Homology

Maxime Willaert

August 25, 2024

Contents

Part I

Homological Algebra, Lectures of Tim Van der Linden [1]

Chapter 1

Remaining questions

Proof that the dimension of a free module over a commutative ring is well-defined using Krull's theorem (example 2.1.10).

Chapter 2

Modules over a ring, exact sequences and homology

Based on lectures given by Tim Van der Linden in 2022-2023 [1] (might turn out to be a copy).

2.1 Modules over a ring

The rings are not assumed to be commutative, only to possess a unit 1.

Definition 2.1.1 (Ring)**.** A **ring** is an abelian group R (written additively) together with a binary operation

$$\cdot : R \times R \to R, (r, a) \to r \cdot a \overset{n}{=} ra$$

such that $(R, \cdot)$ is a monoid with unit 1, and such that $\cdot$ is distributive over $+$, meaning that for all $a, a', r, r' \in R$

(i) (Left-distributivity) $r(a + a') = ra + ra'$;

(ii) (Right-distributivity) $(r + r')a = ra + ra'$.

Given two rings R, S a ring morphism $R \to S$ is a group of morphism $R \to S$ that is also a monoid morphism $(R, \cdot) \to (S, \cdot)$. In other words a ring morphism is a map $\phi : R \to S$ such that

(i) For all $r, r' \in R$, $\phi(r + r') = \phi(r) + \phi(r')$;

(ii) For all $r, r' \in R$, $\phi(rr') = \phi(r)\phi(r')$;

(iii) $\phi(1) = 1$.

Example 2.1.1. By definition, a monoid is always with unit (or identity). A nonzero ring with commutative multiplication and multiplicative inverses for every non-zero element is called a **field**. Note that in any ring R we have $0a = (0+0)a = 0a + 0a$ which implies $0a = 0$ (and similarly we have $a0 = 0$), so unless $0 = 1$, 0 cannot admit a multiplicative inverse, and $1 = 0$ if and only if R is the **zero ring** (the ring with one element, denoted 0).

Example 2.1.2. Let R, S be two rings with S nonzero (for example we could choose $R = S = \mathbb{Z}_2$). The zero map $0 : R \to S$ sending R to $0 \in S$ is a group morphism such that $0(rr') = 0 = 00 = 0(r)0(r')$ for all $r, r' \in R$. However $0(1) \neq 1$ so we see that removing the requirement that the multiplicative identity be preserved from the definition of a ring morphism results in a strictly weaker definition. In other words, the category **Ring** of unitary rings (rings with multiplicative identity) is *not* a full subcategory of **Rng**, the category of **pseudo-rings** (the object obtained by removing the requirement for a multiplicative identity from the definition of a ring - also called a ring by some authors).

Modules are to rings what vector spaces are to fields.

Definition 2.1.2 (Module)**.** Let R be a ring. A **left R-module** is an abelian group A (written additively) together with an operation (scalar multiplication)

$$\cdot : R \times A \to A, (r, a) \to r \cdot a \stackrel{n}{=} ra$$

such that for all $r, r' \in R$, $a, a' \in A$

(i) (Distributivity) $(r + r')a = ra + r'a$ and $r(a + a') = ra + ra'$;

(ii) (Multiplicative compatibility) $(rr')a = r(r'a)$;

(iii) (Identity) $1a = a$.

Given two left R-modules, A and B, an **R-linear map** (or morphism of R-modules) $A \to B$ is a group morphism (for the abelian group structure of A and B) $\phi : A \to B$ such that $\phi(ra) = r\phi(a)$ for $r \in R$, $a \in A$. **Isomorphisms** are define in the usual way (as invertible R-linear maps with R-linear inverses), it turns out that the inverse of a bijective R-linear map is automatically R-linear, so that isomorphisms of R-modules are exactly the bijective R-linear maps.

Remark. An R-linear map $\phi : A \to B$ necessarily sends $0 \in A$ to $0 \in B$ as a morphism of abelian groups. Furthermore, for any pair of R-modules A, B the **zero map** sending A to $0 \in B$ is trivially R-linear.

Remark. We can define **right R-modules** in the obvious way. Given a ring R we can define the **opposite ring** R^{op} with the same underlying set, the same addition and reversed multplication, i.e. $r \cdot_{op} r' := r'r$ for $r, r' \in R$. We can then see that right R-modules are exaclty left R^{op}-modules. For a commutative ring $R = R^{op}$ and there is no distinction between left and right R-modules. In what follows we'll often use "R-modules" to refer to *left* R-modules.

Example 2.1.3. Any ring R is canonically a module over itself. For any ring R there also exists a **zero R-module**, a module with a single element (which must be 0) denoted by 0.

