When one thinks of groups, one often thinks of them acting on some set Ω, whereupon the group is "represented" as a subgroup of the group $\mathrm{Sym}(\Omega)$ of all permutations of Ω. Since a ring has more structure than a group, it is not surprising that the natural object upon which to "represent" a ring also more structure. It is these objects, modules, that we wish to investigate in this lecture. It turns out that when we restrict to the natural class of rings that arise in linear algebra, these objects, in a sense, tell us everything that we need to know.

Let M be an abelian group (written additively) and let $\mathrm{End}(M)$ denote the set of endomorphisms of M (as an abelian group). Unless otherwise stated, we will view an element $\varphi \in \mathrm{End}(M)$ as a LEFT endomorphism. We define two binary operations on $\mathrm{End}(M)$ as follows:

$$(\varphi + \psi)(x) := \varphi(x) + \psi(x) \quad \text{and} \quad (\varphi\psi)(x) := \varphi(\psi(x)),$$

for $\varphi, \psi \in \mathrm{End}(M)$ and $x \in M$. These "sum" and "product" operations turn $\mathrm{End}(M)$ into a ring: the RING OF ENDOMORPHISMS OF M (more generally, see Exercise 1). If R is a unital ring, then a REPRESENTATION of R is a ring homomorphism

$$\lambda\colon R \to \mathrm{End}(M)$$

for some abelian group M; the pair (M, λ) is called an R-MODULE. Wherever possible we will suppress mention of the "action" λ and simply call M and R-module under the action $rx := \lambda(r)(x)$. Thus, an R module can also be characterised by a map $R \times M \to M$, $(r, x) \mapsto rx \in M$ satisfying, for all $r, s \in R$ and all $x, y \in M$,

(M1) $r(x + y) = rx + ry$;

(M2) $(r + s)x = rx + sx$;

(M3) $(rs)x = r(sx)$;

(M4) $1x = x$.

Notation & Terminology

(a) As presented, we have described only a LEFT R-module. A RIGHT R-module is M together with a representation $\rho\colon R \to \mathrm{End}(M)$ (the latter now being the ring of right endomorphisms of M) where the (right) action of R on M is given by $xr := (x)\rho(r)$.

(b) When the action is unambiguous, we denote an R-module M simply by ${}_RM$ (or M_R for a right R-module).

(c) If R is any division ring D (in particular, if it is a field), then we call a D-module M a VECTOR SPACE.

(d) If ${}_RM$ and $X \subseteq M$, then RX denotes the set $\{rx \mid x \in X, r \in R\}$. We say that $N \subseteq M$ is a SUBMODULE of M, denoted ${}_RN \leq {}_RM$, if $RN = N$ (i.e. if N is STABLE or INVARIANT under the action of R). A module ${}_RM$ is SIMPLE (or IRREDUCIBLE) if the only submodules are 0 and M itself.

(e) If $X = \{x_1, \ldots x_n\} \subset {}_RM$ is finite, then $RX = \{r_1x_1 + \ldots + r_nx_n \mid r_1, \ldots, r_n \in R\}$, the set of R-linear combinations of X. A submodule ${}_RN \leq {}_RM$ is FINITELY GENERATED if $N = RX$ for some finite set X; it is called CYCLIC if it is generated by a single elements x (i.e. $N = Rx = \{rx \mid r \in R\}$).

For the rest of the course, "module" will mean "finitely generated module"

(f) An R-MODULE HOMOMORPHISM between R-modules ${}_RM$ and ${}_RN$ is a (right) abelian group homomorphism $\varphi\colon M \to N$ which is R-linear. That is,

$$(rx)\varphi = r(x\varphi) \text{ for all } r \in R \text{ and } x \in M.$$

Notice that, by writing module homomorphisms on the right, where the ring action is on the left, the defining property above becomes a form of associativity. We'll use the terms R-module epimorphism, monomorphism and isomorphism without additional comment. If $\varphi\colon M \to N$ is a module homomorphism, then $\ker\varphi = \{x \in M \mid x\varphi = 0\}$ is a submodule of M and $\text{im}\,\varphi = \{x\varphi \mid x \in M\}$ is a submodule of N.

