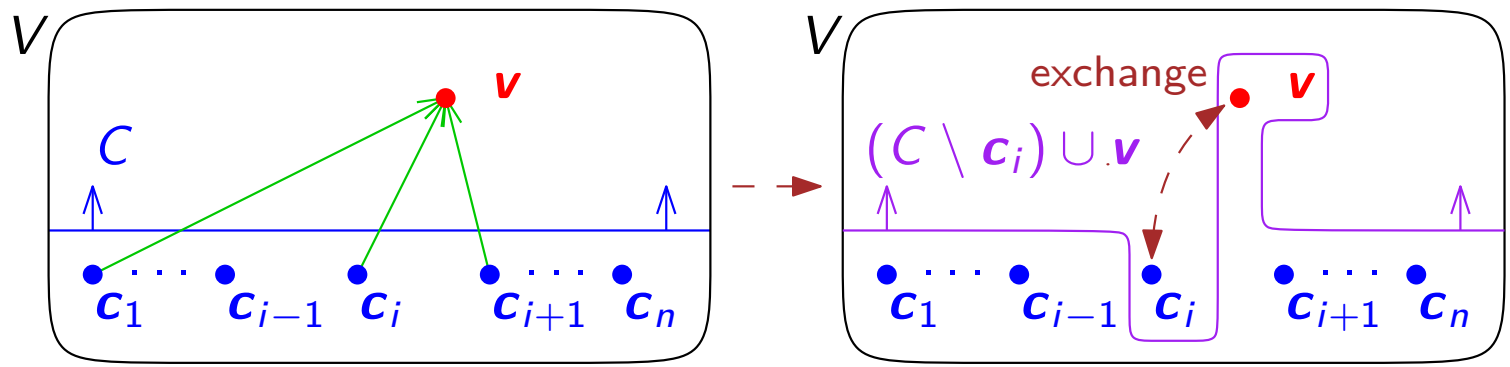
# Exchange lemma

Lemma: Let $C$ generate a vector space $V$ over $F$, $\boldsymbol{c} \in C$ and $\boldsymbol{v} \in V$. If $\boldsymbol{v}$ can be written as a linear combination of vectors from $C$ with a nonzero coefficient by $\boldsymbol{c}$, then $(C \setminus \boldsymbol{c}) \cup \boldsymbol{v}$ generates $V$.

Formally: $\left(\boldsymbol{v} = \sum_{j=1}^{n} a_j \boldsymbol{c}_j \wedge a_i \neq 0\right) \Rightarrow \mathrm{span}((C \setminus \boldsymbol{c}_i) \cup \boldsymbol{v}) = V$




$$\boldsymbol{v} = \sum_{j=1}^{n} a_j \boldsymbol{c}_j \wedge a_i \neq 0$$

The $\boldsymbol{c}$ in the lemma is $\boldsymbol{c}_i$ in the formula and also in the figure.

Example: An elementary row operation corresponds to an exchange by the lemma in the *row space*, generated by rows of the matrix. (Formally, their transpositions, since we use column vectors.)

# Exchange lemma

Lemma: Let $C$ generate a vector space $V$ over $F$, $\boldsymbol{c} \in C$ and $\boldsymbol{v} \in V$. If $\boldsymbol{v}$ can be written as a linear combination of vectors from $C$ with a nonzero coefficient by $\boldsymbol{c}$, then $(C \setminus \boldsymbol{c}) \cup \boldsymbol{v}$ generates $V$.

Example: For the space $V = \mathbb{R}^3$, a system of generators

$$C = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_4\} = \{(1,0,0)^\mathsf{T}, (0,1,0)^\mathsf{T}, (0,0,1)^\mathsf{T}, (1,1,0)^\mathsf{T}\}$$

and vectors $\boldsymbol{v} = (1,1,1)^\mathsf{T}$, $\boldsymbol{v}' = (2,1,0)^\mathsf{T}$.

