4.4. **Modules.** Informally, a module is a structure where you can add elements in the module, and multiply module elements by the ring elements.

Definition. Let A be a ring. A **module** over A (or "A-module") is an abelian group $(M, +)$ equipped with an operation $A \times M \to M$, denoted

$$(a, m) \mapsto am,$$

satisfying

(1) $1m = m \qquad \forall m \in M.$
(2) $a(bm) = (ab)m \qquad \forall a, b \in A, m \in M$
(3) $(a + b)m = am + bm \qquad \forall a, b \in A, m \in M$
(4) $a(m + n) = am + bn \qquad \forall a \in A, m + n \in M.$

Example. For any ring A, the 0-module has one element 0, and addition and multiplication are trivially defined.

Example. Let k be a field. Then a k-module is quite literally the same thing as a k-vector space.

Example. A $\mathbb{Z}$-module is the "same thing" as an abelian group, meaning any abelian group admits a unique structure as a $\mathbb{Z}$-module. To see this, let G be an abelian group. We define a $\mathbb{Z}$-module structure on G by, for $n \in \mathbb{Z}, g \in G$

$$ng = \begin{cases} \overbrace{g + \cdots + g}^{n} \text{ if } n > 0 \\ 0g = 0 \\ ng = \overbrace{(-g) + \cdots + (-g)}^{-n} \text{ if } n < 0. \end{cases}$$

One can check that this is a well-defined $\mathbb{Z}$-module structure. Moreover, this $\mathbb{Z}$-module structure is forced on us by the axioms: If $n > 0$ we must have

$$ng = (1 + \cdots + 1)g = 1g + 1g + \cdots + 1g = \overbrace{g + \cdots + g}^{n},$$

and similar considerations tell us what ng has to be for $n \leq 0$.

Example. Let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ is an A-module in a natural way, since given $x \in A$ and $a \in \mathfrak{a}$, we have $xa \in \mathfrak{a}$, and the operation $(x, a) \mapsto xa$ satisfies the axioms of the definition.

Example. Let $\phi\colon A \to B$ be a homomorphism. Then B has a natural structure of A-module, defined by

$$ab = \phi(a)b \qquad \forall a \in A, b \in B.$$

This generalises the useful fact from field theory that if $\phi\colon k \to k'$ is a homomorphism of fields, then k' is a k-vector space.

Definition. Let M and N be A-modules. A **homomorphism** of A-modules from M to N is a map $\phi\colon M \to N$ such that

$$\phi(m + m') = \phi(m) + \phi(m') \qquad \forall m, m' \in M$$
$$\phi(am) = a\phi(m) \qquad \forall a \in A, m \in M$$

If ϕ is a bijection, we say it is an **isomorphism** of A-modules.

Example. For A-modules M and N, we always have a homomorphism $0\colon M \to N$ given by

$$0(m) = 0 \qquad \forall m \in M.$$

Example. Let k be a field, and let M and N be k-modules. Then a homomorphism $M \to N$ is the same thing as a linear map of vector spaces. So if M and N are finite-dimensional as vector spaces, we can choose bases and represent ϕ by a $(\dim N) \times (\dim M)$-matrix.

Example. A homomorphism of $\mathbb{Z}$-modules is the same thing as a homomorphism of (abelian) groups. This boils down to the fact that given a homomorphism $\phi\colon M \to N$ of abelian groups, the condition

$$\phi(nx) = n\phi(x)$$

is automatically satisfied.

Example. Let $a \in A$, and consider $(a) \subseteq A$ as an A-module. There is a homomorphism of A-modules

$$\phi\colon A \to (a)$$

given by

$$\phi(x) = xa.$$

This is surjective, with kernel equal to $\mathrm{Ann}(a)$.

Definition. Let M and N be A-modules, and let $\mathrm{Hom}_A(M, N)$ be the set of homomorphisms. This set has a structure of an A-module, where for $\phi, \psi \in \mathrm{Hom}_A(M, N), a \in A$ and $m \in M$, we have

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$
$$(a\phi)(m) = a\phi(m)$$

Example. Let k be a field, and consider the modules k^m, k^n. Then $\mathrm{Hom}_k(k^m, k^n)$ is naturally identified with the set of $(n \times m)$-matrices with entries in k, and the above states that this set has a natural structure of k-module (or k-vector space).