(g) If ${}_RM$ and $N \leq M$, then "congruence modulo N" is R-stable in the sense that if $x \equiv y \pmod N$ then $rx \equiv ry \pmod N$. It follows that R acts on the factor group $M/N = \{x + N \mid x \in M\}$ by $r(x + N) = rx + N$ for all $x \in M$, $r \in R$ and, under this action, M/N is an R-module, called the FACTOR MODULE of M MODULO N.

Examples

(a) Each unital ring R is a module over itelf (denoted ${}_RR$ and called the LEFT REGULAR module) where, for $r, x \in R$, $\lambda(r)x = rx$. The submodules of the left regular module are the left ideals of R. One similarly defines the RIGHT REGULAR module.

(b) Let M be *any* abelian group and R be $\mathbb{Z}$. Then the map $\mathbb{Z} \times M \to M$ sending $(n, x) \mapsto x + \ldots + x = nx$ satisfies axioms (M1) through (M4), and hence turns M into $\mathbb{Z}$-module. Conversely if M is a $\mathbb{Z}$-module, then we claim that $\mathbb{Z}$ must act on M via $x \mapsto nx$ for

$n \in \mathbb{Z}$, $x \in M$. For, if $\lambda\colon \mathbb{Z} \to \mathrm{End}(M)$ is *any* representation of $\mathbb{Z}$, by axioms (M2) and (M4),

$$\lambda(n)(x) = \lambda(1 + \ldots + 1)(x) = \lambda(1)x + \ldots + \lambda(1)x = x + \ldots + x = nx.$$

In other words,

$\mathbb{Z}$-modules are precisely the same as abelian groups

The submodules of a $\mathbb{Z}$-module M are simply the subgroups of the abelian group M.

(Mod1) Theorem [lifting homomorphisms] *Let $\pi\colon M \to N$ be an R-epimorphism from ${}_RM$ onto ${}_RN$ with kernel $\ker\pi = K$. Let $\varphi\colon M \to N'$ be another R-homomorphism with $K \leq \ker\varphi = K'$. Then there is a unique R-homomorphism $\varphi'\colon N \to N'$ such that $\varphi = \pi\varphi'$:*

$$\begin{array}{ccc} & & N \\ & \nearrow^{\pi} & \\ M & & \downarrow \varphi' \\ & \searrow_{\varphi} & \\ & & N' \end{array}$$

Moreover, φ' is a monomorphism iff $K' = K$ and φ' is an epimorphism iff φ is an epimorphism.

Proof. Fix $y \in N$, choose $x \in M$ with $x\pi = y$ and define $y\varphi' := x\varphi$. Since π is an epimorphism, this is the only way to define φ' (hence uniqueness is clear). We do, however, need to check that it's well defined. Suppose $x' \in M$ is such that $x'\pi = x\pi = y$. Then $x - x' \in \ker\pi$ and, since $K \leq K'$, it follows that $x - x' \in \ker\varphi$ so that $x\varphi = x'\varphi$. The map φ' is R-linear: fix $r \in R$, $y \in N$ and $x \in M$ with $x\pi = y$ so that $y\varphi' = x\varphi$; then, since π is R-linear, $(rx)\pi = r(x\pi) = ry$ (so we may choose rx as our preimage of ry) and, since φ is R-linear, $(rx)\varphi = r(x\varphi) = r(y\varphi')$. I leave it as an (easy) exercise to verify that φ' is also a homomorphism of abelian groups. □

We get three standard structure theorems as corollaries of **(Mod1)** which I leave as exercises; they are exact analogues of theorems for abelian groups.

