

BASES

BRANKO ČURĀUS

Throughout this note \mathcal{V} is a vector space over a scalar field \mathbb{F} . \mathbb{N} denotes the set of positive integers and $i, j, k, l, m, n, p \in \mathbb{N}$.

1. LINEAR INDEPENDENCE

Definition 1.1. If $m \in \mathbb{N}$, $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ and $v_1, \dots, v_m \in \mathcal{V}$, then

$$\alpha_1 v_1 + \dots + \alpha_m v_m$$

is called a *linear combination* of vectors in \mathcal{V} . A linear combination is *trivial* if $\alpha_1 = \dots = \alpha_m = 0$; otherwise it is a *nontrivial* linear combination.

Definition 1.2. Let \mathcal{A} be a nonempty subset of \mathcal{V} . The *span of \mathcal{A}* is the set of all linear combinations of vectors in \mathcal{A} . The span of \mathcal{A} is denoted by $\text{span } \mathcal{A}$. The span of the empty set is the trivial vector space $\{0_{\mathcal{V}}\}$; that is, the vector space which consists only of $0_{\mathcal{V}}$. If $\text{span } \mathcal{A} = \mathcal{V}$, then \mathcal{A} is said to be a *spanning set* for \mathcal{V} .

Theorem 1.3. Let $\mathcal{A} \subseteq \mathcal{V}$. Then $\text{span } \mathcal{A}$ is a subspace of \mathcal{V} .

Proposition 1.4. If \mathcal{U} is a subspace of \mathcal{V} and $\mathcal{A} \subseteq \mathcal{U}$, then $\text{span } \mathcal{A} \subseteq \mathcal{U}$.

Definition 1.5. Let $\mathcal{A} \subseteq \mathcal{V}$. The set \mathcal{A} is *linearly dependent* if there exist $m \in \mathbb{N}$, $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ and distinct vectors $v_1, \dots, v_m \in \mathcal{A}$ such that

$$\alpha_1 v_1 + \dots + \alpha_m v_m = 0_{\mathcal{V}} \quad \text{and} \quad \alpha_k \neq 0 \text{ for some } k \in \{1, \dots, m\}.$$

Remark 1.6. The definition of linear dependence is equivalent to the following statement: Let $\mathcal{A} \subseteq \mathcal{V}$. The set \mathcal{A} is linearly dependent if there exist $k \in \mathbb{N}$, $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$ and distinct $v_1, \dots, v_k \in \mathcal{A}$ such that

$$\alpha_1 v_1 + \dots + \alpha_k v_k = 0_{\mathcal{V}}.$$

Definition 1.7. Let $\mathcal{A} \subseteq \mathcal{V}$. The set \mathcal{A} is *linearly independent* if for each $m \in \mathbb{N}$ and arbitrary $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ and distinct vectors $v_1, \dots, v_m \in \mathcal{A}$ we have

$$\alpha_1 v_1 + \dots + \alpha_m v_m = 0_{\mathcal{V}} \quad \text{implies} \quad \alpha_k = 0 \text{ for all } k \in \{1, \dots, m\}.$$

The empty set is by definition linearly independent.

It is an interesting exercise in mathematical logic to show that the last two definitions are formal negations of each other. Notice also that the last two definitions can briefly be stated as follows: A set $\mathcal{A} \subseteq \mathcal{V}$ is linearly dependent if there exists a nontrivial linear combination of vectors in \mathcal{A} whose value is $0_{\mathcal{V}}$. A set $\mathcal{A} \subseteq \mathcal{V}$ is linearly independent if the only linear combination whose value is $0_{\mathcal{V}}$ is the trivial linear combination.

The following proposition is an immediate consequence of the definitions.

Proposition 1.8. *Let $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{V}$. If \mathcal{A} is linearly dependent, then \mathcal{B} is linearly dependent. Equivalently, if \mathcal{B} is linearly independent, then \mathcal{A} is linearly independent.*

Proposition 1.9. *Let \mathcal{A} be a linearly independent subset of \mathcal{V} . Let $u \in \mathcal{V}$ be such that $u \notin \mathcal{A}$. Then $\mathcal{A} \cup \{u\}$ is linearly dependent if and only if $u \in \text{span } \mathcal{A}$. Equivalently, $\mathcal{A} \cup \{u\}$ is linearly independent if and only if $u \notin \text{span } \mathcal{A}$.*

Proof. Assume that $u \in \text{span } \mathcal{A}$. Then there exist $m \in \mathbb{N}, \alpha_1, \dots, \alpha_m \in \mathbb{F}$ and distinct $v_1, \dots, v_m \in \mathcal{A}$ such that $u = \sum_{j=1}^m \alpha_j v_j$. Then

$$1 \cdot u - \alpha_1 v_1 - \dots - \alpha_m v_m = 0_{\mathcal{V}}.$$

Since $1 \neq 0$ and $u, v_1, \dots, v_m \in \mathcal{A} \cup \{u\}$ this proves that $\mathcal{A} \cup \{u\}$ is linearly dependent.

