Zornin' time

Theorem. Let k be a field and V a vector space over k. Then V has a basis, i.e. a subset $B \subseteq V$ which spans V and is linearly independent.

Rmk. This is equivalent to the axiom of choice!

Proof. The finite dimensional proof inductively finds a basis. We can't induct naively on a larger infinite set, so we use Zorn as a replacement for induction.

Let $X = \{ S \subseteq V \mid S \text{ lin. indep} \}$, ordered by $\subseteq$.

Claim X is an inductive poset.

i. $X \neq \emptyset$ as $\emptyset \in X$

ii. Let $Y \subseteq X$ be a chain. Consider $T = \bigcup_{S \in Y} S$.
We claim $T \in X$, i.e. that it's lin. indep.
Indeed, let $v_1, \dots, v_n \in T$ s.t. $\sum a_i v_i = 0$.
Each v_i is in some $S_i \in Y$. As Y is totally ordered, $\exists i_0$ s.t. $S_i \subseteq S_{i_0}$ $\forall i$. So all $v_i \in S_{i_0}$, which is lin indep. Thus, T is lin indep.

Hence, by Zorn's lemma, X has a maximal element S.

We claim S is a basis. We know $S \in X$ so it's lin indep. We show that it spans V.

Indeed, let $v \in V$. If $v \in S$, then surely $v \in \operatorname{span}(S)$. Otherwise, $S < S \cup \{v\}$, so $S \cup \{v\}$ is lin. dep.

Hence, $av + \sum a_i v_i = 0$, $a, a_i \in k$ not all 0
$v_i \in S$

If $a = 0$, all $a_i = 0$ as S is lin indep.

Thus, $a \neq 0$. So $v = -\sum a^{-1} a_i v_i \in \operatorname{span}(S)$ $\square$

Rmk. This fails if k is not a field!

$\{2\} \subseteq \mathbb{Z}$ is "$\mathbb{Z}$-lin indep" but does not span!

works if k is, more generally, a division ring.

Inductive proofs occur when you can always push a step forward. Essentially the same occured here. A more evocative connection would be to use transfinite induction, but this requires ordinals.

Thm. Let V be a VS / k a field. Let B_1, B_2 be bases of V.

Then $|B_1| = |B_2|$.

Pf. WLOG $\dim V$ is infinite. The finite case is known.

Let $w \in B_2$. Then w is a unique finite linear combination of elements of B_1.

We write $w = \sum_{v \in B_1} a_v(w) v$.

Let $S_w = \{v \in B_1 \mid a_v(w) \neq 0\}$. This is a finite subset of B_1.

Claim. $B_1 = \bigcup_{w \in B_2} S_w$

Pf. "$\supseteq$" clear.

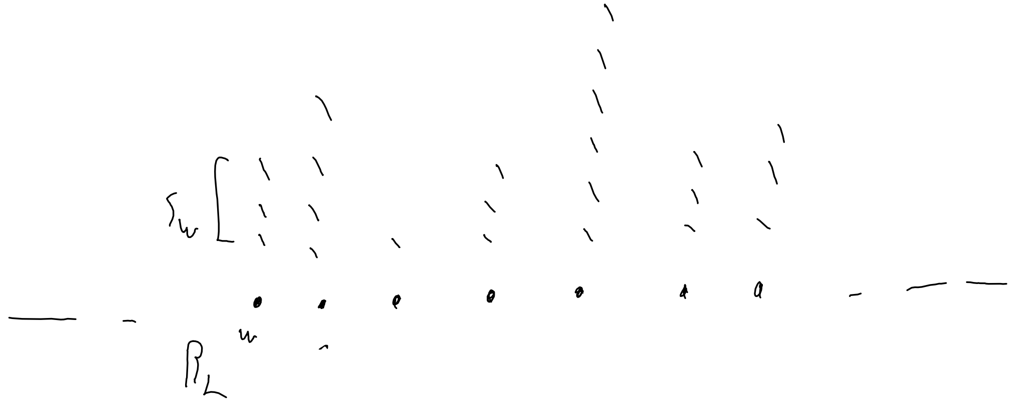
"$\subseteq$" Let $v \in B_1$. Write $v = \sum a_i w_i$, $w_i \in B_2$.

