# 42 Invariant basis number

**42.1 Definition.** A ring $R$ has the *invariant basis number (IBN)* property if for any free $R$-module $F$ and for any bases two $B$, $B'$ of $F$ we have $|B| = |B'|$.

**42.2 Definition.** If a ring $R$ has IBN then for a free $R$-module $F$ the *rank of $F$* is the cardinality of a basis of $F$.

**42.3 Example.** Since free $\mathbb{Z}$-modules correspond to free abelian groups by Proposition 13.3 the ring of integers $\mathbb{Z}$ has IBN.

**42.4 Notation.** For a ring $R$ and $n > 0$ denote $R^n := \bigoplus_{i=1}^{n} R$.

**42.5 Example.** Let $\mathbb{F}$ be a field and let $V$ be an $\mathbb{F}$-vector space with an infinite, countable basis. Let $R$ be the ring of all linear maps $V \to V$ :

$$R = \mathrm{Hom}_{\mathbb{F}}(V, V)$$

with pointwise addition and with multiplication given by composition. We have

$$R^n \cong R^m$$

for every $m, n \geq 0$ (exercise). Thus $R$ does not have IBN.

**42.6 Theorem.** *Let $R$ be a ring with identity and let $F$ be a free $R$-module. If $F$ has an infinite basis $B$ then for any other basis $B'$ of $F$ we have $|B| = |B'|$.*

**42.7 Corollary.** *Let $R$ be a ring with identity. The following conditions are equivalent.*

*1) $R$ has IBN*

*2) If $F$ is a free $R$ module with two finite bases $B$ and $B'$ then $|B| = |B'|$.*

*3) For any $m, n > 0$ if $R^m \cong R^n$ then $m = n$.*

*Proof.* Follows directly from Theorem 42.6. □

*Proof of Theorem 42.6.* Let $F$ be a free $R$ module with an infinite basis $B$. Let $B'$ be any other basis of $F$.

*Claim 1.* The basis $B'$ is infinite.

Indeed, assume that $B'$ is finite. Since $F = \langle B \rangle$ thus every element of $B'$ is a linear combination of a finite number of elements of $B$ and so $B' \subseteq \{b_1, \dots, b_n\}$ where $\{b_1, \dots, b_n\}$ is some finite subset of $B$. This gives

$$\langle b_1, \dots, b_n \rangle \supseteq \langle B' \rangle = F$$

so $\langle b_1, \dots, b_n \rangle = F$. Since $B$ is an infinite set there is $b \in B$ such that $b \notin \{b_1, \dots, b_n\}$. On the other hand $b \in F = \langle b_1, \dots, b_n \rangle$. This is a contradiction since $B$ is a linearly independent set.

Next, assume that $B$, $B'$ are two infinite bases of $F$. We can also assume that $|B'| \leq |B|$.

*Claim 2.* Let $T = \{b'_1, \dots, b'_k\}$ be a finite subset of $B'$ and let

$$B_T := \{b \in B \mid b \in \langle T \rangle\}$$

Then $B_T$ is a finite subset of $B$.

Indeed, each $b'_i$ is a linear combination of a finite number of elements of $B$ and so $T \subseteq \langle b_1, \dots, b_n \rangle$ where $\{b_1, \dots, b_n\}$ is some finite subset of $B$. This gives

$$B_T \subseteq \langle T \rangle \subseteq \langle b_1, \dots, b_n \rangle$$

By linear independence of $B$ we must then have $B_T \subseteq \{b_1, \dots, b_n\}$

*Claim 3.* $|B| \leq |B'|$.

Indeed, let $S_{B'}$ be the set of all finite subsets of $B'$. Note that since $B'$ is an infinite set we have $|S_{B'}| = |B'|$.

We have a map of sets

$$f\colon B \to S_{B'}$$

such that $f(b) = \{b'_1, \dots, b'_k\}$ if we have

$$b = r_1 b'_1 + \cdots + r_k b'_k$$

for some non-zero elements $r_1, \dots, r_k \in R$. Since $B'$ is a basis of $F$ this map is well defined.

Notice that for $T \in S_{B'}$ we have

$$b \in f^{-1}(T) \quad \text{iff} \quad b \in \langle T \rangle$$

and so by Claim 2 the set $f^{-1}(T)$ is finite for all $T \in S_{B'}$. As a consequence we obtain

$$|B| = |\bigcup_{T \in S_{B'}} f^{-1}(T)| \leq |\bigcup_{T \in S_{B'}} \mathbb{N}| = |S_{B'}| \cdot \aleph_0 = |B'| \cdot \aleph_0$$

Since $B'$ is an infinite set we have $|B'| \cdot \aleph_0 = |B'|$, and so $|B| \leq |B'|$.