Direct sums, submodules and quotient modules.

4.5. **Direct sums.** Given a sequence of abelian groups $G_1, \ldots, G_n$, the product set $G_1 \times \cdots \times G_n$ is naturally an abelian group. This generalises directly to modules:

Definition. Let M_1, M_2 be A-modules. The direct sum of the M_1 and M_2 is the module

$$M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\},$$

with

$$(m_1, m_2) + (m_1', m_2') = (m_1 + m_1', m_2 + m_2'), \quad a(m_1, m_2) = (am_1, am_2).$$

Definition. Given A-modules $M_1, \ldots, M_n$, we have the direct sum

$$\bigoplus_{i=1}^{n} M_i = M_1 \oplus \cdots \oplus M_n = \{(m_1, \ldots, m_n) \mid m_i \in M_i\},$$

with addition and A-multiplication similar. If $M_1 = \cdots = M_n = M$, we may write $M^{\oplus n}$ instead.

Given a set of A-modules $\{M_i\}_{i \in S}$, their direct sum is

$$\oplus_{i \in S} M_i = \{(m_i)_{i \in S} \mid m_i \in M_i, \text{ only finitely many } m_i \neq 0\},$$

while their direct product is

$$\prod_{i\in S} M_i = \{(m_i)_{i\in S} \mid m_i \in M_i\},$$

If S is finite, then the direct sum and direct product are the same, but in general they differ.

Example. Let k be a field. Every vector space V over k has a basis, meaning there is a set $\{v_i\}_{i\in S}$ such that every $v \in V$ can be expressed uniquely as a sum

$$\sum_{i\in S} a_i v_i \qquad a_i \in k,$$

with only finitely many $a_i \neq 0$.

Define a homomorphism

$$\phi\colon \bigoplus_{i\in S} k \to V$$

by

$$\phi((a_i)) = \sum_{i\in S} a_i v_i.$$

Since $\{v_i\}_{i\in S}$ is a basis for V, every v equals $\phi((a_i))$ for a unique $(a_i) \in \bigoplus_{i\in S} k$, meaning ϕ is an isomorphism, and $\oplus_{i\in S} k \cong V$.

Example. Consider $\mathbb{R}[x, y]$, and define $T = \mathbb{R}[x, y] \oplus \mathbb{R}[x, y]$. Thus elements of T are pairs (f_1, f_2) with $f_1, f_2 \in \mathbb{R}[x, y]$. We may think of elements of T as vector fields on $\mathbb{R}^2$ with components given by polynomials.

Example. Let A be a ring, and consider $A[x]$ as an A-module, i.e. if $f = a_n x^n + \cdots + a_0 \in A[x]$ and $a \in A$, we have

$$af = aa_n x^n + \cdots aa_1 x + aa_0.$$

We have a homomorphism of A-modules

$$\phi\colon \bigoplus_{i\in\mathbb{N}} A \to A[x],$$

Note that this is just a module isomorphism; in fact the left hand side does not have a natural ring structure.

4.6. **Submodules.** If G is an abelian group, a subset $G' \subseteq G$ which is closed under addition and inverses is a subgroup. We can then form the quotient group $G'' = G/G'$, whose elements are the cosets of G' in G. This concept and most of the theory generalises neatly from abelian groups to modules, where we defined submodules as follows.

Definition. Let M be an A-module. A subset $M' \subseteq M$ is a **submodule** if it is a subgroup and for all $a \in A, m \in M'$, we have $am \in M'$.

Example.

- A submodule of A is the same thing as an ideal in A.
- A submodule of a $\mathbb{Z}$-module M is the same thing as a subgroup of M, since if $M' \subseteq M$ is a subgroup, $n \in \mathbb{Z}$ and $m' \in M'$, we automatically have $nm' = m' + \cdots + m' \in M'$ (when n is positive, similar arguments work when n is negative).

Given $M, M' \subseteq N$, we have their sum defined as $M + M' \subseteq N$, given by

$$M + M' = \{m + m' \mid m \in M, m' \in M\}.$$

This generalises the notion of sum of ideals.

Example. With ring $\mathbb{R}[x, y]$ and $T = \mathbb{R}[x, y]^{\oplus 2}$, we have the submodule $T' \subset T$ given by

$$T' = \{(fx, fy) \mid f \in \mathbb{R}[x, y]\}$$

Informally, this is the submodule of vector fields which point outwards from the origin at all points. We have $\phi\colon \mathbb{R}[x, y] \to T$ given by $\phi(f) = (fx, fy)$, and this is an isomorphism.

