Modules over Principal Ideal Rings and Classification of Finitely Generated Abelian Groups

Alexander Gudev

1 Introduction

Let us consider some questions that one might ask in linear and higher algebra.

1. Often, when studying groups and rings, we aim to describe finite sums of a given element with itself, for example, $a + \cdots + a$. This leads us to use the notation $n \cdot a$ by analogy with multiplication by integers, which we define purely formally in the following way:

$$n \cdot a = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ times}}, & \text{if } n > 0 \\ 0, & \text{if } n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{n \text{ times}}, & \text{if } n < 0 \end{cases}$$

   This is a purely syntactic construct that we define entirely outside the considered structure (group, ring, ...), and in such cases, whenever we write $n \cdot a$, we must remember that this is merely shorthand, and the formal multiplication we use does not necessarily correspond to the operations in the structure.

   For instance, when proving the simplicity of the characteristic of a given field F, we write $p \cdot 1$, but explicitly note that $p \in \mathbb{Z}$ is not necessarily an element of F, and the formal multiplication here has no connection to the operation $*$ in the field.

   Naturally, one might ask if there is a cleaner, more algebraic way to describe this formal operation.

2. For the needs of linear mappings in a linear space over a field F, we introduce the notion of a "matrix" with coefficients from the field F. Of key importance for finding inverse matrices, for example, is the invertibility of all nonzero elements in F.

   However, when looking for eigenvalues and eigenvectors, we define the characteristic polynomial $\det(A - xI)$. The elements of the matrix $A - xI$ in this case turn out to be *polynomials*, and we know well that the set of polynomials over some field (ring) is not a field in itself.

   This raises the question – what happens if we give up the invertibility of scalars in the definition of a linear space?

3. The points with integer coordinates in the plane $\mathbb{Z} \times \mathbb{Z}$ do not form a linear space over any field, even though they "spread everywhere."

   Why? If the field has a nonzero characteristic $p \in \mathbb{N}$, then for any vector (a, b) we have $0 = (p \cdot 1_F) \cdot (a, b) = (a, b) + \cdots + (a, b) = (p \cdot a, p \cdot b)$, and then $(a, b) = (0, 0)$. In the other case, a field with zero characteristic has a simple subfield isomorphic to $\mathbb{Q}$, and multiplying fractions with $(1, 1)$ (for example) takes us out of $\mathbb{Z} \times \mathbb{Z}$.

   What breaks? The division in the field is "incompatible" with integers. If we give up this property – and consider rings in general – what happens?

4. In group theory, we consider so-called *group actions on a set*, where we associate a given group G with some set X via some operation $\cdot : G \times X \to X$. For the set X, we have practically no conditions, except for the natural constraints on the operation – neutrality with respect to the group's identity and associativity.

   As a very special case of this, we can consider linear spaces, where the multiplicative group of the field F *acts* on the set V.

   What happens if we impose some restrictions on the set X, and strengthen the requirements for G? In particular, if we require X to be an abelian group, and G a ring?

5. It is known that the solutions to homogeneous linear differential equations have the structure of a linear space: if y_1, y_2 are solutions to $a_0 y + a_2 y' + a_2 y'' + \ldots + a_n y^{(n)} = 0$, then obviously $\lambda y_1 + \mu y_2$ also solves this equation.

   However, we can observe that for a given solution y_1, each derivative $y_1^{(k)}$ is also a solution for any $k \in \mathbb{N}$, as well as any combination of its derivatives: $\lambda_0 y_1 + \lambda_1 y_1' + \ldots + \lambda_k y_1^{(k)}$.

   Thus, we find that the set of solutions $V \leq C^n(\mathbb{R})$ to the differential equation has a structure richer than that of a linear space — on them, we can act not only with scalar multiplication but also with *arbitrary polynomials of differential operators* – i.e., act with elements (operators) $\theta : V \to V$ of the form $\theta = \lambda_n D^n + \ldots + \lambda_1 D + \lambda_0 I$, where D is the differential operator, and $I = D^0$ is the identity.

   This polynomial structure is not a field, but only a ring, yet it is reasonable to expect some results from it.

Definition 1. A left module M over the ring $(R, +, *)$ is called an abelian group $(M, +)$, together with a scalar multiplication operation $\cdot : R \times M \to M$, satisfying the following properties, where $a, b \in R$ and $m, n \in M$ are arbitrary:

1. $a \cdot (m + n) = a \cdot m + a \cdot n$
2. $(a + b) \cdot m = a \cdot m + b \cdot m$
3. $a \cdot (b \cdot m) = (a * b) \cdot m$
4. $1_R \cdot m = m$

Remark. Similarly, we can define a *right* module.

2 Examples

1. Every ring is a module over itself with multiplication (just as every field is a vector space over itself). More generally:
2. Every ring is a module over any of its subrings (subrings "act" on the overring). Conversely, a subring being a module over the ring is true only if the subring absorbs multiplication with elements outside itself, i.e.:
3. If $I \trianglelefteq R$ is an ideal, then I is a module over R. For example, $2\mathbb{Z} = \langle 2 \rangle \trianglelefteq \mathbb{Z}$ is a module over $\mathbb{Z}$, because the multiplication of any integer by an even number results in another even number.
4. If $n \in \mathbb{N}$, then R^n is a module over R with component-wise multiplication: let $a \in R$ and $(r_1, \ldots, r_n) \in R^n$. Then:
$$a \cdot (r_1, \ldots, r_n) = (a * r_1, \ldots, a * r_n)$$
   If X is a finite set, then $\oplus_X R$ denotes the module $R^{|X|}$.

   Just as in linear algebra, F^n is a vector space over F for any field F, here we generalize F to a ring—for example, the integer points in the space $\mathbb{Z}^3$ form a module over $\mathbb{Z}$.

5. Let $R = \mathbb{Z}$. What can we say about an arbitrary module M over R? It turns out that the action in this case is uniquely determined:

   From the definition of a module, $1 \cdot m = m$. Then $2 \cdot m = (1+1) \cdot m = 1 \cdot m + 1 \cdot m = m + m$, similarly $3 \cdot m = m + m + m$, and in general, we inductively obtain $k \cdot m = \underbrace{m + \cdots + m}_{k \text{ times}}$, i.e., the operation is defined for $k > 0$.

   For $k = 0$, obviously[1] $k \cdot m = 0_M$. For $k = -1$, with a bit more effort[2] we obtain $(-1) \cdot m = -m$, reducing it to the previous case: $\forall k < 0 : k \cdot m = ((-k) * (-1)) \cdot m = (-k) \cdot ((-1) \cdot m) = \underbrace{(-m) + \cdots + (-m)}_{|k| \text{ times}}$.