Now assume that $\mathcal{A} \cup \{u\}$ is linearly dependent. Then there exist $m \in \mathbb{N}, \alpha_1, \dots, \alpha_m \in \mathbb{F}$ and distinct vectors $v_1, \dots, v_m \in \mathcal{A} \cup \{u\}$ such that

$$\alpha_1 v_1 + \dots + \alpha_m v_m = 0_{\mathcal{V}} \quad \text{and} \quad \alpha_k \neq 0 \text{ for some } k \in \{1, \dots, m\}.$$

Since \mathcal{A} is linearly independent it is not possible that $v_1, \dots, v_m \in \mathcal{A}$. Thus, $u \in \{v_1, \dots, v_m\}$. Hence $u = v_j$ for some $j \in \{1, \dots, m\}$. Again, since \mathcal{A} is linearly independent $\alpha_j = 0$ is not possible. Thus $\alpha_j \neq 0$ and consequently

$$u = v_j = -\frac{1}{\alpha_j} \sum_{\substack{i=1 \\ i \neq j}}^m \alpha_i v_i. \quad \square$$

Proposition 1.10. *Let \mathcal{B} be a nonempty subset of \mathcal{V} . Then \mathcal{B} is linearly independent if and only if for every $u \in \mathcal{B}$ we have $u \notin \text{span}(\mathcal{B} \setminus \{u\})$. Equivalently, \mathcal{B} is linearly dependent if and only if there exists $u \in \mathcal{B}$ such that $u \in \text{span}(\mathcal{B} \setminus \{u\})$.*

Proof. We first prove the implication:

$$\mathcal{B} \text{ linearly independent} \quad \Rightarrow \quad \forall u \in \mathcal{B} \quad u \notin \text{span}(\mathcal{B} \setminus \{u\}).$$

Assume that \mathcal{B} is linearly independent. Let $u \in \mathcal{B}$ be arbitrary. Then $\mathcal{B} \setminus \{u\}$ is linearly independent by Proposition 1.8. Now, with $\mathcal{A} = \mathcal{B} \setminus \{u\}$, since $\mathcal{B} = \mathcal{A} \cup \{u\}$ is linearly independent, Proposition 1.9 yields that $u \notin \text{span}(\mathcal{B} \setminus \{u\})$.

To prove the converse of the displayed implication we will prove the contrapositive of the converse. (In mathematical logic the contrapositive of the

converse is called the inverse of the starting implication. Consequently, the converse and the inverse of an implication are equivalent.) That is we prove:

$$\mathcal{B} \text{ linearly dependent} \quad \Rightarrow \quad \exists u \in \mathcal{B} \text{ such that } u \in \text{span}(\mathcal{B} \setminus \{u\}).$$

Assume that \mathcal{B} is linearly dependent. Then there exist $m \in \mathbb{N}$, $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ and distinct vectors $v_1, \dots, v_m \in \mathcal{B}$ such that

$$\sum_{j=1}^m \alpha_j v_j = 0_{\mathcal{V}} \quad \text{and} \quad \alpha_k \neq 0 \text{ for some } k \in \{1, \dots, m\}.$$

Consequently,

$$v_k = -\frac{1}{\alpha_k} \sum_{\substack{j=1 \\ j \neq k}}^m \alpha_j v_j,$$

and thus $v_k \in \text{span}(\mathcal{B} \setminus \{v_k\})$. □

The following equivalence will sometimes be helpful.

Lemma 1.11. *Let \mathcal{B} be a nonempty subset of \mathcal{V} and $u \in \mathcal{B}$. Then*

$$\text{span}(\mathcal{B} \setminus \{u\}) = \text{span} \mathcal{B} \quad \Leftrightarrow \quad u \in \text{span}(\mathcal{B} \setminus \{u\}).$$

With this lemma Proposition 1.10 can be restated as

Corollary 1.12. *Let \mathcal{B} be a nonempty subset of \mathcal{V} . Then \mathcal{B} is linearly independent if and only if*

$$\text{span}(\mathcal{B} \setminus \{u\}) \subsetneq \text{span} \mathcal{B} \quad \forall u \in \mathcal{B}.$$

2. FINITE DIMENSIONAL VECTOR SPACES. BASES

Definition 2.1. A vector space \mathcal{V} over \mathbb{F} is *finite-dimensional* if there exists a finite subset \mathcal{A} of \mathcal{V} such that $\mathcal{V} = \text{span} \mathcal{A}$. A vector space which is not finite-dimensional is said to be *infinite-dimensional*.

Since the empty set is finite and since $\text{span} \emptyset = \{0_{\mathcal{V}}\}$, the trivial vector space $\{0_{\mathcal{V}}\}$ is finite-dimensional.

Definition 2.2. A linearly independent spanning set is called a *basis* of \mathcal{V} .

The next theorem shows that each finite-dimensional vector space has a basis.

Theorem 2.3. *Let \mathcal{V} be a finite-dimensional vector space over \mathbb{F} . Then \mathcal{V} has a basis.*

Proof. If \mathcal{V} is a trivial vector space its basis is the empty set. Let $\mathcal{V} \neq \{0_{\mathcal{V}}\}$ be a finite-dimensional vector space. Let \mathcal{A} be a finite subset of \mathcal{V} such that $\mathcal{V} = \text{span} \mathcal{A}$. Let $p = |\mathcal{A}|$. Set

$$\mathbb{K} = \{k \in \mathbb{N} : \exists \mathcal{C} \subseteq \mathcal{A} \text{ such that } k = |\mathcal{C}| \text{ and } \text{span} \mathcal{C} = \mathcal{V}\}.$$

