LECTURE 7

Subspaces of \mathbb{R}^n

1. Subspaces

DEFINITION 7.1. A subset W of \mathbb{R}^n is said to be closed under vector addition if for all $\mathbf{u}, \mathbf{v} \in W$, $\mathbf{u} + \mathbf{v}$ is also in W. If $r\mathbf{v}$ is in W for all vectors $\mathbf{v} \in W$ and all scalars $r \in \mathbb{R}$, then we say that W is closed under scalar multiplication. A non-empty subset W of \mathbb{R}^n that is closed under both vector addition and scalar multiplication is called a subspace of \mathbb{R}^n .

EXAMPLE 7.2. Let $\mathbf{u} = (1,0)$ and $\mathbf{v} = (0,2)$ be vectors in \mathbb{R}^2 . We can construct a subset that closed under vector addition as follows.

$$W_0 = \{ \mathbf{w} \in \mathbb{R}^n \mid \mathbf{w} = j\mathbf{u} + k\mathbf{v} \quad ; \quad j,k \text{ positive integers} \}$$

To see that this set is closed under vector addition, let $\mathbf{w}, \mathbf{w}' \in W_0$. Then

$$\mathbf{w} = j\mathbf{u} + k\mathbf{v}$$
$$\mathbf{w}' = j'\mathbf{u} + k'\mathbf{v}$$

for some positive integers j, k, j', and k'. But then there are positive integers j, k, j' and k' such that

$$\mathbf{w} + \mathbf{w}' = (j\mathbf{u} + k\mathbf{v}) + (j'\mathbf{u} + k'\mathbf{v}) = (j+j')\mathbf{u} + (k+k')\mathbf{v} \in \mathbf{W}$$

because both (j + j') and (k + k') are positive integers if j, k, j', and k' are positive integers.

The set W_0 is not a subspace, however; because it is not closed under scalar multiplication. To see this, note that the vector

$$\frac{1}{2}\mathbf{u} = \left(\frac{1}{2}, 0\right)$$

can not be represented as sum of \mathbf{u} and \mathbf{v} with positive integer coefficients.

EXAMPLE 7.3. The preceding example, however, does provide a clue as to one way to constructing a subspace. Let $\mathbf{u} = (1,0)$ and $\mathbf{v} = (0,2)$ be vectors in \mathbb{R}^2 . Consider the set

$$W = \{ \mathbf{w} \in \mathbb{R}^n \mid \mathbf{w} = j\mathbf{u} + k\mathbf{v} \quad ; \quad j,k \in \mathbb{R} \}$$

This is closed under vector addition because if $\mathbf{w}, \mathbf{w}' \in W$, then there are real numbers r, s, r' and s' such that

$$\mathbf{w} = r\mathbf{u} + s\mathbf{v}$$
$$\mathbf{w}' = r'\mathbf{u} + s'\mathbf{v}$$

But then

$$\mathbf{w} + \mathbf{w}' = (r + r') \mathbf{u} + (s + s') \mathbf{v} \in W$$

since $(r + r') \in \mathbb{R}$ and $(s + s') \in \mathbb{R}$. And, for any real number t

$$t\mathbf{w} = (tr)\mathbf{u} + (ts)\mathbf{v} \in W$$

since $(tr) \in \mathbb{R}$ and $(ts) \in \mathbb{R}$.

The following theorem generalizes this last example.

THEOREM 7.4. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a set of vectors in \mathbb{R}^n . Then the span of $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is a subspace of \mathbb{R}^n .

Proof. Recall that the span of a set of vector is the set of all possible linear combinations of those vectors. Set

$$W = span\left(\mathbf{v}_{1}, \dots, \mathbf{v}_{k}\right) \equiv \left\{\mathbf{w} \in \mathbb{R}^{n} \mid \mathbf{w} = c_{1}\mathbf{v}_{1} + c_{2}\mathbf{v}_{2} + \dots + c_{k}\mathbf{v}_{k} \quad ; \quad c_{1}, c_{2}, \dots, c_{k} \in \mathbb{R}\right\}$$

Then for any vectors $\mathbf{w}, \mathbf{w}' \in W$ we have

$$\mathbf{w} = c_1 \mathbf{v}_1 + c_2 \mathbf{v}_2 + \dots + c_k \mathbf{v}_k$$
$$\mathbf{w}' = c'_1 \mathbf{v}_1 + c'_2 \mathbf{v}_2 + \dots + c'_k \mathbf{v}_k$$

for some choice of real numbers c_1, \ldots, c_k and c'_1, \ldots, c'_k . But then

$$\mathbf{w} + \mathbf{w}' = (c_1 + c_1') \mathbf{v}_1 + (c_2 + c_2') \mathbf{v}_2 + \dots + (c_k + c_k') \mathbf{v}_k \in W$$

and if t is any real number

$$t\mathbf{w} = (tc_1)\mathbf{v}_1 + (tc_2)\mathbf{v}_2 + \dots + (tc_k)\mathbf{v}_k \in W$$

REMARK 7.5. We shall often refer to the span of a set $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ of vectors in \mathbb{R}^n as the subspace generated by $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$.

