Here is a summary of concepts involved with vector spaces.
For our purposes a field, $k$, is a subset of the complex numbers that is closed under addition, multiplication, and additive and multiplicative inverses. Examples are the rationals, $\mathbf{Q}$, the reals, $\Re$, and the complex numbers, $\mathbf{C}$. In general one can assume one is working with $k=\Re$ although we will need $\mathbf{C}$ at some point.

1. Vector Space. A vector space over a field $k$ is a non empty set $V$ together with a well defined addition ' + ' and a scalar multiplication ''' by elements of the field $k$, satisfying the following axioms.

- Operations. For all $u, v \in V$ and $c \in k$ we have $u+v \in V$ and $c u \in V$. Sometimes, we write $c \cdot u$ but this $\cdot$ is often omitted.
- Addition properties. The addition is commutative $(u+v=v+u)$ and associative $(u+(v+w)=(u+v)+w)$.
- Additive identity and inverse. There is a zero vector, denoted 0 such that $u+0=0+u=u$ for all $u$. Moreover, for each $u$ there is a $u^{*}$ such that $u+u^{*}=u^{*}+u=0$. The $u^{*}$ can be shown to be uniquely defined by $u$ and is denoted as $-u$. The zero vector is also shown to be unique!
- Distributivity and unitariness. The two operations interact naturally:

$$
c(u+v)=c u+c v,(c+d) u=c u+d u,(c d) u=c(d u) .
$$

Moreover, $1(u)=u$ for all $u$.
As noted above this course, the field $k$ is usually $\Re$ the field of real numbers. In that case, we drop the phrase "over the field $\Re$ ".
2. Subspace If $V$ is a vector space over $k$ and $W$ is a non empty subset, then we say that $W$ is a subspace of $V$ if we have:

- For all $w_{1}, w_{2} \in W$ we have $w_{1}+w_{2} \in W$.
- For all $c \in k$ and $w \in W$ we have $c w \in W$.

We note that the vector 0 will always belong to a subspace as soon as it is non empty, since $w \in W$ implies $0 w=0 \in W$ by the second subspace condition above. Hence, you may replace the condition of $W$ being non empty by the simpler condition $0 \in W$, as done in the book.
3. (optional) A challenging example. Here is an exotic example of a vector space which should be studied to verify your understanding of the above definition.
Let $V=\Re$ be made into a vector space over the usual field of real numbers $\Re$ as follows:

- We define a new addition $\oplus$ on $V$ by the formula:

$$
v \oplus w=v+w-1
$$

where the operations on the right hand side are the usual operations in real numbers.

- We define a new scalar multiplication $\odot$ by $\Re$ on $V$ by the formula:

$$
c \odot v=c v+1-c
$$

where, as before, the operations on the right are the usual operations in real numbers.

It is instructive to verify all the axioms from these definitions. You should also identify what $-v$ means. This example should be kept in mind while analyzing all the following concepts.
You should also make an enhanced version of this example by taking $V$ to be $\Re^{n}$ as the set, but using the above definitions of addition and scalar multiplication, suitably generalized. ${ }^{1}$
4. A Universal example. Let $S$ be any non empty set and consider

$$
F_{S}^{k}=\{f: S \rightarrow k \mid \text { where } f(s)=0 \text { for all except finitely many } s \in S .\}
$$

It can be shown that every vector space can be described in this manner, but finding such an explicit $S$ can be tedious and it is better to use the basic definition. If $k=\Re$ we may drop it from the notation.
It is easy to verify how $F_{S}^{k}$ is a vector space by defining $(f+g)(s)=f(s)+g(s)$ and $c f(s)=c f(s)$. The extra condition on $f$ is not necessary, but it is essential if you want to claim that every vector space has a standard structure!
5. Basic examples. Here are some of the standard examples.

