Math 533 Winter 2021, Lecture 8: Modules

website: `https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

1. Modules ([DF, Chapter 10])

1.1. Definition and examples ([DF, §10.1]) (cont'd)

Fix a ring R. Last time, we have defined left R-modules (to remind: these are essentially additive groups whose elements can be scaled by elements of R), and I have started giving examples of them. Let me briefly repeat the two examples I gave:

- The ring R itself becomes a left R-module: Just define the action to be the multiplication of R. This is called the **natural left R-module** R. The R-submodules of this R-module are the left ideals of R. (Every ideal of R is a left ideal of R, but usually not vice versa.)
- For any $n \in \mathbb{N}$, the set
$$R^n = \{(a_1, a_2, \ldots, a_n) \ \mid \ \text{all } a_i \text{ belong to } R\}$$
is a left R-module, with addition and action being entrywise[1] and with the zero vector $(0, 0, \ldots, 0)$. This generalizes the Euclidean space $\mathbb{R}^n$ from linear algebra, and many of its analogues.

Here are some more examples:

- The left R-modules R^n (with $n \in \mathbb{N}$) tend to have many R-submodules. When R is a field, this is well-known from linear algebra (where R-submodules are called R-vector subspaces); in particular, the solution set of any given system of homogeneous linear equations in n variables is an R-submodule of R^n. The same applies to any commutative ring R, but here we have even more freedom: Besides equations, our system can contain congruences too (as long as they are congruent). For instance, for $R = \mathbb{Z}$, the set
$$\Big\{(x, y, z, w) \in \mathbb{Z}^4 \ \mid \ x \equiv y \bmod 2 \text{ and } x + y + z + w \equiv 0 \bmod 3 \\ \text{and } x - y + z - w = 0\Big\}$$

[1] e.g., the action is defined by
$$r \cdot (a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n) \text{ for all } r \in R \text{ and } a_1, a_2, \ldots, a_n \in R.$$

is a $\mathbb{Z}$-submodule of $\mathbb{Z}^4$. To prove this, you need to check the axioms ("closed under addition", "closed under scaling" and "contains the zero vector"). With a bit of practice, you can do this all in your head.

If R is noncommutative, you have to be somewhat careful with the side on which the coefficients stand in your system. If the coefficients are on the **right** of the variables, then the solution set is a **left** R-module (so, e.g., if a and b are two elements of R, then $\left\{(x,y) \in R^2 \mid xa + yb = 0\right\}$ is a left R-module); on the other hand, if the coefficients are on the **left** of the variables, then the solution set is a **right** R-module. (Again, this is not hard to check: e.g., the set $\left\{(x,y) \in R^2 \mid xa + yb = 0\right\}$ is closed under the scaling maps of a left R-module because $xa + yb = 0$ implies $rxa + ryb = r \underbrace{(xa + yb)}_{=0} = 0$. Meanwhile, in general, this set is not closed under the scaling maps of a right R-module, since $xa + yb = 0$ does not imply $xra + yrb = 0$.)

- Just as we defined the left R-module R^n consisting of all n-tuples, we can define a left R-module "R^∞" consisting of all infinite sequences. It is commonly denoted by $R^{\mathbb{N}}$ (since there are different kinds of infinity). Explicitly, we define the left R-module $R^{\mathbb{N}}$ by

  $$R^{\mathbb{N}} := \{(a_0, a_1, a_2, \ldots) \mid \text{all } a_i \text{ belong to } R\},$$

  where addition and action are defined entrywise.

  This left R-module $R^{\mathbb{N}}$ has an R-submodule

  $$R^{(\mathbb{N})} := \left\{(a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \mid \text{only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq 0\right\}.$$

  You can check that this is indeed an R-submodule of $R^{\mathbb{N}}$. (For instance, it is closed under addition, because if only finitely many $i \in \mathbb{N}$ satisfy $a_i \neq 0$ and only finitely many $i \in \mathbb{N}$ satisfy $b_i \neq 0$, then only finitely many $i \in \mathbb{N}$ satisfy $a_i + b_i \neq 0$.)