   Thus, algebraically, we can describe the formal multiplication of elements in an abelian group by a number from earlier by considering the group as a module over the integers.

   This perspective on abelian groups will be used to reduce the classification of finitely generated abelian groups to the theorem we will prove.

   - A special case of this: the module $\mathbb{Z}/n\mathbb{Z}$ over the ring $\mathbb{Z}$. The action follows the standard rules for multiplication of residues: let $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, $r \in \mathbb{Z}$, then $r \cdot (k + n\mathbb{Z}) \coloneqq (r * k) + \mathbb{Z}$.

6. Any ring homomorphism $\varphi : R \to M$ induces a module M over R, where the operation

$$\cdot : R \times M \to M$$

   is: $r \cdot m \coloneqq \varphi(r) *_M m$. We can think of the ring R *acting* on M through φ.

3 Concepts with Analogues in Linear Algebra

We directly transfer some definitions from linear algebra to modules.

Definition 2. A subset $N \subseteq M$ of a module $(M, +)$ over the ring R is called a **submodule** if $(N, +)$ is a subgroup of $(M, +)$ and is closed under multiplication by elements of the ring: $\forall r \in R, n \in N : r \cdot n \in N$.

When discussing a module M and its submodule N, to emphasize the relationship between them or avoid introducing new variables in context, we will refer to M as the **supermodule** of N.

Remark. Every ring R is a module over itself. Then its submodules are precisely the ideals of R.

Definition 3. If N is a submodule of the module M over the ring R, then $N \trianglelefteq M$ is a normal subgroup, and the factor group M/N exists. We call this factor group with the operation $\cdot : R \times M/N \to M/N$, where $r \cdot (m + N) = (r \cdot m) + N$, a **factor module**.

Correctness of the operation definition: let $r \in R$ and $m + N = m' + N$. Then $m - m' \in N$, and from the definition of a submodule, $r \cdot (m - m') \in N$, i.e., $r \cdot m - r \cdot m' \in N$. Therefore, $r \cdot m + N = r \cdot m' + N$.

Definition 4. Let M be a module over R. Then:

- A set $\{m_1, \ldots, m_k\} \subseteq M$ is called **linearly independent** if for any coefficients $\{r_i\}$, $\sum_i r_i m_i = 0$ implies $r_i = 0 \, \forall i$. A subset $S \subseteq M$ is called linearly independent if every finite subset of it is linearly independent.
- The **span** of the set $S \subseteq M$ is the set of all finite linear combinations of elements in B:

$$\operatorname{span}(B) = \left\{ \sum_{i=1}^{n} r_i m_i \,\middle|\, r_i \in R, \{m_i\}_{i=1}^{n} \subseteq B \right\}.$$

[1] It follows from the distributive axioms: $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m$, and by adding $-(0 \cdot m)$ to both sides, we get $0 = 0 \cdot m$

[2] Using that $(-1) + 1 = 0$ and again distributivity: $(-1) \cdot m + m = (-1) \cdot m + 1 \cdot m = (-1+1) \cdot m = 0 \cdot m = 0_M$, i.e., $(-1) \cdot m$ is the additive inverse of m.

We also say that B **generates** the module M if $\text{span}(B) = M$. If there exists such a finite B, we call M a **finitely generated** module.

- A subset $B \subseteq M$ is called a **basis** of M if it is linearly independent and generates the module M.

Now, by analogy with linear mappings, we define:

Definition 5. Let $f : M \to N$ be a function between the modules M and N over the ring R.

- f is called a **homomorphism** of modules if it is a homomorphism of groups and, in addition, is consistent with scalar multiplication, i.e., $f(r \cdot m) = r \cdot f(m)$ for all $r \in R, m \in M$.
- If f is a homomorphism and a bijection, then f is called an **isomorphism**, and the modules M and N are isomorphic.
- We also define the **kernel** $\operatorname{Ker} f \coloneqq \{\, m \in M \mid f(m) = 0_N \,\}$ and the **image** $\operatorname{Im} f \coloneqq \{\, n \in N \mid \exists m : n = f(m) \,\}$ of the homomorphism f.

Theorem 1 (Homomorphism Theorem)**.** *If $f : M \to N$ is a homomorphism of modules, then $M/\operatorname{Ker} f \cong \operatorname{Im} f$.*

Remark. A basis of a module M can also be defined via the so-called universal property: a subset $B \subseteq M$ is a basis if every function $f : B \to N$ in some module N can be uniquely extended to a homomorphism.

Proposition 2. *Let M be a module over R with basis B. Every homomorphism $\varphi : M \to N$ is uniquely determined by its values on this basis. That is, if $f : B \to N$ is any function in some module N, then there exists a unique homomorphism $\varphi : M \to N$ with $\varphi\big|_B = f$.*

Proof. Let B be a basis of the module M over R, N a module over M, and $f : B \to N$ an arbitrary function. Define $\varphi : M \to N$ as follows:

Let $m \in M$ be any element. Then $m = \sum_i r_i b_i$ for some $r_i \in R, b_i \in B \,\forall i$, and this representation is unique. Thus, we can define $\varphi(m) = \sum_i r_i f(b_i)$. Clearly, the φ defined in this way is a homomorphism, and $\varphi\big|_B = f$.

Now, suppose there is another homomorphism ψ with $\psi\big|_B = f$ and let $m = \sum_i r_i b_i$ be arbitrary. Then:

$$\begin{aligned}(\varphi - \psi)(m) = (\varphi - \psi)\left(\sum_i r_i b_i\right) &= \sum_i r_i(\varphi - \psi)(b_i) \\ &= \sum_i r_i(\varphi(b_i) - \psi(b_i)) \\ &= \sum_i r_i(f(b_i) - f(b_i)) = \sum_i r_i 0_N = 0\end{aligned}$$

Hence, $(\varphi - \psi) \equiv 0$, and φ is the unique such homomorphism. □

4 The Importance of Invertibility in Linear Algebra

We will examine some fundamental propositions from linear algebra and trace the key reasoning in their proofs to understand what happens with modules.

Mini-proposition 4.1. Let $\lambda \in F, v \in V$. Then, in a vector space, we have the natural equivalence: $\lambda v = 0 \Leftrightarrow \lambda = 0 \vee v = 0$.