Example 2.1.4. For a field $\mathbb{F}$, a (left or right) $\mathbb{F}$-module is a **vector space** over $\mathbb{F}$.

Example 2.1.5. For an R-module A, we have $0a = (0+0)a = 0a + 0a$ implying $0a = 0$. Combining this with the identity ($1a = a$) we see that the only module over 0 (the zero ring) is the **zero module** (the module with one element, also denoted 0), which is in fact 0 itself.

Example 2.1.6. By definition any $\mathbb{Z}$-module comes with an abelian group structure. Conversely, an abelian group A admits a unique scalar product making A into a $\mathbb{Z}$-module. So we see that the $\mathbb{Z}$-modules are the abelian group (there is an isomorphism of category $\mathrm{Ab} \simeq \mathbb{Z}\text{-Mod}$).

Definition 2.1.3 (Submodules)**.** Let A be an R-module. Given a subset S of A, we say that S is a **submodule** (or R-submodule) of A if S admits an R-module structure for which the injection $\iota : S \hookrightarrow A$ is R-linear. We can show that S is a submodule of A if and only if

(i) S is a subgroup of A (automatically abelian);

(ii) For all $r \in R$, $s \in S$, $rs \in S$.

In that case the R-module structure for which $\iota : S \hookrightarrow A$ is R-linear is unique, and obtained by restricting the operations of A to S.

Proposition 2.1.1. *Submodules are stable by intersection, meaning that for an R-module A and a family $(S_i)_{i \in I}$ of submodules of A, $\bigcap_{i \in I} S_i$ is a submodule of A.*

Definition 2.1.4 (Quotient by a submodule)**.** Let A be an R-module, and S be a submodule of A. For $a, a' \in A$ we write $a \sim_S a'$ if $(a - a') \in S$. $\sim_S$ is then an equivalence relation on A, and we can define the quotient $q : A \to A/S := A/\sim_S$. The **quotient** of A by S is then defined to be A/S equipped with the unique R-module structure for which $q : A \to A/S$ is R-linear. The image of $a \in A$ by $q : A \to A/S$ (so the equivalence class of a for $\sim_S$) is often denoted by $a + S$.

Definition 2.1.5 (Kernel, image and cokernel)**.** Given an R-linear map $\phi : A \to B$. The **image** $\operatorname{im}(\phi)$ of ϕ is a submodule of B, while the **kernel** of ϕ is defined to be submodule $\ker(\phi) := \{a \in A | \phi(a) = 0\}$. The **cokernel** of ϕ is the quotient $q : B \to B/\operatorname{im}(\phi)$ of B by the image of ϕ.

Proposition 2.1.2. *Given an R-linear map $\phi : A \to B$*

(i) ϕ is injective if and only if $\ker(\phi) = 0$*;*

(ii) ϕ is surjective if and only if $\operatorname{coker}(\phi) = 0$.

In particular ϕ is an isomorphism if and only if both $\ker(\phi)$ *and* $\operatorname{coker}(\phi)$ *are zero.*

Definition 2.1.6 (Span of a subset)**.** Let X be a subset of an R-module A. The **span** $\langle X \rangle$ is defined to be the smallest submodule of A containing X, so

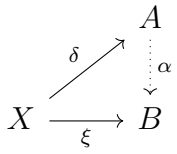
$$\langle X \rangle := \bigcap \{S \text{ submodule of } A | X \subseteq S\}.$$

$\langle X \rangle$ consists of the (finite) linear combinations of elements of X (another possible definition of $\langle X \rangle$)

$$\langle X \rangle = \{\sum_{i=1}^{k} r_i x_i | 0 \leq k < \infty, r_j \in R, x_j \in X\}.$$

2.1.1 Free modules

Definition 2.1.7 (Free over a set)**.** Let A be an R-module and let $\delta : X \to R$ be a map from a set X to the underlying set of R. We say that R is **free over** X (or δ to be more precise) if for any map $\xi : X \to B$ there exists a unique R-linear map $\alpha : A \to B$ such that the following diagram commutes



Definition 2.1.8 (The free module over a set)**.** Given a set X there exists an R-module $R[X]$ together with an set map $\delta : X \to R[X]$ such that $R[X]$ is free over δ. The pair $(R[X], \delta)$ is unique up to isomorphism (as for any other object defined by means of a universal property) and δ is injective.