If we express: $(1,1,1)^\mathsf{T} = (1,0,0)^\mathsf{T} + (0,1,0)^\mathsf{T} + (0,0,1)^\mathsf{T}$, we see that $\boldsymbol{v}$ could be exchanged with any of $\boldsymbol{c}_1$, $\boldsymbol{c}_2$ or $\boldsymbol{c}_3$.

Similarly, if we express: $(1,1,1)^\mathsf{T} = (1,1,0)^\mathsf{T} + (0,0,1)^\mathsf{T}$, we see that $\boldsymbol{v}$ could also be exchanged with $\boldsymbol{c}_4$.

Any combination $a_1\boldsymbol{c}_1 + \cdots + a_4\boldsymbol{c}_4 = (a_1 + a_4, a_2 + a_4, a_3)^\mathsf{T}$ has the third component zero if and only if $a_3 = 0$.

Thus $\boldsymbol{v}'$ cannot be expressed as a linear combination, where $a_3$ is nonzero. We cannot exchange $\boldsymbol{c}_3$ with $\boldsymbol{v}'$ and still generate $V$.

# Exchange lemma

Lemma: Let $C$ generate a vector space $V$ over $F$, $\boldsymbol{c} \in C$ and $\boldsymbol{v} \in V$. If $\boldsymbol{v}$ can be written as a linear combination of vectors from $C$ with a nonzero coefficient by $\boldsymbol{c}$, then $(C \setminus \boldsymbol{c}) \cup \boldsymbol{v}$ generates $V$.

Formally: $\left(\boldsymbol{v} = \sum_{j=1}^{n} a_j \boldsymbol{c}_j \wedge a_i \neq 0\right) \Rightarrow \text{span}((C \setminus \boldsymbol{c}_i) \cup \boldsymbol{v}) = V$

Proof: $\boldsymbol{v} = a_1\boldsymbol{c}_1 + \cdots + a_i\boldsymbol{c}_i + \cdots + a_n\boldsymbol{c}_n \Rightarrow \boldsymbol{c}_i = \frac{1}{a_i}\left(\boldsymbol{v} - \sum_{j \neq i} a_j \boldsymbol{c}_j\right)$.

Write any $\boldsymbol{u} \in V$ as a linear combination of elements from $C$.
If $\boldsymbol{c}_i$ occurs in this combination, substitute the above for $\boldsymbol{c}_i$.
We get $\boldsymbol{u}$ as a linear combination of elements from $(C \setminus \boldsymbol{c}_i) \cup \boldsymbol{v}$
(the combination uses vectors generating $\boldsymbol{u}$ and $\boldsymbol{v}$, but not $\boldsymbol{c}_i$).

In the finite case, if $C = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n\}$ and $\boldsymbol{u} = \sum_{j=1}^{n} b_j \boldsymbol{c}_j$

then we get $\boldsymbol{u} = \frac{b_i}{a_i}\boldsymbol{v} + \sum_{j \neq i}\left(b_j - \frac{a_j b_i}{a_i}\right)\boldsymbol{c}_j$.