(Mod2) First Isomorphism Theorem. *If $\varphi\colon M \to N$ is an R-homomorphism with $K = \ker\varphi$, then there is a unique R-isomorphism $\varphi'\colon M/K \to \mathrm{im}\ \varphi$ such that $(x + K)\varphi' = x\varphi$ for all $x \in M$.*

(Mod3) Second Isomorphism Theorem. *Let K, N be R-submodules of ${}_RM$. Then $x + (N \cap K) \mapsto x + K$ is an R-isomorhism $N/(N \cap K) \to (N + K)/K$.*

(Mod4) Correspondence Theorem. *Let $\varphi\colon M \to N$ be an epimorphism and set $K := \ker\varphi$. Then φ induces a lattice isomorphism*

$$\{\textit{lattice of submodules of } M \textit{ containing } K\} \longrightarrow \{\textit{lattice of submodules of } N\}$$

We would like to study how a given module ${}_RM$ is built up out of certain "basic" submodules. In the very specialised setting that will be the focus of this course, this study will prove especially fruitful. For the time being, however, we will keep our discussion as general as possible.

If $M_1, M_2 \leq {}_RM$, then we say that M is the DIRECT SUM of M_1 and M_2 (denoted $M = M_1 \oplus M_2$) if $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$. In this setting we will also say that each M_i is a DIRECT SUMMAND of M and that each M_i is a DIRECT COMPLEMENT of the other. If $N \leq M$ is a direct summand of M then we write $N \leq_\oplus M$. A nonzero module ${}_RM$ is INDECOMPOSABLE if it cannot be written as a direct sum of submodules (i.e. whenever $M = M_1 \oplus M_2$, then either M_1 or M_2 is 0).

If $M_1, \ldots, M_k$ are submodules of ${}_RM$ such that $M = M_1 + \ldots + M_k$ and $M_i \cap (M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_k) = 0$ for each $1 \leq i \leq k$ then we write $M = M_1 \oplus \ldots \oplus M_k$. The following result gives a useful characterisation of direct sum decompositions.

(Mod5) Lemma. *$M = M_1 \oplus \ldots \oplus M_k$ iff each $x \in M$ can be written **uniquely** in the form $x = x_1 + \ldots + x_k$ where $x_i \in M_i$ for $1 \leq i \leq k$.*

Proof. Suppose that $M = M_1 \oplus \ldots \oplus M_k$. Then clearly each $x \in M$ can be written in the stated form so it suffices to prove uniqueness. If $x_1 + \ldots + x_k = x = x'_1 + \ldots + x'_k$ then, for $1 \leq i \leq k$,

$$\begin{aligned} x'_i - x_i &= (x_1 - x'_1) + \ldots + (x_{i-1} - x'_{i-1}) + (x_{i+1} - x'_{i+1}) + \ldots + (x_k - x'_k) \\ &\in M_i \cap (M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_k). \end{aligned}$$

It follows that $x_i - x'_i = 0$ so that $x_i = x'_i$.

Conversely, if each $x \in M$ can be written in the form $x = x_1 + \ldots + x_k$, then it follows that $M = M_1 + \ldots + M_k$. Suppose that $y \in M_i \cap (M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_k)$. Then $y = y_i$ for some $y_i \in M_i$ and also $y = y_1 + \ldots + y_{i-1} + y_{i+1} + \ldots + y_k$. But since any such expression for y is unique, it follows that $y = 0$ so that $M = M_1 \oplus \ldots \oplus M_k$. □

(Mod6) Lemma. *If ${}_RM$ and ${}_RN$ and $\varphi\colon M \to N$ and $\varphi'\colon N \to M$ are such that $\varphi'\varphi = \mathrm{id}_N$. Then φ is an epimorphism, φ' is a monomorphism, and $M = \ker\varphi \oplus \mathrm{im}\ \varphi'$.*

Proof. It will suffice to prove the final assertion. Suppose, for $x \in M$, that $x \in \ker\varphi \cap \mathrm{im}\ \varphi'$. Then, for some $y \in N$, we have $x = y\varphi'$. But then $x = y\varphi' = y(\varphi'\varphi)\varphi' = x\varphi\varphi' = 0\varphi' = 0$. Finally, for $x \in M$, we have $x = (x - x\varphi\varphi') + x\varphi\varphi' \in \ker\varphi + \mathrm{im}\ \varphi'$. □

The following fact is trivial but useful to keep in mind.