  For example, if $R = \mathbb{Q}$, then

  $$\begin{aligned} & (1,1,1,\ldots) \in R^{\mathbb{N}} \setminus R^{(\mathbb{N})} \\ \text{and} \quad & (0,0,0,\ldots) \in R^{(\mathbb{N})} \\ \text{and} \quad & (1,0,0,0,\ldots) \in R^{(\mathbb{N})} \\ \text{and} \quad & \Big(1,0,4,\underbrace{0,0,0,\ldots}_{\text{zeroes}}\Big) \in R^{(\mathbb{N})} \\ \text{and} \quad & \Big(\underbrace{1,0,1,0,1,0,\ldots}_{\text{ones and zeroes in turn}}\Big) \in R^{\mathbb{N}} \setminus R^{(\mathbb{N})}. \end{aligned}$$

- Generalizing R^n, here is a way to build modules out of other modules:

  Let $n \in \mathbb{N}$, and let $M_1, M_2, \ldots, M_n$ be any n left R-modules. Then, the Cartesian product $M_1 \times M_2 \times \cdots \times M_n$ becomes a left R-module itself, where addition and action are defined entrywise: e.g., the action is defined by

  $$r \cdot (m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n) \text{ for all } r \in R \text{ and } m_i \in M_i.$$

  This left R-module $M_1 \times M_2 \times \cdots \times M_n$ is called the **direct product** of $M_1, M_2, \ldots, M_n$. If all of $M_1, M_2, \ldots, M_n$ are the natural left R-module R, then this direct product is precisely the left R-module R^n defined above.

This direct product $M_1 \times M_2 \times \cdots \times M_n$ can be generalized further, allowing products of infinitely many modules, too. Just as for rings, the best setting for this is using families, not lists:[2]

Proposition 1.1.1. Let I be any set. Let $(M_i)_{i \in I}$ be any family of left R-modules. Then, the Cartesian product

$$\prod_{i \in I} M_i = \left\{ \text{all families } (m_i)_{i \in I} \text{ with } m_i \in M_i \text{ for all } i \in I \right\}$$

becomes a left R-module if we endow it with the entrywise addition (i.e., we set $(m_i)_{i \in I} + (n_i)_{i \in I} = (m_i + n_i)_{i \in I}$ for any two families $(m_i)_{i \in I}, (n_i)_{i \in I} \in \prod_{i \in I} M_i$) and the entrywise scaling (i.e., we set $r (m_i)_{i \in I} = (rm_i)_{i \in I}$ for any $r \in R$ and any family $(m_i)_{i \in I} \in \prod_{i \in I} M_i$) and with the zero vector $(0)_{i \in I}$.

Definition 1.1.2. This left R-module is denoted by $\prod_{i \in I} M_i$ and called the **direct product** of the left R-modules M_i.

If $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then this left R-module is also denoted by $M_1 \times M_2 \times \cdots \times M_n$, and we identify a family $(m_i)_{i \in I} = (m_i)_{i \in \{1,2,\ldots,n\}}$ with the n-tuple $(m_1, m_2, \ldots, m_n)$. (Thus, $M_1 \times M_2 \times \cdots \times M_n$ is precisely the direct product $M_1 \times M_2 \times \cdots \times M_n$ we defined above.)

If all the left R-modules M_i are equal to some left R-module M, then their direct product $\prod_{i \in I} M_i = \prod_{i \in I} M$ is also denoted M^I. Note that this generalizes the $R^{\mathbb{N}}$ defined above.

We set $M^n = M^{\{1,2,\ldots,n\}}$ for each $n \in \mathbb{N}$ and any left R-module M. This generalizes the left R-module R^n for $n \in \mathbb{N}$ discussed above.

This was quite predictable; but there is more. Indeed, we can generalize not just $R^{\mathbb{N}}$ but also its submodule $R^{(\mathbb{N})}$, and the result is at least as important:[3]

[2]The proof of Proposition 1.1.1 is easy and LTTR.

[3]The proof of Proposition 1.1.3 is easy and LTTR.

Proposition 1.1.3. Let I be any set. Let $(M_i)_{i\in I}$ be any family of left R-modules. Define $\bigoplus_{i\in I} M_i$ to be the subset

$$\left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i \ \mid \ \text{only finitely many } i \in I \text{ satisfy } m_i \neq 0 \right\}$$

of $\prod_{i\in I} M_i$. Then, $\bigoplus_{i\in I} M_i$ is a left R-submodule of $\prod_{i\in I} M_i$, and thus becomes a left R-module itself.

Definition 1.1.4. This left R-module $\bigoplus_{i\in I} M_i$ is called the **direct sum** of the R-modules M_i.