Let's take $T'' = \{(g, 0) \mid g \in \mathbb{R}[x, y]\} \subset T$, this is again a submodule, the horizontal vector fields.

We have

$$T' + T'' = \{(fx + g, fy) \mid f, g \in \mathbb{R}[x, y]\} = \{(h, fy) \mid h, f \in \mathbb{R}[x, y]\},$$

vector fields which are horizontal along the x-axis.

4.7. **Quotients.** If M' is a submodule of M, then the group M/M' has a natural structure of A-module such that $M \to M/M'$ is a homomorphism of A-modules. Concretely, we define the A-multiplication on M' by

$$a(m + M') = am + M'$$

In particular, for any ideal $\mathfrak{a}$, the quotient ring $A/\mathfrak{a}$ is an A-module.

4.8. **Kernels, images and cokernels.**

Definition. Let $\phi\colon M \to N$ be a homomorphism of A-modules. We have

- The **kernel** of ϕ,
$$\ker \phi \subseteq M,$$
a submodule of M.
- The **image** of ϕ,
$$\operatorname{im} \phi = \{\phi(m) \mid m \in M\} \subseteq N,$$
a submodule of N.
- The **cokernel** of ϕ,
$$\operatorname{cok} \phi = N/\operatorname{im} M.$$

Example. Let $a_1, \ldots, a_n \in A$, and define

$$\phi\colon \bigoplus_{i=1}^{n} A \to A$$

by

$$\phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i a_i.$$

Then

$$\operatorname{im}(\phi) = \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \mid x_i \in A\} = (a_1, \ldots, a_n) \subseteq A.$$

The following statements are "well known" for abelian groups, and the content of this proposition is that the natural isomorphisms respect the module structures as well.

Proposition ("Module isomorphism theorems")**.**

- *Let $\phi\colon M \to N$ be a homomorphism of modules. We have*
$$\operatorname{im} M \cong M/\ker \phi.$$
- *Let $M'' \subseteq M' \subseteq M$ be A-modules and submodules. There is an isomorphism*
$$M/M' \cong (M/M'')/(M'/M'')$$
- *Let $M, N \subseteq P$ be submodules, so that we have submodules $M + N \subseteq P$ and $M \cap N \subseteq P$. Then*
$$(M + N)/N \cong M/(M \cap N)$$

Definition. A module M is **finitely generated** if either of the following two equivalent conditions hold:

- There exists $m_1, \dots, m_n \in M$ such that every $m \in M$ is of the form $x_1 m_1 + \cdots + x_n m_n$, with $x_i \in A$.
- There exists a surjective homomorphism $\phi\colon \bigoplus_{i=1}^n A \to M$.

Example.

- An abelian group is finitely generated as a group if and only if it is finitely generated as a $\mathbb{Z}$-module.

  So every finitely generated $\mathbb{Z}$-module is isomorphic to one of the form
$$\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \mathbb{Z} \oplus \mathbb{Z}/(p_1^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p_n^{e_n}),$$
  while $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.
- If k is a field, then a finitely generated k-module is the same thing as a finite-dimensional k-vector space.
- An ideal $\mathfrak{a} \subseteq A$ is finitely generated as an A-module if and only if it is finitely generated as an ideal, i.e. it is of the form $(a_1, \dots, a_n)$.

Recall the definitions of local ring and finitely generated module.

Let's now recall that given an ideal $\mathfrak{a}$ and an A-module M, the submodule $\mathfrak{a}M \subset M$ is the module containing all sums

$$a_1 m_1 + \cdots + a_n m_n, \qquad a_i \in \mathfrak{a}, m_i \in M.$$

Lemma (Nakayama's lemma, local version)**.** [5] *Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated module. If $\mathfrak{m}M = M$, then $M = 0$.*

Definition. Let $T = (b_{ij})_{1 \le i,j \le n}$ be an $(n \times n)$-matrix with entries in A, and let T_{ij} be the $(n \times n)$-matrix obtained by deleting row i and column j. The **adjugate** of T is the matrix $\operatorname{adj}(T) = (c_{ij})_{1 \le i,j \le n}$, where

$$c_{ij} = (-1)^{i+j} \det(T_{ji}).$$

Example. The adjugate of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

Theorem. *We have $T \operatorname{adj}(T) = \operatorname{adj}(T) T = \det(T) I_n$, where I_n is the $(n \times n)$ identity matrix.*