Proof. Since F is a field, every nonzero element is invertible. We have two cases for λ:

- $\lambda = 0$, then $\lambda v = 0v = 0$ (we checked earlier).
- $\lambda \neq 0$ and $\exists \lambda^{-1}$, then $\lambda v = 0 \Leftrightarrow \lambda^{-1}\lambda v = \lambda^{-1}0 \Leftrightarrow 1v = 0 \Leftrightarrow v = 0$

From the second point, it directly follows that the only linearly dependent vector is the zero vector.

A key role here is played by the fact that, in a field, all nonzero scalars are invertible. □

Linear Independence and Basis

Now we will examine two propositions connecting linear independence with the "membership" property of a span and two of their consequences, which relate linear (in)dependence of a set with the construction of a basis for the space.

Mini-proposition 4.2. If a set of vectors is linearly dependent, then at least one of the vectors can be expressed as a combination of the others.

Proof. Let $\sum_i \lambda_i a_i = 0$ and $\exists k : \lambda_k \neq 0$. Then, we can write $\lambda_k a_k = -\sum_{i \neq k} \lambda_i a_i$, and using the invertibility of nonzero elements, multiply both sides by λ_k^{-1} to obtain $a_k = \sum_{i \neq k} \left(-\frac{\lambda_i}{\lambda_k}\right) a_i$. □

Somewhat contrapositively[3] to 4.2, we have the following:

Mini-proposition 4.3. If a vector does not lie in the span of some vectors, then it is independent of them. Specifically:

Let $v \notin \text{span}(\{u_i\})$. Then $\mu v + \sum_i \lambda_i u_i = 0$ implies $\mu = 0$.

Proof. Again, this can be easily confirmed by assuming $\mu \neq 0$ and multiplying the equality by μ^{-1}. This yields $v = \sum_i \left(-\mu^{-1}\right) \lambda_i u_i \in \text{span}(\{u_i\})$, which is a contradiction, hence $\mu = 0$. □

Let us see how 4.2 and 4.3 provide the existence of a basis contained within or containing a given set:

- From 4.2, we conclude that if V is a finitely generated vector space by S, then S contains a basis of V.

  If S is linearly independent, S is the basis. Otherwise, the linear dependence of S provides a vector lying in the span of the others, which can be removed without disrupting the span—eventually resulting in a basis after a finite number of steps.

- Statement 4.3 gives us the following: If V is finitely generated, then any linearly independent subset can be extended to a basis.

To understand what happens with modules, we provide the following summary:

If $v \notin \text{span}(S)$, then v is independent of S.	If S is linearly dependent, then $\exists v \in S : v \in \text{span}(S \setminus \{v\})$
If S is linearly independent, then S can be extended to a basis.	If $\text{span}(S) = V$, then S can be reduced to a basis.

We will see how each of these (entirely natural) statements breaks in the general case of modules. To express it in one sentence: the span of a set gives all vectors linearly dependent on it, while everything outside its span is independent of it.

We conclude this section with a few more facts from linear algebra:

1. Perhaps almost trivially, every subspace $V' \leq V$ of a finitely generated space is also finitely generated, and $\dim V' \leq \dim V$.
2. In the above, if $V' \leq V$, then the dimensions are equal exactly when the spaces coincide: $\dim V' = \dim V \Leftrightarrow V = V'$. That is, if a subset is strictly a subspace, then its dimension is strictly lower than that of the superspace.
3. The span of a single vector is invariant under scalar multiplication: $\text{span}(\{v\}) = \text{span}(\{av\}) \forall a \in F$.
4. With elementary row and column transformations, any matrix can be reduced to a form with zeros outside the main diagonal and only ones and zeros along it.

[3] Not exactly contrapositively, since in 4.3, we do not require the given set to be independent.

5 From Vector Spaces to Modules

Now, we will examine how analogous statements for modules break:

1. Regarding ($\lambda v = 0 \Leftrightarrow \lambda = 0 \vee v = 0$), we find a counterexample with any finite module over $\mathbb{Z}$ (essentially all finite abelian groups).

   For example, in $\mathbb{Z}_6$ as a module over $\mathbb{Z}$, we have $2 \cdot \overline{3} = \overline{3} + \overline{3} = \overline{6} = \overline{0}$, but neither 2 is a zero scalar nor $\overline{3}$ a zero vector. In a vector space, we could multiply the equality by 2^{-1}, but 2 is not an invertible element in the ring $\mathbb{Z}$, so this technique is inapplicable here.

2. Every ring is a module over itself—let us consider $\mathbb{Z}$ over $\mathbb{Z}$ and the set $S = \{2, 3\}$. Then S generates the entire ring, since $\mathrm{GCD}(2, 3) = 1$. Moreover, S is linearly dependent: $2 \cdot 3 + (-3) \cdot 2 = 0$ is a nontrivial combination of the zero vector. Clearly, however, we cannot remove any element from S while preserving the span—neither $\{2\}$ nor $\{3\}$ generates the entire module.

   In other words, in modules, generating sets are not necessarily reducible to a basis.

   Conversely, the set $\{2\}$ is linearly independent, but we cannot extend it to a basis, since every element outside the span is dependent on the pair (in the same way as above).

   Here, we directly see how the straightforward connection from vector spaces, *linear span - linear independence*, breaks apart.

   The reason we cannot remove any element of $\{2, 3\}$ while preserving the span is that neither can be expressed in terms of the other: $2 \neq \lambda \cdot 3$ for any $\lambda \in \mathbb{Z}$. In a vector space, we would multiply the zero combination by the inverse of one of the nonzero coefficients, but here neither 2 nor (-3) has an inverse.

3. In general, it is possible for a finitely generated module to have *no* basis at all. The tragedy reaches even greater heights—a module may have no linearly independent vectors whatsoever.

   As noted earlier, in a vector space, the only linearly dependent vector is the zero vector.
   Returning again to the module $M = \mathbb{Z}_n$ over $\mathbb{Z}$ for any fixed $n \in \mathbb{N}$, we can observe that $n \cdot r = 0_M$ for any residue $r \in \mathbb{Z}_n$. That is, every element of the module is dependent... on itself!

   These cross-structural zero divisors arise even when the ring itself has no zero divisors, such as $\mathbb{Z}$, due to the inherent relationship between the two algebraic structures induced by the operation $\cdot$.