(Mod7) Lemma. *For a nonzero module ${}_RM$, the following are equivalent:*

(a) M is indecomposable;

(b) For every pair $M_1, M_2 \leq M$, if $M_1 \cap M_2 = 0$, then $M_1 + M_2 \neq M$;

(c) For every pair $M_1, M_2 \leq M$, if $M_1 + M_2 = M$, then $M_1 \cap M_2 = 0$.

(Mod8) Lemma. *Let $M = M_1 \oplus M_2 \ldots \oplus M_n$ and let $\iota_j \colon M_j \to M$ be the inclusion map for $1 \leq j \leq n$. Then there exist epimorphisms $\pi_j \colon M \to M_j$ $(1 \leq j \leq n)$ such that $\iota_j \pi_k = \delta_{jk} \mathrm{id}_{M_k}$ for $1 \leq j, k \leq n$ and such that $\pi_1 \iota_1 + \ldots + \pi_n \iota_n = \mathrm{id}_M$.*

Sketch of proof. First observe that each $x \in M$ can be written **uniquely** in the form $x = x_1 + x_2 + \ldots + x_n$. Now verify that the map $\pi_j \colon M \to M_j$ sending $x \mapsto x_j$, for $1 \leq j \leq n$, is an epimorphism and that $\pi_1, \ldots, \pi_n$ satisfy the stated conditions. □

In the case when $M = M_1 \oplus M_2$, the map π_1 constructed in the proof above is called the PROJECTION of M on M_1 ALONG M_1. In general a direct summand M_1 of a module M may have many different direct complements; the next result gives a test, using the projection π_1, for deciding whether or not a given submodule of M is a direct complement of M_1.

(Mod9) Lemma. *Let $M = M_1 \oplus M_2$ and let $\pi_2 \colon M \to M_2$ be the projection of M on M_2 along M_1. A submodule $N \leq M$ is a direct complement of M_1 in M iff $\pi_2|_N \colon N \to M_2$ is an isomorphism.*

Proof. For simplicity, let π denote the restriction $\pi_2|_N$. First note that $\ker \pi = M_1 \cap N$ so that $M_1 \cap N = 0$ iff $\ker \pi = 0$. Next

$$\begin{aligned} N\pi &= (M_1 + N)\pi = ((M_1 + N) \cap M)\pi \\ &= ((M_1 + N) \cap (M_1 + M_2))\pi = (M_1 + (M_1 + N) \cap M_2)\pi \\ &= ((M_1 + N) \cap M_2)\pi = (M_1 + N) \cap M_2. \end{aligned}$$

So $N\pi = M_2$ iff $M_2 \leq M_1 + N$ iff $M_1 + N = M$. □

The following notion should sound familiar. A subset X of a module ${}_RM$ is LINEARLY INDEPENDENT if, for every finite set $\{x_1, \ldots, x_n\}$ of **distinct** elements of X and for each $r_1, \ldots, r_n \in R$,

$$r_1 x_1 + r_2 x_2 \ldots + r_n x_n = 0 \quad \Rightarrow \quad r_1 = r_2 = \ldots = r_n = 0.$$

A list $x_1, \ldots, x_n$ of distinct elements of ${}_RM$ is called INDEPENDENT if the set $\{x_1, \ldots, x_n\}$ is linearly independent. We say that a module ${}_RF$ is a FREE MODULE if there exists a (finite) linearly independent set X such that $F = RX$ (i.e. X generates F as R-module). We call each independent list $x_1, \ldots, x_n$ such that $X = \{x_1, \ldots, x_n\}$ generates F a FREE BASIS for F. If ${}_RF$ has free basis $x_1, \ldots, x_n$, then the map $\rho \colon R^n \to F$ sending $(r_1, \ldots, r_n) \mapsto r_1 x_1 + \ldots + r_n x_n$ is an isomorphism of R-modules (see

Exercise 4). Hence, free modules are determined up to isomorphism by their RANK, namely the cardinality of X.

The next result states that when we restrict to the case when $R = \mathbb{F}$ is a field, all modules are free.

