Modules and Vector Spaces

R. C. Daileda

October 16, 2017

1 Modules

Definition 1. A *(left) R-module* is a triple $(R, M, \cdot)$ consisting of a ring R, an (additive) abelian group M and a binary operation $\cdot : R \times M \to M$ (simply written as $r \cdot m = rm$) that for all $r, s \in R$ and $m, n \in M$ satisfies

- $r(m + n) = rm + rn$;
- $(r + s)m = rm + sm$;
- $r(sm) = (rs)m$.

If R has unity we also require that $1m = m$ for all $m \in M$. If $R = F$, a field, we call M a *vector space (over F)*. ▲

Remark 1. One can show that as a consequence of this definition, the zeros of R and M both "act like zero" relative to the binary operation between R and M, i.e. $0_R m = 0_M$ and $r0_M = 0_M$ for all $r \in R$ and $m \in M$. ▼

Example 1. Let R be a ring.

- R is an R-module using multiplication in R as the binary operation.
- Every (additive) abelian group G is a $\mathbb{Z}$-module via $n \cdot g = ng$ for $n \in \mathbb{Z}$ and $g \in G$. In fact, this is the only way to make G into a $\mathbb{Z}$-module. Since we must have $1 \cdot g = g$ for all $g \in G$, one can show that $n \cdot g = ng$ for all $n \in \mathbb{Z}$. Thus there is only one possible $\mathbb{Z}$-module structure on any abelian group.
- $R^n = \underbrace{R \oplus R \oplus \cdots \oplus R}_{n \text{ times}}$ is an R-module via
$$r(a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n).$$
- $M_n(R)$ is an R-module via
$$r(a_{ij}) = (ra_{ij}).$$
- $R[x]$ is an R-module via
$$r \sum_i a_i x^i = \sum_i ra_i x^i.$$
- Every ideal in R is an R-module.
- If R is a subring of S, then S is an R-module using the multiplication in S as the binary operation.
- If $\varphi : R \to S$ is a ring homomorphism, then S is an R-module via
$$r \cdot s = \varphi(r)s.$$

- This generalizes the previous example in which φ is just the inclusion map.
- Let F be a field and $A \in M_n(F)$. Define $\varphi_A : F[x] \to M_n(F)$ by $\varphi_A(f) = f(A)$. The structure of the $F[x]$-module obtained from this homomorphism is closely related to the so-called *canonical forms* of A.

- If M is an R-module and I is an ideal in R so that $IM = \{0\}$, i.e. $am = 0$ for all $a \in I$ and $m \in M$ (I *annihilates* M), then one can show that for $r \in R$ and $m \in M$

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

is a well-defined binary operation of R/I on M, and that it makes M into an R/I-module.

♦

2 Submodules

Definition 2. Let M be an R-module, $N \subseteq M$. N is an R-*submodule* of M if

- N is a subgroup of M (iff $N \neq \varnothing$ and $m - n \in N$ for all $m, n \in N$) ;
- $rn \in N$ for all $r \in R$, $n \in N$.

So N is itself an R-module under the restriction of the binary operation to $N \times R$. If $R = F$, a field, a submodule is called a *subspace*. ▲

Example 2. Let R be a ring.

- If G is an (additive) abelian group ($\mathbb{Z}$-module), the $\mathbb{Z}$-submodules of G are just the subgroups.
- Every ideal in R is an R-submodule of R.
- The upper triangular matrices $U_n(F) = \{(a_{ij}) \mid a_{ij} = 0 \text{ if } i > j\}$ form an R-submodule of $\mathrm{M}_n(R)$.
- The set $R \oplus \{0\} \oplus \{0\} \oplus \cdots \oplus \{0\} = \{(a, 0, 0, \ldots, 0) \mid a \in R\}$ is an R-submodule of R^n. So is

$$\{(a_1, a_2, \ldots, a_n) \in R^n \mid a_1 + a_2 + \cdots + a_n = 0\}.$$

- If M is an R-module and N is an R-submodule of M, then the (additive) coset space M/N has the structure of an abelian group. It is not difficult to show that for $r \in R$ and $m \in M$ the operation

$$r \cdot (m + N) = rm + N$$

is well-defined and makes M/N into an R-module, the *quotient module*.

