Math 332 Winter 2023, Lecture 22: Modules

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

2. Modules

2.7. Bilinear maps

Let R be a commutative ring.

The addition map

$$\begin{aligned} \operatorname{add} : R \times R &\to R, \\ (a, b) &\mapsto a + b \end{aligned}$$

is R-linear (where the domain is the direct product of two copies of R), as you can easily check[1]. However, the multiplication map

$$\begin{aligned} \operatorname{mul} : R \times R &\to R, \\ (a, b) &\mapsto ab \end{aligned}$$

is not. But there is "some linearity" in mul: Namely, if we fix one argument, then mul is linear in the other. That is:

- For any $a \in R$, the map

$$\begin{aligned} R &\to R, \\ b &\mapsto ab \end{aligned}$$

  is R-linear.

[1]Indeed:

- This map add respects addition, since any two elements (a, b) and (c, d) of $R \times R$ satisfy

$$\begin{aligned} \operatorname{add}((a, b) + (c, d)) &= \operatorname{add}(a + c,\ b + d) = (a + c) + (b + d) \\ &= \underbrace{a + b}_{= \operatorname{add}(a,b)} + \underbrace{c + d}_{= \operatorname{add}(c,d)} = \operatorname{add}(a, b) + \operatorname{add}(c, d). \end{aligned}$$

- This map add respects scaling, since any $r \in R$ and $(a, b) \in R \times R$ satisfy

$$\operatorname{add}(r(a, b)) = \operatorname{add}(ra, rb) = ra + rb = r\left(\underbrace{a + b}_{= \operatorname{add}(a,b)}\right) = r \operatorname{add}(a, b).$$

- This map add respects zero, since $\operatorname{add}(0, 0) = 0 + 0 = 0$.

- For any $b \in R$, the map
$$R \to R,$$
$$a \mapsto ab$$
is R-linear.

Maps with these properties are called **bilinear**:

Definition 2.7.1. Let R be a commutative ring. Let M, N and P be three R-modules. A map $f : M \times N \to P$ is said to be R**-bilinear** (or just **bilinear**) if it satisfies the following two conditions:

1. For any $n \in N$, the map
$$M \to P,$$
$$m \mapsto f(m, n)$$
is R-linear. Explicitly, this is saying that for any $n \in N$, we have
$$f(m_1 + m_2,\ n) = f(m_1, n) + f(m_2, n) \qquad \text{for all } m_1, m_2 \in M;$$
$$f(rm, n) = rf(m, n) \qquad \text{for all } r \in R \text{ and } m \in M;$$
$$f(0, n) = 0.$$
This is called "f is **linear in its first argument**".

2. For any $m \in M$, the map
$$N \to P,$$
$$n \mapsto f(m, n)$$
is R-linear. Explicitly, this is saying that for any $m \in M$, we have
$$f(m,\ n_1 + n_2) = f(m, n_1) + f(m, n_2) \qquad \text{for all } n_1, n_2 \in N;$$
$$f(m, rn) = rf(m, n) \qquad \text{for all } r \in R \text{ and } n \in N;$$
$$f(m, 0) = 0.$$
This is called "f is **linear in its second argument**".

Here are some examples of bilinear maps (where R denotes a commutative ring throughout):

- As we just teased, the multiplication map $\mathrm{mul} : R \times R \to R$ is bilinear.

- For any $n \in \mathbb{N}$, the map

$$R^n \times R^n \to R,$$
$$((a_1, a_2, \ldots, a_n), \ (b_1, b_2, \ldots, b_n)) \mapsto a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

is R-bilinear. This map is called the **dot product** or the **standard scalar product**. At least in the case $R = \mathbb{R}$, it should be familiar from basic linear algebra.

- Consider the field $\mathbb{C}$ of complex numbers. For any $n \in \mathbb{N}$, the **standard inner product**

$$\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C},$$
$$((a_1, a_2, \ldots, a_n), \ (b_1, b_2, \ldots, b_n)) \mapsto a_1 \overline{b_1} + a_2 \overline{b_2} + \cdots + a_n \overline{b_n}$$

(where $\overline{z}$ denotes the complex conjugate of a complex number z) is $\mathbb{R}$-bilinear but not $\mathbb{C}$-bilinear (since it is antilinear rather than linear in the second argument). However, it becomes $\mathbb{C}$-bilinear if you view it as a map $\mathbb{C}^n \times \overline{\mathbb{C}}^n \to \mathbb{C}$ (with $\overline{\mathbb{C}}$ being the "twisted" $\mathbb{C}$-module $\mathbb{C}$ constructed in §2.4.3 in Lecture 19).