[^0]- Euclidean spaces. The space $k^{n}$ consisting of all $n$-tuples of elements of $k$, usually written as a column.
This can be described as $F_{S}^{k}$ where $S$ is the set $\{1,2,3, \cdots, n\}$. A typical function $f$ in the vector space may be displayed as
$\left(\begin{array}{r}f(1) \\ f(2) \\ \cdots \\ f(n)\end{array}\right)$. This leads to the usual notation for $k^{n}$. For our purposes $k$ will almost always be $\Re$ in which case we are talking about the familiar $\Re^{n}$.
- The case of an infinite $\mathbf{S}$. If we take $S=\{1,2, \cdots, n, \cdots\}$, the set of natural numbers, then we find it convenient to display $f \in F_{S}$ as

$$
f(1)+f(2) x+f(3) x^{2}+\cdots f(n+1) x^{n}+\cdots .
$$

Note that the description of $F_{S}$ implies that after some large enough exponent $N$, the coefficients are all zero and we have a set of polynomials.
The book denotes $F_{S}^{\Re}$ by the symbol $\mathbb{P}$. A general notation for $F_{S}^{k}$ is also $k[x]$ which is the ring of polynomials in $x$ with coefficients in $k$, where, we have chosen to ignore the usual multiplication of polynomials!
We now note that if we keep the same set $S=\{1,2, \cdots, n, \cdots\}$ but drop the special condition on functions we get a much bigger set, namely

$$
H=\{f: S \rightarrow k\} .
$$

As before, any such $f \in H$ be displayed as $f(1)+f(2) x+f(3) x^{2}+\cdots+f(n+$ 1) $x^{n}+\cdots$.

Since there is no special condition on the function, we now get power series! The general notation for this set is $k[[x]]$, the ring of power series in $x$ with coefficients in $k$, where, as before, we ignore the usual product of power series. It can be shown that $H=F_{T}^{k}$ for some convenient set $T$, but finding such a $T$ is a daunting task!
There is also a well known subset of $H$ when $k=\Re$, namely the set of convergent power series. To write it as $F_{T}^{\Re}$ is an even more daunting task!

- spaces of matrices: $M a t_{m, n}$, the set of $m$ by $n$ matrices with matrix addition and scalar multiplication.
- function spaces: If $X$ is any set then $F_{X}^{\Re}=\{f: X \rightarrow \Re\}$ is a vector space with the usual addition of functions and multiplication of functions by a scalar. (i.e. $(f+g)(x)=f(x)+g(x),(\alpha f)(x)=\alpha f(x))$
- direct sums: If $U$ and $V$ are vector spaces and $U \oplus V=\{(u, v) \mid v \in U, v \in V\}$ then $U \oplus V$ is a vector space with addition $\left(u_{1}, v_{1}\right)+\left(u_{2}, v_{2}\right)=\left(u_{1}+v_{1}, u_{2}+\right.$ $v_{2}$ ) and scalar multiplication $\lambda(u, v)=(\lambda u, \lambda v)$. This allows us to define vector spaces tailored to specific problems and to view more complex spaces as constructed of simpler ones. For example we can, properly interpreted, view $\Re^{7}$ as $\Re^{2} \oplus \Re^{5}$.

6. Important Remark: A subspace of a vector space $V$ is simply a subset of $V$ that is closed under linear combinations. Except for the following exotic example, all of the vector spaces we will encounter in this course either fall in the above list of examples or are subspaces of members of this list. This means that once a prospective vector space has been identified as a subset of a known vector space (e.g. the above examples) then all that is required to verify that it is a vector space is to check that it is closed under linear combinations.

Example: Let $C^{1}(\Re)$ be the set of all differentiable functions $f: \Re \rightarrow \Re$. This is a vector space since:

- it is a subset of the vector space $F_{\Re}^{\Re}$
- If $f, g \in C^{1}(\Re)$ and $\alpha, \beta \in \Re$ then $\frac{d}{d x}(\alpha f+\beta g)=\alpha \frac{d}{d x} f+\beta \frac{d}{d x} g$ so $(\alpha f+\beta g) \in$ $C^{1}(\Re)$