♦

Definition 3. If R is a ring with unity, M is an R-module and $X \subseteq M$, the *submodule generated by* X is

$$\langle X \rangle = RX = \left\{ \sum_{i=1}^{n} r_i x_i \;\middle|\; n \in \mathbb{N}, r_i \in R, x_i \in X \right\}.$$

The expression $\displaystyle\sum_{i=1}^{n} r_i x_i$ is called an R-*linear combination* of the x_i. So $\langle X \rangle$ is the set of all R-linear combinations of elements of X. When $R = F$, a field, we write $\langle X \rangle = \mathrm{Span}(X)$ and call it the *span of* X. If $N \subseteq M$ is a submodule, we say N is *finitely generated* if $N = \langle X \rangle$ for some *finite* set $X \subseteq M$. ▲

Remark 2. Note that since R has unity, $X \subseteq \langle X \rangle$. ▼

Remark 3. If $X = \{x_1, x_2, \ldots, x_N\}$ is finite, then any linear combination of a subset of X can be written as a linear combination of the whole set X simply by inserting terms with zero coefficients. That is

$$\langle x_1, x_2, \ldots, x_N \rangle = \left\{ \sum_{i=1}^{N} r_i x_i \;\middle|\; r_i \in R \right\}.$$

▼

Remark 4. If M is an R-module, N is a submodule and $X \subseteq N$, then $\langle X \rangle \subseteq N$. ▼

Example 3. Let R be a ring with unity.

- R^n is finitely generated as an R-module by the elements $e_i = (0, 0, \ldots, 1, \ldots, 0)$ (the 1 occurs in the ith coordinate), $1 \leq i \leq n$.
- $\mathrm{M}_n(R)$ is finitely generated as an R-module by the matrices $E_{k\ell} = (\delta_{ik}\delta_{j\ell})$ (here $\delta_{ab} = 0$ if $a \neq b$ and $\delta_{aa} = 1$), $1 \leq i, j \leq n$.
- $R[x]$ is *not* a finitely generated R-module. If $X = \{f_1, f_2, \ldots, f_n\} \subset R[x]$ then any $g \in \langle X \rangle$ has the form
$$g = \sum_{i=1}^{n} r_i f_i$$
whose degree is bounded by $M = \max_i\{\deg f_i\}$. Hence $\langle X \rangle \neq R[x]$.
- If we interpret the empty sum as 0, then $\langle \varnothing \rangle = \{0\}$.

♦

3 Module Homomorphisms

Although we won't necessarily need it later, we include this section in the interest of completeness.

Definition 4. Let R be a ring and M and N be R-modules. A map $f : M \to N$ is an *R-module homomorphism* if for all $r \in R$ and $m, n \in M$:

- $f(rm) = rf(m)$;
- $f(m + n) = f(m) + f(n)$.

▲

So an R-module homomorphism is a homomorphism of the underlying abelian groups that respects the action(s) of R on them. R-module epimorphism, monomorphism, isomorphism and endomorphism mean the usual things. If $R = F$, a field, a module homomorphism is called a *linear transformation*.

Example 4. Let R be a ring.

- If M is an R-module and N is an R-submodule of M, then the map $m \mapsto m + N$ is an R-module homomorphism $M \to M/N$.
- If M and N are R-modules, $M = \langle X \rangle$ and $f : M \to N$ is an R-module epimorphism, then $N = \langle f(X) \rangle$.
- The map $\pi_i : R^n \to R$ given by $\pi_i(r_1, r_2, \ldots, r_n) = r_i$ is an R-module epimorphism.