- The determinant map

$$\det : R^2 \times R^2 \to R,$$
$$((a, b), \ (c, d)) \mapsto ad - bc$$

is R-bilinear. (I call it the determinant map because it sends $((a, b), \ (c, d))$ to $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.)

- Matrix multiplication is R-bilinear. That is: For any $m, n, p \in \mathbb{N}$, the map

$$R^{m \times n} \times R^{n \times p} \to R^{m \times p},$$
$$(A, B) \mapsto AB$$

is R-bilinear. (Indeed, this boils down to standard properties of matrix multiplication, such as $(A_1 + A_2) B = A_1 B + A_2 B$ and $A (\lambda B) = \lambda AB$ for any matrices A_1, A_2, A, B and any scalar $\lambda \in R$.)

- The **cross product** map

$$R^3 \times R^3 \to R^3,$$
$$((a, b, c), \ (a', b', c')) \mapsto (bc' - cb', \ ca' - ac', \ ab' - ba')$$

is R-bilinear.

- For any R-module M, the action

$$R \times M \to M,$$
$$(r, m) \mapsto rm$$

is a R-bilinear map. It is a nice exercise to see what the conditions in the definition of "bilinear" translate to for this action (you can find the answer in §3.9 of the text). Note that we really need R to be commutative here.

For free modules, we have proved a universal property (Theorem 2.6.2 in Lecture 21) that lets us define a linear map out of a free module just by specifying its values on a given basis. The same can be done for bilinear maps:

Theorem 2.7.2 (Universal property of free modules wrt bilinear maps)**.** Let R be a commutative ring. Let M be a free R-module with basis $(m_i)_{i \in I}$. Let N be a free R-module with basis $\left(n_j\right)_{j \in J}$. Let P be a further R-module (free or not). Let $p_{i,j}$ be a vector in P for each pair $(i, j) \in I \times J$. Then, there exists a **unique** R-bilinear map $f : M \times N \to P$ such that

$$\text{each } (i, j) \in I \times J \text{ satisfies } f\left(m_i, n_j\right) = p_{i,j}.$$

Proof. Similar to the proof of Theorem 2.6.2 in Lecture 21. (Details can be found in the proof of Theorem 3.9.2 in the text.) □

2.8. Multilinear maps

Multilinear maps are a generalization of linear and bilinear maps. Linear maps have one argument; bilinear maps have two. Multilinear maps are "the same thing" but with n arguments:

Definition 2.8.1. Let R be a commutative ring. Let $M_1, M_2, \ldots, M_n$ be finitely many R-modules. Let P be any R-module. A map $f : M_1 \times M_2 \times \cdots \times M_n \to P$ is said to be R**-multilinear** (or just **multilinear**) if it satisfies the following condition:

- For any $i \in \{1, 2, \ldots, n\}$ and any $m_1, m_2, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n$ in the respective modules (meaning that $m_k \in M_k$ for each $k \neq i$), the map

$$M_i \to P,$$
$$m_i \mapsto f(m_1, m_2, \ldots, m_n)$$

is R-linear. In other words, if we fix all arguments of f other than the i-th argument, then f is R-linear as a function of this i-th argument. This is called "f is **linear in its i-th argument**".

Thus, "bilinear" means "multilinear for $n = 2$", whereas "linear" means "multilinear for $n = 1$".

The simplest example of a multilinear map is the map

$$\operatorname{prod}_n : R^n \to R,$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_1 a_2 \cdots a_n.$$

Another famous example of a multilinear map is

$$\det : \underbrace{R^n \times R^n \times \cdots \times R^n}_{n \text{ times}} \to R,$$
$$(v_1, v_2, \ldots, v_n) \mapsto \det(v_1, v_2, \ldots, v_n),$$

where $\det(v_1, v_2, \ldots, v_n)$ is the determinant of the matrix whose rows are $v_1, v_2, \ldots, v_n$.

There is a universal property of free modules wrt multilinear maps, but you can state and prove it at home. (It involves no new ideas compared to the bilinear one, but a lot more subscripts.)

2.9. Algebras over commutative rings

Convention 2.9.1. In this section, we fix a **commutative** ring R.

2.9.1. Definition

We know rings and we know R-modules. The former have addition and multiplication; the latter have addition and scaling. What happens if we combine these features, to obtain an object that has addition, multiplication and scaling?