4. It is worth noting that these anomalies are closely tied to the ring over which we consider the module.

   As a module over $\mathbb{Z}$, indeed $M = \mathbb{Z}/n\mathbb{Z}$ from the previous point suffers from severe lack of a basis. However, if we consider M as a module over itself (keeping in mind that M is a ring), it immediately turns out that $\{1_M\}$ is a basis. In general, any ring R is a module over itself with basis $\{1_R\}$.

5. Consider the issue with dimensions: $2\mathbb{Z}$ is a strict submodule of $\mathbb{Z}$, yet both modules are generated by a single element—$\mathbb{Z} = \langle 1 \rangle, 2\mathbb{Z} = \langle 2 \rangle$.

   In vector spaces, a subspace of the same dimension must coincide with the original space, but for modules, this is not necessarily the case.

   The lack of division in the ring is a weakness that transfers to the span, preventing it from covering all dependent vectors.

   We will see that submodules can not only fail to shrink in dimension relative to the supermodule but may even grow! Later, we will observe specific conditions under which such growth cannot occur.

6. Let us conclude this list with another striking example: consider the ring $R = \mathbb{R}[x_1, x_2, \dots]$ of polynomials in countably infinite variables as a module over itself. Thus, R is finitely generated and has a basis $\{1_R\}$. We stated that in this case, the ideals of R form submodules of R.

Let I be the ideal generated by $\{x_i\}_{i=1}^{\infty} \subset R$, i.e., $I = \{f \in R \,|\, f(0,\ldots,0) = 0\}$—polynomials without a constant term. We will verify that I is not finitely generated.

Proof. Assume the opposite: let I be finitely generated, $I = \langle f_1, \ldots, f_n \rangle, f_i \in R$. Then, among the generating polynomials f_i, there will be a finite number of variables, and we can choose a variable x_t outside all of them. Then, the polynomial x_t would belong to the ideal, as it has no constant term, and thus can be expressed as a combination $x_t = \sum_{i=1}^{n} r_i f_i$, where r_i are polynomials from R. However, in this sum, each term (after "expanding the parentheses" in the multiplications $r_i f_i$) is divisible by a variable other than x_t, making it impossible to obtain x_t as a sum. The contradiction means that the assumption of I being finitely generated is incorrect; thus, I is not finitely generated. □

It follows that the submodule $I \leq R$ is not finitely generated, even though the module R has a finite basis.

Using similar reasoning, we can verify that in the module $M = R[x_1, \ldots, x_n]$ over itself, the submodule $N = \langle x_1, \ldots, x_n \rangle$ is generated by at least n elements, while M itself is generated directly by the unit:

Again, assume that $N = \langle f_1, \ldots, f_k \rangle$ for some $k < n$. Then $f_i = x_{j_i} * f_i'$, and we select a variable $x_t \neq x_{j_i} \forall i$, which must belong to the ideal, but all f_i either do not contain x_t or are of degree at least 2. Hence, x_t cannot be a combination of the f_i, leading to a contradiction.

Remark. In the last situation, if $n > 1$, then $N \leq M$ has a strictly larger minimal generating set than M.

However, for $n = 1$, the submodule N has the same size generating set—$\langle x \rangle$. Note that in this case, $M = R[x]$ is a principal ideal domain (if R is a field), and the anomaly observed above does not occur. Later, we will see that over principal ideal domains, there is a precise upper bound on the number of generators for submodules of finitely generated modules.

Although a submodule of a finitely generated module is not necessarily finitely generated, we have the following statement:

Proposition 3. *If M is a finitely generated module over R and $N \leq M$ is any submodule, then the factor module M/N is also finitely generated.*

Proof. Here, we simply take the cosets of the generating elements: if $M = \langle m_1, \ldots, m_n \rangle$, then obviously $M/N = \langle m_1 + N, \ldots, m_n + N \rangle$. □

6 Annihilator and Torsion

Here are two definitions motivated by the examples in the previous section. We will use the first in the second, which serves as the first step toward the ultimate goal—the classification of finitely generated modules.

6.1 Annihilator

We saw that in modules, it is possible to have $r \cdot m = 0$ for a nonzero scalar r and a nonzero vector m. Let us study these "cross-structural" zero divisors in more detail.

Definition 6. Let M be a module over R.

- *The annihilator of an element $m \in M$* is defined as the set of scalars that annihilate it:

$$\mathrm{Ann}(m) = \{\, r \in R \,|\, r \cdot m = 0 \,\}.$$

- *The annihilator of a set* $S \subseteq M$ is defined as the set of scalars that annihilate all elements in S:

$$\mathrm{Ann}(S) = \{\, r \in R \,|\, \forall m \in S : r \cdot m = 0 \,\}.$$

For example, in the ring $\mathbb{Z}_{21}$ over $\mathbb{Z}$, the annihilator of $\overline{7} \in \mathbb{Z}_{21}$ is:

$$\mathrm{Ann}(\overline{7}) = \{r \in \mathbb{Z} \,|\, r \cdot \overline{7} = 0\} = \{r \in \mathbb{Z} \,|\, 7r \equiv 0 \bmod 21\} = 3\mathbb{Z}.$$

Here, we notice the relationship between 7, 21, and 3, and observe that $\langle \overline{7} \rangle \cong \mathbb{Z}/3\mathbb{Z}$. The following statement holds:

Proposition 4. *Let R be a ring, M a module over R, and $m \in M$. Consider the module generated by this element: $\langle m \rangle = span(\{m\})$. Then $\langle m \rangle \cong R/\mathrm{Ann}(m)$.*

Proof. We consider the homomorphism (of modules[4]) $\varphi : R \to M$, defined as $\varphi(r) = r \cdot m$. Then, by the homomorphism theorem, $R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$, where in this case $\operatorname{Ker}(\varphi) = \mathrm{Ann}(m)$, and $\operatorname{Im}(\varphi) = \langle m \rangle$. □

Remark. We can draw an analogy with the orbit-stabilizer theorem in group actions on a set X.

It states that the length of the orbit of an element in X is the index of its stabilizer.

In this case, the ring R "acts" on the module M, and the orbit of m under this action is the submodule $\langle m \rangle = Rm$, while the stabilizer of an element corresponds to its annihilator. Thus, the index of the annihilator in the ring is the length of the orbit of the element m. In other words, each element of the orbit $\langle m \rangle$ corresponds to a coset of the annihilator.

These special cases of nonzero vectors being mapped to zero under the action of nonzero scalars from the ring deserve particular attention.

If the ring R contains zero divisors, the existence of such cases is trivial; hence, in the next subsection, we consider only rings without zero divisors. Additionally, we assume commutativity of R to ensure that the next statement (5) holds.