If $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then this left R-module is also denoted by $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

The last part of this definition might raise some eyebrows. In fact, if the set I is finite, then $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ (since the condition "only finitely many $i \in I$ satisfy $m_i \neq 0$" is automatically satisfied for any family $(m_i)_{i\in I}$ when I is finite). Thus, in particular,

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = M_1 \times M_2 \times \cdots \times M_n$$

for any left R-modules $M_1, M_2, \ldots, M_n$. So we have introduced two notations for the same thing. Nevertheless, both are in use.

For $I = \mathbb{N}$ and $M_i = R$, the direct sum $\bigoplus_{i\in I} M_i = \bigoplus_{i\in\mathbb{N}} R$ is precisely the R-module $R^{(\mathbb{N})}$ defined above.

For arbitrary I and any left R-module M, the direct sum $\bigoplus_{i\in I} M$ is denoted by $M^{(I)}$.

1.1.1. Restriction of modules

Here are some more ways to construct modules over rings:

- If R is a subring of a ring S, then S is a left R-module (where the action of R on S is defined by restricting the multiplication map $S \times S \to S$ to $R \times S$) and a right R-module (in a similar way).

  Let me restate this in a more down-to-earth way: If R is a subring of a ring S, then we can multiply any element of R with any element of S (since both elements lie in the ring S); this makes S into a left R-module (and likewise, S becomes a right R-module). Explicitly, the action of R on the left R-module S is given by

  $$rs = rs \qquad \text{for all } r \in R \text{ and } s \in S$$

(where the "rs" on the left hand side means the image of (r, s) under the action, whereas the "rs" on the right hand side means the product of r and s in the ring S).

Thus, for example, $\mathbb{C}$ is an $\mathbb{R}$-module (since $\mathbb{R}$ is a subring of $\mathbb{C}$) and also a $\mathbb{Q}$-module (for similar reasons). (In this example, you can say "vector space" instead of "module", since $\mathbb{R}$ and $\mathbb{Q}$ are fields.)

- More generally: If R and S are any two rings, and if $f : R \to S$ is a ring morphism, then S becomes a left R-module (with the action of R on S being defined by

$$rs = f(r)\, s \qquad \text{for all } r \in R \text{ and } s \in S$$

) and a right R-module (in a similar way). The proof of this is easy. These R-module structures are sometimes said to be **induced** by the morphism f.

Our previous example (in which we made S into an R-module whenever R is a subring of S) is the particular case of this construction obtained when f is the canonical inclusion of R into S.

Here are some other particular cases:

  - Any quotient ring R/I of a ring R (by some ideal I) becomes a left R-module, because the canonical projection $\pi : R \to R/I$ (which sends every $r \in R$ to its residue class $\overline{r} \in R/I$) is a ring morphism. Explicitly, the action of R on R/I is given by

$$r \cdot \overline{u} = \underbrace{\pi(r)}_{=\overline{r}} \cdot \overline{u} = \overline{r} \cdot \overline{u} = \overline{ru} \qquad \text{for all } r, u \in R.$$

  Similarly, R/I becomes a right R-module.

  - Here is another particular case: I claim that the abelian group $\mathbb{Z}/5$ becomes a $\mathbb{Z}[i]$-module[4], if we define the action by

$$(a + bi) \cdot m = \overline{a + 2b} \cdot m \qquad \text{for all } a + bi \in \mathbb{Z}[i] \text{ and } m \in \mathbb{Z}/5.$$

  To wit, the map

$$f : \mathbb{Z}[i] \to \mathbb{Z}/5,$$
$$a + bi \mapsto \overline{a + 2b}$$

[4]As usual, $\mathbb{Z}[i]$ denotes the ring of the Gaussian integers, with $i = \sqrt{-1}$.

is a ring morphism (check this![5]); and this can be used to turn $\mathbb{Z}/5$ into a $\mathbb{Z}[i]$-module by our above construction; this yields precisely the action I claimed above (because all $a+bi \in \mathbb{Z}[i]$ and $m \in \mathbb{Z}/5$ satisfy $(a+bi) \cdot m = \underbrace{f(a+bi)}_{=\overline{a+2b}} \cdot m = \overline{a+2b} \cdot m$).

