QMMM Warm-up 1: Complex vector spaces

Instructor: Grant T. Barkley

1 Linear algebra

For now and forever, $\mathbb{C}$ denotes the field of complex numbers. In linear algebra over the complex numbers, a complex number $\lambda \in \mathbb{C}$ is also called a *scalar*.

1.1 Vector spaces

Definition 1.1.

A *complex vector space* (or just *vector space*) is a set V with two operations:

- An *addition* operation, which takes in two elements of V and outputs another element of V. If the inputs are $\mathbf{v}$ and $\mathbf{w}$ then the output of the addition operation is written as $\mathbf{v} + \mathbf{w}$ and is called the *sum* of $\mathbf{v}$ and $\mathbf{w}$.
- A *scalar multiplication* operation, which takes in an element of $\mathbb{C}$ (the *scalar*) and an element of V (the *vector*) and outputs another element of V (the *scaled vector*). If λ is the scalar and $\mathbf{v}$ is the vector, then the scaled vector is written as $\lambda \cdot \mathbf{v}$, or even just $\lambda\mathbf{v}$.

We also pick a distinguished element of V, called the *zero vector*, which is denoted by $\mathbf{0}$. These operations are required to satisfy certain properties. If $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ are any vectors and $\lambda, \lambda_1, \lambda_2 \in \mathbb{C}$ are any scalars, then we require the following axioms:

$$
\begin{aligned}
&\text{Properties of addition:} \\
\mathbf{u} + (\mathbf{v} + \mathbf{w}) &= (\mathbf{u} + \mathbf{v}) + \mathbf{w} && \text{(Associativity)} \\
\mathbf{v} + \mathbf{w} &= \mathbf{w} + \mathbf{v} && \text{(Commutativity)} \\
\mathbf{v} + \mathbf{0} &= \mathbf{v} && \text{(Identity)} \\
&\text{Properties of scalar multiplication:} \\
\lambda_1 \cdot (\lambda_2 \cdot \mathbf{v}) &= (\lambda_1 \lambda_2) \cdot \mathbf{v} && \text{(Compatibility)} \\
1 \cdot \mathbf{v} &= \mathbf{v} && \text{(Identity)} \\
0 \cdot \mathbf{v} &= \mathbf{0} && \text{(Zero)} \\
&\text{Relating the two operations:} \\
\lambda(\mathbf{v} + \mathbf{w}) &= \lambda\mathbf{v} + \lambda\mathbf{w} && \text{(Distributivity over vectors)} \\
(\lambda_1 + \lambda_2)\mathbf{v} &= \lambda_1\mathbf{v} + \lambda_2\mathbf{v}. && \text{(Distributivity over scalars)}
\end{aligned}
$$

The axioms in Definition 1.1 are designed to encapsulate the core properties of the "standard vector spaces" $\mathbb{C}^n$ for $n \geq 0$. Recall that $\mathbb{C}^n$ is the set of column vectors with n rows, with entries in $\mathbb{C}$. For instance, a typical element of $\mathbb{C}^3$ might look like the vector $\mathbf{v} = \begin{pmatrix} 3.141 \\ 0 \\ 22 - 7i \end{pmatrix}$.

Problem 1.

Check that $\mathbb{C}^n$, with its usual addition and scalar multiplication operations, is a complex vector space.
(In other words, check that these operations satisfy the properties listed in Definition 1.1.)

Problem 2.

Let V be a vector space. Fix any vector $\mathbf{v} \in V$. Prove that there is a **unique** vector $\mathbf{v}' \in V$ satisfying

$$\mathbf{v} + \mathbf{v}' = \mathbf{0}.$$

The unique vector $\mathbf{v}'$ is called the *negation* or *inverse* of $\mathbf{v}$, and is denoted $-\mathbf{v}$.

The negation operation, which takes a vector $\mathbf{v}$ and outputs $-\mathbf{v}$, is usually taken as an additional part of the structure of a vector space. If we did this, then we would add the following axiom to the list in Definition 1.1.

$$\mathbf{v} + (-\mathbf{v}) = \mathbf{0}. \qquad \text{(Inverses)}$$

Problem 3. o

Assume that V is a set with addition and scalar multiplication operations satisfying every axiom in Definition 1.1 except possibly (Zero). Prove that if V has a negation operation satisfying (Inverses), then V satisfies the (Zero) axiom.
Bonus: Can we prove the (Zero) axiom without using the negation operation?