2. Solutions of Homogeneous Systems

We now come to another fundamental way of realizing a subspace of \mathbb{R}^n .

DEFINITION 7.6. A linear system of the form Ax = 0 is called homogeneous.

A homogeneous linear system is always solvable since $\mathbf{x} = \mathbf{0}$ is always a solution. As such, this solution is not very interesting; we call it the **trivial solution**. A homogeneous linear system may possess other **non-trivial** solutions (i.e. solutions $\mathbf{x} \neq \mathbf{0}$), this is where we shall focus our attention today.

LEMMA 7.7. Suppose \mathbf{x}_1 and \mathbf{x}_2 are solutions of a homogeneous system $\mathbf{A}\mathbf{x} = \mathbf{0}$. Then so is any linear combination $r\mathbf{x}_1 + s\mathbf{x}_2$ of \mathbf{x}_1 and \mathbf{x}_2 .

Proof. Since \mathbf{x}_1 and \mathbf{x}_2 are solution of $\mathbf{A}\mathbf{x} = \mathbf{0}$ we have

$$Ax_1 = 0 = Ax_2$$

But then

$$\mathbf{A} (r\mathbf{x}_1 + s\mathbf{x}_2) = \mathbf{A}(r\mathbf{x}_1) + \mathbf{A}(s\mathbf{x}_2)$$
$$= r (\mathbf{A}\mathbf{x}_1) + s (\mathbf{A}\mathbf{x}_2)$$
$$= r\mathbf{0} + s\mathbf{0}$$
$$= \mathbf{0}$$

so $r\mathbf{x}_1 + s\mathbf{x}_2$ is also a solution.

THEOREM 7.8. The solution space of a homogeneous linear system is a subspace of \mathbb{R}^n .

Proof. The preceding lemma demonstrates that the solution space of a homogeneous linear system is closed under both vector addition (take r = 1 and s = 1 in the proof of the preceding lemma) and scalar multiplication (let r be any real number and take s = 0, in the proof of the lemma). Therefore, it is a subspace of \mathbb{R}^n .

3. Subspaces Associated with Matrices

DEFINITION 7.9. The row space of an $m \times n$ matrix **A** is the span of row vectors of **A**.

Since the row vectors of an $m \times n$ matrix are *n*-dimensional vectors, the row space of an $m \times n$ matrix is a subspace of \mathbb{R}^n .

DEFINITION 7.10. The column space of an $m \times n$ matrix **A** is the span of column vectors of **A**.

Since the column vectors of an $m \times n$ matrix are *m*-dimensional vectors, the column space of an $m \times n$ matrix is a subspace of \mathbb{R}^m .

DEFINITION 7.11. The null space of an $m \times n$ matrix **A** is the solution set of homogeneous linear system $\mathbf{Ax} = \mathbf{0}$.

By the theorem of the proceeding section, the null space of an $m \times n$ matrix A will be a subspace of \mathbb{R}^n .

Consider now a non-homogeneous linear system

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

The left hand side of such an equation is

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \cdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix}$$
$$= x_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + x_2 \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots x_n \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix}$$

The final expression on the right hand side is evidently a linear combination of the column vectors of \mathbf{A} . The consistency of the equation $\mathbf{A}\mathbf{x} = \mathbf{b}$ then requires the column vector \mathbf{b} to also lie within the span of the column vectors of \mathbf{A} . Thus we have

THEOREM 7.12. A linear system Ax = b is consistent if and only if b lies in the column space of A.