(Mod10) Theorem. *Let $\mathbb{F}$ be a field and let ${}_{\mathbb{F}}V$ be an $\mathbb{F}$-module (vector space). Then every maximal independent list $v_1, \ldots, v_n$ of elements of V is a (free) basis for V (in particular, every $\mathbb{F}$-space is free).*

Proof. Let $v_1, \ldots, v_n$ be maximal independent and let $w \in V \setminus \{v_1, \ldots, v_n\}$. Then $w, v_1, \ldots, v_n$ is dependent, so there exist $0 \neq \alpha, \alpha_1, \ldots, \alpha_n \in \mathbb{F}$ such that $\alpha w + \alpha_1 v_1 + \ldots + \alpha_n v_n = 0$. But, since $\mathbb{F}$ is a field, we have $w = -(\alpha_1/\alpha)v_1 - \ldots - (\alpha_n/\alpha)v_n \in \mathbb{F}\{v_1, \ldots, v_n\}$. □

It follows from **(Mod10)** that if ${}_{\mathbb{F}}V$ is a finite dimensional vector space, then there exists a free basis, $v_1, \ldots, v_n$ say, such that $V = \mathbb{F}\{v_1, \ldots, v_n\} = \mathbb{F}v_1 \oplus \ldots \oplus \mathbb{F}v_n$. In this setting, a free basis is referred to simply as a BASIS of the vector space V and the (free) rank of V is called the DIMENSION of V and is denoted $\dim(V)$. In any free module ${}_RF$ for an arbitrary ring R, an independent list of elements of ${}_RF$ can be extended to a maximal independent list. The latter, however, need not be a free basis of ${}_RF$. But, in the case when $R = \mathbb{F}$ is a field, any independent list of vectors can be extended to a basis of the vector space.

At the beginning of this lecture we introduced an R-module M by specifying the action of R as endomorphisms of the abelian group M. We have since encountered the notion of an R-module homomorphism and we call an R-homomorphism from M to itself an R-ENDOMORPHISM and denote the set of all such by $\mathrm{End}_R(M)$. We note that $\mathrm{End}_R(M)$ is a ring (see Exercise 1) but it is not, in general, commutative (even if R is!) With this notation, since abelian groups are simply $\mathbb{Z}$-modules, we have $\mathrm{End}(M) = \mathrm{End}_{\mathbb{Z}}(M)$; that is, what we previously understood as an "endomorphism" is really a "$\mathbb{Z}$-endomorphism".

In keeping with our notation for R-homomorphisms, we regard R-endomorphisms as operating on the right. We point out that each R-module ${}_RM$ is therefore a BIMODULE ${}_RM_{\mathrm{End}_R(M)}$; R acting on the left and $\mathrm{End}_R(M)$ acting on the right. We continue now to study R-endomorphisms of a free module ${}_RF$. Try to keep in mind what you already know about linear transformations of a vector space. To help, I will use the letter T to denote a fixed element of $\mathrm{End}_R(F)$.

(Mod11) Lemma. *Let ${}_RF$ be a free module with basis $x_1, \ldots, x_n$ and let $y_1, \ldots, y_n$ be any sequence of elements in ${}_RF$. Then there exists a unique $T \in \mathrm{End}_R(F)$ such that $x_iT = y_i$ for $1 \leq i \leq n$.*

Proof. Define a map $T_0 \colon F \to F$ sending $r_1x_1 + \ldots + r_nx_n \mapsto r_1y_1 + \ldots + r_ny_n$. Clearly $x_iT_0 = y_i$ for $1 \leq i \leq n$ as required and one checks that $T_0 \in \mathrm{End}_R(F)$. For $x \in F$, there exist unique $r_1, \ldots, r_n \in R$ such that $x = r_1x_1 + \ldots + r_nx_n$. Hence, if $T \in \mathrm{End}_R(F)$ is such that $x_iT = y_i$ for $1 \leq i \leq n$ then, $xT = (r_1x_1 + \ldots + r_nx_n)T = r_1(x_1T) + \ldots + r_n(x_nT) = r_1y_1 + \ldots + r_ny_n = xT_0$, so that $T = T_0$. □

In the language of vector spaces, **(Mod11)** states that a linear transformation of a vector space V is completely determined by the images of a basis of V and, furthermore, that a basis can be mapped to any sequence of n points in V using a linear transformation.