Problem 4.

Let X be any set. Define V to be the collection of all functions from X to $\mathbb{C}$. Define addition and scalar multiplication operations on V. Show that V is a vector space with these operations.
What if we look at the collection of all functions from X to W, where W is an arbitrary complex vector space?

1.2 Subspaces and spans

Definition 1.2.

Let W be a subset of a vector space V containing $\mathbf{0}$. Then W is a *subspace* of V if the sum of any two vectors in W is also in W and if any scalar multiple of a vector in W is also in W.

Problem 5.

Let X be a set and V be the vector space of functions from X to $\mathbb{C}$ defined in Problem 4. Fix an element $x \in X$ and define

$$W = \{f \in V \mid f(x) = 0\}.$$

Check that W is a subspace of V.

Problem 6.

Let V be the vector space of functions from $\mathbb{N}$ (the positive integers) to $\mathbb{C}$. Equivalently, V is the set of all sequences of complex numbers. Define

$$W = \{f \in V \mid \exists N \in \mathbb{N},\ \forall n > N,\ f(n) = 0\},$$

the set of all sequences which are eventually 0. Check that W is a subspace of V.

Definition 1.3.

Let X be a subset of a vector space V. The *(linear) span* of X, denoted $\operatorname{span} X$, is the set of all finite linear combinations of elements of X. In symbols,

$$\operatorname{span} X = \{\lambda_1 \mathbf{v}_1 + \ldots + \lambda_r \mathbf{v}_r \mid r \in \mathbb{N},\ \lambda_1, \ldots, \lambda_r \in \mathbb{C},\ \mathbf{v}_1, \ldots, \mathbf{v}_r \in X\}.$$

If X is the empty set $\varnothing$, then we define

$$\operatorname{span} \varnothing = \{\mathbf{0}\}.$$

If W is a subspace of V, then we say that X *spans* W if $\operatorname{span} X = W$.

Recall that a *closure operature* c on a set V is a map taking subsets of V to subsets of V, and satisfying the following three properties, for any subsets X, Y of V:

(i) $X \subseteq c(X)$.

(ii) If $X \subseteq Y$, then $c(X) \subseteq c(Y)$.

(iii) $c(c(X)) = c(X)$.

Problem 7.

Verify the following properties of the linear span.

(a) For any $X \subseteq V$, the set $\operatorname{span} X$ is a subspace of V.

(b) The map taking a subset X of V to the set $\operatorname{span} X$ is a closure operator on V.

(c) If W is a subspace of V which contains a set X, then W also contains the subspace $\operatorname{span} X$.

Problem 8. ♦

Let X be a nonempty subset of a vector space V. Assume $\mathbf{v}$ is a vector in the span of X, but $\mathbf{v}$ is not in the span of any proper subset of X. Show that X is finite, and if $\mathbf{w}$ is any element of X, then $\mathbf{w}$ is in the span of $(X \setminus \{\mathbf{w}\}) \cup \{\mathbf{v}\}$.

The span of a singleton $\{\mathbf{v}\}$ is often denoted $\mathbb{C}\mathbf{v}$. If V_1, V_2 are two subspaces of the same vector space, then we write $V_1 + V_2$ to indicate the span of $V_1 \cup V_2$. Similarly, if $\{V_i\}_{i \in I}$ is any collection of subspaces of V (indexed by a set I), then $\sum_{i \in I} V_i$ denotes the span of $\bigcup_{i \in I} V_i$.

Definition 1.4.

Let $\{V_i\}_{i \in I}$ be a collection of vector subspaces of a vector space V. We say that V is *the (internal) direct sum* of $\{V_i\}_{i \in I}$, written

$$V = \bigoplus_{i \in I} V_i$$

if for all $i \in I$,

$$V_i \cap \sum_{j \in I \setminus \{i\}} V_j = \{\mathbf{0}\},$$

and if $\sum_{i \in I} V_i = V$.

We also say that $V = \bigoplus_{i \in I} V_i$ is a *direct sum decomposition* of V if each V_i is a subspace of V and if V is the direct sum of $\{V_i\}_{i \in I}$.