6.2 Torsion and Free Modules

Definition 7. Let R be an integral domain, and M a module over it. An element $m \in M$ is called **torsion** if it has a nontrivial annihilator:

$$\mathrm{Ann}(m) \neq \{0\}.$$

We denote the set of torsion vectors in M by M_t. The module M is called a **torsion module** if all its vectors are torsion, and **free** if $M_t = \{0\}$.

Remark. To immediately dispel any doubts: the above characterization covers all modules. For example, $\mathbb{Z} \times \mathbb{Z}_n$ over $\mathbb{Z}$ for $n \leq 2$ is neither free:

$$n \cdot (0, \overline{k}) = (0, \overline{n}) = (0, \overline{0}) \Rightarrow \mathrm{Ann}\left((0, \overline{1})\right) \neq \{0\} \Rightarrow \left((0, \overline{1})\right) \in M_t,$$

nor torsion:

$$\forall k : k \cdot (1, \overline{0}) = (k, \overline{0}) \neq (0, \overline{0}).$$

Proposition 5. *If R is an integral domain, then M_t is a submodule of M, and M/M_t is free.*

Proof. Since $M_t \subseteq M$, to prove it is a submodule, we need to check closure properties:

[4]Recall (as I almost forgot) that R is also a module over itself, as is M. Thus, φ is indeed a module homomorphism.

- Let m and n be torsion elements. Then, there exist scalars $r, s \in R$ such that $r \cdot m = s \cdot n = 0$. To show that $m + n \in M_t$, we take the scalar $r * s$ and verify:

$$\begin{aligned}(r * s) \cdot (m + n) &= (r * s) \cdot m + (r * s) \cdot n \\ &= (s * r) \cdot m + (r * s) \cdot n \\ &= s \cdot (r \cdot m) + r \cdot (s \cdot n) \\ &= s \cdot 0 + r \cdot 0 = 0 + 0 = 0,\end{aligned}$$

  meaning $m + n$ is indeed a torsion vector.

  Note that it is crucial here that the ring is commutative to allow swapping $r * s = s * r$.

- Let m be torsion with $t \cdot m = 0$, and let $r \in R$ be arbitrary. We aim to show that $r \cdot m \in M_t$. Take t and verify: $t \cdot (r \cdot m) = (t * r) \cdot m = (r * t) \cdot m = r \cdot (t \cdot m) = r \cdot 0 = 0$, meaning $r \cdot m \in M_t$. Again, the commutativity of R is crucial here.

Thus, M_t is closed under addition and scalar multiplication, making it a submodule.

The verification that M/M_t is free is equally straightforward. We need to show $(M/M_t)_t = \{0\}$.

Let $m + M_t \in (M/M_t)_t$ be an arbitrary torsion element. Then there exists $r \in R \setminus \{0\}$ such that $r \cdot (m + M_t) = 0_{M/M_t} = M_t$. That is, $(r \cdot m) + M_t = M_t$, or $r \cdot m \in M_t$. This gives another scalar $s \in R \setminus \{0\}$ such that $s \cdot (r \cdot m) = 0_M$, i.e., $(s * r) \cdot m = 0_M \Leftrightarrow m \in M_t \Leftrightarrow m + M_t = M_t = 0_{M/M_t}$, meaning M/M_t is free. □

Example 6.1. In the special case of a module over $\mathbb{Z}$, torsion elements are those of finite order in the abelian group. The previous proposition generalizes the fact that the factor group of an abelian group by the subgroup of its finite-order elements contains no torsion elements except the identity.

Example 6.2. Let us illustrate the last proposition with another example. Consider $M = 2\mathbb{Z} \times 3\mathbb{Z} \times \mathbb{Z}_p$ for some $p \in \mathbb{N}$ as a module over $\mathbb{Z}$.

Any vector $(n, m, \overline{r}) \in M$ is torsion if and only if $n = m = 0$—otherwise, the first two components cannot be annihilated by multiplication with an integer. However, multiplying $(0, 0, \overline{r})$ by p yields $(0, 0, p \cdot \overline{r} = \overline{0}) = 0_M$.

Thus, $M_t = \{0_{2\mathbb{Z}}\} \times \{0_{3\mathbb{Z}}\} \times \mathbb{Z}_p$. If we factor out M_t, we obtain:

$$M/M_t = \frac{2\mathbb{Z} \times 3\mathbb{Z} \times \mathbb{Z}_p}{\{\,(0_{2\mathbb{Z}}, 0_{3\mathbb{Z}})\,\} \times \mathbb{Z}_p} \cong \frac{2\mathbb{Z} \times 3\mathbb{Z}}{\{\,(0_{2\mathbb{Z}}, 0_{3\mathbb{Z}})\,\}} \cong 2\mathbb{Z} \times 3\mathbb{Z}.$$

In this simple example, we can make an interesting observation: $M \cong M_t \times (M/M_t)$, that is, our module can be represented as the direct sum of its torsion submodule and a torsion-free module. Furthermore, the torsion-free module $M/M_t \cong 2\mathbb{Z} \times 3\mathbb{Z}$ has a basis: $\{(2, 3)\}$. The goal of this document is to explore precisely this phenomenon.

Example 6.3. It is worth noting that a torsion module is not necessarily finite, as in the examples involving residues. For instance, in the factor module $\mathbb{Q}/\mathbb{Z}$ over $\mathbb{Z}$, the elements are cosets of the form $\frac{p}{q} + \mathbb{Z}$, where $\frac{p}{q}$ is a proper fraction[5], i.e., in the interval $[0, 1)$. Clearly, then, multiplying (in the sense of "scalar multiplication") by the denominator q yields $q \cdot \left(\frac{p}{q} + \mathbb{Z}\right) = p + \mathbb{Z} = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$, meaning every element is torsion, and thus the module itself is torsion.

[5] If it is not, we can separate out the largest integer part and "transfer" it to $\mathbb{Z}$. Formally, the elements in a coset differ by an element from the submodule, i.e., an integer, and we can then take the smallest positive representative.

7 Free Modules

Definition 8. A module M is called **free** if it has a basis.

It turns out that the theorem on the existence of a basis for a vector space over F remains valid under much weaker conditions than requiring F to be a field—it suffices for F to be a division ring.

