that $x, y \in \mathbb{Z}_{(p)}$, so we can write $x = a/b$ and $y = c/d$ for some integers a, b, c and d, where b and d are not divisible by p. As p is prime this means that bd is also not divisible by p. We have

$$\begin{aligned} x + y &= (ad + bc)/(bd) \\ xy &= (ac)/(bd) \\ -x &= -a/b. \end{aligned}$$

As $ad + bc$, ac, $-a$, b and bd are integers, and bd and b are not divisible by p, this means that $x + y$, xy and $-x$ lie in $\mathbb{Z}_{(p)}$. Thus $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$, called the ring of integers localised at p. (There is a long story coming from algebraic geometry that explains why the word "localised" is appropriate.)

Example 2.11. We write $\mathbb{Z}[i]$ for the set of complex numbers of the form $a + bi$, where a and b are integers (possibly zero). Thus 7, $6 - 4i$ and $12i$ are elements of $\mathbb{Z}[i]$, but $2/3$ and $1 - i/5$ are not. Note that

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i \\ -(a + bi) &= (-a) + (-b)i. \end{aligned}$$

It follows easily that $\mathbb{Z}[i]$ is closed under addition, multiplication and negation, so it is a subring of $\mathbb{C}$. The elements of $\mathbb{Z}[i]$ are called *Gaussian integers*.

3. Modules

Definition 3.1. Let R be a ring. A *module* over R is a set M of things with a definition of $m + n$ for all $m, n \in M$ and a definition of am for all $a \in R$ and $m \in M$ such that the following axioms are satisfied:

(a) If $m, n \in M$ then $m + n \in M$. [closure under addition]
(b) There is an element $0 \in M$ such that $m + 0 = m$ for all $m \in M$. [additive identity]
(c) For each $m \in M$ there is an element $-m \in M$ such that $m + (-m) = 0$. [additive inverses]
(d) $m + (n + p) = (m + n) + p$ for all $m, n, p \in M$. [associativity of addition]
(e) $m + n = n + m$ for all $m, n \in M$. [commutativity of addition]
(f) If $a \in R$ and $m \in M$ then $am \in M$. [closure of M under multiplication by R]
(g) $1.m = m$ for all $m \in M$.
(h) $(ab)m = a(bm)$ for all $a, b \in R$ and $m \in M$. [associativity of multiplication]
(i) $(a + b)m = am + bm$ for all $a, b \in R$ and $m \in M$. [left distributivity of multiplication]
(j) $a(m + n) = am + an$ for all $a \in R$ and $m, n \in M$. [right distributivity of multiplication]

Remark 3.2. Note that axioms (a) to (e) say that M is in particular an Abelian group under addition.

Example 3.3. Let R be any ring, and let d be a natural number. We then write R^d for the set of d-tuples $(x_1, \dots, x_d)$ with $x_1, \dots, x_d \in R$. We make R^d into a module over R by defining

$$\begin{aligned} (x_1, \dots, x_d) + (y_1, \dots, y_d) &= (x_1 + y_1, \dots, x_d + y_d) \\ a(x_1, \dots, x_d) &= (ax_1, \dots, ax_d). \end{aligned}$$

It is straightforward to check that the axioms are satisfied. In particular, the case $d = 1$ says that we can regard R as a module over itself.

If R is a field, then an R-module is just a vector space over R. Modules are just the natural generalisation of vector spaces defined over arbitrary rings rather than just fields. It is a basic fact of linear algebra that if K is a field and V is a vector space over K with a finite spanning set, then V is isomorphic to K^d for some integer d, called the *dimension* of V. The situation for modules over non-fields is more complicated; a module is usually not isomorphic to R^d for any d. The next simplest case after fields is when R is a Euclidean domain, and most of the course will be devoted to the study of modules over such rings.

Proposition 3.4. *A $\mathbb{Z}$-module is just an Abelian group. More precisely, if M is an Abelian group (with the group operation written as addition) then there is a unique way to define am for all $a \in \mathbb{Z}$ and $m \in M$ such that axioms (f) to (j) hold, making M a $\mathbb{Z}$-module.*

Sketch proof. Rather than giving a complete proof of this, we will give an outline of the argument with examples.

The basic idea is very simple. We just define

$$\begin{aligned} 3m &= m + m + m \\ -5m &= -(m + m + m + m + m) = (-m) + (-m) + (-m) + (-m) + (-m) \end{aligned}$$

and so on. This defines multiplication (of integers by group elements) in terms of addition and negation of group elements. We actually have no choice about these definitions if we want the axioms to be satisfied: as $3 = 1 + 1 + 1$, axiom (i) says we we must have $3m = (1 + 1 + 1)m = 1m + 1m + 1m$, and axiom (g) says that $1m = m$ so we must have $3m = m + m + m$, and so on.

We now need to check that axioms (f) to (j) are satisfied. Axioms (f) and (g) are immediate. The remaining axioms are easy to check when a and b are nonnegative: for example

$$\begin{aligned} 2(3m) &= 2(m + m + m) \\ &= (m + m + m) + (m + m + m) \\ &= m + m + m + m + m + m \\ &= (2 \times 3)m \\ 2m + 3m &= (m + m) + (m + m + m) \\ &= m + m + m + m + m \\ &= (2 + 3)m \\ 3(m + n) &= (m + n) + (m + n) + (m + n) \\ &= (m + m + m) + (n + n + n) \\ &= 3m + 3n. \end{aligned}$$

If we allow a or b to be negative then there are quite a few more cases to check depending on the various possible combinations of signs, but they are all quite straightforward. For example

$$\begin{aligned} 5m + (-3)m &= (m + m + m + m + m) + ((-m) + (-m) + (-m)) \\ &= m + m + (m + (-m)) + (m + (-m)) + (m + (-m)) \\ &= m + m \\ &= (5 + (-3))m. \end{aligned}$$

□

4. Modules over polynomial rings

We next consider modules over $K[x]$, where K is a field. The upshot here is that the study of modules over $K[x]$ is essentially the same as the study of square matrices over K, or of endomorphisms of vector spaces over K.