Since $p \in \mathbb{K}$, \mathbb{K} is a nonempty set of positive integers. By the Well Ordering Axiom \mathbb{K} has a minimum. Set $n = \min \mathbb{K}$. By the definition of \mathbb{K} there

exists $\mathcal{B} \subseteq \mathcal{V}$ such that $|\mathcal{B}| = n$ and $\text{span } \mathcal{B} = \mathcal{V}$. Since $n = \min \mathbb{K}$ we have $n - 1 \notin \mathbb{K}$. Let $u \in \mathcal{B}$ be arbitrary. Then $|\mathcal{B} \setminus \{u\}| = n - 1$ and consequently

$$\text{span}(\mathcal{B} \setminus \{u\}) \subsetneq \mathcal{V} = \text{span } \mathcal{B}. \quad (\text{strict inclusion})$$

Corollary 1.12 implies that \mathcal{B} is linearly independent. Thus \mathcal{B} is a basis for \mathcal{V} . \square

The second proof of Theorem 2.3. If \mathcal{V} is a trivial vector space its basis is the empty set. Let $\mathcal{V} \neq \{0_{\mathcal{V}}\}$ be a finite-dimensional vector space. Let \mathcal{A} be a finite subset of \mathcal{V} such that $\mathcal{V} = \text{span } \mathcal{A}$. Let $p = |\mathcal{A}|$. Set

$$\mathbb{K} = \{|\mathcal{C}| : \mathcal{C} \subseteq \mathcal{A} \text{ and } \mathcal{C} \text{ is linearly independent}\}.$$

We first prove that $1 \in \mathbb{K}$. Since $\mathcal{V} \neq \{0_{\mathcal{V}}\}$ there exists $v \in \mathcal{A}$ such that $v \neq 0_{\mathcal{V}}$. Set $\mathcal{C} = \{v\}$. Then clearly $\mathcal{C} \subseteq \mathcal{A}$ and \mathcal{C} is linearly independent. Thus $|\mathcal{C}| = 1 \in \mathbb{K}$.

If $\mathcal{C} \subseteq \mathcal{A}$, then $|\mathcal{C}| \leq |\mathcal{A}| = p$. Thus $\mathbb{K} \subseteq \{0, 1, \dots, p\}$. As a subset of a finite set the set \mathbb{K} is finite. Thus \mathbb{K} has a maximum. Set $n = \max \mathbb{K}$. Since $n \in \mathbb{K}$ there exists $\mathcal{B} \subseteq \mathcal{A}$ such that \mathcal{B} is linearly independent and $n = |\mathcal{B}|$.

Next we will prove that $\text{span } \mathcal{B} = \mathcal{V}$. In fact we will prove that $\mathcal{A} \subseteq \text{span } \mathcal{B}$. If $\mathcal{B} = \mathcal{A}$, then this is trivial. So Assume that $\mathcal{B} \subsetneq \mathcal{A}$ and let $u \in \mathcal{A} \setminus \mathcal{B}$ be arbitrary. Then

$$|\mathcal{B} \cup \{u\}| = n + 1 \quad \text{and} \quad \mathcal{B} \cup \{u\} \subseteq \mathcal{A}.$$

Since $n = \max \mathbb{K}$, $n + 1 \notin \mathbb{K}$. Therefore $\mathcal{B} \cup \{u\}$ is linearly dependent. By Proposition 1.9 $u \in \text{span } \mathcal{B}$. Hence $\mathcal{A} \subseteq \text{span } \mathcal{B}$. By Proposition 1.4, $\mathcal{V} = \text{span } \mathcal{A} \subseteq \text{span } \mathcal{B}$. Since $\text{span } \mathcal{B} \subseteq \mathcal{V}$ is obvious, we proved that $\text{span } \mathcal{B} = \mathcal{V}$. This proves that \mathcal{B} is a basis of \mathcal{V} . \square

The third proof of Theorem 2.3. We will reformulate Theorem 2.3 so that we can use the Mathematical induction. Let n be a nonnegative integer. Denote by $P(n)$ the following statement: If $\mathcal{V} = \text{span } \mathcal{A}$ and $|\mathcal{A}| = n$, then there exists linearly independent set $\mathcal{B} \subseteq \mathcal{A}$ such that $\mathcal{V} = \text{span } \mathcal{B}$.

First we prove that $P(0)$ is true. Assume that $\mathcal{V} = \text{span } \mathcal{A}$ and $|\mathcal{A}| = 0$. Then $\mathcal{A} = \emptyset$. Since \emptyset is linearly independent we can take $\mathcal{B} = \mathcal{A} = \emptyset$.

Now let k be an arbitrary nonnegative integer and assume that $P(k)$ is true. That is we assume that the following implication is true: If $\mathcal{U} = \text{span } \mathcal{C}$ and $|\mathcal{C}| = k$, then there exists linearly independent set $\mathcal{D} \subseteq \mathcal{C}$ such that $\mathcal{U} = \text{span } \mathcal{D}$. This is the inductive hypothesis.

Next we will prove that $P(k + 1)$ is true. Assume that $\mathcal{V} = \text{span } \mathcal{A}$ and $|\mathcal{A}| = k + 1$. Let $u \in \mathcal{A}$ be arbitrary. Set $\mathcal{C} = \mathcal{A} \setminus \{u\}$. Then $|\mathcal{C}| = k$. Set $\mathcal{U} = \text{span } \mathcal{C}$. The inductive hypothesis $P(k)$ applies to the vector space \mathcal{U} . Thus we conclude that there exists a linearly independent set $\mathcal{D} \subseteq \mathcal{C}$ such that $\mathcal{U} = \text{span } \mathcal{D}$.

