27.5.24.

Rmk

If M is a free module with basis $\{a_1, \dots a_n\}$

then we can look at the submodule $M_i = Ra_i$ (i.e. the submodule generated by a_i)

If R is regarded as a module over itself, then $r \to ra_i$ is an R-module isom of R and M_i because $\{a_i\}$ is a linearly independent set

Since $\{a_i\}$ span M it follows that M is the sum of submodules M_i and by lin-independence of a_i's the sum is direct. Thus a free module of rank n is a direct sum of copies of underlying ring R.

Conversely, a direct sum of copies of R, R^n, is a free R-module.

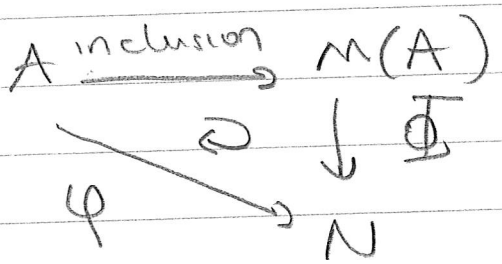
If $e_i = (0, \dots, \underset{\uparrow i\text{th position}}{1}, \dots 0)$ then $\{e_i\}$ form a basis of R^n.

This is why in some references (eg Pinkt's note one has as defn of free module of rank n Any module M which is isomp. as R-module to R^n.

If R is comm and $R^n \cong R^m$ then $n = m$

Prop 9.5 For any set A, there is a free R-module $M(A)$ on the set A and $M(A)$ satisfies the following universal property: if N is any R-module and $\varphi: A \to N$ is any map of sets then $\exists$ a unique R-module hom $\Phi: M(A) \to N$ s.t $\Phi(a) = \varphi(a)$ $\forall a \in N$ ie

the following diagram commutes



When A is the finite set $\{a_1, \ldots a_n\}$

$$M(A) = Ra_1 \oplus \ldots \oplus Ra_n \cong R^n.$$

Proof If $A = \phi$ let $M(A) = \{0\}$.

If $A \neq \phi$ let $M(A)$ be the collection of all set function $f: A \to R$ s.t $f(a) = 0$ for all but finitely many $a \in A$.

Make $M(A)$ into an R-module by pointwise addition of functions and p.w multiplication of a ring element times a function.

ie $(f+g)(a) = f(a) + g(a)$

$(rf)(a) = r f(a)$ $\forall a \in A, r \in R, f, g \in M(A)$

Check that all R-module axioms hold.

We can identify A as a subset of $M(A)$ by

$$a \longmapsto f_a$$

where $f_a : A \to R$ with $f_a(a) = 1$, $f_a(b) = 0$ $\forall b \neq a$.

then $M(A)$ can be thought as all finite R-linear combinations of elements of A by identifying each function f with the sum $r_1 a_1 + \cdots + r_n a_n$ where

$f(a_i) = r_i$ and zero for other els of A.

Each elt of $M(A)$ has a unique expression as a formal sum

If $\varphi : A \to N$ is a map of the set A into the R-module N, define

$\Phi : M(A) \to N$ by

$$\sum_{i=1}^{n} r_i a_i \longmapsto \sum_{i=1}^{n} r_i \varphi(a_i)$$

By uniqueness of the expression for elts of $M(A)$ as linear combinations Φ is a well-defined R-mod hom. Clearly $\Phi|_A = \varphi$. Once we know the values of an R-mod hom on A its values on every elt of $M(A)$ are uniquely determined. Hence Φ is the unique ext of φ

Remark If M is a free module with basis $\{x_i\}$ and N any module, we can construct a module hom φ from M to N by specifying $\varphi(x_i) = y_i \in N$ arbitrarily on basis elements and extend linearly, just as we would do in the case of vector spaces.

We can turn this process around to see that

> If N is an arbitrary module, then N is a homomorphic image of a free module

For this we need a set of generators $\{y_i, i \in I\}$ for N. (We can take y_i to be all elts of N) We then construct a free module with basis $\{x_i, i \in I\}$. To do this take the direct sum of copies of R, as many copies as there are elements of I, and map x_i to y_i for each i.