Since by assumption we had $|B| \leq |B'|$ and by Claim 3 we have $|B| \leq |B'|$ we obtain that $|B| = |B'|$.

□

**42.8 Theorem.** *If $R$ is a division ring then $R$ has IBN.*

*Proof.* By Corollary 42.7 it is enough to show that if $F$ is a free $R$-module with two finite bases $B = \{b_1, \ldots, b_n\}$ and $B' = \{b'_1, \ldots, b'_m\}$ then $n = m$.

We will argue by induction with respect to $n$

Assume that $n = 1$, and so $B = \{b_1\}$. If $B' = \{b'_1, \ldots, b'_m\}$ for some $m > 1$ then we have

$$b'_1 = r_1 b_1 \quad \text{and} \quad b'_2 = r_2 b_1$$

for some $r_1, r_2 \in R$, $r_1, r_2 \neq 0$. Therefore $r_1^{-1} b'_1 - r_2^{-1} b'_2 = 0$ which contradicts the assumption that $B'$ is a inearly independent set. As a consequence we must have $m = 1$.

Next, assume that $n \geq 1$ is a number such that if a free $R$-module has a basis consisting of $n$ elements then every other basis of that module also has $n$ elements.

Let $F$ be a free $R$-module with a basis $B = \{b_1, \ldots, b_{n+1}\}$ consisting of $n+1$ elements and let $B' = \{b'_1, \ldots, b'_m\}$ be another basis of $F$. Since $\langle B' \rangle = F$ we have

$$b_{n+1} = r_1 b'_1 + \ldots + r_m b'_m$$

for some $r_1, \ldots, r_m \in R$. Also, since $b_{n+1} \neq 0$ we have $r_i \neq 0$ for some $i$. We can assume that $r_m \neq 0$. Let $B'' := \{b'_1, \ldots, b'_{m-1}, b_{n+1}\}$. Check: $B''$ is a basis of $F$.

Take the canonical epimorphism

$$\pi \colon F \to F/\langle b_{n+1} \rangle$$

Check: since $F$ is a free module with basis $B := \{b_1, \ldots, b_n, b_{n+1}\}$, thus $F/\langle b_{n+1} \rangle$ is a free module with basis $\{\pi(b_1), \ldots, \pi(b_n)\}$. On the other hand, since $F$ has a basis $B'' := \{b'_1, \ldots, b'_{m-1}, b_{n+1}\}$ therefore $\{\pi(b'_1), \ldots, \pi(b'_{m-1})\}$ is a basis of $F/\langle b_{n+1} \rangle$.

By the inductive assumption we obtain than $n = m - 1$, and so $n + 1 = m$

□

**42.9 Note.** Let $I$ be an ideal of $R$ and let $M$ be an $R$-module. Define:

$$IM := \{rm \mid r \in I,\ m \in M\}$$

Check:

1) $IM$ a submodule of $M$.

2) $M/IM$ has a structure of a $R/I$-module with the multiplication given by

$$(r + I)(m + IM) = rm + IM$$

**42.10 Theorem.** *Let $R$ be a ring with identity and let $I \neq R$ be an ideal of $R$. If $R/I$ has IBN then $R$ also has IBN.*

*Proof.* Let $F$ be a free $R$-module and let $B = \{b_1, \ldots, b_n\}$ be a basis of $F$. Check: $F/IF$ is a free $R/I$-module with basis $\{b_1 + IF, \ldots, b_n + IF\}$.

Since $R/I$ has IBN any basis of $F/IF$ has $n$ elements. As a consequence any basis of $F$ also has $n$ elements. □

**42.11 Corollary.** *If $R$ is a commutative ring with identity $1 \neq 0$ then $R$ has IBN.*

*Proof.* Let $I$ be a maximal ideal in $R$. Then $R/I$ is a field and we have the canonical homomorphism

$$\pi \colon R \to R/I$$

By Theorem 42.8 $R/I$ has IBN, so by Theorem 42.10 $R$ also has IBN. □

**42.12 Note.** Corollary 42.11 can be generalized as follows. If

$$f \colon R \to S$$

is an epimorphism of rings of identity such that $S$ is a division algebra then $R$ has IBN.