Proof. We'll construct a **standard version** of $(R[X], \delta)$. $R[X]$ consists of the **almost zero** functions $\phi : X \to R$, meaning that the support $\operatorname{supp} \phi := \{x \in X | \phi(x) \neq 0\}$

is finite, equipped with pointwise addition and scalar multiplication. The injection $\delta : X \to R[X]$ sends $x \in X$ to the indicator function of x

$$\delta(x) \stackrel{n}{=} \delta_x \stackrel{n}{=} x : X \to R, y \to \begin{cases} 1, \text{ if } x = y \\ 0, \text{ if } x \neq y \end{cases}$$

Any nonzero element ϕ of $R[X]$ is written uniquely $\phi = \sum_{i=1}^{k} r_i x_i$ for $x_1, ..., x_k \in X$ distinct and $r_i = \phi(x_i) \in R - \{0\}$. Given a map $\xi : X \to B$ from X to another R-module B, the unique factoring map $\alpha : R[X] \to B$ sends $\phi = \sum_{i=1}^{k} r_i x_i$ to $\sum_{i=1}^{k} r_i \xi(x_i)$. □

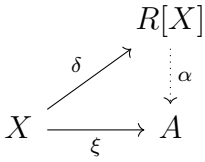
Remark. From now on we'll use $(R[X], \delta)$ to refer to the standard free module over X.

Remark. The universal property of the free module over X can be stated as follows: for any R-module A, we have a canonical bijection

$$\mathrm{Set}(X, UA) \simeq \mathrm{Hom}(R[X], A)$$

where U denotes the forgetful functor $U : R\text{-Mod} \to \mathrm{Set}$. So we see that the existence of free modules is equivalent to the existence of a left-adjoint to the forgetful functor. The universal map $\delta : X \to R[X]$ is the counit of this adjunction.

Proposition 2.1.3. *Given an R-module A, a set X and a map $\xi : X \to A$. By the universal property the free module, there exists a unique R-linear map $\alpha : R[X] \to A$ such that*



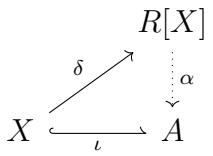
commutes. A is free over ξ if and only if α is an isomorphism. In particular ξ must be injective (for A to be free over ξ).

Definition 2.1.9 (Basis of a module)**.** Let A be an R-module. A subset $X \subseteq A$ is a **basis** of A if A is free over the injection $\iota : X \hookrightarrow A$. In other words, X is a basis of A if and only if for any R-module B, any map $\phi : X \to B$ extends uniquely to an R-linear map $\bar{\phi} : A \to B$.

Proposition 2.1.4. *Given an R-module A, a set X and a map $\xi : X \to A$, A is free over ξ if and only if ξ is injective and* $\mathrm{im}(\xi) \subseteq A$ *is a basis of A.*

Remark. Given a set X, X is a basis of $R[X]$ (when identified with its image by δ).

Proposition 2.1.5. *Let X be a subset of the R-module A. By the universal property of the free module, there exists a unique map $\alpha : R[X] \to A$ such that*



commutes. X is a basis of X if and only if α is an isomorphism.

Corollary 2.1.1. *A subset X of an R-module A is a basis of A if and only if*

*(i) X is **linearly independent**, meaning that for $1 \leq k$ and $x_j \in X$, $r_j \in R$*

$$\sum_{i=1}^{k} r_i x_i = 0$$

if and only if $r_1 = ... = r_k = 0$. This is equivalent to requiring that the unique factoring map $\alpha : R[X] \to A$ be injective.

*(ii) X **spans** A, meaning that $\langle X \rangle = A$ (i.e. that any element of A is a finite linear combination of elements of X). This is equivalent to requiring that the unique factoring map $\alpha : R[X] \to A$ be surjective.*

Equivalently X is a basis of A if and only if for any $a \in A$ there exists a unique almost zero map $\xi : X \to R$ such that

$$a = \sum_{x \in X} \xi(x) x.$$

Definition 2.1.10 (Free module)**.** We say that the R-module A is **free** if A admits a basis.

Example 2.1.7. The zero module over R is free with basis $\emptyset$. This is because for any R-module A, $\mathrm{Hom}(0, A) = \{*\}$ as the only R-linear map $0 \to A$ is the zero map sending $0 \in 0$ to $0 \in A$, while $\mathrm{Set}(\emptyset, A) = \{*\}$ as $\emptyset$ is initial in Set (for any set Y, the empty map $\emptyset \subseteq \emptyset \times Y = \emptyset$ is the only map $\emptyset \to Y$).

Example 2.1.8. Any ring R is canonically a free module over itself, with basis $\{1\}$. $1 = 0$ is a basis of the zero ring, since the only module over 0 is 0 itself.