4. Bases

Consider the subspace generated by the following three vectors in \mathbb{R}^3 :

$$\mathbf{v}_1 = \begin{bmatrix} 1\\0\\1 \end{bmatrix} \quad , \quad \mathbf{v}_2 = \begin{bmatrix} 1\\1\\0 \end{bmatrix} \quad , \quad \mathbf{v}_3 = \begin{bmatrix} 0\\-1\\1 \end{bmatrix}$$

It turns out that this is the same as the subspace generated from just v_1 and v_2 . To see this note that

$$\mathbf{v}_3 = \begin{bmatrix} 0\\1\\-1 \end{bmatrix} = \begin{bmatrix} 1\\0\\1 \end{bmatrix} - \begin{bmatrix} 1\\1\\0 \end{bmatrix} = \mathbf{v}_1 + (-1)\mathbf{v}_2$$

But any vector \mathbf{w} in $span(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is expressible in the form

$$\mathbf{w} = c_1 \mathbf{v}_1 + c_2 \mathbf{v}_2 + c_3 \mathbf{v}_3$$

= $c_1 \mathbf{v}_1 + c_2 \mathbf{v}_2 + c_3 (\mathbf{v}_1 - \mathbf{v}_2)$
= $(c_1 + c_3) \mathbf{v}_1 + (c_2 - c_3) \mathbf{v}_2$
 $\in span(\mathbf{v}_1, \mathbf{v}_2)$

For reasons of efficiency alone, it is natural to try to find the minimum number of vectors needed to specify every vector in a subspace W. Such a set will be called a **basis** for W.

There is also another reason to be interested in basis vectors. Consider the vector

$$\mathbf{w} = \begin{bmatrix} 2\\1\\1 \end{bmatrix}$$

In terms of the vectors \mathbf{v}_1 , \mathbf{v}_2 , and \mathbf{v}_3 , we can write this as either

$$\mathbf{w} = 3\mathbf{v}_1 - \mathbf{v}_2 - 2\mathbf{v}_3$$

or

$$\mathbf{w} = -2\mathbf{v}_1 + 4\mathbf{v}_2 + 3\mathbf{v}_3$$

or even

$$\mathbf{w} = -2\mathbf{v}_1 + 4\mathbf{v}_2 + 3\mathbf{v}_3$$

However, there is only one way to represent \mathbf{w} as a linear combination of the vectors \mathbf{v}_1 and \mathbf{v}_2 . For the condition $\mathbf{w} = c_1 \mathbf{v}_1 - c_2 \mathbf{v}_2$ requires

$$\begin{bmatrix} 2\\1\\1 \end{bmatrix} = c_1 \begin{bmatrix} 1\\0\\1 \end{bmatrix} + c_2 \begin{bmatrix} 1\\1\\0 \end{bmatrix} = \begin{bmatrix} c_1 + c_2\\c_2\\c_1 \end{bmatrix}$$

 c_1

is equivalent to the following linear system

$$\begin{array}{rcl} + c_2 &=& 2\\ c_2 &=& 1\\ c_1 &=& 1 \end{array}$$

which obviously as $c_1 = 1$ and $c_2 = 1$ as its only solution.

This motivates the following definition.

DEFINITION 7.13. Let W be a subspace of \mathbb{R}^n . A subset $\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k\}$ of W is called a **basis** for W if every vector in W can be uniquely expressed as linear combination of the vectors $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k$.

THEOREM 7.14. A set of vectors $\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k\}$ is a basis for the subspace W generated by $\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k\}$ if and only if

 $r_1 \mathbf{w}_1 + r_2 \mathbf{w}_2 + \dots + r_k \mathbf{w}_k = \mathbf{0}$ implies $0 = r_1 = r_2 = \dots = r_k$

Proof.

 \Rightarrow Suppose { $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k$ } is a basis for $W = span(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k)$. Then every vector in W can be uniquely specified as a vector of the form

$$\mathbf{v} = r_1 \mathbf{w}_1 + r_2 \mathbf{w}_2 + \dots + r_k \mathbf{w}_k \quad ; \quad r_1, r_2, \dots, r_k \in \mathbb{R}$$

In particular, the zero vector

(7.1)
$$\mathbf{0} = (0)\mathbf{w}_1 + (0)\mathbf{w}_2 + \dots + (0)\mathbf{w}_k$$

4. BASES

lies in W. Because $\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k\}$ is assumed to be a basis, the linear combination on the right hand side of (7.1) must be the unique linear combination of the vectors $\mathbf{w}_1, \ldots, \mathbf{w}_k$ that is equal to **0**. Hence,

$$r_1 \mathbf{w}_1 + r_2 \mathbf{w}_2 + \dots + r_k \mathbf{w}_k = \mathbf{0}$$
 implies $0 = r_1 = r_2 = \dots = r_k$

 \leftarrow Suppose

$$r_1\mathbf{w}_1 + r_2\mathbf{w}_2 + \dots + r_k\mathbf{w}_k = \mathbf{0}$$
 implies $0 = r_1 = r_2 = \dots = r_k$

