativity:* $\forall\ u_1, u_2, u_3 \in V, a, b \in \mathbb{F}$
$$(u_1 + u_2) + u_3 = u_1 + (u_2 + u_3),$$
$$(a \cdot b) \cdot u_1 = a \cdot (b \cdot u_1),$$
where $a \cdot b$ is multiplication in $\mathbb{F}$.
- *Additive identity:* $\exists 0_V \in V$ s.t. $\forall u \in V$,
$$u + 0_V = u.$$
- *Additive inverse:* $\forall u \in V$, $\exists w \in V$ such that
$$u + w = 0_V.$$
- *Multiplicative identity:* $\forall u \in V$,
$$1 \cdot u = u, \qquad 1 \in \mathbb{F}.$$
- *Distributive property:* $\forall a, b \in \mathbb{F}, u_1, u_2 \in V$,
$$a \cdot (u_1 + u_2) = a \cdot u_1 + a \cdot u_2,$$
$$(a + b) \cdot u_1 = a \cdot u_1 + b \cdot u_1,$$
where $a + b$ is addition in $\mathbb{F}$.

Examples:

1. $V = \{0\}$ — the smallest vector space.
2. $\mathbb{R}^n$ over $\mathbb{R}$; more generally $\mathbb{F}^n$ is a vector space over $\mathbb{F}$.
3. Polynomials of degree at most d with coefficients in $\mathbb{F}$:
$$P_d(\mathbb{F}) = \{\, a_0 + a_1 x + \cdots + a_d x^d \ :\ a_i \in \mathbb{F},\ i \in \{0, \ldots, d\} \,\},$$
with standard addition:
$$p_1 = a_0 + a_1 x + a_2 x^2, \qquad p_2 = b_0 + b_1 x + b_2 x^2,$$
$$p_1 + p_2 = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2,$$
and standard scalar multiplication with $\lambda \in \mathbb{F}$,
$$\lambda\, p_1 = \lambda a_0 + \lambda a_1 x + \lambda a_2 x^2.$$

4. The set of $m \times n$ matrices M (m rows, n columns), where addition and scalar multiplication are componentwise.

Properties:

1. A vector space has a unique 0_V.
2. $\forall u \in V$ has a unique additive inverse, denoted by $(-u)$.
3. $\forall u \in V, \quad 0 \cdot u = 0_V$.
4. $\forall a \in \mathbb{F}, \quad a \cdot 0_V = 0_V$.
5. Let (-1) denote the additive inverse of $1 \in \mathbb{F}$. Then $\forall u \in V$,

$$(-1) \cdot u = (-u).$$

Proof:

(1) Let 0_V and $0'_V$ both be additive identities. $\forall u \in V$,

$$u + 0_V = u \qquad \text{and} \qquad u + 0'_V = u,$$

and furthermore, by commutativity,

$$0_V + u = u, \qquad 0'_V + u = u. \tag{$\circledast$}$$

Hence,

$$0'_V + 0_V = 0'_V. \tag{1}$$
$$0'_V + 0_V = 0_V. \tag{2}$$

which gives $0'_V = 0_V$. Therefore it is unique.

(2) Let $u \in V$, and suppose $w, w' \in V$ are both additive inverses of u:

$$u + w = 0_V \quad (**), \qquad u + w' = 0_V \quad (\circledast).$$

Then

$$\begin{aligned}
w &= w + 0_V && \text{(additive identity)}\\
&= w + (u + w') && \text{(by } \circledast\text{)}\\
&= (w + u) + w' && \text{(associativity)}\\
&= 0_V + w' && (**\ \text{ and commutativity})\\
&= w' && \text{(additive identity).}
\end{aligned}$$

So the additive inverse is unique, and we call $w = w' = (-u)$.