Direct sum notation follows the same conventions used for unions or intersections. For instance, if our index set $I = \{1, 2, \ldots, r\}$, then we write

$$V = V_1 \oplus V_2 \oplus ... \oplus V_r = \bigoplus_{k=1}^{r} V_k,$$

and if $I = \mathbb{N}$, then we write

$$V = V_1 \oplus V_2 \oplus \cdots = \bigoplus_{k=1}^{\infty} V_k.$$

Problem 9. ♦

Let V be a vector space and let $V = V_1 \oplus ... \oplus V_r$ be a direct sum decomposition of V. Prove that for any vector $\mathbf{v} \in V$, there is a unique list of elements $\mathbf{v}_1, ..., \mathbf{v}_r$ satisfying

$$\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + ... + \mathbf{v}_r,$$

and such that $\mathbf{v}_k \in V_k$ for all k.
Generalize this statement to an arbitrary direct sum decomposition $V = \bigoplus_{i \in I} V_i$.

1.3 Linear maps

Definition 1.5.

Let V and W be complex vector spaces and let L be a function from V to W. We say that L is a *linear map* if it satisfies the following, for all $\lambda \in \mathbb{C}$ and $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$:

- $L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2)$, and
- $L(\lambda \mathbf{v}) = \lambda L(\mathbf{v})$.

Problem 10.

Check the following properties of linear maps:

(a) A linear map $L : V \to W$ takes $\mathbf{0} \in V$ to $\mathbf{0} \in W$.

(b) The composition of two linear maps is a linear map.

(c) If a linear map $L : V \to W$ is a bijection, then its inverse function $L^{-1} : W \to V$ is also a linear map.

Describe the linear maps from $\mathbb{C}$ to $\mathbb{C}$.

A linear map $L : V \to W$ is called *invertible* or an *isomorphism* if it is bijective. In this case we say that L is an *isomorphism* between V and W. If there is an isomorphism between V and W, then we say V and W are *isomorphic*.

Definition 1.6.

Let $L : V \to W$ be a linear map. The *kernel* of L is

$$\ker L \doteq \{\mathbf{v} \in V \mid L(\mathbf{v}) = \mathbf{0}\}.$$

The *image* of L is its image as a function. Explicitly,

$$\operatorname{im} L \doteq \{\mathbf{w} \in W \mid \exists \mathbf{v} \in V,\ L(\mathbf{v}) = \mathbf{w}\}.$$

Problem 11.

Show the following properties of the kernel and image of a linear map $L : V \to W$.

(a) $\ker L$ is a subspace of V and $\operatorname{im} L$ is a subspace of W.

(b) L is injective if and only if $\ker L = \{\mathbf{0}\}$.

(c) L is invertible if and only if $\ker L = \{\mathbf{0}\}$ and $\operatorname{im} L = W$.

(d) If $L' : W \to U$ is a linear map to a third vector space U, then

$$\ker(L' \circ L) \supseteq \ker L \qquad \text{and} \qquad \operatorname{im}(L' \circ L) \subseteq \operatorname{im}(L').$$

Problem 12.

Let $V = \bigoplus_{i \in I} V_i$ be a direct sum decomposition of a vector space. Fix an index $j \in I$. As a result of Problem 9, any vector $\mathbf{v}$ can be uniquely decomposed into the sum of an element $\mathbf{v}_j \in V_j$ and an element $\mathbf{v}' \in \sum_{i \in I \setminus \{j\}} V_i$.

Let Π_j be the function from V to V which assigns to a vector $\mathbf{v}$ the vector $\mathbf{v}_j$. Show that Π_j is a linear map and is *idempotent* (i.e. it satisfies $\Pi_j \circ \Pi_j = \Pi_j$).

Any linear map $\Pi : V \to V$ satisfying $\Pi \circ \Pi = \Pi$ is called a *(linear) projection operator* on V. The map Π_j which is constructed in Problem 12 is called the *(linear) projection onto V_j, relative to the decomposition* $\bigoplus_{i \in I} V_i$. As the next problem shows, any projection operator is of this form.

Problem 13. ♦

Let Π be a projection operator on a vector space V. Show that there is a unique pair of subspaces $V_1, V_2 \subseteq V$ such that

$$V = V_1 \oplus V_2$$

and so that Π is the projection onto V_1, relative to $V_1 \oplus V_2$.

