**Theorem.** *Let $R$ be a principal ideal domain. Every submodule of a free $R$-module is free.*

*Proof.* This proof uses the well-ordering principle: for every set $J$, there is an ordering $<$ on $J$ with respect to which $J$ is well-ordered. (An ordered set is *well-ordered* if every nonempty subset has a minimal element. With the usual ordering, the set of non-negative integers is well-ordered, but $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$ are not.) The well-ordering principle is equivalent to the axiom of choice.

This proof is from *A Course in Homological Algebra* by Hilton and Stammbach.

Let $F = \bigoplus_{j\in J} R_j$ be a free module, indexed by the set $J$. Here $R_j = R$ for all $j$: the subscript is merely to indicate which summand it is. Let $M \subseteq F$ be a submodule. Assume that $J$ is well-ordered.

For $j \in J$, let

$$\overline{F}_{(j)} = \bigoplus_{i<j} R_i, \qquad F_{(j)} = \bigoplus_{i\leq j} R_i = \overline{F}_{(j)} \oplus R_j.$$

Because of the direct sum decomposition $F_{(j)} = \overline{F}_{(j)} \oplus R_j$, every element in $F_{(j)} \cap M$ may be written uniquely as $(b,r)$, where $b \in \overline{F}_{(j)}$ and $r \in R_j = R$. Define a map $f_j$ by

$$\begin{aligned} f_j : F_{(j)} \cap M &\longrightarrow R, \\ (b,r) &\longmapsto r. \end{aligned}$$

Then the kernel of $f_j$ is $\overline{F}_{(j)} \cap M$, so there is a short exact sequence

$$0 \to \overline{F}_{(j)} \cap M \to F_{(j)} \cap M \to \operatorname{im} f_j \to 0.$$

$\operatorname{im} f_j$ is an ideal in $R$, and since $R$ is a PID, $\operatorname{im} f_j = (r_j)$ for some $r_j \in R$. If $r_j \neq 0$, there is an element $c_j \in F_{(j)} \cap M$ so that $f_j(c_j) = r_j$.

Claim: $\{c_j : j \in J, r_j \neq 0\}$ is a basis for $M$.

I'll check that the elements of this set are linearly independent. Suppose that $\sum_{k=1}^n s_k c_{j_k} = 0$ for some elements $s_k \in R$, with $j_1 < \cdots < j_n$. Apply $f_{j_n}$:

$$0 = s_n f(c_{j_n}) = s_n r_n,$$

and since $R$ is a domain and $r_n$ is nonzero, then $s_n$ must be zero. By induction, each $s_k$ is zero. This proves linear independence.

Now I'll check that this set generates $M$. Assume not: then there is a smallest $i \in J$ such that there is an element $a \in F_{(i)} \cap M$ which cannot be written in terms of the elements of the set $\{c_j\}$.

Let $J' = \{j \in J : r_j \neq 0\}$ (so our potential basis is $\{c_j : j \in J'\}$). If $i \notin J'$, then the map

$$\overline{F}_{(i)} \cap M \to F_{(i)} \cap M$$

is equality, so $a \in \overline{F}_{(i)} \cap M$. But then there is a $k < i$ in $J$ so that $a \in F_{(k)} \cap M$, contradicting the minimality of $i$. Thus $i \in J'$.

Write $f_i(a)$ as $f_i(a) = sr_i$ and form $b = a - sc_i$. Since $a$ cannot be written as an $R$-linear combination of the $c_j$'s, neither can $b$. Also,

$$f_i(b) = f_i(a) - s f_i(c_i) = 0,$$

so $b \in \overline{F}_{(i)} \cap M$. This contradicts the minimality of the index $i$, and so every element of $M$ can be expressed as a linear combination of the $c_j$'s. $\square$