We distinguish two cases: Case 1. $u \in \mathcal{U} = \text{span } \mathcal{C}$ and Case 2. $u \notin \mathcal{U} = \text{span } \mathcal{C}$. In Case 1 we have $\mathcal{A} \subseteq \text{span } \mathcal{C}$. Therefore, by Proposition 1.4, $\mathcal{V} = \text{span } \mathcal{A} \subseteq \mathcal{U} \subseteq \mathcal{V}$. Thus $\mathcal{V} = \mathcal{U}$ and we can take $\mathcal{B} = \mathcal{D}$ in this case. In Case 2, $u \notin \mathcal{U} = \text{span } \mathcal{D}$. Since \mathcal{D} is linearly independent Proposition 1.9

yields that $\mathcal{D} \cup \{u\}$ is linearly independent. Set $\mathcal{B} = \mathcal{D} \cup \{u\}$. Since $\mathcal{U} = \text{span}\mathcal{C} = \text{span}\mathcal{D} \subseteq \text{span}\mathcal{B}$ we have that $\mathcal{C} \subseteq \text{span}\mathcal{B}$. Clearly $u \in \text{span}\mathcal{B}$. Consequently, $\mathcal{A} \subseteq \text{span}\mathcal{B}$. By Proposition 1.4 $\mathcal{V} = \text{span}\mathcal{A} \subseteq \text{span}\mathcal{B} \subseteq \mathcal{V}$. Thus $\mathcal{V} = \text{span}\mathcal{B}$. As proved earlier \mathcal{B} is linearly independent and $\mathcal{B} \subseteq \mathcal{A}$. This proves $P(k+1)$ and completes the proof. \square

Notice that in the proof of Theorem 2.3 we have proved the following proposition.

Proposition 2.4. *Let \mathcal{V} be a vector space over \mathbb{F} and let $\mathcal{A} \subseteq \mathcal{V}$ be a finite subset of \mathcal{V} such that $\mathcal{V} = \text{span}\mathcal{A}$. Then there exists a basis \mathcal{B} for \mathcal{V} such that $\mathcal{B} \subseteq \mathcal{A}$.*

3. DIMENSION

Theorem 3.1 (The Steinitz exchange lemma). *Let \mathcal{V} be a vector space over \mathbb{F} . Let \mathcal{A} and \mathcal{B} be finite subsets of \mathcal{V} such that \mathcal{A} spans \mathcal{V} and \mathcal{B} is linearly independent. Then $|\mathcal{B}| \leq |\mathcal{A}|$ and there exists $\mathcal{C} \subseteq \mathcal{A}$ such that $|\mathcal{C}| = |\mathcal{A}| - |\mathcal{B}|$ and $\mathcal{B} \cup \mathcal{C}$ spans \mathcal{V} .*

Proof. Let $\mathcal{A} \subseteq \mathcal{V}$ be a finite spanning set for \mathcal{V} such that $|\mathcal{A}| = p$.

The proof is by mathematical induction on $m = |\mathcal{B}|$. Since the empty set is linearly independent the statement is true for $m = 0$. The statement is trivially true in this case. (You should do a proof of the case $m = 1$ as an exercise.)

Now let k be an arbitrary nonnegative integer and assume that the following statement (the inductive hypothesis) is true: If $\mathcal{D} \subseteq \mathcal{V}$ is a linearly independent set such that $|\mathcal{D}| = k$, then $k \leq p$ and there exists $\mathcal{E} \subseteq \mathcal{A}$ such that $|\mathcal{E}| = p - k$ and $\mathcal{D} \cup \mathcal{E}$ is a spanning set for \mathcal{V} .

To prove the inductive step we will prove the following statement: If $\mathcal{B} \subseteq \mathcal{V}$ is a linearly independent set such that $|\mathcal{B}| = k + 1$, then $k + 1 \leq p$ and there exists $\mathcal{C} \subseteq \mathcal{A}$ such that $|\mathcal{C}| = p - k - 1$ and $\mathcal{B} \cup \mathcal{C}$ is a spanning set for \mathcal{V} .

Assume that $\mathcal{B} \subseteq \mathcal{V}$ is a linearly independent set such that $|\mathcal{B}| = k + 1$. Let $u \in \mathcal{B}$ be arbitrary. Set $\mathcal{D} = \mathcal{B} \setminus \{u\}$. Since $\mathcal{B} = \mathcal{D} \cup \{u\}$ is linearly independent, by Proposition 1.10 we have $u \notin \text{span}\mathcal{D}$. Also, \mathcal{D} is linearly independent and $|\mathcal{D}| = k$. The inductive hypothesis implies that $k \leq p$ and there exists $\mathcal{E} \subseteq \mathcal{A}$ such that $|\mathcal{E}| = p - k$ and $\mathcal{D} \cup \mathcal{E}$ is a spanning set for \mathcal{V} . Since $\mathcal{D} \cup \mathcal{E}$ is a spanning set for \mathcal{V} and $u \in \mathcal{V}$, u can be written as a linear combination of vectors in $\mathcal{D} \cup \mathcal{E}$. But, as we noticed earlier, $u \notin \text{span}\mathcal{D}$. Thus, $\mathcal{E} \neq \emptyset$. Hence, $p - k = |\mathcal{E}| \geq 1$. Consequently, $k + 1 \leq p$ is proved. Since $u \in \text{span}(\mathcal{D} \cup \mathcal{E})$, there exist $i, j \in \mathbb{N}$ and $u_1, \dots, u_i \in \mathcal{D}$ and $v_1, \dots, v_j \in \mathcal{E}$ and $\alpha_1, \dots, \alpha_i, \beta_1, \dots, \beta_j \in \mathbb{F}$ such that