1.4 Quotient vector spaces

If $\mathbf{v}$ is a vector in a vector space V, and K is a subset of V, then we set

$$\mathbf{v} + K \doteq \{\mathbf{v} + \mathbf{z} \mid \mathbf{z} \in K\}.$$

Similarly, if X is a subset of V, then we set

$$X + K \doteq \{\mathbf{v} + \mathbf{z} \mid \mathbf{v} \in X,\ \mathbf{z} \in K\}.$$

Lastly, if λ is a scalar and X is a subset of V, then set

$$\lambda X \doteq \{\lambda \mathbf{v} \mid \mathbf{v} \in X\}.$$

Problem 14.

Check the following properties of the operations defined above (set-sum and set-scaling).

(a) If X_1, X_2, X_3 are any subsets of V, then

$$(X_1 + X_2) + X_3 = X_1 + (X_2 + X_3).$$

(b) If X_1, X_2 are any subsets of V, and λ is any scalar, then

$$\lambda(X_1 + X_2) = \lambda X_1 + \lambda X_2.$$

(c) If K is a subspace of V, then $K + K = K$ and $\lambda K = K$ for all nonzero scalars λ.

Definition 1.7.

Let V be a vector space and K a subspace of V. The *quotient (vector) space* V/K is the vector space defined as follows. The underlying set of V/K is

$$\{\mathbf{v} + K \mid \mathbf{v} \in V\}.$$

So V/K is a collection of subsets of V. The addition and scalar multiplication operations on V/K are then given by the set-sum and set-scaling operations defined above (with the exception of scaling by 0, which is defined to always output the set K).

The function

$$\begin{aligned} q : V &\to V/K \\ \mathbf{v} &\mapsto \mathbf{v} + K \end{aligned}$$

is called the *quotient map*.

Problem 15.

Check that V/K is a vector space with these operations and that q is a linear map with kernel equal to K.

Any linear map L from V/K to a vector space W lifts to a map $L \circ q$ from V to W, with (by Problem 11c) $\ker(L \circ q) \supseteq K$. The converse also holds, as the following problem demonstrates.

Problem 16.

Let $L : V \to W$ be a linear map such that $K \subseteq \ker L$. Then there is a unique (*induced*) linear map $\overline{L} : V/K \to W$ such that $\overline{L} \circ q = L$.

Problem 17. ♦

Show, using Problem 16, that any linear map $L : V \to W$ induces a linear map

$$\overline{L} : V/\ker(L) \to \operatorname{im}(L)$$

which is an isomorphism.

Problem 18.

Let $V = V_1 \oplus V_2$ be a direct sum decomposition. Prove, using projection operators and the previous problem, that V/V_2 is isomorphic to V_1.

1.5 Linear dependence

Definition 1.8.

Let $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r$ be a list of vectors in a vector space V. We say that these vectors are *linearly independent* if the only choice of scalars $\lambda_1, ..., \lambda_r \in \mathbb{C}$ such that

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + ... + \lambda_r\mathbf{v}_r = \mathbf{0}$$

is $\lambda_1 = \lambda_2 = ... = 0$. The vectors are *linearly dependent* if there is some nontrivial linear combination of the vectors which is $\mathbf{0}$. If B is a subset of V, then we say B is linearly independent if every finite list of distinct vectors from B is linearly independent. B is a *(linear) basis* for V if it is linearly independent and spans V.

The vector space $\mathbb{C}^n$ comes with a standard ordered basis.

Problem 19.

Prove that a subset B of a vector space V is linearly dependent if and only if there exists a vector $\mathbf{v}$ in B, and vectors $\mathbf{v}_1, ..., \mathbf{v}_r \in B$ all distinct from $\mathbf{v}$, such that

$$\mathbf{v} \in \operatorname{span}\{\mathbf{v}_1, ..., \mathbf{v}_r\}.$$

Problem 20.

Show the following properties of a basis B in a vector space V.

(a) If $X \supsetneq B$, then X is linearly dependent.

(b) V is the direct sum of $\{\mathbb{C}\mathbf{v} \mid \mathbf{v} \in B\}$.

(c) Each vector $\mathbf{v} \in V$ can be written as a unique sum of scalar multiples of elements of B.

Problem 21.

Let X be a finite set and V be the vector space of functions from X to $\mathbb{C}$. Find a basis for V.

Problem 22.