♦

The most important general result about homomorphisms for us is the following.

Theorem 1 (First Isomorphism Theorem for Modules)**.** *Let R be a ring, M and N be R-modules, and $f : M \to N$ an R-module homomorphism. Then*

$$\ker f = f^{-1}(\{0\}) \quad \textit{and} \quad \operatorname{im} f = f(M)$$

are R-submodules of M and N, respectively. The map $\overline{f}$ given by $m + \ker f \mapsto f(m)$ is a well-defined R-module isomorphism $\overline{f} : M/\ker f \to \operatorname{im} f$.

Proof. Exercise. □

4 Linear Independence and Bases

Definition 5. Let M be an R-module, $X \subseteq M$. We say X is *linearly independent* if for all $n \in \mathbb{N}$ and distinct $x_1, x_2, \ldots, x_n \in X$, and $r_1, r_2, \ldots, r_n \in R$,

$$\sum_{i=1}^{n} r_i x_i = 0 \ \ \Rightarrow \ \ r_i = 0 \text{ for all } i.$$

If X is not linearly independent, we say that X is *linearly dependent.* ▲

Remark 5. Let M be an R-module.

- If $X = \{x_1, x_2, \ldots, x_m\}$ is finite, then X is linearly independent if and only if

  $$\sum_{i=1}^{m} r_i x_i = 0 \ \ \Rightarrow \ \ r_i = 0 \text{ for all } i,$$

  i.e. we only need consider linear combinations of the entire set. This is because linear combinations of subsets can be viewed as linear combinations of the entire set simply by inserting zero coefficients as necessary.

- An infinite set X is linearly independent if and only if every finite subset is.
- If $0 \in X$, then X is linearly dependent.
- $\varnothing$ is vacuously linearly *independent.*

▼

Lemma 1. *If V is a vector space over F, then $0 \notin X \subseteq V$ is linearly dependent if and only if there are distinct $z, x_1, x_2, \ldots, x_n \in X$ and $a_1, a_2, \ldots, a_n \in F$ so that*

$$z = \sum_{i=1}^{n} a_i x_i. \tag{1}$$

Proof. To see this, suppose that (1) holds. Then

$$-z + \sum_{i=1}^{n} a_i x_i = 0 \text{ but } -1 \neq 0 \text{ (regardless of the } a_i),$$

proving X is dependent. Conversely, if we assume X is linearly dependent, then there must be $n \in \mathbb{N}_0$, distinct $x_0, x_1, \ldots, x_n \in X$ and $b_0, b_1, \ldots, b_n \in F$, not all zero, so that

$$\sum_{i=0}^{n} b_i x_i = 0.$$

If $n = 0$ then $b_0 x_0 = 0$ and $b_0 \neq 0$. As F is a field, we can multiply by b_0^{-1} to obtain $x_0 = 0$, which is impossible. So $n \geq 1$. Relabelling if necessary, we can assume $b_0 \neq 0$. Then, again since F is a field,

$$x_0 = \sum_{i=1}^{n} (-b_0^{-1} b_i) x_i$$

and we obtain (1) by setting $z = x_0$. □

Our main interest in linear independence is the formulation of the following definition.

Definition 6. Let R be a ring with unity and M an R-module. We say $X \subseteq M$ is a *basis* for M if

- $\langle X \rangle = M$;
- X is linearly independent.

If M has a basis X we say it is *free (on X)*. ▲

Example 5. Let R be a ring with unity.