Write each $w_i = b_i v + \sum_j b_{ij} v_{ij}$, $v_{ij} \neq v$

Then $v = \sum_i a_i b_i v + \sum_{ij} a_i b_{ij} v_{ij}$

As such, $\sum_i a_i b_i = 1$, so some $a_i b_i \neq 0$, whence $b_i \neq 0$,

so $v \in S_{w_i}$. $\square$



$$|B_1| \leq \sum_{w\in B_2} |S_w| \leq \sum_{w\in B_2} |\mathbb{N}| = |B_2|\cdot|\mathbb{N}| = |B_2|$$

$$B_1 \twoheadleftarrow \bigvee_{w\in B_2} S_w \hookrightarrow \bigvee_{w\in B_2} \mathbb{N} \xleftrightarrow{\sim} B_2 \times \mathbb{N} \xleftrightarrow{\sim} B_2$$

So $|B_1| \leq |B_2|$. By symmetry, $|B_2| \leq |B_1|$. Thus, by the Cantor-Schröder-Bernstein theorem, $|B_1| = |B_2|$ □

Def. Let I be any set. We consider $\mathbb{Z}[\{x_i\}_{i\in I}]$ to be the ring of formal polynomials

$$\sum_{\substack{J \subseteq I \\ \text{finite}}} a_J x^J$$

where $a_J \in \mathbb{Z}$, $x^J = \prod_{j\in J} x_j$, and all but finitely many a_J are 0.

e.g. $|I| = n$ yields $\mathbb{Z}[x_1, \ldots, x_n]$

$|I| = 0$ yields $\mathbb{Z}$

$I = \mathbb{N}$ yields $\mathbb{Z}[x_0, x_1, x_2, \ldots]$

Lemma. For any ring R, there is a unique map $\mathbb{Z} \to R$.

Pf. Send $1 \mapsto 1$, the rest is forced by additivity. Check that this is a ring homomorphism by induction.

What is a map $\mathbb{Z}[x] \longrightarrow R$?

Lemma. Let $r \in R$. There is a unique ring homomorphism $\mathbb{Z}[x] \longrightarrow R$ sending $x \mapsto r$. Thus, $\underline{\text{Ring}}(\mathbb{Z}[x], R) \cong U(R)$, the underlying set of R.

Pf. Just check $f(x) \longmapsto f(r)$ is a ring homomorphism. Surely $(fg)(r) = f(r)g(r)$!

So we expect $\mathbb{Z}[x,y] \longrightarrow R$ to be given by 2 elts of R

$\mathbb{Z}[x,y,z] \longrightarrow R$ " " " 3 " "

etc.

Theorem. Given any set map $f: I \longrightarrow R$ $(= u(R))$, there is a unique ring homomorphism

$$\mathbb{Z}[\{x_i\}_{i\in I}] \longrightarrow R$$

sending $x_i \longmapsto f(i)$.

Pf. Let $X = \{(F,\varphi) \mid F \subseteq I,\ \varphi: \mathbb{Z}[\{x_i\}_{i\in F}] \longrightarrow R$ s.t. $\varphi(x_i) = f(i)\}$

ordered via $(F,\varphi) \leq (F',\varphi')$ if $F \subseteq F'$ and $\varphi'|_{\mathbb{Z}[\{x_i\}_{i\in F}]} = \varphi$

(can write $\varphi'|_F = \varphi$)

This is a poset. We claim it's inductive.

Indeed, let $Y \subseteq X$ be a chain.

Consider $\left(\bigcup_{(F,\varphi)\in Y} F,\ \Phi \right)$, where Φ is defined as follows.

Let $\mathcal{F} = \bigcup_{(F,\varphi)\in Y}$. Then $\mathbb{Z}[\{x_i\}_{i\in \mathcal{F}}] = \bigcup_{(F,\varphi)\in Y} \mathbb{Z}[\{x_i\}_{i\in F}]$.

To define $\Phi: \mathbb{Z}[\{x_i\}_{i\in I}] \longrightarrow R$,

we insist $\Phi\big|_{\mathbb{Z}[\{x_i\}_{i\in F}]} = \varphi$ for all $(F,\varphi)\in Y$.

This is well defined as Y is a chain.

Thus, by Zorn's lemma, $\exists\ (F,\varphi)\in Y$ maximal.

We claim that $F = I$.

Indeed, let $i_0 \in I$.

We have φ defined on x_i for all $i\in F$.

Let $S = \mathbb{Z}[\{x_i\}_{i\in F}]$.

Then we have $\varphi: S \longrightarrow R$, $\varphi(x_i) = f(i)$ $\forall i\in F$.

Define $\varphi': S[x_{i_0}] \longrightarrow R$ via

$$\sum_n s_n x_{i_0}^n \longmapsto \sum_n \varphi(s_n) f(i_0)^n$$

Then $(\varphi', F\cup\{i_0\}) \geq (\varphi, F)$, so by maximality, they are equal. Thus, $i_0\in F$ $\forall i_0\in I$, so $F = I$. $\square$

Rmk. $\underline{\text{Ring}}(\mathbb{Z}[\{x_i\}_{i\in I}], R) \cong U(R)^I = \underline{\text{Set}}(I, U(R))$.