Let W be the vector space of all sequences of complex numbers which are eventually 0. Find an (infinite) basis for W.
Can you write down a basis for the space of *all* sequences of complex numbers?

Problem 23. ♦

Let V be a vector space with basis $\{\mathbf{v}_i\}_{i\in I}$, and let W be any vector space. Pick vectors $\mathbf{w}_i \in W$ for each $i \in I$. Prove that there is a **unique** linear map $L : V \to W$ satisfying

$$L(\mathbf{v}_i) = \mathbf{w}_i$$

for all $i \in I$.

Problem 23 is the most important in this section, and (even if not stated explicitly) is the cornerstone of most introductions to linear algebra. Consider its result when applied to $V = \mathbb{C}^n$ and $W = \mathbb{C}^m$. In this case the problem shows that choosing a linear map $L : \mathbb{C}^n \to \mathbb{C}^m$ is equivalent to choosing a list of n vectors in $\mathbb{C}^m$. If those vectors are $\mathbf{w}_1, ..., \mathbf{w}_n$, then we could organize them in a matrix M_L, whose ith column is the column vector $\mathbf{w}_i$. So the matrix would look like:

$$M_L = \begin{pmatrix} | & | & ... & | \\ \mathbf{w}_1 & \mathbf{w}_2 & ... & \mathbf{w}_n \\ | & | & ... & | \end{pmatrix}.$$

This is called the *matrix representation* of L. We can multiply matrices and vectors as usual.

Problem 24.

Prove that for any linear map $L : \mathbb{C}^n \to \mathbb{C}^m$ and any $\mathbf{v} \in \mathbb{C}^n$, we have the identity

$$M_L \cdot \mathbf{v} = L(\mathbf{v}).$$

Hint: Use the previous problem.

Problem 25.

Let $L_1 : \mathbb{C}^n \to \mathbb{C}^m$ and $L_2 : \mathbb{C}^m \to \mathbb{C}^\ell$ be linear maps. (So the matrix representation M_{L_1} tells us where L_1 sends the basis vectors of $\mathbb{C}^n$ and the matrix representation M_{L_2} tells us where L_2 sends the basis vectors of $\mathbb{C}^m$.)
Prove that for any $\mathbf{v} \in \mathbb{C}^n$, we have the identity

$$(M_{L_2} \cdot M_{L_1}) \cdot \mathbf{v} = (L_2 \circ L_1)(\mathbf{v}).$$

In other words,
$$M_{L_2} \cdot M_{L_1} = M_{L_2 \circ L_1}.$$

Remark 1.9. The lesson of this section is that linear maps can be completely described by their action on basis vectors. So we can write statements like the following.

> Let W be the vector space of all sequences of complex numbers which are eventually zero, and let $\mathbf{w}_1, \mathbf{w}_2, ...$ be the natural basis. Then define a linear map $L_1 : W \to W$ by
> $$L_1(\mathbf{w}_k) = \mathbf{w}_{k+1}$$
> and a second linear map $L_2 : W \to W$ by
> $$L_2(\mathbf{w}_k) = e^{\frac{2\pi i k}{3}} \mathbf{w}_k.$$
> Note that the kernel of L_1 is $\mathbb{C}\mathbf{w}_1$, while L_2 is invertible. This is lorem ipsum dolor sit amet....

Matrices, and all the rules we learned to manipulate them, are just a way of organizing this data (using *coordinates*).

1.6 Aside: Transfinite recursion

Let's prove that every vector space has a basis. Modern proofs usually use *Zorn's lemma*, and you can look those up for another perspective[1]. I prefer the method of *transfinite induction*, which is an extension of the usual induction principle to handle sets which are "bigger" than $\mathbb{N}$.

Definition 1.10.

Let $\prec$ be a total ordering on a set S. Recall that a total ordering is a transitive relation $\prec$ such that any $x, y \in S$ satisfy exactly one of the following:
$$x \prec y, \quad x = y, \quad x \succ y.$$
We say $\prec$ is a *well-ordering* if any nonempty subset of S has a minimum element.