- R^n is free on the set $X = \{e_i \mid 1 \leq i \leq n\}$.
- More generally, $R^S = \coprod_{s \in S} R$ is free on the set $X = \{e_s \mid s \in S\}$, where $e_s(s) = 1$ and $e_s(t) = 0$ for all $t \in S \setminus \{s\}$.
- $R[x]$ is free on the powers of x, i.e. $X = \{1, x, x^2, \ldots\}$.
- Let G be an (additive) abelian group viewed as a $\mathbb{Z}$-module as above. If $|G| = n \in \mathbb{N}$, then G is *not* free, since $n \neq 0$ but $ng = 0$ for all $g \in G$. More generally, if the *torsion subgroup*

$$\mathrm{Tor}(G) = \{g \in G \mid ng = 0 \text{ for some } n \in \mathbb{N}\}$$

  is nonzero, then G is *not* a free $\mathbb{Z}$-module.
- Still more generally, if D is a domain, M is a D-module and

$$\mathrm{Tor}_D(M) = \{m \in M \mid am = 0 \text{ for some nonzero } a \in D\}$$

  is nonzero, then M is *not* a free D-module. This and the preceding example follow from the next result.

♦

Lemma 2. *Let R be a ring with unity and M a free R-module with basis X. Then for each $m \in M \setminus \{0\}$ there exist unique (up to order) distinct $x_1, x_2, \ldots, x_n \in X$ and unique nonzero $r_1, r_2, \ldots, r_n \in R$ so that*

$$m = \sum_{i=1}^{n} r_i x_i. \tag{2}$$

Proof. That such an expression exists follows from the fact that $\langle X \rangle = M$. Suppose $m = \sum_{j=1}^{m} s_j y_j$ is another such expression. Let $A = \{x_1, x_2, \ldots, x_n\}$, $B = \{y_1, y_2, \ldots, y_m\}$, $A' = A \setminus B$, $B' = B \setminus A$ and $C = A \cap B$. Relabel A and B so that $A \cap B$ occurs first in both, in the same order (i.e. $x_1 = y_1$, $x_2 = y_2$, etc.). Then

$$0 = m - m = \sum_{x_i \in A'} r_i x_i + \sum_{x_i = y_i \in C} (r_i - s_i) x_i + \sum_{y_j \in B'} (-s_j) y_j.$$

Since X is linearly independent and $r_i, s_j \neq 0$, we must have $A' = B' = \varnothing$, i.e. $A = B = C$, and $r_i = s_i$ for all i. □

Recall that

$$\coprod_{x\in X} R = \{\alpha\colon X \to R \mid \alpha(x) = 0 \text{ for all but finitely many } x \in X\}.$$

In the situation described in Lemma 2, define $C_X(m) \in \coprod_{x\in X} R$ by $C_X(m)(x_i) = r_i$ and $C_X(m)(x) = 0$ otherwise. We will call $C_X(m)$ the *coordinates of* m *relative to* X or the X*-coordinates of* m.

Lemma 3. *Let R be a ring with unity and M a free R-module with finite basis $X = \{x_1, x_2, \ldots, x_N\}$. Then for each $m \in M$ there exist unique $r_1, r_2, \ldots, r_N \in R$ so that*

$$m = \sum_{i=1}^{N} r_i x_i. \tag{3}$$

We call $C_X(m) = (r_1, r_2, \ldots, r_N) \in R^N$ the coordinates of m relative to X*.*

Proof. As above, but simpler because we are allowing zero coefficients. Since $\langle X\rangle = M$ and X is finite, by Remark 3 any $m \in M$ can be written

$$m = \sum_{i=1}^{N} r_i x_i, \quad r_i \in R.$$

Suppose we also have

$$m = \sum_{i=1}^{N} s_i x_i, \quad s_i \in R.$$

Subtracting these gives

$$0 = \sum_{i=1}^{N} (r_i - s_i)x_i \quad\Rightarrow\quad r_i - s_i = 0 \text{ for all } i \quad\Rightarrow\quad r_i = s_i \text{ for all } i$$

by linear independence of X. Hence the r_i are unique, as claimed. $\square$

In the setting of the Lemma 3, notice that since N is finite, $R^N = \coprod_{x\in X} R$. Therefore the coordinate "vector" $C_X(m) \in \coprod_{x\in X} R$ in any case and satisfies

$$m = \sum_{x\in X} C_X(m)(x)\cdot x,$$

where its understood that terms with zero coefficients are omitted from the sum when X is infinite. In fact, $\coprod_{x\in X} R$ is an R-module under coordinate-wise operations, and, based on what we have shown, it is not hard to show that $C_X : M \to \coprod_{x\in X} R$ is an R-module isomorphism.