This is not the only way to turn $\mathbb{Z}/5$ into a $\mathbb{Z}[i]$-module. We could just as well use the ring morphism

$$g : \mathbb{Z}[i] \to \mathbb{Z}/5,$$
$$a + bi \mapsto \overline{a+3b}$$

instead of f. This would give us a $\mathbb{Z}[i]$-module $\mathbb{Z}/5$ with action given by

$$(a+bi) \cdot m = \overline{a+3b} \cdot m \qquad \text{for all } a+bi \in \mathbb{Z}[i] \text{ and } m \in \mathbb{Z}/5.$$

Thus, we have obtained two **different** $\mathbb{Z}[i]$-module structures on $\mathbb{Z}/5$ – that is, two different $\mathbb{Z}[i]$-modules that are equal as sets (and even as additive groups) but different as $\mathbb{Z}[i]$-modules (and not even isomorphic as such). None of these two module structures is more natural or otherwise better than the other. Thus, when you speak of a "$\mathbb{Z}[i]$-module $\mathbb{Z}/5$", you need to clarify which one you mean. (Such situations are rather frequent in algebra. "Natural" R-module structures – i.e., structures that are clearly "the right one" – are rare in comparison.)

- Even more generally: If R and S are two rings, and if $f : R \to S$ is a ring morphism, then any left S-module M (not just S itself) naturally becomes a left R-module, with the action defined by

$$rm = f(r)\, m \qquad \text{for all } r \in R \text{ and } m \in M.$$

[5]Indeed, it is pretty easy to see that this map f respects addition, the zero and the unity. It remains to show that this map respects multiplication. To show this, we fix any $x, y \in \mathbb{Z}[i]$. We then need to show that $f(xy) = f(x) f(y)$.

Write x and y as $x = a + bi$ and $y = c + di$ for some $a, b, c, d \in \mathbb{Z}$. Then, $xy = (a+bi)(c+di) = (ac-bd) + (ad+bc)i$ (by the rule for multiplying complex numbers). Hence,

$$f(xy) = f((ac-bd) + (ad+bc)i) = \overline{ac - bd + 2(ad+bc)} \qquad (1)$$

(by the definition of f). On the other hand, $x = a + bi$ entails $f(x) = f(a+bi) = \overline{a+2b}$, and similarly we find $f(y) = \overline{c+2d}$. Multiplying these two equalities, we find

$$f(x) f(y) = \overline{a+2b} \cdot \overline{c+2d} = \overline{(a+2b)(c+2d)} = \overline{ac + 2^2bd + 2(ad+bc)} \qquad (2)$$

(since $(a+2b)(c+2d) = ac + 2^2bd + 2(ad+bc)$). Now, the right hand sides of the equalities (1) and (2) are identical (since $2^2 \equiv -1 \mod 5$ and thus $\overline{2}^2 = \overline{-1}$, so that $\overline{2^2bd} = \overline{-bd}$); hence, so are the left hand sides. In other words, $f(xy) = f(x) f(y)$. This completes the proof that the map f respects multiplication; therefore, f is a ring morphism.

This method of turning S-modules into R-modules is called **restricting** an S-module to R. If we apply this to a canonical inclusion (i.e., if R is a subring of S and if $f : R \to S$ is the canonical inclusion), then we conclude that any module over a ring naturally becomes a module over any subring. For example, any $\mathbb{C}$-module naturally becomes an $\mathbb{R}$-module (this is known as "decomplexification" in linear algebra[6]) and a $\mathbb{Q}$-module and a $\mathbb{Z}$-module.

1.1.2. More examples

Here is another general construction:

Proposition 1.1.5. Let R be a ring. Let I be an ideal of R. Let M be a left R-module. An (I, M)**-product** shall mean a product of the form im with $i \in I$ and $m \in M$. Then,

$$IM := \{\text{finite sums of } (I, M)\text{-products}\}$$

is an R-submodule of M.

Proof. This is fairly similar to the proof of the fact that the product IJ of two ideals I and J is again an ideal (see Exercise 8 **(a)** on homework set #1). □

Proposition 1.1.6. Let R be a commutative ring. Let $a \in R$. Let M be an R-module. Then,

$$aM := \{am \mid m \in M\}$$

is an R-submodule of M.

In particular, $0M = \{0_M\}$ and $1M = M$ are R-submodules of M.