Next let $\mathbb{M}_n(R)$ denote the ring of all $n \times n$ matrices over R. For a given $A = [[a_{ij}]] \in \mathbb{M}_n(R)$ define points $y_j := \sum_{i=1}^{n} a_{ij}x_i$ for $1 \leq j \leq n$. By Lemma 5, there exists a unique R-endomorphism $T_A \colon F \to F$ sending $x_j \mapsto y_j$ for $1 \leq j \leq n$. Hence we obtain a map $\lambda \colon \mathbb{M}_n(R) \to \mathrm{End}_R(F)$ sending $A \mapsto T_A$ from which the following powerful observation follows.

(Mod12) Theorem. If ${}_RF$ is a free module with free basis $x_1, \ldots, x_n$, then $\lambda \colon \mathbb{M}_n(R) \to \mathrm{End}_R(F)$ is a ring isomorphism.

Proof. Exercise 5.

In particular, when studying endomorphisms of a vector space we can, whenever we deem it useful, work instead with matrices having entries in a division ring.

Exercises.

1. For an R-module ${}_RM$, show that $\mathrm{End}_R(M)$ is a ring.
2. Show that if $X \subseteq M$ is any set, then $RX \leq {}_RM$; RX is the submodule generated by X.
3. Show that if $N_1, N_2 \leq {}_RM$, then $N_1 \cap N_2 \leq {}_RM$ and $N_1 + N_2 \leq {}_RM$.
4. If ${}_RF$ has free basis $x_1, \ldots, x_n$, show that the map $\rho \colon R^n \to F$ sending $(r_1, \ldots, r_n) \mapsto r_1x_1 + \ldots + r_nx_n$ is an isomorphism of R-modules.
5. Show that the map $A \mapsto \lambda_A$ defines an isomorphism of rings $\mathbb{M}_n(R) \to \mathrm{End}_R(F)$.
6. Let $\mathbb{F}$ be a field, V a vector space over $\mathbb{F}$, and $T \in \mathrm{End}_{\mathbb{F}}(V)$. For $f(x) = a_nx^n + \ldots + a_1x + a_0$ in the polynomial ring $\mathbb{F}[x]$, define a map $f(T) \colon V \to V$ as follows: for each $v \in V$, $v(f(T)) := a_n(vT^n) + \ldots + a_1(vT) + a_0v$, where $vT^i = ((\ldots(vT)\ldots)T)T$.
   (a) Show that $f(T) \in \mathrm{End}_{\mathbb{F}}(V)$.
   (b) If $\langle T \rangle = \{f(T) \mid f(x) \in \mathbb{F}[x]\}$, show that $\langle T \rangle$ is a subring of $\mathrm{End}_{\mathbb{F}}(V)$. The map $\varphi_T \colon \mathbb{F}[x] \to \langle T \rangle$ sending $f(x) \mapsto f(T)$ is clearly an epimorphism of rings. Discuss the kernel, $\ker \varphi_T$, of this epimorphism.

   Notice what this exercise demonstrates. For each $T \in \mathrm{End}_{\mathbb{F}}(V)$ we get a module $V_{\mathbb{F}[x]}$, where the action of $\mathbb{F}[x]$ on V is given by φ_T: for $v \in V$ and $f(x) \in \mathbb{F}[x]$, $vf(x) := v(f(T))$. This construction will play a key role in what is to follow.
7. Prove **Schur's Lemma:** *If the module ${}_RM$ is simple then* $\mathrm{End}_R(M)$ *is a field.*
   Is the converse true?

8. Show that the map $\varphi\colon \mathbb{F}[x] \to \mathbb{F}[x]$ sending $f(x) \mapsto f(x^2)$ is a ring homomorphism but is not an $\mathbb{F}[x]$-endomorphism of the regular module ${}_{\mathbb{F}[x]}\mathbb{F}[x]$. Note that im φ is a subring of $\mathbb{F}[x]$ but is not an ideal (why not?); hence im φ is not a submodule of ${}_{\mathbb{F}[x]}\mathbb{F}[x]$.