Remark 6. Free R-modules are the beginning of general structure theory for R-modules. If M is an R-module generated by a subset X, define $\varphi\colon \coprod_{x\in X} R \to M$ by

$$\alpha \mapsto \sum_{x\in X} \alpha(x)x.$$

One can readily show this is a module epimorphism. Hence *every module over a ring with unity is the homomorphic image of a free module* (one can always take $X = M$). The kernel of φ is called the *first syzygy module* of M relative to X:

$$\mathrm{Syz}_M(X) = \ker\varphi.$$

By the first isomorphism theorem

$$M \cong \coprod_{x\in X} R \Big/ \mathrm{Syz}_M(X),$$

i.e. when R has unity, every R-module is isomorphic to a quotient of a free R-module. ▼

An extremely useful property of a free R-modules is the ability to "freely" construct homomorphisms from them.

Theorem 2. *Let R be a ring with unity and M a free R-module with basis X. Let N be any R-module and $f : X \to N$ any function. Then there exists a unique R-module homomorphism $\widehat{f} : M \to N$ so that $\widehat{f}(x) = f(x)$ for all $x \in X$.*

Proof. If such an $\widehat{f}$ exists, then for any $m \in M$ it must satisfy

$$\widehat{f}(m) = \widehat{f}\left(\sum_{x \in X} C_X(m)(x) \cdot x\right) = \sum_{x \in X} C_X(m)(x) \cdot \widehat{f}(x) = \sum_{x \in X} C_X(m)(x) \cdot f(x), \tag{4}$$

and is therefore unique, by the uniqueness of coordinates. So it suffices to prove that the right-hand side of (4) defines an R-module homomorphism. This follows from the fact that the coordinate map C_X is R-linear. The details are left to the reader. $\square$

On to the existence of bases.

Lemma 4. *Let R be a ring with unity and M an R-module. Every linearly independent subset of M is contained in a maximal linearly independent subset.*

Proof. This is a standard application of Zorn's Lemma. $\square$

Theorem 3. *Let X be a maximal linearly independent subset of a vector space V over F. Then X is a basis for V.*

Proof. We only need to show that $\mathrm{Span}(X) = V$. To that end, let $v \in V$. If $v \in X$, then $v \in \langle X \rangle$ so there's nothing to prove. So suppose $v \notin X$. Then, by maximality, $Y = X \cup \{v\}$ must be linearly dependent. Hence there exist distinct $x_0, x_1, \ldots x_n \in Y$ and $a_0, a_1, \ldots, a_n \in F$, not all zero, so that

$$0 = \sum_{j=0}^{n} a_j x_j.$$

As in an earlier argument, we cannot have $n = 0$, so $n \geq 1$. If $x_j \in X$ for all j, this contradicts linear independence of X. So, without loss of generality, $x_0 = v$ and $x_j \in X$ for $j \geq 1$. If $a_0 = 0$ we again contradict X's linear independence (as $n \geq 1$), so $a_0 \neq 0$ and is therefore invertible in F. Thus

$$v = \sum_{j=1}^{n} (-a_0^{-1} a_j) x_j \in \mathrm{Span}(X),$$

which is what we needed to show. $\square$

Corollary 1. *Every vector space has a basis. In particular any linearly independent set of vectors is contained in a basis.*

Lemma 5. *Let R be a ring with unity and M a free R-module with bases X and Y. For any $a \in X$ there exists $b \in Y$ so that $C_X(b)(a) \neq 0$ (equivalently, $b \notin \langle X \setminus \{a\} \rangle$).*