We want to show that $\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k\}$ is a basis for $W = span(\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k)$. In other words, we need to show that there is only one choice of coefficients r_1, \ldots, r_k such that a vector $\mathbf{v} \in W$ can be expressed in the form $\mathbf{v} = r_1 \mathbf{w}_1 + r_2 \mathbf{w}_2 + \cdots + r_k \mathbf{w}_k$. Suppose there were in fact two distinct ways of representing \mathbf{v} :

(7.2)
$$\mathbf{v} = r_1 \mathbf{w}_1 + r_2 \mathbf{w}_2 + \dots + r_k \mathbf{w}_k$$

(7.3)
$$\mathbf{v} = s_1 \mathbf{w}_1 + s_2 \mathbf{w}_2 + \dots + s_k \mathbf{w}_k$$

Subtracting the second equation from the first yields

$$\mathbf{0} = (r_1 - s_1) \mathbf{w}_1 + (r_2 - s_2) \mathbf{w}_2 + \dots + (r_k - s_k) \mathbf{w}_k$$

Our hypothesis now implies

$$0 = r_1 - s_1 = r_2 - s_2 = \dots = r_k - s_k$$

In other words

$$r_1 = s_1$$

$$r_2 = s_2$$

$$\vdots$$

$$r_k = s_k$$

and so the two linear combinations on the right hand sides of (7.2) and (7.3) must be identical.

THEOREM 7.15. Let **A** be an $n \times n$ matrix. Then the following statements are equivalent.

- 1. The linear system $\mathbf{A}\mathbf{x} = \mathbf{b}$ has a unique solution for each vector $\mathbf{b} \in \mathbb{R}^n$.
- 2. The matrix \mathbf{A} is row equivalent to the identity matrix.
- 3. The matrix \mathbf{A} is invertible.
- 4. The column vectors of **A** form a basis for \mathbb{R}^n .

Proof. We have already demonstrated the equivalence of statements 2, 3 and 4. It therefore suffices to show that statement 4 is equivalent to statement 1.

To see that statement 4 implies statement 1, suppose that the column vectors $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ of **A** form a basis for \mathbb{R}^n . Then by Theorem 7.12, the linear system $\mathbf{A}\mathbf{x} = \mathbf{b}$ is consistent for all vectors $\mathbf{b} \in span(\mathbf{c}_1, \ldots, \mathbf{c}_n) = \mathbb{R}^n$. But a direct calculation reveals

$$\mathbf{b} = \mathbf{A}\mathbf{x} = x_1\mathbf{c}_1 + x_2\mathbf{c}_2 + \dots + x_n\mathbf{c}_n$$

Because the vectors $\mathbf{c}_1, \ldots, \mathbf{c}_n$ form a basis, there choice of coefficients x_1, x_2, \ldots, x_n must be unique. Therefore, the linear system $\mathbf{A}\mathbf{x} = \mathbf{b}$ has a unique solution for each vector $\mathbf{b} \in \mathbb{R}^n$.

On the other hand, suppose the linear system $\mathbf{A}\mathbf{x} = \mathbf{b}$ has a unique solution for each vector $\mathbf{b} \in \mathbb{R}^n$. In particular, this must be true for $\mathbf{b} = \mathbf{0}$. Therefore, there is only one choice of coefficients x_1, x_2, \ldots, x_n such that

$$\mathbf{0} = x_1 \mathbf{c}_1 + x_2 \mathbf{c}_2 + \dots + x_n \mathbf{c}_n = \mathbf{A} \mathbf{x}$$

By the preceding theorem we can conclude that the column vectors of A form a basis for \mathbb{R}^n .

EXAMPLE 7.16. Show that the vectors $\mathbf{v}_1 = (1, 1, 3)$, $\mathbf{v}_2 = (3, 0, 4)$, and $\mathbf{v}_3 = (1, 4, -1)$ form a basis for \mathbb{R}^3 .

By the preceding theorem, it suffices to show that the matrix

$$\mathbf{A} = \begin{bmatrix} 1 & 3 & 1 \\ 1 & 0 & 4 \\ 3 & 4 & -1 \end{bmatrix}$$

is invertible. Row reducing A yields

$$\begin{bmatrix} 1 & 3 & 1 \\ 1 & 0 & 4 \\ 3 & 4 & -1 \end{bmatrix} \xrightarrow{R_2 \to R_2 - R_1} \begin{bmatrix} 1 & 3 & 1 \\ 0 & -3 & 3 \\ 0 & -5 & -4 \end{bmatrix} \xrightarrow{R_3 \to R_3 - \frac{5}{3}R_2} \begin{bmatrix} 1 & 3 & 1 \\ 0 & -3 & 3 \\ 0 & 0 & -9 \end{bmatrix}$$

The matrix on the far right is upper triangular so it's obviously invertible. Hence, **A** is invertible; hence the column vectors of **A** form a basis for \mathbb{R}^3 ; hence the vectors \mathbf{v}_1 , \mathbf{v}_2 , and \mathbf{v}_3 form a basis for \mathbb{R}^3 .