That kind of object turns out to be very useful. Here is its precise definition (we do impose an extra axiom to keep the multiplication and scaling in harmony):

Definition 2.9.2. An **R-algebra** is a set A that is endowed with

- two binary operations (i.e., maps from $A \times A$ to A) that are called **addition** and **multiplication** and denoted by $+$ and $\cdot$,
- a map $\cdot$ from $R \times A$ to A that is called **action** of R on A (and should not be confused with the multiplication map, which is also denoted by $\cdot$), and
- two elements of A that are called **zero** and **unity** and are denoted by 0 and 1,

such that the following properties (the "**algebra axioms**") hold:

- The addition, the multiplication, the zero and the unity satisfy all the ring axioms (so that A becomes a ring).

- The addition, the action and the zero satisfy all the module axioms (so that A becomes an R-module).

- **Scale-invariance of multiplication:** We have

$$r\,(ab) = (ra)\,b = a\,(rb) \qquad \text{for all } r \in R \text{ and } a, b \in A.$$

Here (and in the following), we omit the $\cdot$ signs.

Thus, an R-algebra is an R-module that is also a ring at the same time, with the same addition, and satisfying the "scale-invariance" axiom so that the structures work together nicely.

The "scale-invariance" axiom can be replaced by requiring that the multiplication map

$$A \times A \to A,$$
$$(a, b) \mapsto ab$$

be R-bilinear. (This R-bilinearity also includes the distributive laws $(a_1 + a_2)\,b = a_1 b + a_2 b$ and $a\,(b_1 + b_2) = ab_1 + ab_2$ as well as the axioms $a0 = 0$ and $0b = 0$, but these are also part of the ring axioms.)

A simple-to-memorize way to restate the "scale-invariance" axiom is the following: "Scalars commute with vectors". Here, "scalars" mean elements of R (as expected, since A is an R-module), while "vectors" mean elements of A, and the word "commute" is used in a slightly broader sense as usual (as we are dealing with actions, not just products).

Examples of R-algebras include the following:

- The commutative ring R itself is an R-algebra. (Here, the multiplication of R plays both the role of multiplication and the role of action.)

- The zero ring $\{0\}$ is an R-algebra.

- The matrix ring $R^{n\times n}$ is an R-algebra for any $n \in \mathbb{N}$ (since it is both a ring and an R-module, and "scale-invariance" is easily seen to hold). (Note that $R^{n\times n}$ is usually not commutative!)

- The ring $\mathbb{C}$ is an $\mathbb{R}$-algebra (since it is both a ring and an $\mathbb{R}$-module, and "scale-invariance" is easily seen to hold).

- The ring $\mathbb{R}$ is a $\mathbb{Q}$-algebra (similarly).

- More generally: If a commutative ring R is a subring of a **commutative** ring S, then S becomes an R-module in a natural way (by the method we have learnt in §2.1.5 in Lecture 18: the action of R on S is just the multiplication of S, restricted to $R \times S$), and thus becomes an R-algebra (because it is also a ring and satisfies the "scale-invariance" axiom).

- Even more generally: If R and S are two **commutative** rings, and if $f : R \to S$ is a ring morphism, then S becomes an R-module (by the method we have learnt in §2.1.5 in Lecture 18: the action of R on S is given by

$$\underbrace{rs}_{\text{action}} = \underbrace{f(r) \cdot s}_{\substack{\text{multiplication}\\ \text{inside } S}} \qquad \text{for all } r \in R \text{ and } s \in S$$

), and thus becomes an R-algebra (since it is also a ring and satisfies the "scale-invariance axiom"). This R-algebra structure on S is said to be **induced** by the morphism f.

- Even more generally: If R and S are two commutative rings, and if $f : R \to S$ is a ring morphism, then any S-algebra A becomes an R-algebra via the "restriction of scalars" rule

$$r \cdot a = f(r) \cdot a \qquad \text{for all } r \in R \text{ and } a \in A.$$

(Again, this is the same rule that we have seen in §2.1.5 in Lecture 18, but we now additionally have a ring structure on A, so that A becomes not just an R-module but also an R-algebra.)