Proof of Nakayama's lemma. Let M be a module, generated by $m_1, \ldots, m_n \in M$, meaning $M = \{a_1 m_1 + \cdots + a_n m_n \mid a_i \in A\}$. We know that $\mathfrak{m}M = M$, which means that for every m_i, we have $m_i \in \mathfrak{m}M$, which means we can write

$$m_i = \sum_{j=1}^{n} b_{ij} m_j,$$

with $b_{ij} \in \mathfrak{m}$. Letting $T = I_n - (b_{ij})$, we then get that

$$T \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} = 0,$$

and so

$$\operatorname{adj}(T) T \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} = 0,$$

which since $\operatorname{adj}(T)T = \det(T) I_n$ gives $\det(T) m_i = 0$ for all i. But looking at the cofactor expansion of $\det(T)$ shows that

$$\det(T) = 1 + X,$$

where all the terms of X are divisible by b_{ij}, which implies that $X \in \mathfrak{m}$. Hence $\det(T)$ is a unit, and so $\det(T) m_i = 0$ implies $m_i = 0$. Thus all the $m_i = 0$, and so $M = 0$. □

Corollary. *Let A be a local ring, and let $\phi \colon M \to N$ be a homomorphism of modules, such that $\widetilde{\phi} \colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Then ϕ is surjective.*

Proof. The trick is to reinterpret "ϕ is surjective" as $\operatorname{cok} \phi = N/\phi(M) = 0$. Assume that $\widetilde{\phi}$ is surjective. That means $N = \phi(M) + \mathfrak{m}N$ (after some thought). We get

$$\mathfrak{m}(N/\phi(M)) = (\mathfrak{m}N + \phi(M)/\phi(M)) = N/\phi(M),$$

[5] The textbook states a more general version where A is not necessarily local, where $\mathfrak{m}$ is replaced with the Jacobson radical of A.

Since N is finitely generated, so is $N/\phi(M)$. We can then apply Nakayama's lemma to $N/\phi(M)$, and get $N/\phi(M) = 0$. $\square$

Example. Work in $A \subset \mathbb{R}(x)$ from before. Consider the matrix

$$B = \begin{pmatrix} \frac{1+x^2}{1-x^2} & \frac{x^2}{1-x^3} \\ \frac{x^4}{2-5x} & \frac{1+x}{1-x} \end{pmatrix}$$

which gives a homomorphism of A-modules $\phi\colon A^{\oplus 2} \to A^{\oplus 2}$ by

$$\phi(f,g) = B \begin{pmatrix} f \\ g \end{pmatrix}.$$

The associated homomorphism of $\widetilde{\phi}\colon A^{\oplus 2}/\mathfrak{m}A^{\oplus 2} \to A^{\oplus}2/\mathfrak{m}A^{\oplus 2}$ can be identified with the linear map $\mathbb{R}^2 \to \mathbb{R}^2$ obtained by setting $x = 0$ in the above matrix. That map is clearly surjective, hence ϕ is.

4.9. **Exact sequences and additivity.** Given $\phi\colon M \to N$ a homomorphism, we know about $\ker\phi \subset M$, $\operatorname{im}\phi \subset N$, $\operatorname{cok}\phi = N/\operatorname{im}\phi$.

Definition. A sequence of morphisms $M_1 \overset{\phi_1}{\to} M_2 \to \cdots \to M_{n-1} \overset{\phi_{n-1}}{\to} M_n$ is **exact at** M_i, $2 \le i \le n-1$, if we have

$$\operatorname{im}\phi_i = \ker\phi_{i+1}.$$

It is **exact** A sequence of the form

$$0 \to M' \to M \to M'' \to 0$$

is called **short exact**.

Example. If $M_i = 0$, then we have $\operatorname{im}\phi_i = 0$, so $\ker\phi_{i+1}$, and exactness at M_{i+1} means simply that $\ker\phi_{i+1} = 0$, i.e. that ϕ_{i+1} is injective. We also have $\ker\phi_{i-1} = M_{i-1}$, so exactness at M_{i-1} means that $\operatorname{im}\phi_{i-2} = M_{i-1}$, i.e. that ϕ_{i-2} is surjective.