Proposition 6. *If R is a division ring and M is a module over R, then M is a free module. In particular, if R is a field, every vector space over R has a basis.*

Proof. The proof proceeds verbatim as in the case of vector spaces, as it relies only on the invertibility needed to show that any vector outside a given span is independent of all vectors within it—this forms the induction step in the proof. □

Proposition 7. *If a module M over R has a basis B, then $M \cong R^{(B)} = \oplus_B R$. In particular, if the basis is finite with $|B| = n < \infty$, then $M \cong R^n$, i.e., we can think of free modules as sets of ordered n-tuples, i.e., as Cartesian products of n copies of the ring.*

We verify only the finitely generated case.

Proof. Let $B = \{e_i\}$. It is natural to define the map $\varphi : M \to R^n$ as:

$$\varphi(v) = \varphi\left(\sum_i \lambda_i e_i\right) = (\lambda_1, \ldots, \lambda_n) \in R^n.$$

Clearly, φ is a homomorphism.

We check for bijection:

- Suppose $\varphi\left(\sum_i \lambda_i e_i\right) = \varphi\left(\sum_i \mu_i e_i\right)$. Then:

  $$(\lambda_1, \ldots, \lambda_n) = (\mu_1, \ldots, \mu_n),$$

  which implies $\lambda_i = \mu_i \, \forall i$, and hence $\sum_i \lambda_i e_i = \sum_i \mu_i e_i$. Therefore, φ is injective.
- For any vector $(\lambda_1, \ldots, \lambda_n) \in R^n$, clearly $\sum_i \lambda_i e_i$ is a preimage. Thus, φ is surjective.

Hence, φ is an isomorphism, and $M \cong R^n$. □

With the following proposition, we ensure that in the case of a finite basis, the number of copies of the ring in the product to which the module is isomorphic is uniquely determined:

Proposition 8. *If R is a nonzero commutative ring, then $R^m \cong R^n$ as modules over R implies $m = n$.*

Proof. We will reduce the task to the well-known theorem from linear algebra, which states that $V \cong W \Leftrightarrow \dim V = \dim W$ for any finitely generated vector spaces.

First, we draw upon Zorn's lemma[6]: any proper ideal of R does not contain the unit, and thus any union of proper ideals (in particular, an ascending chain of such ideals) also does not contain the unit, making it a proper ideal.

By Zorn's lemma, a maximal such (proper) ideal exists[7] I. From advanced algebra, we know that in this case, R/I is a field—and here we use the commutativity of R. We will prove that $(R/I)^n \cong (R/I)^m$ as modules over R/I, and from linear algebra, we deduce $n = m$.

Let $R^n \cong R^m$, and let $\varphi : R^n \to R^m$ be an isomorphism. We will prove that:

$$R^n/IR^n \cong R^m/IR^m$$

[6] From which every proper ideal of R is contained in a maximal ideal.
[7] Maximal in the sense of inclusion of sets.

as modules over R/I, and that:

$$R^k/IR^k \cong (R/I)^k$$

again as modules over R/I. From this, it follows that $(R/I)^n \cong (R/I)^m$, and from linear algebra, we deduce $n = m$.

1. Between R^n/IR^n and R^m/IR^m, we directly construct the homomorphism:

   $$(\vec{r} + IR^n) \mapsto (\varphi(\vec{r}) + IR^m).$$

   Since φ is an isomorphism, this mapping is also a bijection.

2. We prove that

   $$R^k/IR^k \cong (R/I)^k$$

   using the homomorphism theorem for the map:

   $$\left((r_1, \ldots, r_k) + IR^k\right) \mapsto (r_1 + I, \ldots, r_k + I)\,.$$

   This is clearly surjective, and its kernel is IR^k.

□

This seemingly obvious statement might appear uninteresting to some and unworthy of attention. However, in reality, the truth about rings is much harsher, and the above proposition is not valid if we abandon the assumption of commutativity of R.

Example 7.1. Consider the set $E = \mathbb{CFM}_N(R)$ of infinite matrices (in both rows and columns) with finitely many nonzero columns. Clearly, the sum of two matrices in E is well-defined (it has finitely many nonzero columns).

Each matrix in E has entirely zero columns after a certain point, allowing the definition of multiplication as for finite matrices (row-by-column):

$$\begin{pmatrix} \boldsymbol{a_{1,1}} & \boldsymbol{\cdots} & \boldsymbol{a_{1,n}} & 0\cdots \\ \vdots & \ddots & \vdots & \vdots \\ \boldsymbol{a_{m,1}} & \boldsymbol{\cdots} & \boldsymbol{a_{m,n}} & 0\cdots \\ a_{m+1,1} & \cdots & a_{m+1,n} & 0\cdots \\ \vdots & & \vdots & \vdots \end{pmatrix} \times \begin{pmatrix} \boldsymbol{b_{1,1}} & \boldsymbol{\cdots} & \boldsymbol{b_{1,m}} & 0\cdots \\ \vdots & \ddots & \vdots & \vdots \\ \boldsymbol{b_{n,1}} & \boldsymbol{\cdots} & \boldsymbol{b_{n,m}} & 0\cdots \\ b_{n+1,1} & \cdots & b_{n+1,m} & 0\cdots \\ \vdots & & \vdots & \vdots \end{pmatrix}.$$

Since only a finite number of columns in the right-hand matrix are nonzero, rows of the left-hand matrix beyond the mth do not contribute. Similarly, rows of the right-hand matrix beyond the nth also do not participate in the product. As a result, only the top-left $m \times n$ submatrix can have nonzero entries.

Then E forms a ring with the natural addition and multiplication of matrices.

For this ring, it turns out that $E \cong E^2$ as modules over E. How? Consider the following map:

$$\varphi : E \to E^2,$$
$$\left(\vec{a_1}, \vec{b_1}, \ldots, \vec{a_n}, \vec{b_n}, \vec{0}, \ldots\right) \mapsto \left(\left(\vec{a_1}, \ldots, \vec{a_n}, \vec{0}, \ldots\right), \left(\vec{b_1}, \ldots, \vec{b_n}, \vec{0}, \ldots\right)\right).$$

To each matrix A with finitely many columns, we assign two matrices—one consisting of the even-numbered columns of A and the other of the odd-numbered columns. Clearly, φ is a bijection, with the inverse map "merging" two matrices back into one in reverse. It is equally evident that φ is a homomorphism of groups.

To avoid deviating too much from the topic, we will skip verifying that $\varphi(A \cdot B) = \varphi(A) \cdot B$. Ultimately, φ is an isomorphism of modules, illustrating the validity of Proposition 8.

The last example motivates the following definition, which we will not use further but is worth noting:

Definition 9. A ring R is said to be **invariant with respect to the lengths of bases** if $R^n \cong R^m$ as modules over R implies $n = m$.

