SF2729 Groups and Rings
Modules over rings and applications

Tilman Bauer

February 22, 2013

1 Modules

Throughout, let R be a (not necessarily commutative) ring with unity.

Definition. A **left (resp. right) module** over R is an abelian group M with a bilinear map (called R-action, scalar multiplication, or just multiplication)

$$\cdot\colon R \times M \to M \quad (\text{resp. } M \times R \to M)$$

with the following properties:

Unitality: $1 \cdot m = m$ (resp. $m \cdot 1 = m$) for all $m \in M$;

Associativity: $(rs) \cdot m = r \cdot (s \cdot m)$ (resp. $m \cdot (rs) = (m \cdot r) \cdot s$).

Note that the distinction between left and right modules is not just typographical (i. e. which element do we write on the left and which one on the right). They differ in how associativity works: if M was a right module and we insisted on writing the R-action on the left, we would have

$$(rs) \cdot m = s \cdot (r \cdot m).$$

As we did for rings, we will often omit the symbol "$\cdot$" for the bilinear map.

Remark 1.1. If R is commutative, then any left module is also a right module and vice versa, hence we will just speak of an R**-module**.

Example 1.2. The trivial group 0 is a (left or right) module over any ring.

Example 1.3. The ring R with its multiplication $R \times R \to R$ is a module over itself – both a right module and a left module.

Remark 1.4. If k is a field then k-modules are the same as k-vector spaces. The term "vector space" is only used for fields.

Lemma 1.5. *Let M be a left R-module. Then:*

1. $n \cdot m = m + \cdots + m \quad (n \in \mathbf{N}_0$ *factors;* $m \in M)$
2. $(-1) \cdot m = -m$

Proof. Here we think of $n \in \mathbf{Z}$ as an element of R by the unique ring map $\mathbf{Z} \to R$. Part (1) follows by induction from bilinearity and unitality:

$$n \cdot m = (1 + \cdots + 1) \cdot m = 1 \cdot m + \cdots + 1 \cdot m = m + \cdots + m.$$

For (2), we compute

$$(-1) \cdot m + m = (-1) \cdot m + 1 \cdot m = (-1 + 1) \cdot m = 0 \cdot m = 0,$$

using bilinearity and unitality again. □

Corollary 1.6. *Every abelian group A is a $\mathbf{Z}$-module in a unique way, and every $\mathbf{Z}$-module occurs in this way.*

Proof. Lemma 1.5 tells us that there is precisely one way of defining a $\mathbf{Z}$-action (for $n < -1$: we have to define $n \cdot m = -[(-n) \cdot m]$ by associativity. □

Example 1.7 (products of modules)**.** If M and N are left R-modules then we define their **product** $M \times N$ to be the module whose underlying abelian group is $M \times N$, and where the R-action is defined by

$$r \cdot (m, n) = (r.m, r.n)$$

More generally, if I is a possibly infinite set and $\{M_i\}_{i \in I}$ is a family of left R modules indexed by I, we define their product $\prod_{i \in I} M_i$ in the same way:

$$r \cdot (m_i)_{i \in I} = (rm_i)_{i \in I}.$$

Example 1.8 (direct sums of modules)**.** If I is again a possibly infinite set and $\{M_i\}_{i \in I}$ is a family of left R-modules, we define their **direct sum**

$$\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$$

to be the subgroup of those families $(m_i)_{i \in I}$ where all but finitely many m_i are 0. This is clearly again a left R-module.

Remark 1.9. Clearly, products and direct sums can be defined for right modules in the same way. The direct sum and the product of finitely many modules are the same, since then the condition that all but finitely many m_i vanish is empty.

1.1 Submodules and quotient modules

From now on, we will restrict our attention to *left* R-modules, with the understanding that everything we say has an analog for right R-modules.

Definition. Let M be a left R-module. An *left R-submodule* of M is a sub-abelian group $N < M$ which is closed under scalar multiplication, i. e. which satisfies

$$r \cdot n \in N \quad \text{for } r \in R, n \in N.$$

Remark 1.10. If we consider the ring R as a module over itself (Ex. 1.3) then the left R-submodules of R are precisely the left ideals of R. This follows immediately from the definition.