Example 2.1.9. We know that $\mathbb{Z}_2$ is a free module over itself, but as an abelian group $\mathbb{Z}_2$ is also a $\mathbb{Z}$-module. Since $\mathbb{Z}_2$ is **torsion** (all elements of $\mathbb{Z}_2$ have finite order), $\mathbb{Z}_2$ admits no nonempty $\mathbb{Z}$-linearly independent subset, so $\mathbb{Z}_2$ is *not* free as a $\mathbb{Z}$-module. This applies to any nonzero abelian torsion group, in particular for any $n \geq 2$, $\mathbb{Z}_n$ is not

free as a $\mathbb{Z}$-module (the trivial abelian group $\mathbb{Z}_1 = 0$ is free as a $\mathbb{Z}$-module with empty basis, see previous example).

This shows that not all modules are free, and that when discussing bases and free modules, specifying the base ring is of crucial importance.

Example 2.1.10. The fact that the zero ring seen as an 0-module admits both $\{1 = 0\}$ and $\emptyset$ as bases already shows that the dimension of a free module is not well-defined in general. We can find an example that is not as trivial. Let $\mathbb{F}$ be a field, and let V be the free vector space $\mathbb{F}(\mathbb{N})$ with basis $\{v_0, ..., v_n, ...\}$. Let $R := \mathrm{End}(V)$ be the ring of endomorphisms of V. Define $\phi, \psi \in R$ by $\phi(v_n) = v_{2n}$ and $\psi(v_n) = v_{2n+1}$. Let $L \in R$, there exist unique families $(A^i_j)_{i,j\in\mathbb{N}}$ and $(B^i_j)_{i,j\in\mathbb{N}}$ such that

$$L(v_m) = \sum_{n\in\mathbb{N}} (A^n_m v_{2n} + B^n_m v_{2n+1})$$

and we see that $A, B \in R$ defined by $A(v_m) = \sum_{n\in\mathbb{N}} A^n_m v_n$, $B(v_m) = \sum_{n\in\mathbb{N}} B^n_m v_n$ are the only pair of elements of R such that

$$L = \phi \circ A + \psi \circ B.$$

This shows that $\{\phi, \psi\}$ is a basis for R seen as a right module over itself. But we also know that $\{1_V\}$ is a basis for R. Using Krull's theorem on the existence of maximal ideals (which is equivalent to Zorn's lemma), one can show that the dimension of a free module over a **commutative** ring *is* well-defined.

2.1.2 Representations of groups and monoids

Definition 2.1.11 (Monoid)**.** A **monoid** is a set M with a binary operation

$$\cdot : M \times M \to M, (a, b) \to a \cdot b \overset{n}{=} ab$$

which is associative and for which there exists a **unit** (or **identity element**) 1.

Given two monoids M, N, a morphism of monoids $M \to N$ is a map $\phi : M \to N$ such that

(i) For all $a, b \in M$, $\phi(ab) = \phi(a)\phi(b)$;

(ii) $\phi(1) = 1$.

Example 2.1.11. $\{0, 1\}$ equipped with the $\vee$ operation

$\vee$	0	1
0	0	1
1	1	1

is a monoid with identity 0, which we denote by OR. Let 0 be the monoid with one element (the **zero monoid**, written additively) and let $1 : 0 \to \mathrm{OR}$ be the unique map sending $0 \in 0$ to $1 \in \mathrm{OR}$ verifies $1(0+0) = 1 = 1 \vee 1 = 1(0) \vee 1(0)$ but $1(0) = 1$ is *not* the identity of OR. So we see that removing the requirement that the identity be preserved from the definition of monoid morphism would yield a non-equivalent definition. In other words monoids do not form a full subcategory of semigroups. Recall that a magma is a set equipped with an internal binary operation, while a semigroup is an associative magma. A monoid is a semigroup with identity.

Example 2.1.12. A group is a monoid G such that any element has a (left and right) inverse. If it exists, such an inverse is unique, so when a monoid G admits an inverse map $G \to G$ making it into a group, this map is unique (a monoid admits at most one compatible group structure). Given two groups G, H, a magma morphism $G \to H$ will automatically preserve identities and inverses, so groups form a full subcategory of magmas (and semigroups and monoids).

Definition 2.1.12 (Representation)**.** Let M be a monoid and let R be a ring. An R-linear **representation** of M over A is a monoid morphism $M \to \mathrm{End}(A)$, where $\mathrm{End}(A)$ is defined to be the monoid of endomorphisms of A, that is the monoid consisting of R-linear maps $A \to A$.