7. Basic structures in a vector space. Now let $V$ be a $k$-vector space (i.e. vector space over a field $k$ ).
Foe any subset $A \subset V$, we define its span:
$\operatorname{Span} A=\left\{c_{1} v_{1}, \cdots+c_{m} v_{m} \mid\right.$ where $c_{i} \in k, v_{i} \in A$ and $m$ is some non negative integer. $\}$.
Note that Span $A$ can be described as the set of all possible linear combinations of elements of $A$. Note that even when $A$ is infinite, we only allow finitely many elements of it at a time! Also note that $m$ is allowed to be zero and it gives the combination 0 , by a standard convention.
We say that a set $A$ spans $\mathbf{V}$ or is a spanning set for $\mathbf{V}$ if $\operatorname{Span} A=V$.
A subset $A \subset V$ is said to be linearly dependent if there are elements $v_{1}, \cdots, v_{m} \in$ $A$ such that $c_{1} v_{1}+\cdots+c_{m} v_{m}=0$ for some $c_{1}, \cdots, c_{m} \in k$ with at least one non zero element $c_{i}$ among them.
In application, other convenient forms of this condition are used. One such version is:

A subset $A \subset V$ is said to be linearly dependent if there is some $v \in A$ such that $v$ is a linear combination of some elements $w_{1}, \cdots, w_{r} \in A$ which are distinct from $v$. A compact way of saying this is to write that $v \in \operatorname{Span} A \backslash\{v\}$.
A set $A \subset V$ is said to be linearly independent, if it is not linearly dependent.
We often drop the word "linearly" from these terms.
A subset $A \subset V$ is said to be a basis of $V$ if

$$
\operatorname{Span} A=V \text { and } A \text { is linearly independent. }
$$

Convention: If $V$ is any vector space then $\{O\}$, the set consisting only of $O$, the zero vector of $V$ is a subspace of $V$. It is logically true that the empty set, $\Phi$ is independent and by convention it is a basis for $\{O\}$.
We say that $V$ is finite dimensional if it has a finite basis.

Important Observation: If $V$ is a vector space and $B_{1}$ and $B_{2}$ are bases for $V$ with $B_{1} \subset B_{2}$ then $B_{1}=B_{2}$.
proof: If $B_{1} \neq B_{2}$ then there would have to be $b \in B_{2}$ that is not in $B_{1}$. However $B_{1}$ is a spanning set for $V$ which means that $b_{2}$ must be a linear combination of elements in $B_{1}$. But $B_{1} \subset B_{2}$ so $b_{2}$ is a linear combination of the other elements of $B_{2}$ which says that $B_{2}$ is dependent which is a contradiction.
Definition: The number of elements in a basis for $V$, is said to be the dimension of $V$. We write $\operatorname{dim} V$ or $\operatorname{dim}_{k} V$ if we wish to identify $k$.

We will soon argue that the dimension is a well defined number for any vector space, i.e. every basis of a vector space has the same number of elements.

## Examples:

- The standard basis $\left\{e_{1}, e_{2}, \cdots, e_{n}\right\}$ is linearly independent and a spanning set for $\Re^{n}$, thus the dimension of $\Re^{n}$ is $n$.
- If $V$ is a vector space, recall that by convention the empty set $\Phi$ is a basis for the zero subspace $\{O\}$. Thus the zero subspace has dimension 0 since $\Phi$ has 0 elements.

Infinite Dimensional Spaces A vector space that is not finite dimensional (i.e. does not have a finite basis is said to be infinite dimensional. It is true that even infinite dimensional spaces do have bases (linearly independent spanning sets). However we don't say that the dimension is the "number of elements in a basis". For infinite dimensional spaces we need to use the finer notion of "number of "
called "cardinality ${ }^{2}$ " which distinguishes between different infinite sets. Properly dealing with "cardinality" would take too much time so, for our purposes, we won't try to define the dimension of a vector space that is not finite dimensional but will rather simply say that all such spaces are infinite dimensional.
8. Homomorphisms, Isomorphisms and Automorphisms. Given $k$-vector spaces $V, W$ a map $T: V \rightarrow W$ is said to be a linear transformation if it satisfies these two conditions:

- $T\left(v_{1}+v_{2}\right)=T\left(v_{1}\right)+T\left(v_{2}\right)$ for all $v_{1}, v_{2} \in V$.
- $T(c v)=c T(v)$ for all $c \in k$ and $v \in V$.