(3) $\forall u \in V$,

$$\begin{aligned}
0 \cdot u &= (0 + 0) \cdot u && (0 \in \mathbb{F},\ 0 + 0 = 0)\\
0 \cdot u &= 0 \cdot u + 0 \cdot u && \text{(distributive property).}
\end{aligned}$$

Since $0 \cdot u \in V$, it has an additive inverse $(-0 \cdot u)$. Adding it to both sides,

$$\begin{aligned}
\underbrace{0 \cdot u + (-0 \cdot u)}_{0_V} &= 0 \cdot u + \underbrace{0 \cdot u + (-0 \cdot u)}_{0_V} \\
0_V &= 0 \cdot u + 0_V \\
0_V &= 0 \cdot u
\end{aligned}$$

(4) For $a \in \mathbb{F}$ and $0_V \in V$,

$$\begin{aligned}
a \cdot 0_V &= a \cdot (0_V + 0_V) && \text{(additive identity)} \\
a \cdot 0_V &= a \cdot 0_V + a \cdot 0_V && \text{(distributive property).}
\end{aligned}$$

Since $a \cdot 0_V \in V$, it has an additive inverse $(-a \cdot 0_V)$. Adding it to both sides,

$$\begin{aligned}
\underbrace{a \cdot 0_V + (-a \cdot 0_V)}_{0_V} &= a \cdot 0_V + \underbrace{a \cdot 0_V + (-a \cdot 0_V)}_{0_V} \\
0_V &= a \cdot 0_V + 0_V \\
0_V &= a \cdot 0_V
\end{aligned}$$

(5) $\forall u \in V$:

$$\begin{aligned}
u + (-1) \cdot u &= 1 \cdot u + (-1) \cdot u \\
&= \big(1 + (-1)\big) \cdot u \\
&= 0 \cdot u && \big(1 + (-1) = 0 \text{ since } (-1) \text{ is the additive inverse of } 1\big) \\
&= 0_V.
\end{aligned}$$

Adding $(-u)$ to both sides,

$$\begin{aligned}
u + (-u) + (-1) \cdot u &= 0_V + (-u) \\
0_V + (-1) \cdot u &= (-u) && \big(u + (-u) = 0_V \text{ since } (-u) \text{ is the additive inverse of } u\big) \\
(-1) \cdot u &= (-u)
\end{aligned}$$

6 Subspaces

A subset $U \subseteq V$ of a vector space $[(V, +, \cdot\,)$ over $\mathbb{F}]$ is called a *subspace* (denoted by $U \leq V$), if $(U, +, \cdot\,)$ over $\mathbb{F}$ is a vector space where $+$ and $\cdot$ are the same operations as in V restricted to the subset $U \subseteq V$.

Example: With

$$\mathbb{F}^3 = \{\,(x_1, x_2, x_3) \;:\; x_i \in \mathbb{F}\,\}, \qquad U = \{\,(x_1, x_2, 0) \;:\; x_1, x_2 \in \mathbb{F}\,\},$$

we have $U \subseteq \mathbb{F}^3$ and in fact $U \leq \mathbb{F}^3$.

Sufficient Conditions for a subspace: Let $U \subseteq V$. Then $U \leq V$ (U is a subspace of V) iff

(a) $0_V \in U$ (the set is non-empty, and the additive identity is in the subset);

(b) U is closed under addition: $u_1, u_2 \in U \implies u_1 + u_2 \in U$;

(c) U is closed under scalar multiplication: $a \in \mathbb{F}$ and $u_1 \in U \implies au_1 \in U$.

Proof. ($\Longrightarrow$) Assume $U \leq V$. Then U is also a vector space, so:

- $u_1 \in U$, $a \in \mathbb{F} \implies au_1 \in U$, i.e. U is closed under scalar multiplication;
- $u_1, u_2 \in U \implies u_1 + u_2 \in U$, i.e. U is closed under addition $\quad (\circledast)$
- $u_1 \in U \implies (-u_1) \in U$, the additive inverse of u_1.

By $(\circledast)$, U is closed under addition, so

$$u_1 + (-u_1) \in U,$$

and since $u_1 + (-u_1) = 0_V$ in V, and U preserves the same operations, this gives $0_V \in U$.

($\Longleftarrow$) Suppose (a), (b), (c) hold, and we also have $U \subseteq V$.

- All properties except the additive inverse are automatically satisfied, since they hold for the larger space V (V is a vector space).
- Since $1 \in \mathbb{F}$, we have $(-1) \in \mathbb{F}$. For $u_1 \in U$, we know that U is closed under scalar multiplication, so

  $$(-1) \cdot u_1 \in U,$$

  and also $(-1) \cdot u_1 \in V$. By the properties of a vector space,

  $$(-1)u_1 = (-u_1),$$

  and $(-u_1)$ is the additive inverse of u_1. Hence $(-u_1) \in U$.

This completes the remaining criterion for U to be a vector space.