Example. Let $M' \subseteq M$ be a submodule. Then the sequence

$$0 \to M' \to M \to M/M' \to 0$$

is exact, since (1) $M' \to M$ is injective, (2) $M \to M/M'$ is surjective, and (3) $\ker(M \to M/M') = \operatorname{im}(M' \to M)$.

"Up to isomorphism", every short exact sequence is of this form, meaning if

$$0 \to M_1 \to M \to M_2 \to 0$$

is short exact, them M_1 is isomorphic to some submodule $M' \subset M$, and M_2 is isomorphic to M/M'.

Example. The sequence $0 \to \mathbb{Z} \overset{\phi}{\to} \mathbb{Z} \to \mathbb{Z}/(n) \to 0$ is exact, where $\phi(k) = nk$.

Example. The sequence $0 \to \mathbb{Z}/(2) \to \mathbb{Z}/(4) \to \mathbb{Z}/(2) \to 0$ is exact, where $\mathbb{Z}/(2)$ is the inclusion $1 \mapsto 2$.

Example. Let V be the $\mathbb{R}$-vector space of all smooth vector fields on $\mathbb{R}^3$, and let W be the $\mathbb{R}$-vector space of all functions on $\mathbb{R}^3$. The sequence

$$0 \to \mathbb{R} \overset{a \mapsto f(x)=a}{\to} W \overset{\nabla}{\to} V \overset{\nabla\times}{\to} V \overset{\nabla\cdot}{\to} W \to 0$$

is exact.

Example. For any modules M and N, the sequence

$$0 \to M \to M \oplus N \to N \to 0$$

is exact, where $M \to M \oplus N$ is the map $m \mapsto (m, 0)$ and $M \oplus N \to N$ is the map $(m, n) \to n$.

We can break up exact sequences into short ones, as follows: If $M_{i-1} \to M_i \to M_{i+1}$ is an exact sequence, we can take $0 \to \operatorname{im}(\phi_{i-1}) \to M_i \to \operatorname{im}(\phi_i) \to 0$ as a short exact sequence. This motivates the following definition

Definition. A function from some set of modules to an abelian group G is called **additive** if for all short exact sequences

$$0 \to M' \to M \to M'' \to 0$$

we have $\nu(M) = \nu(M') + \nu(M'')$.

Example. If M', M, M'' are finite-dimensional vector spaces, then $\dim(-)$ is additive, since we can extend a basis for M' to a basis for M, and the new elements give a basis for M'' after projection.

Example. If M', M, M'' are finite abelian groups, then $\nu(M) = |M|$, the number of elements of M, is an additive function to the group $\mathbb{Q}_{>0}$ with the operation of multiplication, since Lagrange's theorem says that for subgroups $M' \subset M$ we always have

$$|M| = |M'||M/M'|.$$

Theorem. *Let $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ be an exact sequence, and let ν be an additive function. Then*

$$\sum (-1)^i \nu(M_i) = 0$$

Proof. We have $\nu(M_i) = \nu(\operatorname{im} \phi_i) + \nu \operatorname{im}(\phi_{i-1})$. Inserting this in $\sum(-1)^i \nu(M_i)$ everything cancels to give 0. □

Example. In an exact sequence of vector spaces $0 \to V_1 \to V_2 \to \cdots \to V_n \to 0$, we have $\sum(-1)^i \dim V_i = 0$.

Example. Given an exact sequence

$$0 \to M_1 \to \cdots \to M_n \to 0$$

of finite $\mathbb{Z}$-modules, we have

$$\prod_{i=1}^{n} |M_i|^{(-1)^i} = 1.$$

Definition. A diagram of modules and homomorphisms between them is called **commutative** if the composed maps between any two modules agree.

Example. The diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle g} \\ N & \xrightarrow{h} & N' \end{array}$$

is commutative if $g \circ f = h \circ i$.

Lemma (The snake lemma)**.** *Assume that we are given modules and homomorphisms that fit into the following commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0. \end{array}$$

If both rows are exact, we get an exact sequence of modules

$$0 \to \ker \phi' \to \ker \phi \to \ker \phi'' \to \operatorname{cok} \phi' \to \operatorname{cok} \phi \to \operatorname{cok} \phi'' \to 0$$