By the isom theorem every module N is a quotient of a free module

—o—

Let N be a free R-module of rank n with basis $\{w_1, \dots w_n\}$ and M a free module of rank m with basis $\{v_1, \dots v_m\}$

Let $\varphi : M \to N$ be a module hom. We can then represent φ by a $n \times m$ matrix as in the case of lin transformations on a finite dim'l vector space

For each j, $\varphi(v_j)$ is a lin combination of w_j's so that

$$\varphi(v_j) = \sum_{i=1}^{n} a_{ij} w_i \qquad j = 1, \dots m.$$

with $a_{ij} \in R$ gives a matrix

$$A \in Mat_{n \times m}(R)$$

Conversely any matrix $A \in Mat_{n \times m}(R)$ gives a hom $L_A : M \to N$, $m \mapsto Am$, where we write M, (resp N) as the set of all m (resp n) tuples in R.

Rmk. $Hom_R(M, N)$ is not necessarily an R-module if R is not commutative

If $\varphi \in Hom_R(M, N)$, $s \in R$, we can define $s\varphi$ in a natural way as $s\varphi(x) = s\varphi(x)$

But if we try to check that $s\varphi \in Hom_R(M, N)$ we see that we need $\tilde{\varphi}(rx) = r\tilde{\varphi}(x)$ for $\tilde{\varphi} = s\varphi$

but

$(s\varphi)(rx) = s\,\varphi(rx) = sr\,\varphi(x)$ and

$r(s\varphi)(x) = rs\,\varphi(x)$ and if R is not comm.

then they don't have to be equal!

Examples (1) $R = \mathbb{Z}$, the free module on a set A is the free abelian group on A.

If $|A| = n$ then $M(A)$ is the free abelian group of rank n and is isomorphic to $\mathbb{Z} \oplus \dots \oplus \mathbb{Z} = \mathbb{Z}^n$.

(2) $R[T]$ - polynomials in T, is an R-module

$\{1, T, T^2, \dots\}$ span $R[T]$ since every poly is a finite lin. comb. of powers of T.

$R[T]$ does not have a finite spanning set as an R-module

Note $\{1, T, T^2 \dots\}$ is also a basis

As an $R[T]$ module (rather than an R-module) $R[T]$ has a finite spanning set, namely $\{1\}$

(3) $N = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not free as a $\mathbb{Z}$-module

an elt $m \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ can be written uniquely as $m_1 + m_2$ with $m_1, m_2 \in \mathbb{Z}/2\mathbb{Z}$ but it does not have a unique representation as $r_1 a_1 + r_2 a_2$ with $r_1, r_2 \in \mathbb{Z}$, $a_1, a_2 \in \mathbb{Z}/2\mathbb{Z}$

For example $(1, 1) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ has a rep $(1,1) = 1(1,0) + 1(0,1)$ but also the rep

$$(1,1) = 3(1,0) + 5(0,1)$$

Note the difference between the uniqueness property of direct sums and the uniqueness property of free modules.

In the direct sum of 2 modules, say $M_1 \oplus M_2$ each elt of $M = M_1 \oplus M_2$ is uniquely written as $m_1 + m_2$, $m_1 \in M_1$, $m_2 \in M_2$. Here uniqueness refers to the module elts m_1, m_2.

In the case of free modules, the uniqueness is on the ring elements as well as module elts.

Every non-zero finitely generated vector space has a basis but

(4) Some finitely generated modules do not have a basis!

eg let $R = \mathbb{Z}[\sqrt{-5}]$,

$I = (2, 1+\sqrt{-5})$ the ideal in R generated by 2 and $1+\sqrt{-5}$

Then $\{2, 1+\sqrt{-5}\}$ span I as an R-module (by definition)

but this subset is linearly dependent

$2a + b(1+\sqrt{-5}) = 0$ with $a = 1+\sqrt{-5}$, $b = -2$

More generally all pairs $x, y \in I$ are lin. dependent over R

$ax + by = 0$ with $a = y$, $b = -x$.

with a, b non zero if x, y non-zero

if one of x or $y = 0$ then one of a, b is non-zero.

if $x = y = 0$ then can take $a = b = 1$.