We may also use the term "homomorphism" ( meaning similar structure) to denote such a map.
There are two concepts associated with the notion of a linear transformation (homomorphism).
First is "the image of $T$ " which can be formally denoted as

$$
T(V)=\{T(v) \mid v \in V\} .
$$

Second is "the Kernel of $T$ " which can be defined as:

$$
\operatorname{Ker} T=\{v \in V \mid T(v)=0\} .
$$

It is easy to verify that both the Kernel and the Image are respectively subspaces of $V$ and $W$.
The homomorphism $T$ is injective (or "one to one ") iff $\operatorname{Ker} T=0$ where we have used a slightly abused notation 0 in place of $\{0\}$. This abuse is routinely done!

The homomorphism $T$ surjective (or "onto") if $T(V)=W$ i.e. $W$ is its total image.
The homomorphism $T$ is said to be an isomorphism if it is both injective and surjective i.e. bijective. The word "iso" denotes sameness and the concept says that the two vector spaces with an isomorphism mapping one to the other are essentially the same. They, can be treated as replacements for each other in analyzing their properties.
An isomorphism of $V$ to itself is called an automorphism.

[^1]9. A Fundamental Theorem (existence of bases). This is the fundamental theorem in the theory of vector spaces.
Let $V$ be a vector space with a spanning set $A$. Then there is a subset $B$ of $A$ such that $B$ is a basis of $V$. That is $B$ is also a spanning set for $V$ and $B$ is independent.
We shall give a complete proof in case $A$ is finite and a partial proof in case $A$ is infinite.

## Proof.

If $A$ is independent, then it is a basis and we are done. If $A$ is dependent, then there is some vector $v \in A$ which is a linear combination of vectors in $A_{1}=A \backslash\{v\}$. We now claim that Span $A=\operatorname{Span} A_{1}$ by the following argument.
Proof of claim. Note that any $w \in \operatorname{Span} A$ can be written as: $w=c v+w_{1}$ where $c \in k$ and $w_{1} \in \operatorname{Span} A_{1}$.
By assumption, $v \in \operatorname{Span} A_{1}$, so $c v$ and hence $w$ belongs to Span $A_{1}$. Thus $\operatorname{Span} A \subset \operatorname{Span} A_{1}$. Clearly Span $A_{1} \subset \operatorname{Span} A$ since $A_{1} \subset A$.
This shows Span $A=\operatorname{Span} A_{1}$.
Thus, if $V=\operatorname{Span} A$ and $A$ is dependent, then we get a proper subset $A_{1}$ of $A$ such that $V=\operatorname{Span} A_{1}$. We can now apply the same argument to $A_{1}$ and either get a basis or a smaller spanning set $A_{2}$.
In case $A$ is a finite set to begin with, this cannot continue indefinitely and we must get a basis at some stage.
We remark that we may run into an empty subset of $A$, in case the vector space is the zero space $\{0\}$. However, in this case the whole set $A$ can only be $\{0\}$ or empty and we have nothing to argue!
It is also possible to do the above proof in a reversed process. We can start with independent subsets of $A$ and enlarge them as much as possible. We argue that eventually we should get a basis.
In case the set $A$ is infinite requires a more general inductive principle called Zorn's Lemma. This lemma allows us (we omit the details here) to prove that there are maximal independent subsets in any vector space. Such sets are easily seen to be spanning sets.
Theorem A: Suppose $V$ is a vector space and $F=\left\{F_{1}, F_{2}, \cdots, F_{s}\right\}$ is a finite subset of $V$. Suppose further that the set of vectors $B=\left\{B_{1}, B_{2}, \cdots, B_{s}, B_{s+1}\right\}$ is contained in the linear span of $F$. Then $B$ is linearly dependent set.

Proof: For each $i=1 \cdots s+1$ there is a linear combination

$$
a_{i, 1} F 1+a_{i, 2} F_{2}+\cdots+a_{i, s} F_{s}=B_{i}
$$

Let $A$ be the $s+1 \times s$ matrix

$$
\left(\begin{array}{cccc}
a_{1,1} & a_{1,2} & \cdots & a_{1, s} \\
a_{2,1} & a_{2,2} & \cdots & a_{2, s} \\
\vdots & \vdots & \vdots & \vdots \\
a_{i, 1} & a_{i, 2} & \cdots & a_{i, s} \\
\vdots & \vdots & \vdots & \vdots \\
a_{s, 1} & a_{s, 2} & \cdots & a_{s, s} \\
a_{s+1,1} & a_{s+1,2} & \cdots & a_{s+1, s}
\end{array}\right)
$$