Proof. This is easy and LTTR. □

The last statement of Proposition 1.1.6 holds for noncommutative rings R, too: If M is a left R-module, then $\{0_M\}$ and M are R-submodules of M. These are the "bookends" for the R-submodules of M (in the sense that every R-submodule N of M satisfies $\{0_M\} \subseteq N \subseteq M$).

Here are a few more examples of modules:

- Let $n \in \mathbb{N}$, and let R be a ring. The set R^n is not only a left R-module (as we have seen), but also a right $R^{n \times n}$-module[7], where the action of $R^{n \times n}$

[6]Of course, again, linear algebraists speak of vector spaces instead of modules.

From linear algebra, you might also know a procedure going in the other direction: "complexification", which turns an $\mathbb{R}$-vector space into a $\mathbb{C}$-vector space. We will later learn how to generalize this to arbitrary ring morphisms.

[7]Recall that $R^{n \times n}$ is the ring of $n \times n$-matrices over R.

on R^n is the vector-by-matrix multiplication map

$$R^n \times R^{n\times n} \to R^n,$$
$$(v, M) \mapsto vM$$

(where we identify n-tuples $v \in R^n$ with row vectors).

- More generally, for any $n, m \in \mathbb{N}$, the set $R^{n\times m}$ of all $n \times m$-matrices is a left $R^{n\times n}$-module and a right $R^{m\times m}$-module (since an $n \times m$-matrix can be multiplied by an $n \times n$-matrix from the left and by an $m \times m$-matrix from the right, and since the module axioms follow from the standard laws of matrix multiplication such as associativity and distributivity). Even better, this set is a so-called $(R^{n\times n}, R^{m\times m})$-bimodule (we will later define this notion; essentially it means a left and a right module structure that fit together well).

- Let us study a particular case of this.

  Namely, let R be a field F, and let $n = 2$. So F^2 is a left F-module, with the action given by

  $$\lambda (a, b) = (\lambda a, \lambda b) \qquad \text{for all } \lambda, a, b \in F,$$

  and is a right $F^{2\times 2}$-module, with the action given by

  $$(a, b) \begin{pmatrix} x & y \\ z & w \end{pmatrix} = (ax + bz, ay + bw) \qquad \text{for all } a, b, x, y, z, w \in F.$$

  What are the F-submodules of F^2 ? These are precisely the F-vector subspaces of F^2; as you know from linear algebra, these subspaces are the whole F^2 as well as the zero subspace $\{0_{F^2}\}$ and all lines through the origin.

  What are the $F^{2\times 2}$-submodules of F^2 ? Only F^2 and $\{0_{F^2}\}$, because any two nonzero vectors in F^2 can be mapped to one another by a 2×2-matrix.

  Now, consider the subring

  $$F^{2\leq 2} := \left\{ \begin{pmatrix} x & 0 \\ z & w \end{pmatrix} \mid x, z, w \in F \right\}$$

  of $F^{2\times 2}$. This is the ring of all lower-triangular 2×2-matrices over F. (Yes, it is a subring of $F^{2\times 2}$, since the sum and the product of two lower-triangular matrices are lower-triangular and since the zero and identity matrices are lower-triangular.) Since F^2 is a right $F^{2\times 2}$-module, F^2 must also be a right $F^{2\leq 2}$-module (by restriction). What are the $F^{2\leq 2}$-submodules of F^2 ? Only F^2 and $\{0_{F^2}\}$ and $\{(a, 0) \mid a \in F\}$. (You might have to prove this on a future homework set.)

1.2. A couple generalities

Let us show a few general properties of modules. Recall that when a group is written additively (i.e., its operation is denoted by $+$), the inverse of an element a of this group is denoted by $-a$ (and is called its additive inverse). The following proposition says that the additive inverse of a vector in an R-module can be obtained by scaling the vector by -1:

Proposition 1.2.1. Let R be a ring. Let A be a left R-module. Then, $(-1)\,a = -a$ for each $a \in A$.

Proof. Let $a \in A$. Then, $1a = a$ (by one of the module axioms). Thus,

$$\begin{aligned}(-1)\,a + \underbrace{a}_{=1a} &= (-1)\,a + 1a \\ &= \underbrace{((-1)+1)}_{=0}\,a \qquad \text{(by the right distributivity axiom)} \\ &= 0a = 0 \qquad \text{(by one of the module axioms)}\,.\end{aligned}$$

In other words, $(-1)\,a$ is an additive inverse of a. But the additive inverse of a is $-a$. Thus, we conclude that $(-1)\,a = -a$. This proves Proposition 1.2.1. □

Further properties of negation can easily be derived from this. For example,

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

Proposition 1.2.2. Let R be a ring. Let A be a left R-module. Then, any R-submodule of A is a subgroup of the additive group $(A, +, 0)$.