So any lin-indep-set of I must have only 1 member which means if I has a basis it has 1 elt. But if $\{a\}$ is a basis of I as an R-module it means $I = Ra$

i.e. I is principal but one can show that I is not principal

$(2, 1+\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$ is not pincipal.

Suppose $(2, 1+\sqrt{-5}) = (\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$

Then since $2 \in (\alpha)$, $\alpha \mid 2$ in $\mathbb{Z}[\sqrt{-5}]$

taking norms in $2 = \alpha\beta$ we get

$$N(\alpha) \mid 4 \text{ in } \mathbb{Z}$$

Similarly $N(\alpha) \mid N(1+\sqrt{-5}) = 6$

Hence $N(\alpha) \mid 2 \Rightarrow N(\alpha) = 2$ or 1

but $a^2 + 5b^2 = 2$ has no soln in integers

Hence $N(\alpha) = 1 \Rightarrow \alpha$ is a unit

and $(2, 1+\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$

$\Rightarrow \exists\ x, y \in \mathbb{Z}[\sqrt{-5}]$ s.t. $2x + (1+\sqrt{-5})y = 1$

Multiplying both sides w $1-\sqrt{-5}$ gives

$$2(1-\sqrt{-5})x + 6y = 1-\sqrt{-5}$$

$2 \mid$ LHS hence $2 \mid (1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$

$\Rightarrow 2(a+b\sqrt{-5}) = 1-\sqrt{-5}$ for some $a, b \in \mathbb{Z}$

$\Rightarrow 2a = 1$ ↯.

Examples for vector spaces versus Modules.

(1) In a vector space every non-zero elt $\{v\}$ is a linearly indep. set
In a module this does not hold.

let $M = \mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module
$x \in M$, $x \neq 0$
we then have $n \cdot x = 0$
so $\{x\}$ is lin. dependent

Hence every non-empty subset of M is also lin. dependent.

Note this also shows that M has no basis since linear span of empty set is defined to be $\{0\}$.
(by convention a lin comb. of no vectors sums to 0)

(2) In a fin. gen. vector space a maximal linearly independent subset is a spanning set
Not true for modules
eg. $\mathbb{Z}$ as a $\mathbb{Z}$-module has $\{2\}$ a maximal lin. indep. set
since for any 2 elements $x, y \in \mathbb{Z}$ $ax + by = 0$ with $a = y$ $b = -x$, they are lin. dependent

but $\{2\}$ is not a spanning set since $2\mathbb{Z} \neq \mathbb{Z}$.

(3) In a (fin. gen) vector space a minimal spanning set is lin. indep.

In a module this is false
eg $\mathbb{Z}$ as a $\mathbb{Z}$-module
$\{2, 3\}$ span $\mathbb{Z}$ since for any $n \in \mathbb{Z}$

$$n = 3n - 2n$$

and is minimal since neither $\{2\}$ nor $\{3\}$ span $\mathbb{Z}$, but $\{2, 3\}$ is lin dep. as

$$2 \cdot 3 - 3 \cdot 2 = 0.$$

(4) If V, W are finite dim'l vector spaces over a field F with same dimension $\varphi : V \to W$ is linear map. Then we have that if φ is injective then φ is surjective.
For modules this is
False e.g. View $\mathbb{Z}$ as $\mathbb{Z}$-module with basis $\{1\}$ let $\varphi : \mathbb{Z} \to \mathbb{Z}$

$$n \to 2n$$

It is injective but not surjective.

(5) In a vector space every lin indep set can be enlarged to a basis and every spanning set contains a basis.
Not true in modules
$\mathbb{Z}$ as a $\mathbb{Z}$-module has basis $\{1\}$.