Example 1.11 (non-direct sums)**.** If N_1 and N_2 are left R-submodules of a left R-module M then the module

$$N_1 + N_2 = \{n_1 + n_2 \in M \mid n_1 \in N_1,\ n_2 \in N_2\}$$

is a submodule of M as well.

Lemma 1.12. *Let $N < M$ be a left R-submodule. Then the quotient abelian group M/N becomes a left R-module (the **quotient module**) by defining $r \cdot [m] = [r \cdot m]$.*

Proof. We have to check well-definedness. Given another representative $m + n$ of the equivalence class $[m]$, with $n \in N$, we compute

$$r \cdot (m + n) = r \cdot m + r \cdot n \in r \cdot m + N$$

because N is a submodule. Hence $[r \cdot (m + n)] = [r \cdot m]$. □

Notice that in contrast to groups and rings, where quotients can only be formed under additional hypotheses (normal subgroups resp. ideals), quotient modules always exist.

1.2 Homomorphisms

Definition. A **homomorphism** of left R-modules M, N is an abelian group homomorphism $f\colon M \to N$ which is **R-linear**, i. e. which satisfies

$$f(r \cdot m) = r \cdot f(m) \quad \text{for all } r \in R, m \in M$$

A bijective homomorphism is called an **isomorphism**, and if an isomorphism between two modules M, N exists then we call them **isomorphic** and write $M \cong N$.

Lemma 1.13. *Let $f\colon M \to N$ be a homomorphism of left R-modules. Then the kernel and image of f are left R-submodules.*

Proof. We know they are sub-abelian groups, so it suffices to show they are closed under scalar multiplication. If $r \in R$ and $m \in \ker(f)$ then

$$f(r \cdot m) = r \cdot f(m) = r \cdot 0 = 0,$$

so $r \cdot m \in \ker(f)$. Similarly, if $n \in \mathrm{im}(f)$, say $n = f(m)$, then $r \cdot n = r \cdot f(m) = f(r \cdot m) \in \mathrm{im}(f)$. □

Remark 1.14. If $N < M$ is a left sub-R-module then the canonical map $M \to M/N$ sending m to $[m]$, is a homomorphism. If a homomorphism $f\colon M \to N$ of left R-modules is an isomorphism then the inverse map f^{-1} is also an isomorphism.

Definition. A left R-module M is called **free** if it is isomorphic to a (possibly infinite) direct sum of copies of the R-module R. If $M \cong R^n = \bigoplus_{i=1}^n R$ then we say that M has **rank** n.

A basic theorem of linear algebra says that any vector space (over a field k) has a basis, i. e. it is free as a module over k. This does not hold for general rings: the $\mathbf{Z}$-module $\mathbf{Z}/n\mathbf{Z}$, for instance, cannot be free because it is finite, and any nontrivial free $\mathbf{Z}$-module is infinite.

It is not at all obvious that the notion of rank is well-defined; why couldn't we have that $R^n \cong R^m$ for some $n \neq m$? Surprisingly, this can indeed happen, but only for noncommutative rings. (And also for the trivial ring $R = 0$.)

Theorem 1.15. *Let R be a nontrivial commutative, unital ring. Then $R^m \cong R^n \Rightarrow m = n$.*

Before proving this, we need one more construction:

Lemma 1.16. *Let R be a ring with a two-sided ideal $I \triangleleft R$ and let M be a left R-module. Then*

$$IM = \{\sum_{i=1}^n x_i \cdot m_i \mid x_i \in I, m_i \in M\}$$

is a sub-R-module of M, and the quotient group $M/I := M/IM$ is an R/I-module.

This construction is what is called functorial*: if $\phi\colon M \to N$ is a module homomorphism then there is an induced homomorphism $\overline{\phi}\colon M/I \to N/I$ such that $\overline{\mathrm{id}} = \mathrm{id}$ and $\overline{\phi \circ \psi} = \overline{\phi} \circ \overline{\psi}$.*

Proof. Clearly IM is an abelian subgroup of M. It is also closed under the R-action:

$$r \cdot \sum_{i=1}^n x_i \cdot m_i = \sum_{i=1}^n (rx_i) \cdot m_i \in IM$$

because I is a left ideal.