Proof of Proposition 1.2.2. Let B be an R-submodule of A. Then, B is closed under addition and under scaling and contains the zero vector. Since B is closed under scaling, we have $(-1)\,b \in B$ for each $b \in B$. However, each $b \in B$ satisfies $(-1)\,b = -b$ (by Proposition 1.2.1, applied to $a = b$) and thus $-b = (-1)\,b \in B$. In other words, B is closed under negation (= taking additive inverses). Thus, B is a subgroup of $(A, +, 0)$. □

Next, let us recall how we defined finite sums $\sum\limits_{s \in S} a_s$ of elements of a ring. In the same way, we can define a finite sum $\sum\limits_{s \in S} a_s$ of elements of any additive group, and thus a finite sum $\sum\limits_{s \in S} a_s$ of elements of any R-module (since any R-module is an additive group). Thus, in particular, if $a_1, a_2, \ldots, a_n$ are n elements of an R-module A, then the finite sum $a_1 + a_2 + \cdots + a_n \in A$ is well-defined.

The following "generalized distributivity laws" hold in any left R-module:

Proposition 1.2.3. Let R be a ring. Let M be a left R-module. Then:

(a) We have

$$(r_1 + r_2 + \cdots + r_k)\, m = r_1 m + r_2 m + \cdots + r_k m$$

for any $r_1, r_2, \ldots, r_k \in R$ and $m \in M$.

(b) We have

$$r\,(m_1 + m_2 + \cdots + m_i) = rm_1 + rm_2 + \cdots + rm_i$$

for any $r \in R$ and $m_1, m_2, \ldots, m_i \in M$.

Proof. **(a)** This follows by applying the right distributivity law (one of the module axioms) many times. (More precisely, this follows by induction on k; the right distributivity law is used in the induction step. The induction base follows from the $0m = 0$ axiom.)

(b) This follows by applying the left distributivity law (one of the module axioms) many times. (More precisely, this follows by induction on i; the left distributivity law is used in the induction step. The induction base follows from the $r \cdot 0_M = 0_M$ axiom.) □

The following convention is useful when dealing with R-modules. Essentially, it says that (just as with products of multiple elements in a ring or in a group) we can drop parentheses when we scale an element of an R-module by several elements of R:

Convention 1.2.4. Let R be a ring. Let M be a left R-module. Let $r, s \in R$ and $m \in M$. Then, $(rs)\, m$ and $r\,(sm)$ are the same vector (by the associativity axiom in the definition of a left R-module). We shall denote this vector by rsm. Likewise, expressions like $r_1 r_2 \cdots r_k m$ (for $r_1, r_2, \ldots, r_k \in R$ and $m \in M$) will be understood.

Everything we said above about left R-modules can be adapted to right R-modules in a straightforward way; we leave the details to the reader.

1.3. Abelian groups as $\mathbb{Z}$-modules ([DF, §10.1])

Now, let us try to understand $\mathbb{Z}$-modules in particular.

Proposition 1.3.1. Let A be an abelian group. Assume that A is written additively (i.e., the operation of A is denoted by $+$, and the neutral element by 0). For any $n \in \mathbb{Z}$ and $a \in A$, define

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}}\right), & \text{if } n < 0. \end{cases} \tag{3}$$

Thus, we have defined a map $\mathbb{Z} \times A \to A,\ (n, a) \mapsto na$.

(a) The group A becomes a $\mathbb{Z}$-module (where we take this map as the action of $\mathbb{Z}$ on A, and the pre-existing addition of A as the addition).

(b) This is the **only** $\mathbb{Z}$-module structure on A. That is, if A is **any** $\mathbb{Z}$-module, then the action of $\mathbb{Z}$ on A is given by the formula (3) (and therefore uniquely determined by the abelian group structure on A).

(c) The $\mathbb{Z}$-submodules of A are precisely the subgroups of A.