We start with some comments about the process of "substituting a matrix into a polynomial". Let K be a field, and let A be an $n \times n$ matrix over K. Using the usual matrix multiplication we can define A^2, A^3 and so on; all of these are again $n \times n$ matrices over K. Thus, given a polynomial $f(x) = a_0 + a_1 x + \ldots + a_d x^d \in K[x]$ we can define another $n \times n$ matrix $f(A)$ by $f(A) = a_0 I + a_1 A + \ldots + a_d A^d$.

Example 4.1. If $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$ and $f(x) = 7 + 6x + 5x^2$ then $A^2 = \left(\begin{smallmatrix} 7 & 10 \\ 15 & 22 \end{smallmatrix}\right)$ and so

$$\begin{aligned} f(A) &= 7\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + 6\left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right) + 5\left(\begin{smallmatrix} 7 & 10 \\ 15 & 22 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 7 & 0 \\ 0 & 7 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 6 & 12 \\ 18 & 24 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 35 & 50 \\ 75 & 110 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 48 & 62 \\ 93 & 141 \end{smallmatrix}\right). \end{aligned}$$

Example 4.2. Consider a diagonal matrix $A = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$. Then

$$A^2 = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} = \begin{pmatrix} \lambda^2 & 0 \\ 0 & \mu^2 \end{pmatrix},$$

and more generally it is not hard to see that

$$A^k = \begin{pmatrix} \lambda^k & 0 \\ 0 & \mu^k \end{pmatrix}.$$

(Exercise: prove this by induction.) It follows that

$$\begin{aligned} f(A) &= a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} + \ldots + a_d \begin{pmatrix} \lambda^d & 0 \\ 0 & \mu^d \end{pmatrix} \\ &= \begin{pmatrix} a_0 + a_1\lambda + \ldots a_d\lambda^d & 0 \\ 0 & a_0 + a_1\mu + \ldots a_d\mu^d \end{pmatrix} \\ &= \begin{pmatrix} f(\lambda) & 0 \\ 0 & f(\mu) \end{pmatrix}. \end{aligned}$$

More generally, if A is an $n \times n$ matrix with entries $\lambda_1, \ldots, \lambda_n$ on the diagonal and zeros elsewhere, then $f(A)$ has entries $f(\lambda_1), \ldots, f(\lambda_n)$ on the diagonal and zeros elsewhere.

Example 4.3. Consider the matrix $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. It is easy to check that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix},$$

and thus that $A^k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ for all k. It follows that

$$\begin{aligned} f(A) &= a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \ldots + a_d \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_0 + \ldots + a_d & a_1 + 2a_2 + \ldots + da_d \\ 0 & a_0 + \ldots + a_d \end{pmatrix}. \end{aligned}$$

Note that $f(1) = a_0 + \ldots + a_d$. Note also that the derivative $f'(x)$ is given by $f'(x) = a_1 + 2a_2x + \ldots + da_dx^{d-1}$, so that $f'(1) = a_1 + 2a_2 + \ldots + da_d$. We can thus rewrite the above result as

$$f(A) = \begin{pmatrix} f(1) & f'(1) \\ 0 & f(1) \end{pmatrix}.$$

Exercise 4.4. Put $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ and $f(x) = x^4 - 3x$. Calculate $f(A)$.

Exercise 4.5. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a 2×2 matrix, and put $f(x) = x^2 - (a+d)x + (ad - bc)$. Show that $f(A) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. (This is the 2×2 case of the Cayley-Hamilton theorem.)

Exercise 4.6. Show that

$$f\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \frac{f(1)}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{f(-1)}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

We next need to check that some things work out as they "ought" to when we substitute matrices into polynomials. (Recall that matrix multiplication is noncommutative, there are nonzero matrices whose square is zero, and numerous other funny things can happen; so we need to be on our guard.)

Proposition 4.7. *Let A be an $n \times n$ matrix over a field K. Then for any two polynomials $f, g \in K[x]$ we have*

$$\begin{aligned} (f+g)(A) &= f(A) + g(A) \\ (fg)(A) &= f(A)g(A). \end{aligned}$$

Proof. Suppose that $f(x) = \sum_i a_i x^i$ and $g(x) = \sum_j b_j x^j$. Then $(f+g)(x) = \sum_i c_i x^i$ where $c_i = a_i + b_i$, and

$$(fg)(x) = (\sum_i a_i x^i)(\sum_j b_j x^j) = \sum_{i,j} a_i b_j x^{i+j} = \sum_k d_k x^k,$$

where $d_k = \sum_{i=0}^k a_i b_{k-i}$.

Thus

$$\begin{aligned}(f+g)(A) &= \sum_i c_i A^i \\ &= \sum_i (a_i A^i + b_i A^i) \\ &= \sum_i a_i A^i + \sum_i b_i A^i \\ &= f(A) + g(A).\end{aligned}$$

Similarly

$$\begin{aligned}(fg)(A) &= \sum_k d_k A^k \\ &= \sum_k \sum_{i=0}^k a_i b_{k-i} A^k \\ &= \sum_k \sum_{i=0}^k (a_i A^i)(b_{k-i} A^{k-i}) \\ &= \sum_i \sum_j (a_i A^i)(b_j A^j) \\ &= \sum_i a_i A^i \sum_j b_j A^j \\ &= f(A)g(A).\end{aligned}$$

□

We are now ready to construct some modules over $K[x]$.

Construction 4.8. Let A be an $n \times n$ matrix over a field K; we will use this to define a module M_A over $K[x]$. The elements of M_A are just the vectors $v = (v_1, \dots, v_n)$ of length n over K, so $M_A = K^n$ as a set. Addition and subtraction of vectors is defined in the usual way. All that is left is to define the product fv for $f \in K[x]$ and $v \in K^n$, which we do by the formula $fv = f(A)v$. Here $f(A)$ is an $n \times n$ matrix, so the right hand side is defined by the ordinary multiplication of vectors by matrices.