We define an R/I-module structure on the abelian group M/I by defining

$$[r] \cdot [m] = [rm]$$

and need to check that this is well-defined, i. e. independent of the choice of representative of $[r]$. (That it is independent of the choice of representative of $[m]$ was proven in Lemma 1.12.) Indeed, given $x \in I$, we verify:

$$(r + x) \cdot m = rm + xm \in rm + IM.$$

For the functoriality statement, it suffices to show that $\phi(IM) \subseteq IN$. But this follows from the R-linearity since

$$\phi(\sum_{i=1}^{n} x_i \cdot m_i) = \sum_{i=1}^{n} x_i \cdot \phi(m_i) \in IN.$$

□

Proof of Theorem 1.15. Let I be any maximal ideal of R. (That every ring has such a maximal ideal follows Zorn's Lemma and is a theorem due to Krull (1929) and was a bonus problem. We will skip its proof here. You have shown it for PIDs at least in an exercise.) Assume we have an isomorphism $\phi\colon R^n \to R^m$ of R-modules. Then $\overline{\phi}$ defines a homomorphism from $(R/I)^n$ to $(R/I)^m$, and $\overline{\phi^{-1}}$ defines a homomorphism in the opposite direction. Since $\overline{\phi} \circ \overline{\phi^{-1}} = \overline{\phi \circ \phi^{-1}} = \overline{\mathrm{id}} = \mathrm{id}$ and analogously for the converse composition, we see that $\overline{\phi}$ is in fact an isomorphism of R/I-modules. But R/I is a field because I was chosen maximal, and $(R/I)^n$ and $(R/I)^m$ are n- and m-dimensional vector spaces over it, respectively. Since dimension is well-defined for vector spaces, it follows that $m = n$. □

1.3 Finitely generated modules

Given a left R-module M and a collection (m_i) of elements of M, we say that M is **generated** by (m_i) if every element of M can be written as an R-linear combination of the m_i, i. .e. for every $m \in M$ there are $r_i \in R$, all but finitely many zero, such that

$$m = \sum_i r_i m_i. \tag{1.17}$$

Clearly the whole module M is a generating set for M, albeit not a very economical one. The module M is called **finitely generated** if it has a finite generating set.

A finitely generated module over a field is thus just a finite-dimensional vector space. But this does not mean that finitely generated modules behave as nicely as finite-dimensional vector spaces:

Example 1.18. Submodules of finitely generated modules can fail to be finitely generated. Take $R = k[x_1, x_2, \dots]$ to be the polynomial ring in countably many variables; its elements are polynomials involving a finite but arbitrary number of the variables x_i. Then R is a finitely generated module over itself (generated by one element, the unity). However, the ideal I consisting of all nonconstant polynomials and 0 is not finitely generated. If it were generated by a finite set of nonconstant polynomials $p_1, \dots, p_n$,

then there would have to be some N such that the variable x_N does not occur in any of the p_i. But then the nonconstant polynomial x_N would not be in the ideal generated by the p_i, either.

Remark 1.19. A ring with the property that submodules of finitely generated modules are again finitely generated is called *noetherian*, after Emmy Noether. Although the theory of noetherian rings is important and extensive, we will not pursue it further here.

Definition. A collection (m_i) of element of M is said to be a **free set of generators** (or that M is **freely generated by the** (m_i)) if every m can be written in the form (1.17) for *uniquely determined* coefficients $r_i \in R$.

Lemma 1.20. *A module M is freely generated (by some collection of elements (m_i)) iff it is free.*

Proof. If M is freely generated by $(m_i)_{i\in I}$ then the map

$$M \to \bigoplus_{i\in I} R; \quad (m = \sum_{i\in I} r_i m_i) \mapsto (r_i)_{i\in I},$$

is well-defined and an isomorphism. Conversely, the elements $\delta_i \in \bigoplus_{i\in I} R$ defined by $(\delta_i)_j = 1$ for $i = j$ and $(\delta_i)_j = 0$ for $i \neq j$ form a free set of generators for $\bigoplus_{i\in I} R$. □

Remark 1.21. The (infinite) product $\prod_{i\in I} R$ is not free in general. Think about this.

2 Finitely generated modules over principal ideal domains

Recall that a principal ideal domain is an integral domain where every ideal is principal, i. e. generated by a single element. Examples include fields, $\mathbf{Z}$ and $k[x]$ for fields k.