Then letting $F=\left(\begin{array}{c}F_{1} \\ F_{2} \\ \vdots \\ F_{i} \\ \vdots \\ F_{s}\end{array}\right)$ and $B=\left(\begin{array}{c}B_{1} \\ B_{2} \\ \vdots \\ B_{i} \\ \vdots \\ B_{s} \\ B_{s+1}\end{array}\right)$ we write

$$
A F=B
$$

Now we augment $A$ by the $s+1 \times s+1$ identity matrix to get $\langle A \mid I\rangle$ which we then row reduce to get $\langle R \mid Q\rangle$ where $R$ is an REF of $A$ and $Q$ is an invertible matrix such that $Q A=R$.

Since $R$ has more rows than pivots its last row must be all zeros and therefore the last row of $Q$ is a row of the consistency matrix which cannot be all zero since it is a row of an invertible matrix!. Let this last row be $C=\left[c_{1}, c_{2}, \cdots, c_{s+1}\right]$ then $C A=[0,0, \ldots, 0]$ the row $s$ zeros.
But recall that we had $A F=B$ so
$C(A F)=C B$
Since $C(A F)=(C A) F=\left[[0,0, \ldots, 0]\left(\begin{array}{c}F_{1} \\ F_{2} \\ \vdots \\ F_{i} \\ \vdots \\ F_{s}\end{array}\right)=O\right.$ and
$C B=c_{1} F_{1}+c_{2} F_{2}+\cdots+c_{s} F_{s}+c_{s+1} F_{s+1}$ and not all of the $c_{i}$ are 0 we have that $B$ is linearly dependent.
10. Example: Let $P_{3}$ be the vector space of polynomials of degree at most 3 and let $F_{1}=x, F_{2}=x^{2}, F_{3}=x^{3}$ and $B_{1}=x+x^{2}, B_{2}=x-4 x^{3}, B_{3}=x+3 x^{2}+x^{3}$, $B_{4}=2 x-x^{2}+x^{3}$ then according to the theorem the four elements of $B=$ $\left\{B_{1}, B_{2}, B_{3}, B_{4}\right\}$ are linearly dependent since they are linear combinations of the three members of $F=\left\{F_{1}, F_{2}, F_{3}\right\}$. Moreover, we can calculate a dependence relation. Here

$$
\begin{gathered}
1 F_{1}+1 F_{2}+0 F_{3}=B_{1} \\
1 F_{1}+0 F_{2}+-4 F_{3}=B_{2} \\
1 F_{1}+3 F_{2}+1 F_{3}=B_{3} \\
2 F_{1}-1 F_{2}+1 F_{3}=B_{4}
\end{gathered}
$$

so setting

$$
A=\left(\begin{array}{ccc}
1 & 1 & 0 \\
1 & 0 & -4 \\
1 & 3 & 1 \\
2 & -1 & 1
\end{array}\right)
$$

We have $A\left(\begin{array}{c}F_{1} \\ F_{2} \\ F_{3}\end{array}\right)=\left(\begin{array}{c}B_{1} \\ B_{2} \\ B_{3} \\ B_{4}\end{array}\right)$
and $R E F(<A \mid I>)=\left(\begin{array}{ccccccc}1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -4 & -1 & 1 & 0 & 0 \\ 0 & 0 & -7 & -3 & 2 & 1 & 0 \\ 0 & 0 & 0 & -\frac{32}{7} & \frac{5}{7} & \frac{13}{7} & 1\end{array}\right)$
According to the theorem it must be true that

$$
\left(\begin{array}{llll}
-\frac{32}{7} & \frac{5}{7} & \frac{13}{7} & 1
\end{array}\right)\left(\begin{array}{l}
B_{1} \\
B_{2} \\
B_{3} \\
B_{4}
\end{array}\right)=0
$$

In fact $\frac{-32}{7}\left(x+x^{2}\right)+\frac{5}{7}\left(x-4 x^{3}\right)+\frac{13}{7}\left(x+3 x^{2}+x^{3}\right)+(1)\left(2 x-x^{2}+x^{3}\right)=0$
11. Theorem B: Any two bases of a vector space have the same number of elements. Proof: We prove the theorem for finite dimensional vector spaces. The theorem is true for infinite dimensional spaces but requires the idea of cardinality to replace
"number of" and that would take too much time for an introductory course.