Proof. Suppose not. Then there is an $a \in X$ so that $Y \subseteq \langle X \setminus \{a\} \rangle$. Thus $M = \langle Y \rangle \subseteq \langle X \setminus \{a\} \rangle \subseteq M$ and hence $M = \langle X \setminus \{a\} \rangle$. In particular, $a \in \langle X \setminus \{a\} \rangle$. By Lemma 1, this means X is linearly dependent, a contradiction. So the conclusion of the lemma holds. $\square$

Lemma 6 (The Replacement Lemma)**.** *Let V be a vector space over a field F with bases X and Y. For every $a \in X$, there is a $b \in Y$ so that $X' = (X \setminus \{a\}) \cup \{b\}$ is a basis for V.*

Proof. Let $a \in X$ and use Lemma 5 to choose $b \in Y$ with $\alpha = C_X(b)(a) \neq 0$. Then

$$a = \alpha^{-1} b - \sum_{x \in X \setminus \{a\}} (\alpha^{-1} C_X(b)(x)) \cdot x \in \mathrm{Span}(X').$$

Hence $X \subseteq \mathrm{Span}(X')$ so that $M = \mathrm{Span}(X) \subseteq \mathrm{Span}(X') \subseteq M$. Consequently $\mathrm{Span}(X') = M$.

It remains to show that X' is linearly independent. Let $S \subseteq X'$ be finite. If $b \notin S$, then $S \subset X$ and so

$$\sum_{s \in S} r_s s = 0 \quad \Rightarrow \quad r_s = 0 \text{ for all } s \in S$$

because X is linearly independent. If $b \in S$, write $S = \{b\} \cup S'$ with $S' \subseteq X \setminus \{a\}$. Suppose

$$\beta b + \sum_{s \in S'} r_s s = 0.$$

If $\beta \neq 0$, this yields

$$b = \sum_{s \in S'} (-\beta^{-1} r_s) s \in \langle X \setminus \{a\} \rangle,$$

contradicting the fact that $C_X(b)(a) \neq 0$. So $\beta = 0$ and we are left with

$$\sum_{s \in S'} r_s s \quad \Rightarrow \quad r_s = 0 \text{ for all } s \in S',$$

again because since $S' \subseteq X$, a linearly independent set. So in any case, the only linear combinations of elements of X' that are equal to 0 are trivial combinations, and X' is linearly independent. □

Theorem 4. *Let V be a vector space over a field F. If V has a finite basis, then all its bases are finite and have the same size.*

Proof. Let $X = \{x_1, x_2, \ldots, x_n\}$ be a finite basis for V and let Y be any other basis. By the Replacement Lemma, we may successively replace $x_1, x_2, \ldots$ with $y_1, y_2, \ldots \in Y$ while still maintaining a basis for V. Since the lemma guarantees we can do this for each x_i in turn, it must be the case that $|Y| \geq n$. But since $X' = \{y_1, y_2, \ldots y_n\}$ spans V, if $X' \subset Y$ then Y isn't linearly independent. So $X' = Y$ and $|Y| = |X| = n$. □

Remark 7. Theorem 4 shows that if a vector space has an infinite basis, all its bases are infinite. One can prove more, specifically that if a vector space has an infinite basis, then all its bases are infinite and have the same cardinality. This cardinality is the dimension. See [1]. ▼

Definition 7. Let V be a vector space with a finite basis X. We call $|X|$ the *dimension* of V, write $\dim V = |X|$ and call V a *finite dimensional vector space*. Theorem 4 shows that notion of dimension is well-defined, i.e. does not depend on the basis chosen. ▲

Remark 8. Let V be a finite dimensional vector space of dimension n.