The preceding theorem is applicable only to square matrices \mathbf{A} and linear systems of n equations in n unknowns. It can be extended to more general matrices and linear systems in the following manner.

THEOREM 7.17. Let A be an $m \times n$ matrix. Then the following are equivalent.

- 1. Each consistent system Ax = b has a unique solution.
- 2. The reduced row echelon form of A consists of the $n \times n$ identity matrix followed by m n rows containing only zeros.
- 3. The column vectors of \mathbf{A} form a basis for the column space of \mathbf{A} .

Proof.

 $1 \iff 2$: From Theorem 5.8 of Lecture 5 (Theorem 1.7 in text), we know that a consistent linear system $\mathbf{Ax} = \mathbf{b}$ has a unique solution if and only if \mathbf{A} is row equivalent to a matrix \mathbf{A}' in row-echelon form such that every column of \mathbf{A}' has a pivot. Since \mathbf{A} , and hence \mathbf{A}' , has *n* columns, we can conclude that the solution of every consistent linear system $\mathbf{Ax} = \mathbf{b}$ is unique if and only if we have must have *n* pivots. In order to have *n* pivots the number *m* of rows must be $\geq n$. When n = m there will be one pivot for each row, and the pivots will all reside along the diagonal, like so

$$\mathbf{A}' = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

occuring in at least n rows. If \mathbf{A}' is further reduced to a matrix \mathbf{A}'' in **reduced** row-echelon form, then all the pivots are re-scaled to 1 and all the entries above the pivots are equal to 0. Thus,

$$\mathbf{A}^{\prime\prime} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \mathbf{I}$$

If m > n, we still require n pivots, that means the only way we can consistently add rows to the picture above is by adding rows without pivots; i.e., rows containing only 0's.

 $1 \iff 3$: Suppose $\mathbf{A}\mathbf{x} = \mathbf{b}$ has a unique solution for each \mathbf{b} in the column space $C(\mathbf{A})$ of \mathbf{A} . (Recall \mathbf{b} must lie in the column space of \mathbf{A} in order for the linear system to be consistent.) Then, if we denote the column vectors of \mathbf{A} by $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ we have

$$\mathbf{b} = \mathbf{A}\mathbf{x} \equiv x_1\mathbf{c}_1 + x_2\mathbf{c}_2 + \dots + x_n\mathbf{c}_n \quad , \quad \text{for all } \mathbf{b} \in C(\mathbf{A}) \equiv span\left(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n\right)$$

If the solution \mathbf{x} is unique, then there is only one such linear combination of the column vectors \mathbf{c}_i for each vector $\mathbf{b} \in C(\mathbf{A})$. Hence, the column vectors \mathbf{c}_i provide a basis for $C(\mathbf{A})$. On the other hand, if the column vectors were not a basis for $C(\mathbf{A}) \equiv span(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n)$, then that would mean that there are vectors \mathbf{b}

lying in $C(\mathbf{A})$ such that the expansion $\mathbf{b} = x_1\mathbf{c}_1 + x_2\mathbf{c}_2 + \cdots + x_n\mathbf{c}_n$ in terms of the \mathbf{c}_i is not unique. Hence, a solution \mathbf{x} to $\mathbf{A}\mathbf{x} = \mathbf{b}$ would not be unique.

THEOREM 7.18. Let $\mathbf{A}\mathbf{x} = \mathbf{b}$ be a non-homogeneous linear system, and let \mathbf{p} be any particular solution of this system. Then every solution of $\mathbf{A}\mathbf{x} = \mathbf{b}$ can be expressed in the form

$$\mathbf{x} = \mathbf{p} + \mathbf{h}$$

where \mathbf{h} is a solution of the corresponding homogeneous system $\mathbf{A}\mathbf{x} = \mathbf{0}$.

Proof. Suppose \mathbf{p} and \mathbf{x}_1 are both solutions of $\mathbf{A}\mathbf{x} = \mathbf{b}$. Then set

$$h = x_1 - p$$

Then ${\bf h}$ satisfies

$$Ah = A (x_1 - p) = Ax_1 - Ap = b - b = 0$$

Hence, $\mathbf{x}_1 = \mathbf{p} + \mathbf{h}$ with \mathbf{h} a solution of $\mathbf{A}\mathbf{x} = \mathbf{0}$.