We need to check the module axioms. Axioms (a) to (e) only involve addition and negation so they are clear. Axiom (f) is also clear because fv is certainly a vector in K^n. If $f(x)$ is constant polynomial 1, then $f(A)$ is the identity matrix, so $fv = Iv = v$ for all v; this gives axiom (g). For axiom (h) we recall that $(fg)(A) = f(A)g(A)$ so

$$\begin{aligned}(fg)v &= (fg)(A)v \\ &= f(A)g(A)v \\ &= f(A)(gv) \\ &= f(gv).\end{aligned}$$

Similarly, axiom (i) follows from the fact that $(f+g)(A) = f(A) + g(A)$. Finally, axiom (j) is clear, because $B(v+w) = Bv + Bw$ for any matrix B and any vectors v and w.

Remark 4.9. Let A and B be two different $n \times n$ matrices. Then M_A and M_B have the same elements but the multiplication rules in M_A and M_B are different, so M_A and M_B are different modules.

Example 4.10. Let A be the matrix $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ over $\mathbb{Q}$, so that $f(A) = \left(\begin{smallmatrix} f(2) & 0 \\ 0 & f(3) \end{smallmatrix}\right)$ (by Example 4.2). Then $M_A = \mathbb{Q}^2$, with the multiplication rule $f.(s,t) = (f(2)s, f(3)t)$. For example, if $g(x) = x^2 - 6$ then $g(2) = -2$ and $g(3) = 3$ so we have

$$(x^2 - 6)(10, 11) = (-2 \times 10, 3 \times 11) = (-20, 33).$$

Example 4.11. Let A be the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ over $\mathbb{Q}$, so that $f(A) = \left(\begin{smallmatrix} f(1) & f'(1) \\ 0 & f(1) \end{smallmatrix}\right)$ (by Example 4.3). Then M_A is the set $\mathbb{Q}^2$ with the group operation $f.(s,t) = (f(1)s + f'(1)t, f(1)t)$. For example, if $g(x) = x^2 - 6$ then $g(1) = -5$ and $g'(1) = 2$ so we have

$$(x^2 - 6)(10, 11) = (-5 \times 10 + 2 \times 11, -5 \times 11) = (-28, -55).$$

Example 4.12. The simplest examples are where A is just a 1×1 matrix, or in other words just an element $\lambda \in K$. The module M_λ is just a copy of K, with the multiplication rule $f.a = f(\lambda)a$. For example, the polynomial $f(x) = 1 + x + x^2$ satisfies $f(2) = 7$, so in the module M_2 over $\mathbb{Q}[x]$ we have $f.6 = 7 \times 6 = 42$.

There is a well-known correspondence between matrices and endomorphisms, and for many purposes it is more natural to use the latter. Let V be a vector space over a field K, and let ϕ be an endomorphism of V (in other words, a linear map from V to itself). Then we can define $\phi^2(v) = \phi(\phi(v))$ to get a new endomorphism of V, and similarly we can define ϕ^k for all $k \geq 0$. More generally, for any polynomial $f(x) = a_0 + a_1 x + \ldots + a_d x^d \in K[x]$ we can define an endomorphism $f(\phi)$ by

$$f(\phi)(v) = a_0 v + a_1 \phi(v) + \ldots + a_d \phi^d(v).$$

We can then make V into a module over $K[x]$ by defining $fv = f(\phi)(v)$.

We will next give an example involving differentiation, which is the basis of the applications of module theory to differential equations. To avoid annoying technicalities, it is best to restrict attention to functions that can be differentiated as many times as we like. We therefore introduce the following definition.

Definition 4.13. A function $f\colon \mathbb{R} \to \mathbb{R}$ is *smooth* if the n'th derivatives $f^{(n)}(t)$ are defined and continuous everywhere on $\mathbb{R}$ for all $n \geq 0$. In particular, the function $f = f^{(0)}$ itself must be defined and continuous everywhere.

For example, $\sin(t)$, $\cos(t)$, e^t, t^2 and so on are smooth. However, the functions $1/t$ and $\log(t)$ are not defined at $t = 0$, so they are not smooth. The function $f(t) = |t|$ is defined and continuous everywhere and $f'(t) = -1$ for $t < 0$ and $f'(t) = 1$ for $t > 0$ but $f'(0)$ is undefined so f is not smooth. Similarly, if $g(t) = t^{1/3}$ then $g'(t) = t^{-2/3}/3$, which is undefined at $t = 0$ so g is not smooth.

We write $C^\infty(\mathbb{R}, \mathbb{R})$ for the set of all smooth functions from $\mathbb{R}$ to $\mathbb{R}$. If f and g are smooth and a is constant then one can show that $f + g$ and af are smooth. It follows that $C^\infty(\mathbb{R}, \mathbb{R})$ is a vector space over $\mathbb{R}$. Similarly, the set $C^\infty(\mathbb{R}, \mathbb{C})$ of smooth functions from $\mathbb{R}$ to $\mathbb{C}$ is a vector space over $\mathbb{C}$.

Now define $\partial\colon C^\infty(\mathbb{R}, \mathbb{R}) \to C^\infty(\mathbb{R}, \mathbb{R})$ by $\partial(f) = f'$. If f and g are smooth and a and b are constant, we have

$$\partial(af + bg) = (af + bg)' = af' + bg' = a\partial(f) + b\partial(g),$$

which shows that ∂ is an $\mathbb{R}$-linear map.

Similarly, differentiation gives a $\mathbb{C}$-linear map from $C^\infty(\mathbb{R}, \mathbb{C})$ to itself, which we again call ∂.

We could use the endomorphism ∂ of $C^\infty(\mathbb{R}, \mathbb{R})$ to make $C^\infty(\mathbb{R}, \mathbb{R})$ into a module over $\mathbb{R}[x]$. However, it is more standard and notationally less confusing to rename the variable x and call it D instead. We will also write $p(D)$ for a typical polynomial in D, to avoid confusion with elements of $C^\infty(\mathbb{R}, \mathbb{R})$, which are typically called f.