Suppose the vector space has two linearly independent spanning sets, $B$ and $C$ and that $B$ has $m$ elements and $C$ has $n$ elements. We can assume $m \leq n$. If $m<n$ then $c_{1}, c_{2}, \cdots, c_{m}, c_{m+1}$ are all in the linear span of the $m$ elements of $B$ and are therefore linearly dependent, a contradiction. Thus $m=n$.
12. Definition: If $V$ is a vector space then the dimension of $V$ is the number of elements in any basis of $V$.

The above theorem says that dimension is well-defined since all bases have the same number of elements.

Theorem: Any $n+1$ elements in a vector space of dimension $n$ is linearly dependent.
Proof: This follows immediately from Theorem A.
Corollary: If $V$ is a vector space of dimension $n$ and $W$ is a subspace of $V$ then $\operatorname{dim}(W) \leq n$.
Corollary: If $V$ is a vector space of dimension $n$ then any $n$ linearly independent elements of $V$ is a basis of $V$.

Proof: Let $B=\left\{b_{1}, b_{2}, \cdots, b_{n}\right\}$ be a set of $n$ linearly independent elements of $V$. We need only show that $V$ is in the linear span of $B$ since we know it is linearly independent. Let $v$ be any element of $V$. Then $\left\{b_{1}, b_{2}, \cdots, b_{n}, v\right\}$ is a set with $n+1$ elements in an $n$-dimensional vector space so it is dependent. This means that there are scalars $\alpha_{i}$, not all zero, such that

$$
\alpha_{1} b_{1}+\alpha_{2} b_{2}+\cdots+\alpha_{n} b_{n}+\alpha_{n+1} v=O
$$

It must be true that $\alpha_{n+1} \neq 0$ since otherwise

$$
\alpha_{1} b_{1}+\alpha_{2} b_{2}+\cdots+\alpha_{n} b_{n}=O
$$

but that is not possible sinc e If $\alpha_{n+1} \neq 0$ then $v=-\frac{\alpha_{1}}{\alpha_{n+1}} b_{1}+-\frac{\alpha_{2}}{\alpha_{n+1}} b_{2}+\cdots+-\frac{\alpha_{n}}{\alpha_{n+1}} b_{n}$ and we are done.
Corollary: If $V$ is a vector space of dimension $n$ and $W$ is a subspace of $V$ of dimension $n$ then $W=V$.
Proof: The basis for $W$ has $n$ independent elements so it must be a basis for $V$.

## 13. Extension of independent sets to Bases

Theorem: Suppose $V$ is a vector space and $A$ is a linearly independent subset of $V$ then there is a basis $B$ of $V$ which contains $A$.
Proof: Although the theorem is true in general, the proof for infinite dimensional spaces requires extra tools and we will restrict our attention to the case when $V$ is a subspace of some finite dimensional space $W$. Let $W$ have dimension $N$.

Suppose $L$ is the linear span of $A$ and $A=\left\{a_{1}, a_{2}, \cdots, a_{s}\right\} . A$ is a basis for $L$ so if $L=V$ then $V$ has a basis containing $A$.
If $L \neq V$ then there is $a_{s+1} \in V$ that is not in $L$. It follows then that $\left\{a_{1}, a_{2}, \cdots, a_{s}, a_{s+1}\right\}$ is linearly independent. If this were not the case then there would be

$$
\alpha_{1} a_{1}+\alpha_{2} a_{2}+\cdots+\alpha_{s} a_{s}+\alpha_{s+1} a_{s+1}=O
$$

with not all of the $\alpha_{i}=0$. But $\alpha_{s+1}$ must be 0 or $a_{s+1}$ is in the span of $A$. However if this is the case then $A$ is linearly dependent.
If $\left\{a_{1}, a_{2}, \cdots, a_{s}, a_{s+1}\right\}$ does not span $V$ then the process can be repeated to find $a_{s+2}, \cdots, a_{s+k}$. Since $s+k \leq N$ and $N$ is the maximum number of elements in an independent subset of $V$ the process must stop at which time $\left\{a_{1}, a_{2}, \cdots, a_{s}, a_{s+k}\right\}$ is a spanning set for $V$. But since it is independent it must be a bais and $s=k=$ $N$.