Theorem 2.1. *Let R be a principal ideal domain (PID). Then submodules of finitely generated free R-modules are finitely generated free of smaller or equal rank.*

Proof. Let M be freely generated by the elements $x_1, \ldots, x_n$. We will use induction on n. The claim is clear for $n = 0$, so assume it is true for $n - 1$.

Now let $N < M$ be a submodule, let $M' = \langle x_1, \ldots, x_{n-1}\rangle$ be the submodule of M generated by the first $n - 1$ elements, and consider the module $N' = N \cap M' < M'$. If $N' = N$, then $N < M'$, and we are done by induction. So let us assume that $N' \lneq N$. Let $\phi\colon R \to M/(M' + N)$ be the R-module map which is defined by $\phi(r) = [rx_n]$ and let $I = \ker(\phi) \lhd R$. Note that ϕ is surjective because the canonical projection $M/M' \to M/(M' + N)$ is surjective and M/M' is generated by $[x_n]$. However, ϕ cannot be an isomorphism because that would imply that $N \subseteq M'$ and hence $N' = N$, which we excluded. Thus $\ker(\phi)$ is an ideal generated by a single nonzero element $a \in R$. Since $\phi(a) = 0$, $ax_n \in M' + N$, thus there is an element $w \in N$ whose coefficient for x_n is a. For any element $x \in N$, its coefficient of x_n is divisible by a, hence $x - cw \in N'$ for some $c \in R$, hence $N = N' + (w)$. Since $N' \cap (w) = (0)$, we have that the sum $N = N' \oplus (w) \cong N' \oplus R$ is direct. By induction, $N' < M'$ is free of rank $\leq n - 1$ and we are done. □

Definition. Given a module M over any commutative ring R, let $M_{\text{tor}} < M$ be the submodule of those elements m ("torsion elements") for which there is an $r \in R - \{0\}$ such that $r \cdot m = 0$.

Example 2.2. If $R = \mathbf{Z}$, we have that $\mathbf{Z}_{\text{tor}} = \mathbf{Z}$ and $(\mathbf{Z}/n\mathbf{Z})_{\text{tor}} = \mathbf{Z}/n\mathbf{Z}$.

Theorem 2.3. *Let M be a finitely generated module over a PID R. Assume that M is torsion-free, i. e. $M_{\text{tor}} = 0$. Then M is free.*

Proof. Let M be generated by a finite set $x_1, \ldots, x_n$. Order these elements in such a way that $x_1, \ldots, x_k$ are linearly independent, but adding any element x_i for $i > k$ makes the set $\{x_1, \ldots, x_k, x_i\}$ linearly dependent. Denote by N the free submodule of M generated by $x_1, \ldots, x_k$.

Thus for $i > k$, we can find a linear relation

$$a_i x_i + \lambda_1 x_1 + \cdots + \lambda_k x_k = 0$$

with $a_i \neq 0$. Let $a = a_{k+1} \cdots a_n$. Since R is an integral domain, $a \neq 0$. The map $\phi\colon M \to N$ defined by $\phi(x) = ax$ is well-defined because for any $m \in M$, $am \in N$. It is also injective because M is torsion free, thus in particular a is not a torsion element. Thus M is a submodule of the finitely generated module N, hence free. □

Theorem 2.4. *Let M be a finitely generated module over a PID R. Then M/M_{tor} is free, and $M \cong M_{\text{tor}} \oplus M/M_{\text{tor}}$.*

Proof. We first check that M/M_{tor} is indeed free; by Theorem 2.3 it suffices to show it is torsion free. Thus assume $[x] \in M/M_{\text{tor}}$ is torsion, i. e. there is an $r \in R - \{0\}$ such that $rx \in M_{\text{tor}}$. This says that there is an $s \in R - \{0\}$ such that $srx = 0$. Then $(sr)x = 0$ and $sr \neq 0$, so $x \in M_{\text{tor}}$, so $[x] = 0$.