In the event that M is a group, the image of M in $\mathrm{End}(A)$ (which will always be a submonoid) will automatically be a subgroup of $\mathrm{Aut}(A)$, the group of automorphisms of A (i.e. bijective R-linear maps $A \to A$). And indeed, an R-linear representation of a group G over A is defined to be a group morphism $G \to \mathrm{Aut}(A)$.

Definition 2.1.13 (Monoid (group) ring)**.** Given a monoid M and a ring R, the **monoid ring** $R[M]$ of M over R is the free R-module $R[M]$ over M with the multiplication obtained by extending the product of M linearly, meaning that for two almost zero maps $\phi, \psi : M \to R$ we set

$$\phi\psi := \sum_{a,b \in M} \phi(a)\phi(b)ab.$$

When M is a group G, we call $R[G]$ the **group ring** of G over R.

Remark. When R is a commutative ring, the product of $R[M]$ is R-bilinear i.e. for any $\phi, \phi', \psi, \psi' \in R[M]$, $r \in R$

(i) $\phi(\psi + \psi') = \phi\psi + \phi\psi'$ and $(\phi + \phi')\psi = \phi\psi + \phi'\psi$;

(ii) $r(\phi\psi) = (r\phi)\psi = \phi(r\psi)$.

Thus in that case $R[M]$ is an associative R-algebra (not just an R-module), called the monoid (group) algebra of M (or G) over R.

Theorem 2.1.1. *Let M be a monoid and R be a ring. There is a one-to-one correspondence between R-linear representations of M and $R[M]$-modules. Of course this applies to group representations as well.*

Proof. Let A be an R-module and let

$$\rho : M \to \mathrm{End}(A), m \to \rho(m) \stackrel{n}{=} \rho_m$$

be a representation of M over A. We make A into an $R[M]$-linear module by setting $ma := \rho_m a$ for all $m \in M$, and $a \in A$, and extending in the only possible, meaning that for an almost zero map $\phi : M \to R$ and $a \in A$ we have

$$\phi a = \sum_{m \in M} \phi(m) \rho_m a.$$

Let A be an $R[M]$-module. The universal property of free modules guarantees the existence of a unique R-linear map $R \to R[M]$ sending $1 \in R$ to the identity e of M. This map is in fact a ring morphism, and through this ring morphism A is canonically an R-module. For $m \in M$, we define $\rho_m a := ma$, where ma is the multiplication of $a \in A$ by $m \in R[M]$). The resulting map $\rho : M \to \mathrm{End}(A)$ (where $\mathrm{End}(A)$ is the monoid of R-linear maps $A \to A$).

These two processes are clearly inverse to each other, and the equations that $\rho : M \to \mathrm{End}(A)$ must satisfy to be a monoid morphism are exactly the equations that $\cdot : R[M] \times A \to A$ must satisfy to be an $R[M]$-module. □

Example 2.1.13. The case of the monoid $\mathbb{N}$ (with addition) is interesting. $\mathbb{N}$ is the free monoid over the singleton, with basis $\{1\}$, meaning that given another monoid M, the datum of a monoid morphism $\mathbb{N} \to M$ is equivalent to a choice of element $a \in M$. The monoid morphism corresponding to the element $a \in M$ sends $n \in \mathbb{N}$ to $na := \underbrace{a + ... + a}_{n \text{ times}}$ (where we write the operation of M additively).

Given a field $\mathbb{F}$ and a vector space V over $\mathbb{F}$, an $\mathbb{F}$-linear representation of $\mathbb{N}$ over V, so a monoid morphism $\mathbb{N} \to \mathrm{End}(V)$, is equivalent to a choice of endomorphism $\tau : V \to V$. By theorem 2.1.1, an $\mathbb{F}$-linear representation of $\mathbb{N}$ is equivalent to an $\mathbb{F}(\mathbb{N})$-module. As it turns out, $\mathbb{F}(\mathbb{N})$ is the associative (and commutative) $\mathbb{F}$-algebra $\mathbb{F}[x]$ of polynomials over $\mathbb{F}$ with one variable. Thus we see that an $\mathbb{F}[x]$-module is equivalent to the data of a vector space V over $\mathbb{F}$ together with a choice of endomorphism $\tau : V \to V$. The (compatible) $\mathbb{F}[x]$-module structure on V corresponding to $\tau \in \mathrm{End}(V)$ is given by

$$(\sum_{k=0}^{n} s_k x^k) v = \sum_{k=0}^{n} s_k \tau^k(v)$$

for all $v \in V$ and $\sum_{k=0}^{n} s_k x^k \in \mathbb{F}[x]$.

Bibliography

[1] Tim van der Linden. *Homological Algebra*. 2022-2023.