Proof of Proposition 1.3.1. LTTR. Here are the main ideas:

(a) You have to prove axioms like $(n+m)\,a = na + ma$ and $n\,(a+b) = na + nb$ and $(nm)\,a = n\,(ma)$ for all $n, m \in \mathbb{Z}$ and $a, b \in A$. These facts are commonly proved for $A = \mathbb{Z}$ in standard texts on the construction of the number system; if you pick the "right" proofs, then you can adapt them to the general case just by replacing $\mathbb{Z}$ by A. The main idea is "reduce to the case when n and m are nonnegative, and then prove them by induction on n and m". The details are rather laborious, as there are several cases to discuss based on the signs of n, m and $n+m$.

(b) Given **any** $\mathbb{Z}$-module structure on A, we must have

$$\begin{aligned} na &= \underbrace{(1+1+\cdots+1)}_{n \text{ times}}\,a = \underbrace{1a+1a+\cdots+1a}_{n \text{ times}} && \text{(by Proposition 1.2.3 } \textbf{(a)}\text{)} \\ &= \underbrace{a+a+\cdots+a}_{n \text{ times}} && \text{(by the } 1a = a \text{ axiom)} \end{aligned}$$

for any $n \in \mathbb{N}$ and any $a \in A$. This proves the "top half" of (3). It is not hard to prove the "bottom half" either (use the right distributivity axiom to see that $na + (-n)\,a = \underbrace{(n+(-n))}_{=0}\,a = 0a = 0$).

(c) Proposition 1.2.2 shows that any $\mathbb{Z}$-submodule of A is a subgroup of A. Conversely, we must prove that if B is a subgroup of A, then B is a $\mathbb{Z}$-submodule of A. So let B be a subgroup of A. Then, any $n \in \mathbb{Z}$ and $b \in B$ satisfy

$$nb = \begin{cases} \underbrace{b+b+\cdots+b}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{b+b+\cdots+b}_{-n \text{ times}}\right), & \text{if } n < 0 \end{cases} \in B$$

(since B is closed under addition and negation and contains 0). In other words, B is closed under scaling. Hence, B is a $\mathbb{Z}$-submodule of A (since B is a subgroup of A and therefore closed under addition and contains 0), qed. □

Proposition 1.3.1 reveals what $\mathbb{Z}$-modules really are: In general, when R is a ring, an R-module is an abelian group A with an extra structure (namely, an action of R on A); however, for $R = \mathbb{Z}$, this extra structure is redundant (in the sense that it can always be constructed in a unique way from the abelian group structure), and so a $\mathbb{Z}$-module is just an abelian group in fancy clothes.[8] Thus, we shall identify abelian groups with $\mathbb{Z}$-modules (at least when the abelian groups are written additively).

This has a rather convenient consequence: The theory of R-modules is a generalization of the theory of abelian groups. In particular, anything we have proved or will prove for R-modules can therefore be applied to abelian groups (by setting $R = \mathbb{Z}$).

Thus, we have understood what $\mathbb{Z}$-modules are. What about $\mathbb{Q}$-modules? Not every abelian group can be made into a $\mathbb{Q}$-module:

Example 1.3.2. There is no $\mathbb{Q}$-module structure on $\mathbb{Z}/2$ (that is, there is no $\mathbb{Q}$-module whose additive group is $\mathbb{Z}/2$).

Proof. This follows from linear algebra (since $\mathbb{Q}$-modules are $\mathbb{Q}$-vector spaces and thus have dimensions; but $\mathbb{Z}/2$ is too large to have dimension 0 and yet too small to have dimension > 0). Alternatively, you can do it by hand: Assume that $\mathbb{Z}/2$ is a $\mathbb{Q}$-module in some way. Then,

$$\frac{1}{2} \cdot \left(2 \cdot \overline{1}\right) = \underbrace{\left(\frac{1}{2} \cdot 2\right)}_{=1} \cdot \overline{1} = 1 \cdot \overline{1} = \overline{1},$$

so that

$$\overline{1} = \frac{1}{2} \cdot \underbrace{\left(2 \cdot \overline{1}\right)}_{=\overline{0}} = \frac{1}{2} \cdot \overline{0} = \overline{0},$$

which contradicts $\overline{1} \neq \overline{0}$. □

Thus we see that not every abelian group can be made into a $\mathbb{Q}$-module (unlike for $\mathbb{Z}$-modules). However, any abelian group that can be made into a $\mathbb{Q}$-module can only be made so in one way. (This will be exercise 3 on homework set #3.)