$$u = \alpha_1 u_1 + \dots + \alpha_i u_i + \beta_1 v_1 + \dots + \beta_j v_j.$$

(If $\mathcal{D} = \emptyset$, then $i = 0$ and the vectors from \mathcal{D} are not present in the above linear combination.) Since $u \notin \text{span}\mathcal{D}$ at least one of $\beta_1, \dots, \beta_j \in \mathbb{F}$ is

nonzero. But, by dropping v -s with zero coefficients we can assume that all $\beta_1, \dots, \beta_j \in \mathbb{F}$ are nonzero. Then

$$v_1 = \frac{1}{\beta_1}(u - \alpha_1 u_1 - \dots - \alpha_i u_i - \beta_2 v_2 - \dots - \beta_j v_j).$$

Now set $\mathcal{C} = \mathcal{E} \setminus \{v_1\}$. Then $|\mathcal{C}| = p - k - 1$. Notice that $u, u_1, \dots, u_i \in \mathcal{B}$ and $v_2, \dots, v_j \in \mathcal{C}$; so the last displayed equality implies that $v_1 \in \text{span}(\mathcal{B} \cup \mathcal{C})$. Since $\mathcal{E} = \mathcal{C} \cup \{v_1\}$ and $\mathcal{D} \subseteq \mathcal{B}$, it follows that $\mathcal{D} \cup \mathcal{E} \subseteq \text{span}(\mathcal{B} \cup \mathcal{C})$. Therefore,

$$\mathcal{V} = \text{span}(\mathcal{D} \cup \mathcal{E}) \subseteq \text{span}(\mathcal{B} \cup \mathcal{C}).$$

Hence, $\text{span}(\mathcal{B} \cup \mathcal{C}) = \mathcal{V}$ and the proof is complete. \square

The following corollary is a direct logical consequence of the Steinitz exchange lemma. It is in fact a partial contrapositive of the lemma.

Corollary 3.2. *Let \mathcal{B} be a finite subset of \mathcal{V} . If \mathcal{V} is a finite-dimensional vector space over \mathbb{F} , then there exists $p \in \mathbb{N}$ such that $|\mathcal{B}| > p$ implies \mathcal{B} is linearly dependent.*

Proof. Assume that \mathcal{B} is a finite subset of \mathcal{V} and \mathcal{V} is a finite-dimensional vector space over \mathbb{F} . Then there exists a finite subset \mathcal{A} of \mathcal{V} such that $\mathcal{V} = \text{span } \mathcal{A}$. Set $p = |\mathcal{A}|$. Then the Steinitz exchange lemma yields the following implication: If \mathcal{B} is linearly independent, then $|\mathcal{B}| \leq p$. The contrapositive of the last implication is the claim of the corollary. \square

Corollary 3.3. *Let \mathcal{V} be a finite-dimensional vector space over \mathbb{F} . If \mathcal{C} is an infinite subset of \mathcal{V} , then \mathcal{C} is linearly dependent.*

Proof. Let $p \in \mathbb{N}$ be a number whose existence has been proved in Corollary 3.2. Let \mathcal{C} be an infinite subset of \mathcal{V} . Since \mathcal{C} is infinite it has a finite subset \mathcal{A} such that $|\mathcal{A}| = p + 1$. Corollary 3.2 yields that \mathcal{A} is linearly dependent. Since $\mathcal{A} \subseteq \mathcal{C}$, by Proposition 1.8, \mathcal{C} is linearly dependent. \square

Theorem 3.4. *Let \mathcal{V} be a finite-dimensional vector space and let \mathcal{B} and \mathcal{C} be bases of \mathcal{V} . Then both \mathcal{B} and \mathcal{C} are finite sets and $|\mathcal{B}| = |\mathcal{C}|$.*

Proof. Let \mathcal{B} and \mathcal{C} be bases of \mathcal{V} . Since both \mathcal{B} and \mathcal{C} are linearly independent Corollary 3.3 implies that they are finite. Now we can apply the Steinitz exchange lemma to the finite spanning set \mathcal{B} and the finite linearly independent set \mathcal{C} . We conclude that $|\mathcal{C}| \leq |\mathcal{B}|$. Applying again the Steinitz exchange lemma to the finite spanning set \mathcal{C} and the finite linearly independent set \mathcal{B} we conclude that $|\mathcal{B}| \leq |\mathcal{C}|$. Thus $|\mathcal{B}| = |\mathcal{C}|$. \square

Definition 3.5. The *dimension* of a finite-dimensional vector space is the number of vectors in its basis. The dimension of a vector space \mathcal{V} is denoted by $\dim \mathcal{V}$.

The following corollary restates a part of Theorem 3.1 in terms of the dimension.