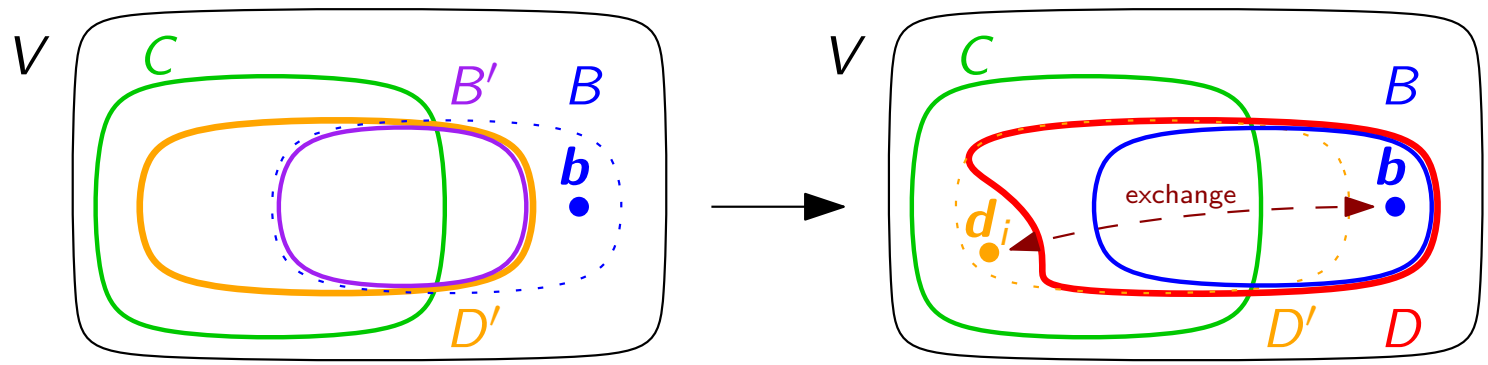
# Steinitz exchange theorem

Theorem: Let $B$ be a finite linearly independent set in a vector space $V$ and $C$ be a generating set of $V$. Then there exists $D$ s.t.:

▶ $\mathrm{span}(D) = V$ ▶ $B \subseteq D$ ▶ $|D| = |C|$ ▶ $D \setminus B \subseteq C$

Proof: By induction on $|B \setminus C|$. If $B \setminus C = \emptyset$, then $D = C$.
Otherwise choose any $\boldsymbol{b} \in B \setminus C$ and set $B' = B \setminus \boldsymbol{b}$.
As the set $B'$ is linearly independent and $|B' \setminus C| < |B \setminus C|$,
by induction hypothesis there exists $D'$ for $B'$ and $C$ such that:

▶ $\mathrm{span}(D') = V$ ▶ $B' \subseteq D'$ ▶ $|D'| = |C|$ ▶ $D' \setminus B' \subseteq C$




Express $\boldsymbol{b}$ w.r.t. $\{\boldsymbol{d}_1 \ldots, \boldsymbol{d}_n\} \subseteq D'$. As $B$ is linearly independent, $a_i \neq 0$ for some $\boldsymbol{d}_i \in D' \setminus B$. Then $D = D' \cup \boldsymbol{b} \setminus \boldsymbol{d}_i$ satisfies all four properties (the first one due to the exchange lemma).

# Example in $V = \mathbb{Z}_2^4$

The proof yields an iterative procedure where we we gradually replace the vectors $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\} = B \setminus C$ with suitable vectors from $C$, which yields a sequence $D_0 = C, D_1, \ldots, D_k = D$.

Given a linearly independent set $B = \{(1,1,0,0)^\mathsf{T}, (1,1,0,1)^\mathsf{T}\}$ and a system of generators $C = D_0 = \{(1,0,0,0)^\mathsf{T}, (0,1,0,0)^\mathsf{T}, (0,0,1,0)^\mathsf{T}, (0,0,0,1)^\mathsf{T}, (1,1,1,1)^\mathsf{T}\}$.

1. We express e.g.: $(1,1,0,0)^\mathsf{T} = (1,0,0,0)^\mathsf{T} + (0,1,0,0)^\mathsf{T}$ and exchange $(1,0,0,0)^\mathsf{T}$ with $(1,1,0,0)^\mathsf{T}$.

We have $D_1 = \{(1,1,0,0)^\mathsf{T}, (0,1,0,0)^\mathsf{T}, (0,0,1,0)^\mathsf{T}, (0,0,0,1)^\mathsf{T}, (1,1,1,1)^\mathsf{T}\}$.

2. We express e.g.: $(1,1,0,1)^\mathsf{T} = (1,1,0,0)^\mathsf{T} + (0,0,0,1)^\mathsf{T}$ and exchange $(0,0,0,1)^\mathsf{T}$ with $(1,1,0,1)^\mathsf{T}$.