$\{2\}$ is a lin indep set of $\mathbb{Z}$ which can't be enlarged to a basis

$\{2,3\}$ is a spanning set of $\mathbb{Z}$ that doesn't contain a basis.

There are many examples of modules that do not have bases

eg
$\mathbb{Q}$ as a $\mathbb{Z}$-module
A subset with 1 elt doesn't span $\mathbb{Q}$ since if $r = \frac{p}{q} \in \mathbb{Q}$
then for $n \in \mathbb{Z}$, $|nr| > \left|\frac{1}{2q}\right|$
So $\frac{1}{2q} \notin \operatorname{span}\{r\}$ so $\{r\}$ cannot be a basis

A subset with 2 elts or more is lin depen.
let $S \in \mathbb{Q}$ with $|S| \geq 2$, let $r_1 = \frac{p_1}{q_1}$, $r_2 = \frac{p_2}{q_2} \in S$
Then $(q_1 p_2) r_1 - (q_2 p_1) r_2 = 0$, so S is a dependent set.

Even for free modules, for modules with basis, we have differences to vector spaces.

(6) In a vectorspace with a finite basis a subspace also has a finite basis

Not true for modules.
Let $M = \mathbb{Z}[\sqrt{-5}]$ as a $\mathbb{Z}[\sqrt{-5}]$-module

$I = (2, 1+\sqrt{-5})$ a submodule

M has basis $\{1\}$, I is finitely generated but has no basis.

(7) A subspace of a vector-space with the same finite dimension must be the entire space

We can have a free module of rank n which contains a free module of some rank.

eg Let $R = \mathbb{Z}$, $M = \mathbb{Z}^d$
$N = (2\mathbb{Z})^d$ $d \geq 1$ $N \subsetneq M$

but has same rank
More generally R any I.Domain, which is not a field, $a \in R \setminus R^\times$, $a \neq 0$ $M = R^d$
$N = (Ra)^d$ has same rank as R-modules.

Finally

The following example is also fundamental and is the basis for the study of canonical forms of matrices.

Example Let F be a field, V a vector space over F, $T: V \to V$ a linear transformation.

We can make V into a $F[x]$ module using T as follows:

We define an action of ring element $p(x) \in F[x]$ on the module element $v \in V$ by

$$p(x)v = (a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0)v$$

$$= a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_0 v.$$

$(p(x) = a_n x^n + \cdots + a_0)$ ie $p(x)$ acts by substituting the linear transformation T for x in $p(x)$ and applying the resulting linear transformation to v.

Here $T^n = T \circ T \circ \cdots \circ T$ (n times)

$T^0 = I$

It is easy to check that this multiplication of $F[x]$ on V satisfy the module axioms.

The way $F[x]$ act on V depends on the choice of T. So there are many different $F[x]$-module structures on the same vector space V.

The construction of an $F[x]$-module from a vector space V over F and a lin transformation T describes <u>all</u> $F[x]$-modules

An $F[x]$-module is a vector space together with a lin. transformation which specifies the action of x.
This is because if V is an $F[x]$-module then it is an F-module, hence a vector space
And the action of the any element x on V is a linear transformation T from V to V.
The axioms for a module ensure that the actions of F and x on V uniquely determine the action of any element of $F[x]$ on V.

Thus there is a bijection between

$$\left\{ V \text{ an } F[x]\text{-module} \right\} \longleftrightarrow \left\{ \begin{array}{c} V \text{ a v.s over } F \\ \text{and} \\ T: V \to V \text{ a lin} \\ \text{transformation} \end{array} \right\}$$

given by
the element x acts on V as the lin. transformation T.

Let V be an F-vector space viewed as a $F[x]$ module using 2 different linear transformations represented as matrices

$$A, B \in Mat_{n\times n}(F)$$

Let V_A be V with multiplication by $F[x]$ given as $x \cdot v := Av$

and V_B be V " " " "
$x \cdot v := Bv$

Then we have

Thm 9.5 As $F[x]$ modules $V_A \cong V_B$ if and only if $B = UAU^{-1}$ for some $U \in GL_n(F)$

Proof Exercise.