- If $n = 0$ then $\varnothing$ is the only basis of V.
- If $S \subseteq V$ is linearly independent, then by Corollary 1 S is contained in some basis of V. Hence $|S| \leq n$.
- If $S \subseteq V$, then any maximal linearly independent $T \subseteq S$ will satisfy $\mathrm{Span}(T) = \mathrm{Span}(S)$ (exercise). So if $\mathrm{Span}(S) = V$, then S must contain a basis of V, and hence $|S| \geq n$.

▼

Example 6. Let F be a field.

- For $n \in \mathbb{N}$, $\dim F^n = n$ since $\{e_i \,|\, 1 \leq i \leq n\}$ is a basis.
- For $n \in \mathbb{N}$, $\dim \mathrm{M}_n(F) = n$ since $\{E_{ij} \,|\, 1 \leq i, j \leq n\}$ is a basis.
- For $n \in \mathbb{N}_0$ let $F_n[x] = \{f \in F[x] \,|\, \deg f \leq n\}$ is a vector space over F of dimension $n + 1$, since $\{1, x, x^2, \ldots, x^n\}$ is a basis.

♦

Finally, we establish an essential result about linear transformations of finite dimensional vector spaces.

Lemma 7. *Let V be a finite dimensional vector space and W a subspace.*

- $\dim W \leq \dim V$ *with equality if and only if* $V = W$.
- $\dim V/W = \dim V - \dim W$.

Proof. Let Y be a basis for W. Then Y is linearly independent in V, so it is contained in a basis of V by Corollary 1. Thus $\dim W = |Y| \leq \dim V$. If the dimensions agree, Y must already be a basis for V and hence $W = \mathrm{Span}(Y) = V$.

Regarding the second result, it clearly holds if $V = W$, so we assume $W \subset V$. Let Y be a basis for W and, as above, complete it to a basis $X = Y \vee X'$ for V. We claim that the cosets $x + W$ with $x \in X'$ form a basis for V/W. Establishing this claim will prove the second part of the lemma.

Let $v \in V$ and write

$$v = \sum_{x \in X} c_X(v)(x) \cdot x = \underbrace{\sum_{y \in Y} c_X(v)(y) \cdot y}_{\text{in } W} + \sum_{x \in X'} c_X(v)(x) \cdot x,$$

which shows that

$$v + W = \sum_{x \in X'} c_X(v)(x) \cdot (x + W).$$

Hence $\{x + W \,|\, x \in X'\}$ spans V/W. As far as linear independence goes, suppose

$$W = \sum_{x \in X'} a_x(x + W) = \left(\sum_{x \in X'} a_x x \right) + W.$$

Then

$$\sum_{x \in X'} a_x x \in W \cap \langle X' \rangle = \langle Y \rangle \cap \langle X' \rangle = \{0\}$$

and hence $a_x = 0$ for all x, since X' is linearly independent. The set $\{x + W \,|\, x \in X'\}$ is thererfore linearly independent, finishing the proof. □

Definition 8. Let $T : V \to W$ be a linear transformation of vector spaces over F. The *null space of T* is

$$\mathrm{null}\, T = \ker T.$$

The *rank of T* is

$$\mathrm{rank}\, T = \dim \mathrm{im}\, T.$$

▲

We can now state and prove one of the fundamental theorems of undergraduate linear algebra.

Theorem 5. *Let $T : V \to W$ be a linear transformation of vector spaces over F and suppose that V is finite dimensional. Then*

$$\dim V = \dim \mathrm{null}\, T + \mathrm{rank}\, T.$$

Proof. According to the First Isomorphism Theorem, there is an isomorphism $\overline{T} : V/\,\mathrm{null}\, T \to \mathrm{im}\, T$. Since isomorphisms preserve dimension (exercise), by Lemma 7 we have

$$\mathrm{rank}\, T = \dim \mathrm{im}\, T = \dim V/\,\mathrm{null}\, T = \dim V - \dim \mathrm{null}\, T,$$

which is equivalent to the conclusion of the theorem. □

References

[1] Hungerford, T. W., *Algebra*, GTM 73, Springer, 1974.