For the isomorphism $\phi\colon M_{\text{tor}} \oplus M/M_{\text{tor}} \to M$, let $\{[x_1], \ldots, [x_n]\}$ be a basis of M/M_{tor}. (That is, pick some arbitrary representatives $x_i \in M$.) Then define $\phi(m, a_1[x_1] + \cdots + a_n[x_n]) = m + a_1x_1 + \cdots + a_nx_n$. Since the $[x_i]$ are linearly independent, this map is well-defined. An inverse map is given as follows: for $m \in M$, let $[m] = a_1[x_1] + \cdots + a_n[x_n] \in M/M_{\text{tor}}$ and define

$$\psi(m) = (m - a_1x_1 - \cdots - a_nx_n, [m]).$$

Since $[m - a_1x_1 - \cdots - a_nx_n] = [m] - a_1[x_1] - \cdots - a_n[x_n] \in M/M_{\text{tor}}$, the element $m - a_1x_1 - \cdots - a_nx_n$ is indeed torsion. □

We have thus shown that any finitely generated module M over a PID is a direct sum of a free module (of a well-defined rank) and a torsion module. We will now study the structure of torsion modules further.

Definition. Let $r \in R$ an element of a PID. Denote by M_r the kernel of the multiplication-by-r map $M \xrightarrow{r\cdot -} M$. In other words,

$$M_r = \{x \in M \mid r \cdot x = 0\}.$$

For an irreducible element $p \in R$, and $x \in M - \{0\}$, the **order of** x **at** p is the minimal $n \in \mathbf{N}_0$ such that $p^n \cdot x = 0$, or ∞ if such an n does not exist. A torsion R-module M is called **a** p**-primary torsion module** if $\mathrm{ord}_p(m) < \infty$ for every element $m \in M$. For any R-module M, denote by $M(p)$ the submodule of all elements with finite p-order. Thus

$$M(p) = \bigcup_{n \geq 0} M_{p^n}.$$

Example 2.5. Over $R = \mathbf{Z}$, the modules $\mathbf{Z}/p^n\mathbf{Z}$ are p-primary for any prime number p and any natural number n. For the module $M = \mathbf{Z}/12\mathbf{Z}$, we have $M(2) = \{0, 3, 6, 9\} \cong \mathbf{Z}/4\mathbf{Z}$, $M(3) = \{0, 4, 8\} \cong \mathbf{Z}/3\mathbf{Z}$, and $M(p) = 0$ for all other primes p.

Lemma 2.6. *Let M be a finitely generated torsion module over a PID R. Then*

$$M \cong \bigoplus_p M(p),$$

where p runs through all indecomposable elements.

Proof. Let $a \in R$ be such that $aM = 0$ (such an a exists because M is torsion and finitely generated). If a is a prime power, we are done. Otherwise write $a = bc$ with $\gcd(b, c) = 1$ and use the Euclidean algorithm to find elements $\beta, \gamma \in R$ such that

$$1 = \beta b + \gamma c.$$

Now consider the homomorphism

$$M_b \oplus M_c \xrightarrow{(x,y) \mapsto x+y} M.$$

This homomorphism is injective: suppose $x + y = 0$. Then $bx = 0$ and $cx = c(-y) = -cy = 0$. Hence

$$x = 1 \cdot x = (\beta b + \gamma c)x = 0.$$

The homomorphism is also surjective: given any $z \in M$.

$$z = 1 \cdot z = (\beta b + \gamma c)z = c(\gamma z) + b(\beta z),$$

where the first summand is killed by b and the second by c (both because $bcM = 0$).

Now since a can be uniquely written as a product of powers of indecomposable elements, we get the stated decomposition by induction. □

Theorem 2.7. *Let $p \in R$ be an irreducible element in a PID and let M be a finitely generated p-primary torsion module. Then there is a sequence of nonzero integers $(k_1, \ldots, k_n)$, such that*

$$M \cong R/(p^{k_1}) \oplus \cdots \oplus R/(p^{k_n}).$$

Proof. Let k_1 be minimal such that $p^{k_1}M = 0$ (such a k_1 exists because M is finitely generated) and choose an element $x_1 \in M$ of order k_1. Let $N = M/\langle x_1 \rangle$. By induction, there is an isomorphism

$$\phi\colon R/(p^{k_2}) \oplus \cdots \oplus R/(p^{k_n}) \to N;$$

denote the images of the standard elements $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ by $\overline{x}_i$ ($i = 2, \ldots, n$). We thus know that $\overline{p}^{k_i} x_i = 0 \in M/\langle x \rangle$. Thus if $x_i \in M$ is a representative of $\overline{x}_i$ then $p^{k_i} x_i = \alpha_i x_1$ for some $\alpha_i \in R$. Let $s_i = \operatorname{ord}_p(\alpha_i)$. Then $\operatorname{ord}(\alpha_i x_1) = k_1 - s$ and hence $\operatorname{ord}(x_i) = k_i + k_1 - s$. Since the maximal order of all elements in M is k_1, we have $k_i - s \leq 0$; in other words, $p^{k_i} | \alpha_i$. Let β_i such that $\alpha_i = p^{k_i}\beta_i$.