What about $\mathbb{R}$-modules? Here, we get neither existence nor uniqueness: There are abelian groups that cannot be made into $\mathbb{R}$-modules; there are also abelian groups that can be made into $\mathbb{R}$-modules in multiple different ways. So the action of $\mathbb{R}$ on an $\mathbb{R}$-module cannot be reconstructed from the underlying group of the latter (unlike for $\mathbb{Z}$ and $\mathbb{Q}$). "Most" rings behave more like $\mathbb{R}$ than like $\mathbb{Z}$ and $\mathbb{Q}$ in this regard.

[8] Don't get me wrong: "redundant" and "in fancy clothes" doesn't mean "useless"; it just means that the scaling is determined by the abelian group structure.

1.4. Module morphisms ([DF, §10.2])

Module morphisms are defined similarly to ring morphisms, but you probably already know their definition from linear algebra: they are also known as linear maps. Let me recall the definition:

Definition 1.4.1. Let R be a ring. Let M and N be two left R-modules.

(a) A **left R-module homomorphism** (or, for short, **left R-module morphism**, or **left R-linear map**) from M to N means a map $f : M \to N$ that

- **respects addition** (i.e., satisfies $f(a+b) = f(a) + f(b)$ for all $a, b \in M$);
- **respects scaling** (i.e., satisfies $f(ra) = rf(a)$ for all $r \in R$ and $a \in M$);
- **respects the zero** (i.e., satisfies $f(0_M) = 0_N$).

You can drop the word "left" (and, e.g., just say "R-module morphism") when it is clear from the context.

(b) A **left R-module isomorphism** (or, informally, **left R-module iso**) from M to N means an invertible left R-module morphism $f : M \to N$ whose inverse $f^{-1} : N \to M$ is also a left R-module morphism.

(c) The left R-modules M and N are said to be **isomorphic** (this is written $M \cong N$) if there exists a left R-module isomorphism $f : M \to N$.

(d) We let $\operatorname{Hom}_R(M, N)$ be the set of all left R-module morphisms from M to N.

(e) Right R-module morphisms are defined similarly.

It is not hard to show that the "respects the zero" axiom in Definition 1.4.1 **(a)** is redundant. (In fact, it is "doubly redundant": It follows from each of the other two axioms!)

Here are some examples of R-module morphisms:

- You have seen linear maps between vector spaces in linear algebra. These are precisely the left R-module morphisms when R is a field.
- Let $k \in \mathbb{Z}$. The map $\mathbb{Z} \to \mathbb{Z},\ a \mapsto ka$ is always a $\mathbb{Z}$-module morphism. (For comparison: It is a ring morphism only when $k = 1$.)
- More generally: Let R be a **commutative** ring. Let $k \in R$. Let M be any R-module. Then, the map $M \to M,\ a \mapsto ka$ is an R-module morphism. (This is the map that we have called "scaling by k".) If R is not commutative, then this map is not a (left) R-module morphism in general!
- Let R be a ring. Let $n \in \mathbb{N}$. For any $i \in \{1, 2, \ldots, n\}$, the map

$$\pi_i : R^n \to R,$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_i$$

is a left R-module morphism.

More generally: If $(M_i)_{i \in I}$ is a family of left R-modules, and if $j \in I$, then the map

$$\pi_j : \prod_{i \in I} M_i \to M_j, \\ (m_i)_{i \in I} \mapsto m_j$$

is a left R-module morphism. This follows immediately from the fact that the structure of $\prod_{i \in I} M_i$ (addition, action and zero) is defined entrywise.

- If M and N are two R-modules, then the map

$$M \times N \to N \times M, \\ (m, n) \mapsto (n, m)$$

is an R-module isomorphism.

The $\mathbb{Z}$-module morphisms (i.e., the $\mathbb{Z}$-linear maps) are simply the group morphisms of additive groups:

Proposition 1.4.2. Let M and N be two $\mathbb{Z}$-modules. Then,

$$\operatorname{Hom}_{\mathbb{Z}}(M, N) = \{\text{group morphisms } (M, +, 0) \to (N, +, 0)\}.$$

Proof. We have to show that any group morphism $f : (M, +, 0) \to (N, +, 0)$ automatically respects the scaling – i.e., that it satisfies $f(na) = nf(a)$ for all $n \in \mathbb{Z}$ and $a \in M$. This is LTTR. $\square$