

Here is a sketch of the proof that any two bases of a vector space are equinumerous. I couldn't find a single proof that works for both finite and infinite dimensionality. This sketch combines Van der Waerden's proof for the finite case with Zariski & Samuel's for the infinite case. The originals are shown at the end of this document.

1. For $n \in \mathbb{N}$ let $\Phi(n)$ denote the following proposition about a vector space V :
 - a. For every independent $A \subseteq V$ with n elements, and every subset $B \subseteq V$, if $A \subseteq \overline{B}$ then there is an injection $f: A \rightarrow B$ such that $\overline{A \cup (B - \text{Rng } f)} = \overline{B}$.
 - b. I'll prove $\forall n \Phi(n)$ by recursion on n , following Van der Waerden [1937] 1953, 101–102.
 - c. $\Phi(0)$ is trivial, since $n = 0$ implies $A = f = \phi$.
 - d. Assume $\Phi(n)$.
 - e. To prove: $\Phi(n + 1)$.
 - f. Given an independent $A \subseteq V$ with $n + 1$ elements, and a subset $B \subseteq V$ such that $A \subseteq \overline{B}$.
 - g. To find: an injection $f: A \rightarrow B$ such that $\overline{A \cup (B - \text{Rng } f)} = \overline{B}$.
 - h. There exists an element $a \in A$.
 - i. Let $A' = A - \{a\}$, so that
 - j. A' has n elements,
 - k. and $A' \subseteq A \subseteq \overline{B}$.
 - l. By (d) there is an injection $e: A' \rightarrow B$ such that $\overline{A' \cup (B - \text{Rng } e)} = \overline{B}$.
 - m. By (f,h), $a \in \overline{B}$.
 - n. By the finiteness principle, $a \in \overline{E}$ for some finite $E \subseteq A' \cup (B - \text{Rng } e)$; choose E as small as possible.
 - o. If $E \cap (B - \text{Rng } e) = \phi$, then $a \in \overline{A'}$, contrary to the independence of A . Thus there exists $b \in E \cap (B - \text{Rng } e)$.
 - p. $a \notin \overline{E - \{b\}}$ by the minimality of E .
 - q. $a \in \overline{E} = \overline{(E - \{b\}) \cup \{b\}}$ by (n).
 - r. By the exchange principle, $b \in \overline{(E - \{b\}) \cup \{a\}}$.
 - s. Consider $f = e \cup \{ \langle a, b \rangle \}$.
 - t. $f: A \rightarrow B$ injectively because e is injective, $a \notin \text{Dom } e$, and $b \notin \text{Rng } e$.
 - u. Every element of B depends on $A' \cup (B - \text{Rng } e)$ by (l),
 - v. and thus on $A' \cup (B - \text{Rng } f) \cup \{b\}$ by (s),
 - w. and thus on $A' \cup (B - \text{Rng } f) \cup (E - \{b\}) \cup \{a\}$
 $= A' \cup \overline{(B - \text{Rng } f) \cup \{a\}} = A \cup (B - \text{Rng } f)$ by (i,n,o,r).
 - x. Therefore $\overline{B} \subseteq \overline{A \cup (B - \text{Rng } f)}$. The reverse inclusion follows from the assumption $A \subseteq \overline{B}$.
 - y. Thus f satisfies the requirements of (g).
2. Corollaries of Van der Waerden's theorem:
 - a. If A is independent and finite and B spans V , then $\#A \leq \#B$.

- b. If A is independent and B is finite and spans V , then $\#A \leq \#B$.
- i. Proof: Apply (a) to every finite subset of A : they must all have cardinals $\leq \#B$. Were A infinite, it would have a countably infinite subset by the axiom of choice, and thus subsets of every finite cardinality. Thus A must be finite, and (a) yields the result.
- c. If A, B are bases of V and one is finite, then $\#A = \#B$.
- i. If B is finite, use (b) to get $\#A \leq \#B$, then interchange A, B to get the reverse inequality.
3. Proposition, following Zariski and Samuel 1958–1960, volume 1, 99.
- a. Suppose A spans V and B is a basis of V .
- b. To prove: $\#B \leq (\#A)\omega$.
- c. Let \mathcal{E} be the family of all nonempty finite subsets of B .
- d. By the finiteness principle, $(\forall x \in A)(\exists S \in \mathcal{E})[x \in \bar{S}]$.
- e. By the axiom of choice, there is a choice function $E \in \prod_{x \in A} \{S \in \mathcal{E} : x \in \bar{S}\}$.
- i. Zariski and Samuel presented an involved construction of E without using the axiom; but since they used it elsewhere, there's little point to that.
- f. Since $x \in \bar{E}_x$ for each $x \in A$, $A \subseteq \overline{\bigcup_{x \in A} E_x}$. Since A spans V , so does $\bigcup_{x \in A} E_x$.
- g. Since $E_x \subseteq B$ for each $x \in A$, $\bigcup_{x \in A} E_x \subseteq B$. Since B is a basis, $\bigcup_{x \in A} E_x = B$.
- h. $\#B = \#\left(\bigcup_{x \in A} E_x\right) \leq \sum_{x \in A} (\#E_x) \leq \sum_{x \in A} \omega = (\#A)\omega$.
- i. There is probably a tacit application of the axiom of choice in the second inequality here.
4. Corollaries of Zariski and Samuels's proposition:
- a. If A is infinite and spans V , and B is a basis of V , then $\#B \leq \#A$.
- i. Proof: $(\#A)\omega = \#A$.
- b. If A spans V , B is a basis of V , and B is infinite, then so is A and $\#B \leq \#A$.
- c. If A and B are bases of V , then $\#A = \#B$.
- i. Proof: if A or B is finite, use (2c); otherwise use (4a or 4c).