But then $p^{k_i}(x_i - \beta_i x_1) = p^{k_i} x_i - \alpha_i x_1 = 0$ and $x_i - \beta_i x_1$ is also a representative of $\overline{x}_i$. Thus we can assume without loss of generality that $\operatorname{ord}_p(x_i) = p^{k_i}$ in M.

Now consider the map

$$\Phi\colon R/(p^{k_1}) \oplus \cdots \oplus R/(p^{k_n}) \to M$$

which is defined by $\Phi(e_i) = x_i$. By the surjectivity of ϕ, Φ is also surjective. For injectivity, assume that

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0.$$

Then in N, $\alpha_2 \overline{x}_2 + \cdots + \alpha_n \overline{x}_n = 0$, hence by injectivity of ϕ, $\alpha_i = 0 \in R/(p^{k_i})$ for all $i = 2, \ldots, n$. But then $\alpha_1 x_1 = 0 \in M$, which implies $\alpha_1 = 0 \in R/p^{k_1}$. □

Remark 2.8. There is also a uniqueness result about this decomposition, which we will skip here.

Corollary 2.9. *Any finitely generated module M over a PID R is isomorphic to a direct sum of a free module and modules of the form*

$$R/(p^i),$$

where p is an irreducible element and $i \in \mathbf{N}$.

3 An application: the Jordan normal form

A field k is called **algebraically closed** if every nonconstant polynomial in $k[x]$ has a zero in k. The *fundamental theorem of algebra* (which we will not prove here) says that $\mathbf{C}$ is algebraically closed.

A field k is thus algebraically closed if and only if the irreducible elements of $k[x]$ are all linear polynomials of the form $x - a$ for some $a \in k$.

Now let V be a vector space over k of dimension n, and let $f\colon V \to V$ be a vector space homomorphism. Then we can think of V as a $k[X]$-module in the following way:

$$k[X] \times V \xrightarrow{(a_0 + a_1 X + \cdots + a_k X^k, v) \mapsto a_0 v + a_1 f(V) + \cdots + a_k f^{(k)}(v)} V, \tag{3.1}$$

where $f^{(i)}$ denotes the i-fold composition of f with itself. Since V is finite-dimensional over k, it surely is finitely generated over the bigger ring $k[X]$.

Lemma 3.2. *V is a $k[X]$-torsion module.*

Proof. Let $v \in V$ be any nonzero element. Since $\dim(V) = n$, the elements $v, f(v), \ldots, f^{(n)}(v)$ have to be linearly dependent, let's say

$$a_0 v + a_1 f(v) + \cdots + a_n f^{(n)}(v) = 0.$$

But this element is exactly $(a_0 + a_1 X + \cdots + a_n X^n) \cdot v$. □

Corollary 3.3. *If k is algebraically closed then $V \cong k[X]/(X - a_1)^{n_1} \oplus \cdots \oplus k[X]/(X - a_k)^{n_k}$ for certain elements $a_i \in k$ and $n_i \in \mathbf{N}$.*

Proof. This follows from the characterization of irreducible elements in $k[X]$ and the structure theorem for finitely generated abelian groups over the PID $k[X]$. □

This says that we can write V as $V_1 \oplus \cdots \oplus V_k$ in such a way that f maps V_i to itself for all i. Let us find out what form the restriction of f to V_i takes.