Corollary 3.6. *Let \mathcal{V} be a finite-dimensional vector space over \mathbb{F} . Let \mathcal{A} and \mathcal{B} be finite subsets of \mathcal{V} . The following statements hold.*

- (a) *If $\text{span } \mathcal{A} = \mathcal{V}$, then $|\mathcal{A}| \geq \dim \mathcal{V}$.*
- (b) *If \mathcal{B} is linearly independent, then $|\mathcal{B}| \leq \dim \mathcal{V}$.*
- (c) *If $|\mathcal{A}| < \dim \mathcal{V}$, then $\text{span } \mathcal{A} \subsetneq \mathcal{V}$.*
- (d) *If $|\mathcal{B}| > \dim \mathcal{V}$, then \mathcal{B} is linearly dependent.*

Proposition 3.7. *Let \mathcal{V} be a finite-dimensional vector space over \mathbb{F} and let \mathcal{B} be a finite subset of \mathcal{V} . Then any two of the following three statements imply the remaining one.*

- (a) $|\mathcal{B}| = \dim \mathcal{V}$.
- (b) $\text{span } \mathcal{B} = \mathcal{V}$.
- (c) \mathcal{B} is linearly independent.

Proof. The easiest implication is: (b) and (c) imply (a). This is the definition of the dimension.

Next we prove the implication (a) and (b) imply (c). Assume (a) and (b). If \mathcal{B} is an empty set, then by definition it is linearly independent, that is (c) holds in this case. Assume now that $\mathcal{B} \neq \emptyset$. Let $u \in \mathcal{B}$ be arbitrary. Then $|\mathcal{B} \setminus \{u\}| < \dim \mathcal{V}$, so Corollary 3.6(c) yields $\text{span}(\mathcal{B} \setminus \{u\}) \subsetneq \mathcal{V}$. Hence, for every $u \in \mathcal{B}$ we have that $\text{span}(\mathcal{B} \setminus \{u\}) \subsetneq \text{span } \mathcal{B}$, which, by Proposition 1.10, implies that \mathcal{B} is linearly independent.

Now assume (a) and (c). Let \mathcal{A} be a basis of \mathcal{V} . By the Steinitz exchange lemma there exists $\mathcal{C} \subseteq \mathcal{A}$ such that $|\mathcal{C}| = |\mathcal{A}| - |\mathcal{B}| = 0$ and $\text{span}(\mathcal{B} \cup \mathcal{C}) = \mathcal{V}$. Since $\mathcal{C} = \emptyset$, (b) follows. \square

Remark 3.8. Notice that Corollary 3.6(a) and Proposition 3.7 imply that a finite spanning set for \mathcal{V} is a basis if and only if it has the smallest possible cardinality. Similarly, Corollary 3.6(b) and Proposition 3.7 imply that in a finite-dimensional vector space a linearly independent subset is a basis if and only if it has the largest possible cardinality.

In the following proposition we characterize infinite-dimensional vector spaces.

Proposition 3.9. *Let \mathcal{V} be a vector space over \mathbb{F} . Set $\mathcal{A}_0 = \emptyset$. The following statements are equivalent.*

- (a) *The vector space \mathcal{V} over \mathbb{F} is infinite-dimensional.*
- (b) *For every $n \in \mathbb{N}$ there exists linearly independent set $\mathcal{A}_n \subseteq \mathcal{V}$ such that $|\mathcal{A}_n| = n$ and $\mathcal{A}_{n-1} \subsetneq \mathcal{A}_n$.*
- (c) *There exists an infinite linearly independent subset of \mathcal{V} .*

Proof. We first prove (a) \Rightarrow (b). Assume (a). For $n \in \mathbb{N}$, denote by $P(n)$ the following statement:

There exists linearly independent set $\mathcal{A}_n \subseteq \mathcal{V}$ such that $|\mathcal{A}_n| = n$ and $\mathcal{A}_{n-1} \subsetneq \mathcal{A}_n$.

We will prove that $P(n)$ holds for every $n \in \mathbb{N}$. Mathematical induction is a natural tool here. Since the space $\{0_{\mathcal{V}}\}$ is finite-dimensional, we have $\mathcal{V} \neq \{0_{\mathcal{V}}\}$. Therefore there exists $v \in \mathcal{V}$ such that $v \neq 0_{\mathcal{V}}$. Set $\mathcal{A}_1 = \{v\}$ and the proof of $P(1)$ is complete. Let $k \in \mathbb{N}$ and assume that $P(k)$ holds. That is assume that there exists linearly independent set $\mathcal{A}_k \subseteq \mathcal{V}$ such that $|\mathcal{A}_k| = k$. Since \mathcal{V} is an infinite-dimensional, $\text{span } \mathcal{A}_k$ is a proper subset of \mathcal{V} . Therefore there exists $u \in \mathcal{V}$ such that $u \notin \text{span } \mathcal{A}_k$. Since \mathcal{A}_k is also linearly independent, Proposition 1.9 implies that $\mathcal{A}_k \cup \{u\}$ is linearly independent. Set $\mathcal{A}_{k+1} = \mathcal{A}_k \cup \{u\}$. Then, since $|\mathcal{A}_{k+1}| = k + 1$ and $\mathcal{A}_k \subset \mathcal{A}_{k+1}$, the statement $P(k + 1)$ is proved. This proves (b).