Definition 4.14. We regard $C^\infty(\mathbb{R},\mathbb{R})$ as a module over $\mathbb{R}[D]$ by the rule $p(D)f = p(\partial)(f)$, or equivalently

$$\begin{aligned}(a_0 + a_1D + \ldots + a_mD^m)f &= a_0\partial^0(f) + a_1\partial^1(f) + \ldots + a_m\partial^m(f)\\ &= a_0f + a_1f' + \ldots + a_mf^{(m)}.\end{aligned}$$

We regard $C^\infty(\mathbb{R},\mathbb{C})$ as a module over $\mathbb{C}[D]$ by the same rule.

Example 4.15.

$$\begin{aligned}(1 + D + D^2).(1 + t + t^2) &= (1 + t + t^2) + (1 + t + t^2)' + (1 + t + t^2)''\\ &= (1 + t + t^2) + (1 + 2t) + (2)\\ &= 4 + 3t + t^2.\end{aligned}$$

Example 4.16. Consider the function $f(t) = t\sin(t)$; I claim that $(D^2 + 1)^2f = 0$. Indeed, we have

$$\begin{aligned}f'(t) &= \sin(t) + t\cos(t)\\ f''(t) &= 2\cos(t) - t\sin(t)\\ ((D^2 + 1)f)(t) &= f(t) + f''(t) = 2\cos(t)\end{aligned}$$

We also have $\cos'(t) = -\sin(t)$ and so $\cos''(t) = -\cos(t)$ so $(D^2 + 1)\cos = 0$. It follows that $(D^2 + 1)^2f = (D^2 + 1)(2\cos) = 0$.

Example 4.17. Consider a function of the form $f(t) = e^{\lambda t} + e^{\mu t}$. I claim that

$$(p(D)f)(t) = p(\lambda)e^{\lambda t} + p(\mu)e^{\mu t}.$$

Indeed, we have

$$\begin{aligned}f'(t) &= \lambda e^{\lambda t} + \mu e^{\mu t}\\ f''(t) &= \lambda^2 e^{\lambda t} + \mu^2 e^{\mu t}\end{aligned}$$

and more generally $f^{(k)}(t) = \lambda^k e^{\lambda t} + \mu^k e^{\mu t}$ (as one can easily check by induction). If $p(D) = a_0 + a_1D + \ldots + a_mD^m$ then we have

$$\begin{aligned}(p(D)f)(t) &= a_0(e^{\lambda t} + e^{\mu t}) + a_1(\lambda e^{\lambda t} + \mu e^{\mu t}) + \ldots + a_m(\lambda^m e^{\lambda t} + \mu^m e^{\mu t})\\ &= (a_0 + a_1\lambda + \ldots + a_m\lambda^m)e^{\lambda t} + (a_0 + a_1\mu + \ldots + a_m\mu^m)e^{\mu t}\\ &= p(\lambda)e^{\lambda t} + p(\mu)e^{\mu t}.\end{aligned}$$

Exercise 4.18. Put $f(t) = te^t$. Show that $(D^kf)(t) = (k + t)e^t$ for all $k \geq 0$ and thus that $(p(D)f)(t) = (p'(1) + p(1)t)e^t$.

We explained above how a vector space V over K with an endomorphism ϕ can be regarded as a $K[x]$-module. We conclude this section by showing that *every* $K[x]$-module arises in this way.

Indeed, let M be a module over $K[x]$. As mentioned previously, axioms (a) to (e) say that M is an Abelian group under addition. Also, if $a \in K$ then we can regard a as a constant polynomial, so am is defined for all $m \in M$. As M is a module over $K[x]$, axioms (f) to (j) are valid for all polynomials a and b, so certainly they are valid for the special case of constant polynomials. Thus, we can regard M as a module over K. A module over a field is the same thing as a vector space, so M is a vector space over K.

Next, if $m \in M$ then xm is another element of M, so we can define a function $\phi\colon M \to M$ by $\phi(m) = xm$. I claim that this is a K-linear endomorphism. Indeed, for any $m, n \in M$ we have $x(m + n) = xm + xn$ by the right distributivity law, which means that $\phi(m + n) = \phi(m) + \phi(n)$. Moreover, for $a \in K$ we have $ax = xa$, so

$$a\phi(m) = a(xm) = (ax)m = (xa)m = x(am) = \phi(am)$$

(using axiom (h) twice). This shows that ϕ is linear, as claimed. Now consider a polynomial $f(x) = \sum_i a_i x^i \in K[x]$. I claim that $fm = \sum_i a_i \phi^i(m) = f(\phi)(m)$ for all $m \in M$. Indeed, we have

$$(x^2)m = x(xm) = x\phi(m) = \phi(\phi(m)) = \phi^2(m)$$
$$(x^3)m = x(x^2m) = x\phi^2(m) = \phi(\phi^2(m)) = \phi^3(m).$$

Extending this by induction, we see that $x^k m = \phi^k(m)$ for all k. Thus

$$\begin{aligned} fm &= (\sum_i a_i x^i)m \\ &= \sum_i a_i x^i m \\ &= \sum_i a_i \phi^i(m) \\ &= f(\phi)(m). \end{aligned}$$

Thus, the module structure is obtained from the endomorphism ϕ in the way considered previously.

5. General module theory

Let R be a ring.

Definition 5.1. Let M be an R-module. A *submodule* of M is a subset $N \subseteq M$ such that

(a) $0 \in N$
(b) If $n, m \in M$ then $n + m \in N$ (ie N is closed under addition)
(c) If $n \in N$ and $a \in R$ then $an \in N$ (ie N is closed under multiplication by elements of R).

Note that if N is a submodule and $n \in N$ then $-n = (-1)n \in N$, so N is closed under negation and thus is a subgroup of M under addition. It is easy to see that N can itself be considered as an R-module.

Example 5.2. If R is a field, then modules are just the same as vector spaces, and submodules are just the same as vector subspaces.

Example 5.3. If $R = \mathbb{Z}$, then modules are just the same as Abelian groups, and submodules are just the same as subgroups.