Lemma 3.4. *Let $f\colon V \to V$ be a homomorphism such that $V \cong k[X]/(X - a)^n$ under the module structure* (3.1)*. Then V has a basis in which the representing matrix of f has the form*

$$\begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & & \vdots \\ & & \ddots & & 0 \\ & & & a & 1 \\ 0 & \cdots & & 0 & a \end{pmatrix} \tag{3.5}$$

Proof. Let $\phi\colon K[X]/(X - a)^n \to V$ be an isomorphism and define

$$x_i = \phi((X - a)^i) \in V.$$

Then $x_0, \ldots, x_{n-1}$ form a basis for V and

$$f(x_i) = X \cdot x_i = (X - a) \cdot x_i + a \cdot x_i = x_{i+1} + a x_i.$$

□

Corollary 3.6. *Let $f\colon k^n \to k^n$ be a linear map, where k is algebraically closed. Then there is a basis of k^n in which f has a matrix representation consisting of diagonal blocks of the form* (3.5) *for various $a \in k$ (not necessarily distinct).*

4 Exercises

Exercise 1. Let $R = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ be the subring of $\mathbf{C}$ of elements that can be written in the form $a + b\left(\frac{1}{2}(1 + \sqrt{-3})\right)$ for $a, b \in \mathbf{Z}$. Show that R is a Euclidean domain.

Exercise 2. Let A be an abelian group and denote by $\mathrm{End}(A)$ the set of all abelian group homomorphisms $A \to A$.

1. Show that $\mathrm{End}(A)$ with addition and composition forms a ring with unity
2. Show that $\mathrm{End}(A) \times A \to A$, $(f, a) \mapsto f(a)$, defines an $\mathrm{End}(A)$-module structure on A.

Exercise 3. Let R be a commutative ring and M and N be two R-modules. Show that the set $\mathrm{Hom}_R(M, N)$ of all R-module homomorphisms from M to N has an R-module structure with addition given by pointwise addition of functions ($(f+g)(m) = f(m) + g(m)$).

Exercise 4. Show, using the axioms, that the abelian group $\mathbf{Z}$ cannot be given a $\mathbf{Z}[i]$-module structure. For which primes p does $\mathbf{Z}/p\mathbf{Z}$ have a $\mathbf{Z}[i]$-module structure?

Exercise 5. For a ring R, consider R as a left module over itself by left multiplication. Determine all R-module homomorphisms $R \to R$.

Exercise 6. Let M be a left R-module. The **annihilator** $\mathrm{Ann}(M)$ is the set of all $r \in R$ such that $r \cdot m = 0$ for all $m \in M$. Show that $\mathrm{Ann}(M)$ is a left ideal in R.

Exercise 7. Show that for any ring R, the set $R[x]$ of polynomials over R forms a free R-module.

Exercise 8. Let k be a field and $I \triangleleft k[X, Y]$ denote the ideal (X, Y). Is I a free $k[X, Y]$-module?

Exercise 9. Let R be a commutative ring with unit. Assume that R has the property that every R-module is free. Show that R has to be a field.

Exercise 10. Show that the following two statements are equivalent for a finitely generated module M over a principal ideal domain R:

1. M is free;
2. Every surjective R-module homomorphism $f\colon N \to M$ has a right inverse $g\colon M \to N$.

Exercise 11. Show that $\mathbf{Q}$ is a torsion-free $\mathbf{Z}$-module which is not a free $\mathbf{Z}$-module. (This shows that the finite generation assumption is needed.)

Exercise 12. For the following maps $f\colon \mathbf{Z} \to \mathbf{Z} \oplus \mathbf{Z}$, write the quotient $(\mathbf{Z} \oplus \mathbf{Z}) / \mathrm{im}(f)$ as a sum of cyclic groups:

1. $f(x) = (x, 0)$
2. $f(x) = (0, 3x)$
3. $f(x) = (4x, 6x)$.

Exercise 13. Up to isomorphism, how many abelian groups of order 12 are there?

Exercise 14. Up to isomorphism, how many abelian groups of order 200 are there?

Exercise 15. Classify all finitely generated modules over the ring $\mathbf{Z}/8\mathbf{Z}$.

Exercise 16. Show that any finitely generated module M over a PID R is isomorphic to a quotient of a finitely generated free module by a finitely generated free submodule.

Exercise 17. Show that the abelian group $\mathbf{Q}/\mathbf{Z}$ is not a direct sum of cyclic groups.

Exercise 18. Determine the Jordan normal form of the matrix $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ over $\mathbf{C}$.

Exercise 19. Determine the Jordan normal form of the matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

over $\mathbf{C}$.

Exercise 20. Let k be a field and A an $n \times n$-matrix over k which is **idempotent**, i. e. $A^2 = A$. Show that if $k = \mathbf{C}$ then A is diagonalizable. Show by example that this does not hold over arbitrary fields k.