Thus, Proposition 8 essentially states that commutative rings are invariant with respect to the lengths of bases.

We will now see that anomalies such as cross-structural zero divisors cannot occur in free modules.

Proposition 9. *Let R be an integral domain[8], and let M be a free module over R. Then M is free of torsion.*

The main reasoning here is that bases provide unique representations of zero, whereas torsion, or zero divisors, provide *different* representations of zero. In a sense, bases "protect" us from zero anomalies.

Proof. Let M have a basis $B = \{b_i\}$, $m \in M$, and $r \cdot m = 0$. We will prove that $r = 0_R \vee m = 0_M$. We have:

$$0 = r \cdot m = r \cdot \sum_i r_i \cdot b_i = \sum_i r \cdot (r_i \cdot b_i) = \sum_i (r \cdot r_i) \cdot b_i.$$

Since B is a basis, the only representation of zero in it is with zero coefficients. Hence:

$$r \cdot r_i = 0 \quad \forall i.$$

R has no zero divisors, so either $r = 0_R$, or $r_i = 0_R \, \forall i$. The latter implies $m = 0_M$. □

The presence of a basis excludes the possibility of torsion elements. However, the absence of such elements is far from sufficient for a module to be free:

Example 7.2. As a module over $R = \mathbb{Z}[x]$, the ideal submodule $I = \langle 2, x \rangle \leq R$ clearly has no torsion elements, as $\mathbb{Z}[x]$, along with its ideals, forms an integral domain—multiplication by a nonzero polynomial cannot reduce the degree.

I is torsion-free, but it cannot possibly have a basis. Why? Its supermodule R over R is generated by $\{1_R\}$, meaning the maximal number of linearly independent vectors in R is 1. Thus, any basis of I contains at most one element, but from advanced algebra, we know that $I \leq R$ is not a principal ideal and cannot be generated by a single element.

Therefore, I does not admit a basis, even though it is a torsion-free module over R. Moreover, it is a submodule of a free module!

The fundamental issue in this counterexample is the fact that the ring R contains non-principal ideals. In other respects, the modules I and R possess many appealing properties—both are torsion-free and finitely generated. It is natural to ask whether a finitely generated torsion-free module can be made free if its ring is a principal ideal domain.

We now shift focus precisely to modules over principal ideal domains.

8 Modules Over Principal Ideal Domains

Proposition 10. *Let M be a torsion-free finitely generated module over a principal ideal domain R. Then M admits a finite basis.*

Remark. All three conditions are key. If we drop any of them:

- Dropping the finitely generated condition gives a counterexample—$\mathbb{Q}$ over $\mathbb{Z}$.

[8] Recall that in the definition of torsion and free modules, we required the ring to be an integral domain, so this condition does not narrow the scope of the proposition.

- If R is not a principal ideal domain, see the example with $\langle 2, x\rangle \leq R[x]$.
- If M is not torsion-free—$\mathbb{Z}_n$ over $\mathbb{Z}$ is not free (note: it is still finitely generated).

For convenience, some of the following statements will rely on the lemma below. We will use it to inductively reason about the dimensions of modules.

Lemma 11. *If $\varphi : M \to M$ is an idempotent endomorphism of a free module, then:*

$$M \cong \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi.$$

It might be surprising, but in general, we cannot simply "transfer" the kernel to the other side with a $\times$ sign by invoking the isomorphism theorem.

For instance, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, but for $n \geq 2$, it is not true that $\mathbb{Z} \cong n\mathbb{Z} \times \mathbb{Z}_n$ under the standard operations for the Cartesian product of groups. Assuming the existence of such an isomorphism ψ leads to a contradiction:

$$\begin{aligned}
(k, \overline{0}) &= (k, \overline{0+0})) \\
(k, \overline{0}) &= (k, \overline{0}) + (k, \overline{0}) \\
\mathbf{0}_{n\mathbb{Z}\times\mathbb{Z}_n} &= (k, \overline{0}) \\
\psi(\mathbf{0}) &= \psi((k, \overline{0}))\forall k \\
(k, \overline{0}) &\in \operatorname{Ker}\psi \\
\operatorname{Ker}\psi &\neq \{0\}
\end{aligned}$$

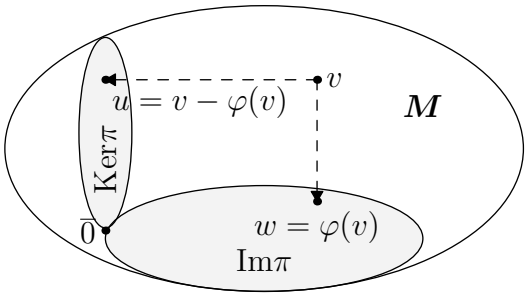
Proof Let us assume that $\varphi(M) \leq N \leq M$ and construct a direct isomorphism:

$$\psi : M \to \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi.$$

Let $v \in M$ be arbitrary. We seek a representation of the form:

$$v = u + w,$$

where $u \in \operatorname{Ker}\varphi$, and $w \in \operatorname{Im}\varphi$. A natural choice for w is simply $\varphi(v)$.



Then, the only possibility for u is $u = v - w = v - \varphi(v)$.

$$v = \underbrace{(v - \varphi(v))}_{\text{We want to be from } \operatorname{Ker}\varphi} + \underbrace{\varphi(v)}_{\text{by } \operatorname{Im}\varphi}$$

We verify that this indeed holds:

$$\begin{aligned}
u \in \operatorname{Ker}\varphi \\
\Leftrightarrow \varphi(u) = 0 \\
\Leftrightarrow \varphi(v - \varphi(v)) = 0 \\
\Leftrightarrow \varphi(v) - \varphi(\varphi(v)) = 0 \\
\Leftrightarrow \varphi(v) - \varphi(v) = 0 \quad \checkmark.
\end{aligned}$$

Thus, it is correct to define $\psi : M \to \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$ in this way:

$$\psi(v) = (v - \varphi(v),\, \varphi(v))\,.$$

Clearly, ψ is a homomorphism. It remains to check whether it is a bijection:

- Let $(u, w) \in \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$. For surjectivity, we need to find $m \in M$ such that $\psi(m) = (u, w)$.