Example 5.4. If M is a module over any ring R, it is clear that $\{0\}$ and M itself are submodules of M.

Example 5.5. Let V be a vector space over a field K, equipped with a K-linear endomorphism $\phi\colon V \to V$. We regard V as a $K[x]$-module in the usual way. We say that a subset $W \subseteq V$ is *stable under* ϕ if $\phi(w) \in W$ for all $w \in W$ (or more briefly, if $\phi(W) \subseteq W$).

I claim that a subset $W \subseteq V$ is a $K[x]$-submodule if and only if it is a vector subspace and is stable under ϕ. Indeed, suppose that W is a submodule. Then it is certainly closed under addition and under multiplication by constant polynomials (ie elements of K) so it is a vector subspace. Also, it is closed under multiplication by x, so for $w \in W$ we have $\phi(w) = xw \in W$; this shows that W is stable under ϕ, as claimed.

Conversely, suppose that W is a vector subspace and is stable under ϕ. Clearly W is closed under addition. For any $w \in W$ we have $\phi(w) \in W$. Thus $\phi^2(w) = \phi(\phi(w)) = \phi(\text{an element of } W) = $ another element of W , so $\phi^2(W) \subseteq W$. Thus $\phi^3(w) = \phi(\phi^2(w)) = \phi(\text{an element of } W) = $ another element of W , so $\phi^3(W) \subseteq W$, and so on, so $\phi^k(w) \in W$ for all $k \geq 0$. Now consider a polynomial $f(x) = a_0 + \ldots + a_d x^d \in K[x]$. We then have $fw = \sum_i a_i \phi^i(w)$. The vectors $\phi^i(w)$ lie in W, the coefficients a_i lie in K, and W is a vector subspace of V, so we see that $\sum_i a_i \phi^i(w) \in W$. Thus $fw \in W$ for all $w \in W$ and $f \in K[x]$, so W is a submodule of V.

Example 5.6. Let A be the matrix $\begin{pmatrix} 0 & -6 \\ 1 & 5 \end{pmatrix}$ over $\mathbb{Q}$, and use this to make $\mathbb{Q}^2$ into a module over $\mathbb{Q}[x]$. Put $W_0 = \{(u,v) \in \mathbb{Q}^2 \mid u = -3v\}$ and $W_1 = \{(u,v) \in \mathbb{Q}^2 \mid u = -4v\}$. A typical element of W_0 has the form $(-3v, v)$ and we have

$$\begin{pmatrix} 0 & -6 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} -3v \\ v \end{pmatrix} = \begin{pmatrix} -6v \\ 2v \end{pmatrix},$$

which also lies in W_0. Thus W_0 is stable under A and thus is a submodule of $\mathbb{Q}^2$.

However, W_1 is not a submodule. Indeed, the vector $(-4, 1)$ lies in W_1 but

$$\begin{pmatrix} 0 & -6 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} -4 \\ 1 \end{pmatrix} = \begin{pmatrix} -6 \\ 1 \end{pmatrix},$$

which does not lie in W_1.

Example 5.7. Suppose that $\lambda, \mu \in K$ and $\lambda \neq \mu$. Define $\phi\colon K^2 \to K^2$ by $\phi(u,v) = (\lambda u, \mu v)$, and use this to make K^2 into a module over $K[x]$. Define

$$L = \{(u,0) \mid u \in K\} \subset K^2$$
$$M = \{(0,v) \mid v \in K\} \subset K^2.$$

I claim that L and M are $K[x]$-submodules of K^2, and moreover that the only submodules are $\{0\}$, L, M and K^2 itself.

It is clear that L and M are vector subspaces of K^2. Moreover we have $\phi(u,0) = (\lambda u, 0) \in L$, so L is stable under ϕ and thus is a submodule. Similarly $\phi(0,v) = (0, \mu v) \in M$, so M is a submodule. It is trivial to check that $\{0\}$ and K^2 are subspaces of K^2.

We will not give a complete proof that these are the only submodules, but here is the key point. We assumed that $\lambda \neq \mu$, so $\lambda - \mu$ is a nonzero element of the field K, so $(\lambda - \mu)^{-1}$ is defined. We thus have elements $\pi_0 = (\lambda - \mu)^{-1}(x - \mu) \in K[x]$ and $\pi_1 = 1 - \pi_0 \in K[x]$. Note that

$$\begin{aligned} \pi_0(u,v) &= (\lambda - \mu)^{-1}(x(u,v) - \mu(u,v)) \\ &= (\lambda - \mu)^{-1}(\phi(u,v) - (\mu u, \mu v)) \\ &= (\lambda - \mu)^{-1}((\lambda u, \mu v) - (\mu u, \mu v)) \\ &= (u, 0) \end{aligned}$$

and

$$\begin{aligned} \pi_1(u,v) &= (1 - \pi_0)(u,v) \\ &= (u,v) - \pi_0(u,v) \\ &= (u,v) - (u,0) \\ &= (0,v). \end{aligned}$$

Now let W be a submodule of K^2. Suppose that W contains an element (u,v) with $u \neq 0 \neq v$. Then for any $a, b \in K$ we have $au^{-1}\pi_0 + bv^{-1}\pi_1 \in K[x]$ and

$$(au^{-1}\pi_0 + bv^{-1}\pi_1)(u,v) = au^{-1}(u,0) + bv^{-1}(0,v) = (a,b).$$

As W is a submodule this means that $(a,b) \in W$. As a and b were arbitrary this shows that $W = K^2$. If W does not contain any elements (u,v) with $u \neq 0 \neq v$ then one has to fiddle around a bit more but one can show that $W = \{0\}$ or $W = L$ or $W = M$.

Example 5.8. The set $\mathbb{R}[t]$ of polynomial functions is a vector subspace of the space $C^\infty(\mathbb{R}, \mathbb{R})$ of all smooth functions from $\mathbb{R}$ to $\mathbb{R}$. Moreover if $f \in \mathbb{R}[t]$ then the derivative of f is again a polynomial, in other words $\partial(f) = f' \in \mathbb{R}[t]$. This means that the subspace $\mathbb{R}[t]$ is stable under the endomorphism ∂, so it is an $\mathbb{R}[D]$-submodule of $C^\infty(\mathbb{R}, \mathbb{R})$.