So for instance, the usual ordering on $\mathbb{N}$ is a well-ordering, while the usual orders on $\mathbb{Z}$ and $\mathbb{R}$ are not. A more exotic example of a well-ordering is the lexicographic order on $\mathbb{N} \times \mathbb{N}$:
$$(1,1) \prec (1,2) \prec (1,3) \prec ... \prec (2,1) \prec (2,2) \prec (2,3) \prec ... \prec (3,1) \prec (3,2) \prec (3,3) \prec ... \prec ....$$
There is a classification of well-orderings by *ordinal numbers* — the order on $\mathbb{N}$ corresponds to the ordinal ω and the order on $\mathbb{N} \times \mathbb{N}$ corresponds to ω^2. We won't need this, though.

Proposition 1.11 (Transfinite recursion)**.** *Let $\prec$ be a well-ordering on a set S. We want to define a function f on S. Suppose for each $t \in S$ we uniquely specify a definition of $f(t)$, possibly using the values $f(s)$ for $s \prec t$ in our definition. Then the principle of* transfinite recursion *says that $f(t)$ is well-defined for all $t \in S$.*

For example, recursively defined sequences such as

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2$$

satisfy the requirements of transfinite recursion (since $\mathbb{N}$ is well-ordered), and therefore give a well-defined sequence (the Fibonacci numbers). Meanwhile, you can't write down a recursive function on the integers without flipping the ordering on the negative integers. The recursion needs a "base case" — that's what well-ordering provides.

A special case of transfinite recursion, often used in conjunction with recursive definitions, is the principle of transfinite induction.

Proposition 1.12 (Transfinite induction). *Let $\prec$ be a well-ordering on a set S. Let $\varphi(t)$ be a proposition about elements t of S. Assume, for each $t \in S$, that we can prove $\varphi(t)$ if we assume that $\varphi(s)$ holds for all $s < t$. Then the principle of* transfinite induction *says that $\varphi(t)$ holds for all $t \in S$.*

With these principles, we can easily prove that all vector spaces have a basis. Let V be any complex vector space. Assume for now that V has a well-ordering $\prec$. Using transfinite recursion, we will define sets $B_{\mathbf{w}}$ indexed by the elements $\mathbf{w}$ of V. The goal is to construct a basis by adding vectors from V one at a time, at each step adding the next vector which is linearly independent from the ones we have added so far. Our sets are defined as follows:

- If $\mathbf{w}$ is in the span of $\bigcup_{\mathbf{v} \prec \mathbf{w}} B_{\mathbf{v}}$, then we set

$$B_{\mathbf{w}} \doteq \varnothing.$$

- Otherwise, set

$$B_{\mathbf{w}} \doteq \{\mathbf{w}\}.$$

Now define B to be

$$\bigcup_{\mathbf{w} \in V} B_{\mathbf{w}}.$$

Then the span of B is all of V, since any element $\mathbf{w} \in V$ is in the span of $\bigcup_{\mathbf{v} \preceq \mathbf{w}} B_{\mathbf{v}}$, which is a subset of B. We also claim that B is linearly independent. Assume for a contradiction that the vectors in B are dependent. Then (by Problem 19 and Problem 8) there are vectors $\mathbf{v}_1 \prec \mathbf{v}_2 \prec \ldots \prec \mathbf{v}_r$ in B such that

$$\mathbf{v}_r \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{r-1}\}.$$

But then, by definition, $B_{\mathbf{v}_r}$ does not contain $\mathbf{v}_r$, and so neither does B. But this is a contradiction, since $\mathbf{v}_r \in B$. Hence, B is a basis for V.

Now the only step missing from our proof that every vector space has a basis is justifying our assumption that every vector space has a well-ordering. For this we can use the following proposition (which, like Zorn's lemma, is equivalent to the axiom of choice).

Proposition 1.13 (Well-ordering theorem)**.** *Any set has a well-ordering.*

The following problem is harder than the ones so far.

Problem 26. o

Let B be a basis for a vector space V, and let X be a linearly independent set of vectors in V. Assume B and X are both well-ordered and, for simplicity, assume $B \cap X = \varnothing$. Using transfinite recursion on X, construct a set $Y \subseteq B$ and a bijection $\phi : X \to Y$, such that $(B \setminus Y) \cup X$ is a basis of V.

Using this, prove that any two bases of V have the same size. (That is, if B and X are two bases of V, then there is a bijection from B to X.)

Using transfinite induction on a set which is well-ordered using the axiom of choice, as we do here, usually gives an equivalent proof to one using Zorn's lemma. But transfinite induction is more generally applicable, as we may see later.