We have obtained the desired set of generators $D_2 = D = \{(1,1,0,0)^\mathsf{T}, (0,1,0,0)^\mathsf{T}, (0,0,1,0)^\mathsf{T}, (1,1,0,1)^\mathsf{T}, (1,1,1,1)^\mathsf{T}\}$.

E.g. step 2. matches to the proof for $\boldsymbol{b} = (1,1,0,1)^\mathsf{T}$ and $D' = D_1$.

# Consequences of the exchange theorem

Theorem: Let $B$ be a finite linearly independent set in a vector space $V$ and $C$ be a generating set of $V$. Then there exists $Z$ s.t.:
▶ $\text{span}(D) = V$ ▶ $B \subseteq D$ ▶ $|D| = |C|$ ▶ $D \setminus B \subseteq C$

Corollary: If a vector space is finitely generated
then any linearly independent set can be extended to a basis.

Proof: It suffices to restrict $D$ to a linearly independent set while preserving $B$.

Corollary: If a vector space is finitely generated then all its bases have the same cardinality.

Proof: Consider bases $B, C$ of $V$ then:

$$\left.\begin{array}{l} B \text{ independent, } C \text{ generates } V \Rightarrow |B| \leq |C| \\ C \text{ independent, } B \text{ generates } V \Rightarrow |C| \leq |B| \end{array}\right\} \Rightarrow |C| = |B|$$

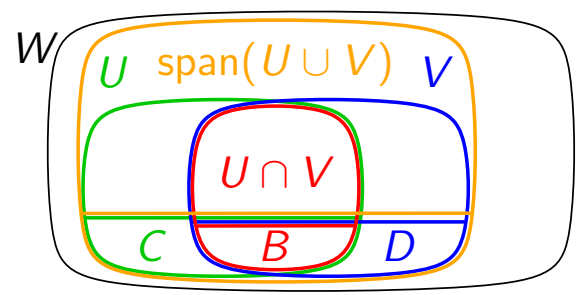
# Dimension and the intersection–sum theorem

Definition: The *dimension* of a finitely generated vector space $V$ is the cardinality of any of its bases. It is denoted by $\dim(V)$.

Examples:

- $\dim(F^n) = n$.
- A plane as a subspace of $\mathbb{R}^3$ has dimension $2$.
- The space of polynomials of degree $\leq n$ has dimension $n+1$.

Observation: If $V$ is a subspace of a finitely generated space $W$ then $\dim(V) \leq \dim(W)$




Proof: A basis of $V$ is linearly independent in $W$ and can be extended to a basis of $W$.

Theorem: If $U, V$ are subspaces of a finitely generated $W$ then $\dim(U) + \dim(V) = \dim(U \cap V) + \dim(\text{span}(U \cup V))$

Proof: Extend a basis $B$ of the intersection $U \cap V$ to a basis $C$ of $U$ as well as to a basis $D$ of $V$. Then $|C| + |D| = |B| + |C \cup D|$. Linear independence of $C \cup D$: if $\boldsymbol{v} \in \text{span}(C) \cap \text{span}(D \setminus B)$, then $\boldsymbol{v} \in U \cap V \;\Rightarrow\; [\boldsymbol{v}]_{D\setminus B} = \mathbf{0}_{|D\setminus B|} \;\Rightarrow\; \boldsymbol{v} = \mathbf{0} \;\Rightarrow\; [\boldsymbol{v}]_C = \mathbf{0}_{|C|}$.

# Questions to understand the lecture topic

- Which quantifiers and variables are omitted from the formal notation of the exchange lemma for brevity?
- Which of the required properties of the set $D$ from the exchange theorem would be violated if we performed the same procedure but did not require $B$ to be linearly independent?
- Is finiteness used in the exchange lemma?
- At what point does the proof of Steinitz's exchange theorem fail if $B$ is not finite?
- Is Steinitz's exchange theorem necessary for the uniqueness of the dimension, or does it follow from other arguments?
- The analogy (based on the principle of inclusion and exclusion) of the intersection and union theorem does not hold for three spaces. Can you find a counterexample and use it to determine a property that cannot be guaranteed for the proof?