Example 5.9. Let W be the space of functions of the form $f(t) = a\cos(t) + b\sin(t)$ (with $a, b \in \mathbb{R}$). Because $\partial(a\cos(t) + b\sin(t)) = b\cos(t) - a\sin(t)$, we see that W is stable under ∂. It is thus an $\mathbb{R}[D]$-submodule of $C^\infty(\mathbb{R}, \mathbb{R})$.

Remark 5.10. Suppose that N_0 and N_1 are two submodules of an R-module M. I claim that $N_0 \cap N_1$ is again a submodule. Indeed, as $0 \in N_0$ and $0 \in N_1$ we have $0 \in N_0 \cap N_1$. Suppose that $n, m \in N_0 \cap N_1$. As $n, m \in N_0$ and N_0 is a submodule we have $n + m \in N_0$. As $n, m \in N_1$ and N_1 is a submodule we have $n + m \in N_1$. Thus $n + m \in N_0 \cap N_1$. Now suppose that $a \in R$. As N_0 is a submodule and $n \in N_0$ we have $an \in N_0$. As N_1 is a submodule and $n \in N_1$ we also have $an \in N_1$, so $an \in N_0 \cap N_1$. This shows that $N_0 \cap N_1$ is a submodule, as claimed.

Definition 5.11. Suppose that N_0 and N_1 are two submodules of an R-module M. We define $N_0 + N_1$ to be the set of elements $x \in M$ that can be written in the form $x = n_0 + n_1$ for some $n_0 \in N_0$ and $n_1 \in N_1$. I claim that this is a submodule of M. Indeed, suppose that $x, y \in N_0 + N_1$, so we can write $x = n_0 + n_1$ and $y = m_0 + m_1$ with $n_0, m_0 \in N_0$ and $n_1, m_1 \in N_1$. Then $x + y$ can be written as $(n_0 + m_0) + (n_1 + m_1)$, with $n_0 + m_0 \in N_0$ and $n_1 + m_1 \in N_1$, so $x + y \in N_0 + N_1$. Similarly, if $a \in R$ then $an_0 \in N_0$ and $an_1 \in N_1$ so $ax = an_0 + an_1 \in N_0 + N_1$. This shows that $N_0 + N_1$ is closed under addition and under multiplication by R, so it is a submodule as claimed.

Definition 5.12. Let N_0 and N_1 be R-modules. We define $N_0 \oplus N_1$ to be the set of pairs (n_0, n_1) with $n_0 \in N_0$ and $n_1 \in N_1$. We make this set into an R-module by defining

$$(n_0, n_1) + (m_0, m_1) = (n_0 + m_0, n_1 + m_1)$$
$$a(n_0, n_1) = (an_0, an_1).$$

(It is a longish but straightforward exercise to check that the axioms are satisfied.) This R-module is called the *external direct sum* of N_0 and N_1.

Example 5.13. The group $\mathbb{Z}_2$ has elements $\overline{0}$ and $\overline{1}$, and the group $\mathbb{Z}_3$ has elements $\overline{0}$, $\overline{1}$ and $\overline{2}$. Thus, the group $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ has elements $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{1})$, $(\overline{0}, \overline{2})$, $(\overline{1}, \overline{0})$, $(\overline{1}, \overline{1})$ and $(\overline{1}, \overline{2})$. To illustrate the additiion law, we have $(\overline{1}, \overline{2}) + (\overline{1}, \overline{2}) = (\overline{2}, \overline{4})$. The first component is to be interpreted as an element of $\mathbb{Z}_2$, so $\overline{2} = \overline{0}$. The second component is to be interpreted as an element of $\mathbb{Z}_3$, so $\overline{4} = \overline{1}$. Thus $(\overline{1}, \overline{2}) + (\overline{1}, \overline{2}) = (\overline{0}, \overline{1})$.

Example 5.14. An element of $R^n \oplus R^m$ is a pair (u, v) with $u \in R^n$ and $v \in R^m$, or in other words a list $(u_1, \dots, u_n, v_1, \dots, v_m)$ where each u_i and v_j is an element of R. Thus, $R^n \oplus R^m = R^{n+m}$.

The next example relies on the following definition:

Definition 5.15. Let A and B be matrices over a field K, of sizes $p \times q$ and $n \times m$. The *block sum* of A and B is the matrix $\left(\begin{array}{c|c} A & 0_{n\times q} \\ \hline 0_{p\times m} & B \end{array}\right)$, of size $(p + n) \times (q + m)$. This is denoted by $A \oplus B$. For example, if $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right)$ then the block sum of A and B is

$$A \oplus B = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right) \oplus \left(\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & 5 & 6 \\ 0 & 0 & 7 & 8 \end{smallmatrix}\right).$$

Note that an element $w \in R^{p+n}$ can be written as $w = (u, v)$ with $u \in R^p$ and $v \in R^n$, and we have

$$(A \oplus B)w = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\frac{u}{v}\right) = \left(\frac{Au}{Bv}\right).$$

Example 5.16. Let A and B be square matrices over a field K, of sizes n and m say. We then have modules M_A and M_B over $K[x]$. The elements of $M_A \oplus M_B$ are pairs $w = (u, v)$ with $u \in K^n$ and $v \in K^m$, or equivalently they are elements of K^{n+m}. The module structure is given by the rule $x(u, v) = (xu, xv) = (Au, Bv)$, or in other words $xw = (A \oplus B)w$. Thus $M_A \oplus M_B = M_{A\oplus B}$.

Definition 5.17. Let M be an R-module, and let N_0 and N_1 be submodules. We say that M is the *internal direct sum* of N_0 and N_1 if $N_0 + N_1 = M$ and $N_0 \cap N_1 = \{0\}$.