## 14. A matrix approach to extension of independent sets to bases

The following is a method for implementing the previous theorem in the case where $V$ is $\Re^{n}$ and $A$ is a linearly independent subset of $\Re^{n}$.

Suppose $A_{1}, A_{2}, \ldots, A_{r}$ are independent vectors in $\Re^{n}$. Then the above theorem says that one can find vectors $A_{r+1}, \cdots, A_{n}$ such that the vectors $A_{1}, \cdots, A_{n}$ are linearly independent and are therefore a basis for $\Re^{n}$. If $A_{1}$ is the matrix with columns $A_{1}, A_{2}, \ldots, A_{r}$ then this is equivalent to saying that we can add $n-r$ columns to $A_{1}$ to get a matrix $A$ with $n$ linearly independent columns. The following construction does this.
Form $\left(A_{1} \mid I\right)$ by augmenting $A_{1}$ by the $n$ by $n$ identity and let $R$ be an REF of $\left(A_{1} \mid I\right)$. Let $C$ be the consistency matrix of $A_{1}$. Since $\operatorname{rank}\left(A_{1}\right)=r$ and has $n$ rows, the REF of $A_{1}$ has exactly $n-r$ zero rows and hence the consistency matrix $C$ has $n-r$ rows. If $C^{t}$ is the transpose of $C$ then its columns are independent since they are columns of an invertible matrix. Then $A=A_{1} \mid C^{t}$, is $n$ by $n$ and we claim its columns are linearly independent. We will prove this later as an application of orthogonality.

Example: Let $A_{1}=\left(\begin{array}{cc}1 & 3 \\ 0 & 1 \\ 2 & 4 \\ 3 & -1\end{array}\right)$ then the REF of $\langle A \mid I\rangle$ is $\left(\begin{array}{cccccc}1 & 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 7 & \frac{-3}{2} & 1\end{array}\right)$.
The consistency matrix is $C=\left(\begin{array}{cccc}-2 & 2 & 1 & 0 \\ 0 & 7 & \frac{-3}{2} & 1\end{array}\right)$. So $A=<A_{1} \left\lvert\, C^{t}>=\left(\begin{array}{cccc}1 & 3 & -2 & 0 \\ 0 & 1 & 2 & 7 \\ 2 & 4 & 1 & \frac{-3}{2} \\ 3 & -1 & 0 & 1\end{array}\right)\right.$
To see that $A$ has independent rows we can, for instance calculate its REF and
get $\left(\begin{array}{cccc}1 & 3 & -2 & 0 \\ 0 & 1 & 2 & 7 \\ 0 & 0 & 9 & \frac{25}{2} \\ 0 & 0 & 0 & \frac{314}{9}\end{array}\right)$


[^0]:    ${ }^{1}$ Can you make other examples of such weird operations? Here is a general hint and secret of all such constructions. Let $V$ be any vector space over a field $k$. Let $\psi$ be any bijective (ii.e. injective and surjective) function from $V$ to itself. Define a new vector space $W$ which uses the same $V$ as an underlying set but defines operations as follows.

    $$
    w_{1} \oplus w_{2}=\psi^{-1}\left(\psi\left(w_{1}\right)+\psi\left(w_{2}\right)\right) \text { and } c \odot w=\psi^{-1}(c \psi(w))
    $$

    It can be shown that $W$ is a vector space "isomorphic" to $V$ which means essentially the same as $V$. See below for explanation of "isomorphic".

    Can you guess the $\psi$ for the example given above? Hint: try $x \rightarrow x+\alpha$ for some $\alpha$.

[^1]:    ${ }^{2}$ Two sets $A, B$ are said to have the same cardinality if there is a bijective map from $A$ to $B$. As the example of the sets $\{1,2,3, \cdots, n \cdots\}$ and $\{2,4,6, \cdot, 2 n, \cdots\}$ shows, a set can have the same cardinality as a proper subset. This suggests that one has to be very careful in dealing with infinite cardinality.