Now we prove (b) \Rightarrow (c). Assume (b) and set $\mathcal{C} = \cup\{\mathcal{A}_n : n \in \mathbb{N}\}$. Then \mathcal{C} is infinite. To prove that \mathcal{C} is linearly independent, let $m \in \mathbb{N}$ be arbitrary and let v_1, \dots, v_m be distinct vectors in \mathcal{C} and let $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ such that

$$\alpha_1 v_1 + \dots + \alpha_m v_m = 0_{\mathcal{V}}.$$

By the definition of \mathcal{C} , for every $k \in \{1, \dots, m\}$ there exists $n_k \in \mathbb{N}$ such that $v_k \in \mathcal{A}_{n_k}$. Set $q = \max\{n_k : k \in \{1, \dots, m\}\}$. By the inclusion property of the sequence \mathcal{A}_n , we have $\mathcal{A}_{n_k} \subseteq \mathcal{A}_q$ for all $k \in \{1, \dots, m\}$. Therefore, $v_k \in \mathcal{A}_q$ for all $k \in \{1, \dots, m\}$. Since the set \mathcal{A}_q is linearly independent we conclude that $\alpha_k = 0_{\mathbb{F}}$ for all $k \in \{1, \dots, m\}$. This proves (c).

The implication (c) \Rightarrow (a) is a partial contrapositive of Corollary 3.3. This completes the proof. \square

4. SUBSPACES

Proposition 4.1. *Let \mathcal{U} be a subspace of \mathcal{V} . If \mathcal{U} is infinite-dimensional, then \mathcal{V} is infinite-dimensional. Equivalently, if \mathcal{V} is finite-dimensional, then \mathcal{U} is finite-dimensional. (In plain English, every subspace of a finite-dimensional vector space is finite-dimensional.)*

Proof. Assume that \mathcal{U} is infinite-dimensional. Then, by the sufficient part of Proposition 3.9, for every $n \in \mathbb{N}$ there exists $\mathcal{A} \subseteq \mathcal{U}$ such that $|\mathcal{A}| = n$ and \mathcal{A} is linearly independent. Since $\mathcal{U} \subseteq \mathcal{V}$, we have that for every $n \in \mathbb{N}$ there exists $\mathcal{A} \subseteq \mathcal{V}$ such that $|\mathcal{A}| = n$ and \mathcal{A} is linearly independent. Now by the necessary part of Proposition 3.9 we conclude that \mathcal{V} is infinite-dimensional. \square

Theorem 4.2. *Let \mathcal{V} be a finite-dimensional vector space and let \mathcal{U} be a subspace of \mathcal{V} . Then there exists a subspace \mathcal{W} of \mathcal{V} such that $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$.*

Proof. Let \mathcal{B} be a basis of \mathcal{V} and let \mathcal{A} a basis of \mathcal{U} . By Proposition 4.1, the Steinitz exchange lemma applies to the finite spanning set \mathcal{B} and the finite linearly independent set \mathcal{A} . Consequently, there exists $\mathcal{C} \subseteq \mathcal{B}$ such that $|\mathcal{C}| = |\mathcal{B}| - |\mathcal{A}|$ and such that $\text{span}(\mathcal{A} \cup \mathcal{C}) = \mathcal{V}$. Applying the Steinitz exchange lemma again to the linearly independent set \mathcal{B} and the spanning set $\mathcal{A} \cup \mathcal{C}$ we conclude that $|\mathcal{A} \cup \mathcal{C}| \geq |\mathcal{B}|$. Since clearly $|\mathcal{A} \cup \mathcal{C}| \leq |\mathcal{A}| + |\mathcal{C}| = |\mathcal{B}|$ we have $|\mathcal{A} \cup \mathcal{C}| = |\mathcal{A}| + |\mathcal{C}| = |\mathcal{B}| = \dim \mathcal{V}$. Now the statement (a) and

(b) imply (c) from Proposition 3.7 yields that $\mathcal{A} \cup \mathcal{C}$ is a basis of \mathcal{V} . Set $\mathcal{W} = \text{span } \mathcal{C}$. Then, since $\mathcal{A} \cup \mathcal{C}$ is a basis of \mathcal{V} , $\mathcal{V} = \mathcal{U} + \mathcal{W}$. It is not difficult to show that $\mathcal{U} \cap \mathcal{W} = \{0_{\mathcal{V}}\}$. Thus $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$. This proves the theorem. \square

Lemma 4.3. *Let \mathcal{V} be a finite-dimensional vector space and let \mathcal{U} and \mathcal{W} be subspaces of \mathcal{V} such that $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$. Then $\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{W}$.*

Proof. Let \mathcal{A} and \mathcal{B} be basis of \mathcal{U} and \mathcal{W} respectively. Using $\mathcal{V} = \mathcal{U} + \mathcal{W}$, it can be proved that $\mathcal{A} \cup \mathcal{B}$ spans \mathcal{V} . Using $\mathcal{U} \cap \mathcal{W} = \{0_{\mathcal{V}}\}$, it can be shown that $\mathcal{A} \cup \mathcal{B}$ is linearly independent and $\mathcal{A} \cap \mathcal{B} = \emptyset$. Therefore $\mathcal{A} \cup \mathcal{B}$ is a basis of \mathcal{V} and consequently $\dim \mathcal{V} = |\mathcal{A} \cup \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}| = \dim \mathcal{U} + \dim \mathcal{W}$. \square