Remark 5.18. We can define a function $\sigma\colon N_0 \oplus N_1 \to M$ by $\sigma(n_0, n_1) = n_0 + n_1$. When we have defined homomorphisms and isomorphisms of modules, we will see that σ is always a homomorphism, and that σ is an isomorphism if and only if M is the internal direct sum of N_0 and N_1. This is the precise sense in which internal direct sums are "the same" as external ones.

Example 5.19. In example 5.7 we see that K^2 is the internal direct sum of L and M.

Example 5.20. Consider the Abelian group $M = \mathbb{Z}_{12}$ as a module over $\mathbb{Z}$. Put $N_0 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ and $N_1 = \{\overline{0}, \overline{4}, \overline{8}\}$. It is easy to see that N_0 and N_1 are subgroups, and obviously $N_0 \cap N_1 = \{\overline{0}\}$. I claim that we also have $N_0 + N_1 = M$. Indeed, we have $\overline{1} = \overline{9} + \overline{4} \in N_0 + N_1$ and $N_0 + N_1$ is a submodule so for any $a \in \mathbb{Z}$ we have $\overline{a} = a.\overline{1} \in N_0 + N_1$, as required. Thus M is the internal direct sum of N_0 and N_1.

Example 5.21. Let V be the space of functions $f \in C^\infty(\mathbb{R}, \mathbb{R})$ that satisfy $f'' = f$. This is a vector space closed under differentiation, so it is an $\mathbb{R}[D]$-submodule of $C^\infty(\mathbb{R}, \mathbb{R})$. Put $W_0 = \{f \mid f' = f\}$ and $W_1 = \{f \mid f' = -f\}$. These are also vector spaces closed under differentiation, so they are $\mathbb{R}[D]$-submodules of $C^\infty(\mathbb{R}, \mathbb{R})$. If $f \in W_1$ then $f'' = (-f)' = -(-f) = f$, so $f \in V$. This shows that $W_1 \subseteq V$ and similarly $W_0 \subseteq V$, so W_0 and W_1 are submodules of V.

I claim that V is the direct sum of W_0 and W_1. One way to see this is just to solve the differential equations. We find that V consists of all functions of the form $ae^t + be^{-t}$, that W_0 consists of all functions of the form ae^t, and that W_1 consists of all functions of the form be^{-t}, and the claim is clear from this.

We can also prove the claim without solving the differential equations explicitly. Indeed, if $f \in W_0 \cap W_1$ then $f = f'$ (because $f \in W_0$) and $f' = -f$ (because $f \in W_1$) so $f = -f$, so $f = 0$. This shows that $W_0 \cap W_1 = \{0\}$. Next, suppose that $g \in V$, so $g'' = g$. Put $g_0 = (g + g')/2$ and $g_1 = (g - g')/2$. We find that $g_0' = (g' + g'')/2 = (g' + g)/2 = g_0$, so $g_0 \in W_0$. Similarly, we have $g_1' = (g' - g'')/2 = (g' - g)/2 = -g_1$, so $g_1 \in W_1$. As $g = g_0 + g_1$ it follows that $g \in W_0 + W_1$, and we conclude that $V = W_0 + W_1$ as required.

Definition 5.22. Let M be a module over a ring R, and let $m_1, \dots, m_r$ be elements of M. Let N be the set of elements $x \in M$ that can be written in the form $x = a_1 m_1 + \dots + a_r m_r$ for some $a_1, \dots, a_r \in M$. I claim that this is a submodule of M. Indeed, if $x, y \in N$ then we have $x = \sum_i a_i m_i$ and $y = \sum_i b_i m_i$ for some $a_1, \dots, a_r, b_1, \dots, b_r \in R$. We then have $x + y = \sum_i (a_i + b_i) m_i$ so $x + y \in N$; this shows that N is closed under addition. Similarly, if $c \in R$ we have $cx = \sum_i (ca_i) m_i \in N$, so N is closed under multiplication by R, so it is a submodule as claimed.

We call N *the submodule generated by* $\{m_1, \dots, m_r\}$. In particular, we say that M *is generated by* $\{m_1, \dots, m_r\}$ if $N = M$, or equivalently if every element $x \in M$ can be written in the form $a_1 m_1 + \dots + a_r m_r$. We say that M is *finitely generated* if there is some finite list of elements that generates M. We say that M is *cyclic* if there is a single element $m \in M$ that generates M, which means that every element $x \in M$ can be written in the form $x = am$ for some $a \in R$.

Example 5.23. The module R^d is clearly generated by the standard basis elements $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$ and so on. In particular it is finitely generated. It is not cyclic unless $d = 1$.

Example 5.24. Let M be a finite Abelian group, considered as a $\mathbb{Z}$-module. Let the elements of M be $m_1, \dots, m_d$. Then any element $m \in M$ is equal to m_i for some i, so certainly it can be expressed in the form $\sum_i a_i m_i$ (for example, $m_2 = 0.m_1 + 1.m_2 + 0.m_3 + \dots + 0.m_d$). Thus, M is finitely generated as a $\mathbb{Z}$-module.

Example 5.25. Let W_2 be the space of functions of the form $f(t) = a + bt + ct^2$, considered as a module over $\mathbb{R}[D]$ in the usual way. In particular, the function $g(t) = t^2$ gives an element of W_2. I claim that W_2 is generated by g, and thus is cyclic. Indeed, we have $g'(t)/2 = t$ and $g''(t)/2 = 1$. It follows that for any function $f(t) = a + bt + ct^2$, we have $(c + (b/2)D + (a/2)D^2)g = cg + (b/2)g' + (a/2)g'' = f$, so $f \in \mathbb{R}[D]g$. This proves that $\mathbb{R}[D]g = W_2$ as required.

It is not hard to extend this method to show that the space W_d of polynomials of degree at most d is also a cyclic module over $\mathbb{R}[D]$ generated by the function $g(t) = t^d$.