- The quaternion ring $\mathbb{H}$ is an $\mathbb{R}$-algebra, but **not** a $\mathbb{C}$-algebra (despite $\mathbb{C}$ being a subring of $\mathbb{H}$). Why not? Because it violates the scale-invariance axiom, which in this case says that

$$r(ab) = (ra)b = a(rb) \qquad \text{for all } r \in \mathbb{C} \text{ and } a, b \in \mathbb{H}.$$

For example, for $r = i$ and $a = j$ and $b = 1$, we have

$$(ra)b = (ij)1 = k1 = k \qquad \text{but}$$
$$a(rb) = j(i1) = ji = -k \neq k.$$

In a nutshell, this axiom is failing because quaternions don't commute with complex numbers. As we said, the vectors in an R-algebra must "commute" with the scalars (meaning $ra = a(r1_A)$ for all $r \in R$ and $a \in A$).

- The polynomial ring $R[x]$ (to be defined soon) is an R-algebra.

- More examples can be found in §3.11.2 of the text.

2.9.2. Rings as $\mathbb{Z}$-algebras

Proposition 2.3.1 **(a)** in Lecture 19 shows that every abelian group (written additively) automatically becomes a $\mathbb{Z}$-module. Likewise (and in fact extending this construction), any ring automatically becomes a $\mathbb{Z}$-algebra:

Proposition 2.9.3. Let A be any ring. Then, A is an abelian group (with respect to addition), and thus becomes a $\mathbb{Z}$-module (by Proposition 2.3.1 **(a)** in Lecture 19). Combining this $\mathbb{Z}$-module structure with the given ring structure on A, we obtain a $\mathbb{Z}$-algebra. Thus, A becomes a $\mathbb{Z}$-algebra.

Proof. Easy. □

2.9.3. The underlying structures

Every R-algebra A has an underlying ring (i.e., the ring that you are left with if you forget the action of R on A) and an underlying R-module (i.e., the R-module that you are left with if you forget the multiplication and the unity of A). This ring and this R-module are inherent in A; we will refer to them simply as "the ring A" and "the R-module A".

Thus, when A and B are two R-algebras, a "ring morphism from A to B" means a ring morphism from the underlying ring of A to the underlying ring of B, whereas an "R-module morphism from A to B" means an R-module morphism from the underlying R-module of A to the underlying R-module of B.

Warning: The notion of an "underlying ring" has nothing to do with the notion of a "base ring"! The **base ring** of an R-algebra A is defined to be R (not A).

2.9.4. Commutative R-algebras

Definition 2.9.4. An R-algebra is said to be **commutative** if its underlying ring is commutative (i.e., its multiplication is commutative).

2.9.5. Subalgebras

Subalgebras are to algebras what subrings are to rings (and what submodules are to modules):

Definition 2.9.5. Let A be an R-algebra. An R**-subalgebra** of A means a subset of A that is simultaneously a subring and an R-submodule of A (that is, that is closed under addition, multiplication and scaling and contains 0 and 1).

Every R-subalgebra of an algebra A becomes an algebra in its own right automatically (by inheriting the operations from A).

2.9.6. R-algebra morphisms

As you could expect, R-algebras (just like rings and modules) have their own kind of morphisms and isomorphisms:

Definition 2.9.6. Let A and B be two R-algebras.

(a) An R**-algebra morphism** (or, short, **algebra morphism**) from A to B means a map $f : A \to B$ that is both a ring morphism and an R-module morphism.

(b) An R**-algebra isomorphism** from A to B means an invertible R-algebra morphism $f : A \to B$ whose inverse $f^{-1} : B \to A$ is also an R-algebra morphism.

(c) The R-algebras A and B are said to be **isomorphic** (this is written $A \cong B$) if there exists an R-algebra isomorphism from A to B.

All the fundamental properties of ring morphisms and of ring isomorphisms (as discussed in §1.7 of Lecture 6) have analogues for algebras instead of rings. For example:

- Any invertible R-algebra morphism is an isomorphism. (This is an analogue of Proposition 1.7.6 in Lecture 6.)
- The image of an R-algebra morphism $f : A \to B$ is an R-subalgebra of B. (This is an analogue of Proposition 1.7.5 in Lecture 6.)

The proofs of these analogues are analogous to the proofs of the original results.

Furthermore, if A and B are two $\mathbb{Z}$-algebras, then the $\mathbb{Z}$-algebra morphisms from A to B are precisely the ring morphisms from A to B. (In fact, this follows easily from Proposition 2.4.2 in Lecture 19.)

2.9.7. Direct products

Definition 2.9.7. Direct products of R-algebras are defined just as for rings and R-modules: Addition, multiplication and action are entrywise.

For details, see §3.11.8 in the text.