Theorem 4.4. *Let \mathcal{V} be a finite-dimensional vector space and let \mathcal{U} and \mathcal{W} be subspaces of \mathcal{V} such that $\mathcal{V} = \mathcal{U} + \mathcal{W}$. Then*

$$\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{W} - \dim(\mathcal{U} \cap \mathcal{W}).$$

Proof. Since $\mathcal{U} \cap \mathcal{W}$ is a subspace of \mathcal{U} , Theorem 4.2 implies that there exists a subspace \mathcal{U}_1 of \mathcal{U} such that

$$\mathcal{U} = \mathcal{U}_1 \oplus (\mathcal{U} \cap \mathcal{W}) \quad \text{and} \quad \dim \mathcal{U} = \dim \mathcal{U}_1 + \dim(\mathcal{U} \cap \mathcal{W}).$$

Similarly, there exists a subspace \mathcal{W}_1 of \mathcal{W} such that $\mathcal{W} = \mathcal{W}_1 \oplus (\mathcal{U} \cap \mathcal{W})$ and $\dim \mathcal{W} = \dim \mathcal{W}_1 + \dim(\mathcal{U} \cap \mathcal{W})$. Next we will prove that $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}_1$. Let $v \in \mathcal{V}$ be arbitrary. Since $\mathcal{V} = \mathcal{U} + \mathcal{W}$ there exist $u \in \mathcal{U}$ and $w \in \mathcal{W}$ such that $v = u + w$. Since $\mathcal{W} = \mathcal{W}_1 \oplus (\mathcal{U} \cap \mathcal{W})$ there exist $w_1 \in \mathcal{W}_1$ and $x \in \mathcal{U} \cap \mathcal{W}$ such that $w = w_1 + x$. Then $v = u + w_1 + x = (u + x) + w_1$. Since $u + x \in \mathcal{U}$ this proves that $\mathcal{V} = \mathcal{U} + \mathcal{W}_1$. Clearly $\mathcal{U} \cap \mathcal{W}_1 \subseteq \mathcal{U} \cap \mathcal{W}$ and $\mathcal{U} \cap \mathcal{W}_1 \subseteq \mathcal{W}_1$. Thus,

$$\mathcal{U} \cap \mathcal{W}_1 \subseteq (\mathcal{U} \cap \mathcal{W}) \cap \mathcal{W}_1 = \{0_{\mathcal{V}}\}.$$

Hence, $\mathcal{U} \cap \mathcal{W}_1 = \{0_{\mathcal{V}}\}$. This proves $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}_1$. By Lemma 4.3, $\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{W}_1 = \dim \mathcal{U} + \dim \mathcal{W} - \dim(\mathcal{U} \cap \mathcal{W})$. This completes the proof. \square

Combining the previous theorem and Lemma 4.3 we get the following corollary.

Corollary 4.5. *Let \mathcal{V} be a finite-dimensional vector space and let \mathcal{U} and \mathcal{W} be subspaces of \mathcal{V} such that $\mathcal{V} = \mathcal{U} + \mathcal{W}$. Then the sum $\mathcal{U} + \mathcal{W}$ is direct if and only if $\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{W}$.*

The previous corollary holds for any number of subspaces of \mathcal{V} . The proof is by mathematical induction on the number of subspaces.

Proposition 4.6. *Let \mathcal{V} be a finite-dimensional vector space and let $\mathcal{U}_1, \dots, \mathcal{U}_m$ be subspaces of \mathcal{V} such that $\mathcal{V} = \mathcal{U}_1 + \dots + \mathcal{U}_m$. Then the sum $\mathcal{U}_1 + \dots + \mathcal{U}_m$ is direct if and only if $\dim \mathcal{V} = \dim \mathcal{U}_1 + \dots + \dim \mathcal{U}_m$.*

5. PROBLEMS

Problem 5.1. Prove that \mathcal{V} is finite dimensional if and only if all linearly independent subsets of \mathcal{V} are finite. (Give a complete proof without citing propositions in this section. You can, of course, use ideas utilized in the proofs of this section.)

Problem 5.2. Let \mathcal{V} be a finite-dimensional nonzero vector space \mathcal{V} over a scalar field \mathbb{F} . Let $n = \dim \mathcal{V}$ and let $\{v_1, \dots, v_n\}$ be a basis of \mathcal{V} . Let \mathcal{U} and \mathcal{W} be subspaces of \mathcal{V} such that \mathcal{V} is a direct sum of \mathcal{U} and \mathcal{W} , that is

$$\mathcal{V} = \mathcal{U} \oplus \mathcal{W}.$$

Let

$$v_k = u_k + w_k, \quad \text{where } u_k \in \mathcal{U}, \quad w_k \in \mathcal{W} \text{ for all } k \in \{1, \dots, n\}.$$

Prove that there exist subsets \mathbb{A} and \mathbb{B} of $\{1, \dots, n\}$ such that:

$$\{1, \dots, n\} = \mathbb{A} \cup \mathbb{B} \quad \text{and} \quad \mathbb{A} \cap \mathbb{B} = \emptyset$$

and

$$\{u_k : k \in \mathbb{A}\} \text{ is a basis for } \mathcal{U} \quad \text{and} \quad \{w_k : k \in \mathbb{B}\} \text{ is a basis for } \mathcal{W}.$$