$\square$

Sum of subspaces: Let V be a vector space and $U_1, \ldots, U_m \leq V$. Then we define their sum as

$$U_1 + \cdots + U_m \;=\; \sum_{i=1}^{m} U_i \;:=\; \{\,\tilde{u}_1 + \cdots + \tilde{u}_m \;:\; \tilde{u}_i \in U_i \text{ for } 1 \leq i \leq m\,\}.$$

Example. Let

$$U = \{\,(x, 0, 0) : x \in \mathbb{F}\,\}, \quad W = \{\,(0, y, 0) : y \in \mathbb{F}\,\}, \quad Z = \{\,(0, 0, \tilde{z}) : \tilde{z} \in \mathbb{F}\,\}.$$

Then $U, W, Z \leq \mathbb{F}^3$, and

$$U + W = \{ (x, y, 0) : x, y \in \mathbb{F} \},$$
$$U + W + Z = \{ (x, y, \tilde{z}) : x, y, \tilde{z} \in \mathbb{F} \} = \mathbb{F}^3.$$

Proposition: Let $U_i \leq V$ for $1 \leq i \leq m$. Then

$$\sum_{i=1}^{m} U_i \leq V,$$

and it is the smallest subspace of V that contains all the U_i as subspaces.

Proof. First verify that $\sum_{i=1}^{m} U_i \subseteq V$. Let $\tilde{u}_1 + \cdots + \tilde{u}_m \in \sum_{i=1}^{m} U_i$ be arbitrary, where $\tilde{u}_i \in U_i$ for $1 \leq i \leq m$. Since $U_i \leq V$, we have $U_i \subseteq V$, so $\tilde{u}_i \in V$ for every i. As V is a vector space, it is closed under addition, hence

$$\tilde{u}_1 + \cdots + \tilde{u}_m \in V.$$

Therefore

$$\sum_{i=1}^{m} U_i \subseteq V.$$

(a) Note that $0 \in U_i$ for all i (the U_i are subspaces). Then

$$0 = \underbrace{0}_{\in U_1} + 0 + \cdots + \underbrace{0}_{\in U_m} \in \sum_{i=1}^{m} U_i.$$

(b) Let $W, Z \in \sum_{i=1}^{m} U_i$, say

$$W = w_1 + \cdots + w_m \quad \text{where } w_i \in U_i,$$
$$Z = z_1 + \cdots + z_m \quad \text{where } z_i \in U_i.$$

Then

$$W + Z = (w_1 + z_1) + \cdots + (w_m + z_m).$$

Since $w_i, z_i \in U_i$ and U_i is a vector space, $w_i + z_i \in U_i$. Hence $W + Z \in \sum_{i=1}^{m} U_i$, so the sum is closed under addition.

(c) Let $a \in \mathbb{F}$ and, with the same $W \in \sum_{i=1}^{m} U_i$,

$$a \cdot W = a \cdot w_1 + \cdots + a \cdot w_m.$$

Since $w_i \in U_i$ and U_i is a vector space, $a \cdot w_i \in U_i$. Hence $a \cdot W \in \sum_{i=1}^{m} U_i$, so the sum is closed under scalar multiplication.

Therefore, by the conditions for a subspace,

$$\sum_{i=1}^{m} U_i \leq V.$$

We want to show $U_i \subseteq \sum_{i=1}^{m} U_i$. Let $\tilde{u}_i \in U_i$. Then

$$\tilde{u}_i = 0 + \cdots + 0 + \tilde{u}_i + 0 + \cdots + 0,$$

with $\tilde{u}_i$ in the i-th position and $0 \in U_j$ for each $j \neq i$. Hence

$$\tilde{u}_i \in \sum_{i=1}^{m} U_i, \qquad \text{so} \qquad U_i \subseteq \sum_{i=1}^{m} U_i.$$

Finally, we show minimality. Let $X \leq V$ be any subspace with $U_i \subseteq X$ for all i, and let $\tilde{u}_1 + \cdots + \tilde{u}_m$ be an arbitrary element of $\sum_{i=1}^m U_i$, where $\tilde{u}_i \in U_i$. Then $\tilde{u}_i \in X$ for every i, and since X is closed under addition,

$$\tilde{u}_1 + \cdots + \tilde{u}_m \in X.$$

Hence $\sum_{i=1}^m U_i \subseteq X$, so $\sum_{i=1}^m U_i$ is the smallest subspace of V containing every U_i. $\square$