Example 5.26. Consider $\mathbb{R}[x]$ as a module over $\mathbb{R}$; I claim it is not finitely generated. Indeed, suppose we have a finite list $f_1, \dots, f_n$ of elements of $\mathbb{R}[x]$. Let d_i be the degree of the polynomial f_i, and put $d = \max(d_1, \dots, d_n)$. Then each of the polynomials f_i only involves the powers $1, x, x^2, \dots, x^d$, so any polynomial of the form $a_1 f_1 + \dots + a_n f_n$ (with $a_1, \dots, a_n \in \mathbb{R}$) also

involves only these powers. This means that x^{d+1} cannot be written in the form $a_1 f_1 + \ldots + a_n f_n$, so the elements $f_1, \ldots, f_n$ do not generate $\mathbb{R}[x]$ as a module over $\mathbb{R}$.

6. Homomorphisms

Definition 6.1. Let M and N be modules over a ring R. An *R-module homomorphism* (or just *homomorphism*) from M to N is a function $\alpha\colon M \to N$ such that

(a) $\alpha(m_0 + m_1) = \alpha(m_0) + \alpha(m_1)$ for all $m_0, m_1 \in M$.
(b) $\alpha(am) = a\alpha(m)$ for all $a \in R$ and $m \in M$.

Note that this implies that $\alpha(0) = \alpha(0.0) = 0\alpha(0) = 0$ and $\alpha(-m) = \alpha((-1).m) = (-1).\alpha(m) = -\alpha(m)$.

An *isomorphism* is a homomorphism which is also a bijection.

Remark 6.2. Let $\alpha\colon M \to N$ be an isomorphism. As α is a bijection, there is an inverse function $\alpha^{-1}\colon N \to M$ such that $\alpha(\alpha^{-1}(n)) = n$ for all $n \in N$ and $\alpha^{-1}(\alpha(m)) = m$ for all $m \in M$. I claim that α^{-1} is also a homomorphism. To see this, suppose that $n_0, n_1 \in N$. We then have elements $\alpha^{-1}(n_0)$ and $\alpha^{-1}(n_1)$ in M. As α is a homomorphism, we have $\alpha(\alpha^{-1}(n_0) + \alpha^{-1}(n_1)) = \alpha(\alpha^{-1}(n_0)) + \alpha(\alpha^{-1}(n_1)) = n_0 + n_1$. We can apply α^{-1} to this equation to get $\alpha^{-1}(\alpha(\alpha^{-1}(n_0)) + \alpha(\alpha^{-1}(n_1))) = \alpha^{-1}(n_0 + n_1)$. Because $\alpha^{-1}(\alpha(m)) = m$ for all m, the left hand side is just $\alpha^{-1}(n_0) + \alpha^{-1}(n_1)$. We thus have $\alpha^{-1}(n_0) + \alpha^{-1}(n_1) = \alpha^{-1}(n_0 + n_1)$, showing that α^{-1} respects addition.

Similarly, suppose that $n \in N$ and $a \in R$. As α respects multiplication by R, we have $\alpha(a\alpha^{-1}(n)) = a\alpha(\alpha^{-1}(n)) = an$. By applying α^{-1} to this equation we get $\alpha^{-1}(\alpha(a\alpha^{-1}(n))) = \alpha^{-1}(an)$. The left hand side is just $a\alpha^{-1}(n)$, so we have $a\alpha^{-1}(n) = \alpha^{-1}(an)$, completing the proof that α^{-1} is a homomorphism.

Example 6.3. Let R be any ring. Define $\tau\colon R^2 \to R^2$, $\sigma\colon R^3 \to R$ and $\delta\colon R^2 \to R^3$ by

$$\begin{aligned}\tau(u, v) &= (v, u)\\ \sigma(x, y, z) &= x + y + z\\ \delta(u, v) &= (u, v - u, -v).\end{aligned}$$

It is easy to check that these are all homomorphisms. For example, we have

$$\begin{aligned}\delta(u_0, v_0) + \delta(u_1, v_1) &= (u_0, v_0 - u_0, -v_0) + (u_1, v_1 - u_1, -v_1)\\ &= (u_0 + u_1, v_0 + v_1 - u_0 - u_1, -v_0 - v_1)\\ &= \delta(u_0 + u_1, v_0 + v_1)\\ &= \delta((u_0, v_0) + (u_1, v_1))\end{aligned}$$

and

$$\begin{aligned}a\delta(u, v) &= a.(u, v - u, -v)\\ &= (au, a(v - u), -av)\\ &= \delta(a.(u, v)),\end{aligned}$$

so δ is a homomorphism.

Example 6.4. I would like to define two homomorphisms $\alpha, \beta\colon \mathbb{Z}_3 \to \mathbb{Z}_{12}$ by $\alpha(\overline{m}) = \overline{4m}$ and $\beta(\overline{m}) = \overline{5m}$. There is a potential problem with this kind of definition, which means that the definition of β is actually invalid, although it turns out that α is OK. Consider the element $x = \overline{1} \in \mathbb{Z}_3$, which can also be described as $x = \overline{4}$. Using the description $x = \overline{1}$ we get $\beta(x) = \overline{5} \in \mathbb{Z}_{12}$. Using the description $x = \overline{4}$ we get $\beta(x) = \overline{20} \in \mathbb{Z}_{12}$. As $20 \neq 5 \pmod{12}$, the elements $\overline{5}$ and $\overline{20}$ in $\mathbb{Z}_{12}$ are not the same, so our definition of β is not self-consistent.

However, this problem does not occur with α. To see why, suppose we describe an element $y \in \mathbb{Z}_3$ in two different ways, say $y = \overline{n} = \overline{m}$. As $\overline{n} = \overline{m}$ in $\mathbb{Z}_3$, we have $n = m \pmod 3$, so $n = m + 3k$ for some integer k. This means that $4n = 4m + 12k$, so $\overline{4n} = \overline{4m}$ in $\mathbb{Z}_{12}$. This means that we get the same answer for $\alpha(y)$ no matter which description we use, so α is a well-defined function from $\mathbb{Z}_3$ to $\mathbb{Z}_{12}$.