Van Der Waerden [1937] 1953, 101–102

DEFINITION. *Two finite sets u_1, \dots, u_n and v_1, \dots, v_s are said to be (linearly) equivalent if every v_k is linearly dependent on u_1, \dots, u_n , and every u_i on v_1, \dots, v_s .*

The equivalence definition is symmetric by definition; it is reflexive by the First Basic Theorem, and transitive by the Third Basic Theorem. If an element w is linearly dependent on one of the two equivalent sets, it is linearly dependent on the other one as well, according to the Third Basic Theorem. By the Third Corollary, every finite set is equivalent to a linearly independent subset.

FOURTH COROLLARY. (Exchange Theorem) *If v_1, \dots, v_s are linearly independent, and if every v_j is linearly dependent on u_1, \dots, u_n , then there is in the set of the u_i a subset $\{u_{i_1}, \dots, u_{i_s}\}$ of exactly s elements, which may be replaced by $\{v_1, \dots, v_s\}$ so that the system obtained from $\{u_1, \dots, u_n\}$ by this replacement is equivalent to the original set $\{u_1, \dots, u_n\}$. This implies $s \leq n$.*

PROOF. For $s=0$ the proposition is trivial; for there are no v_j , and nothing is replaced. Now suppose the theorem holds for $\{v_1, \dots, v_{s-1}\}$, and let $\{v_1, \dots, v_{s-1}\}$ be replaceable by $\{u_{i_1}, \dots, u_{i_{s-1}}\}$. This replacement gives rise to a set $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$ equivalent to $\{u_1, \dots, u_n\}$. Now, v_s is linearly dependent on $\{u_1, \dots, u_n\}$ and, therefore, on the equivalent set $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$. Thus, there is a minimal subset $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$, on which v_s still depends linearly. This minimal subset cannot consist of v_j 's only, since the v_i and v_s are linearly independent. Hence the minimal subset

contains at least one u_k which we shall call u_{i_s} . By the Second Fundamental Theorem $u_k = u_{i_s}$ is linearly dependent on the set which arises from $\{v_j, \dots, u_k\}$ by replacing u_k by v_s and, therefore, on the larger set which arises from $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$ by the replacement $u_k \rightarrow v_s$.

Let this system be $\{v_1, \dots, v_{s-1}, v_s, u_l, \dots\}$. It is equivalent to $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$ since u_k is linearly dependent on the first set, and v_s on the latter. In this manner we have carried the replacement one step further. The new set $\{v_1, \dots, v_{s-1}, v_s, u_l, \dots\}$ is equivalent to $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$, and, therefore, to the original system $\{u_1, \dots, u_n\}$.

Zariski and Samuel 1958–1960, volume 1, 99

COROLLARY 1. *If L is a transcendence set in K/k and S is a subset of K such that K is an algebraic extension of $k(S)$, then there exists a subset S' of S such that $L \cap S'$ is empty and $L \cup S'$ is a transcendence basis of K/k .*

COROLLARY 2. *Any subset S of K such that K is an algebraic extension of $k(S)$ contains a transcendence basis of K/k .*

We have only to apply Corollary 1 to the case in which L is the empty set.

COROLLARY 3. *There exist transcendence bases of K/k .*

We apply Corollary 2 for the case $S = K$.

NOTE. In the case of a vector space V over a field k , Theorem 23 guarantees the existence of a *basis* (or *vector basis*) of V over k .

The following is a generalization of Theorem 22 in I, § 21:

THEOREM 24. *Any two bases of V have the same cardinal number.*

PROOF. This theorem has been proved in I, § 21 under the assumption that there exists at least one finite basis of V . We shall therefore assume now that every basis of V is infinite.

Let B be a basis of V and let x be any element of V . By (S_2) , there exist finite subsets E of B such that $x \in s(B)$. We assert that there exists a smallest finite subset E_x of B such that $x \in s(E_x)$ (and such that any other subset E of B with the property $x \in s(E)$ contains E_x). To see this, it is sufficient to prove the following: *if E' and E'' are two subsets of B such that $x \in s(E') \cap s(E'')$ and if we have $x \notin s(E'_1)$ for every proper subset E'_1 of E' , then $E' \subset E''$.* Assuming the contrary, let y be an element of E' not in E'' and let E'_1 denote the set $E' - y$. We have $x \notin s(E'_1)$ and $x \in s(E'_1, y)$. Hence, by (S_5) , we have $y \in s(E'_1, x)$. Since $x \in s(E'')$ it follows that $y \in s(E'_1 \cup E'')$. This is in contradiction with the fact that $y \notin E'_1 \cup E''$ and that $E'_1 \cup E'' \cup \{y\} \subset B$ is a free set.

Now let B' be another basis of V . We consider the mapping $x \rightarrow E_x (x \in B', E_x \subset B)$, where E_x is the finite subset of B defined above. From set theory it is known that the cardinal number of B' is not less than the cardinal number of the set $\bigcup_{x \in B'} E_x$ (since each set E_x is finite). On the other hand, we have $B' = \bigcup_{x \in B'} E_x$ since $B' \subset s(\bigcup E_x)$, $V = s(B') = s(\bigcup E_x)$, and therefore the subset $\bigcup_{x \in B'} E_x$ of B must coincide with the basis B . Hence the cardinal number of B' is not less than the cardinal number of B . Interchanging the roles of B and B' we conclude that B and B' have the same cardinal number. Q.E.D.

As a consequence we have the following result:

THEOREM 25. *Any two transcendence bases of K/k have the same cardinal number.*