  Since $w \in \operatorname{Im}\varphi$, there exists $v \in M$ such that $\varphi(v) = w$. Then $m = \varphi(v) + u$ will suffice:

$$\begin{aligned}\psi(m) &= (m - \varphi(m), \varphi(m)) \\ &= (\varphi(v) + u - \varphi(\varphi(v) + u), \varphi(\varphi(v) + u)) \\ &= (\varphi(v) + u - \varphi(v) - \varphi(u), \varphi(\varphi(v)) + \varphi(u)) \\ &= (\varphi(v) + u - \varphi(v) - 0, w + 0) \\ &= (u, w).\end{aligned}$$

  Thus, ψ is surjective.

- Let $\psi(v) = \psi(v')$ for some $v, v' \in M$. Subtracting and expanding directly yields $v = v'$. These calculations involve no interesting reasoning.

Hence, ψ is an isomorphism, and $M \cong \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$. □

Earlier, we promised that over principal ideal domains, submodules of free modules are also free modules, with bases no larger than those of the supermodule.[9] This result can now be obtained as a corollary of the previous proposition:

Proposition 12. *If R is a principal ideal domain, then every submodule N of a free module M is free, with a rank no greater than that of M.*

Proof. Let $M = R^n$ (by Proposition 7). We proceed by induction on n:

1. For $n = 1$, $M = R$, and $N \leq M$ is an ideal of R. Since R is a principal ideal domain, $N = \langle x \rangle$ for some $x \in N$, and $\{x\}$ forms a basis of N of length $1 \leq \dim M$.
2. Assume all submodules of R^n are free of rank at most n. We will prove the statement for $M = R^{n+1}$.

   To utilize the induction hypothesis, consider M as the direct sum $R \oplus R^n$ and its projection

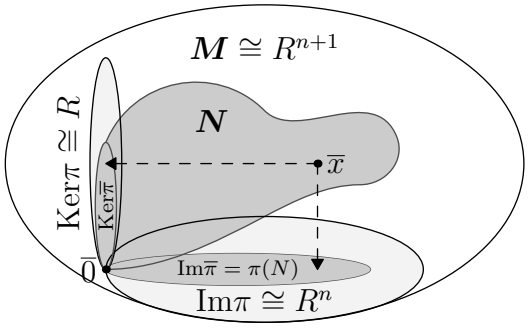
$$\pi : (R \oplus R^n) \twoheadrightarrow \pi(M) \cong R^n$$

   onto the second component:

$$\pi(r_1, \ldots, r_{n+1}) = (0, r_2, \ldots, r_{n+1}).$$

   This decomposes M into two parts: $\operatorname{Im}\pi$ and $\operatorname{Ker}\pi$.

   As a projection, π satisfies $\pi \circ \pi = \pi$. Let us consider its restriction to N: $\overline{\pi} \coloneqq \pi|_N : N \to R^n$.



   Applying the previous lemma with a minor adjustment[10], we obtain:

$$N \cong \operatorname{Ker}\overline{\pi} \oplus \operatorname{Im}\overline{\pi}.$$

   Thus, $N = \operatorname{Ker}\overline{\pi} \oplus \operatorname{Im}\overline{\pi}$. Both components of the sum are free:

   - By induction, $\operatorname{Im}\overline{\pi}$ is a free module of rank at most n, as it is a submodule of $\operatorname{Im}\pi \cong R^n$.
   - $\operatorname{Ker}\overline{\pi} \leq \operatorname{Ker}\pi \cong R$, and since it is (isomorphic to) a submodule of a ring, it is (isomorphic to) an ideal of R, which is a principal ideal domain. Thus, $\operatorname{Ker}\overline{\pi}$ is a principal ideal and a free module over its ring.

[9] Recall Proposition 8, where we established that free modules over a principal ideal domain (utilizing their commutativity) have a strictly determined dimension (rank).

[10] It is not an issue to assume $\pi(M) \leq N$, as we can always find an isomorphic copy N' of $\pi(N)$ within N with a corresponding isomorphism $h : \pi(N) \cong N'$, such that $h \circ \overline{\pi} = \mathrm{id}$, and then prove the statement for $\pi' = h \circ \pi$.

Consequently, N is also free.

By induction, the statement holds for all $n \in \mathbb{N}$. □

For the next theorem, it will be convenient to provide an equivalent condition for a module to be finitely generated:

Lemma 13. *A module M is finitely generated by S over R if and only if there exists a surjective homomorphism from the free module $R^{(S)}$ onto M.*

Proof. Essentially, we associate each generating element of M with one "coordinate axis" in $R^{(S)}$.

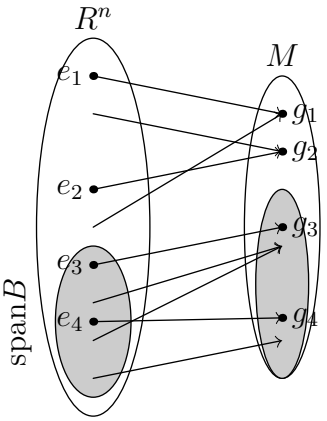
- In one direction, if $f : R^{(S)} \twoheadrightarrow M$ is a surjective homomorphism, then the images of the basis vectors e_i in $R^{(S)}$ form a (finite) generating set: $M = \operatorname{span}(\{f(e_i)\}_{i=1}^n)$.
- Conversely, if $M = \operatorname{span}(\{a_i\}_{i=1}^n)$, then we can construct the desired homomorphism (by Proposition 2 on the universal property), defining it on the standard basis of $R^{(S)}$: $f(e_i) = a_i$.

  Every $m \in M$ is a combination of elements $\{a_i\}$ and therefore has a preimage in $R^{(S)}$, meaning the homomorphism constructed in this way is surjective.

□

Proposition 14 (Paul Garrett, 2.0.7)**.** *If R is a principal ideal domain and M is a finitely generated module over R, then every submodule $N \leq M$ is also finitely generated.*

In other words, the statement says that if we drop the condition for M to be torsion-free, instead of a finite basis, we will obtain a finite generating set. That is, the presence of torsion elements breaks linear independence, but we still have finite generation.



Proof For any finitely generated module M over R, there exists a surjective homomorphism $\varphi : R^d \twoheadrightarrow M$ for some $d \in \mathbb{N}$. The lack of torsion here implies that some of the copies of R in R^d are mapped to the torsion part of M and are "collapsed" in the process.

The preimage of $N \leq M$ in R^d, however, is a submodule $\varphi^{-1}(N) \leq R^d$ of a free module, and as such, it is also free with some basis $B = \{x_1, \ldots, x_m\}$ with $|B| \leq \dim M$, by Proposition 12. This basis, if M were torsion-free, would map to a basis[11] of N. In the general case, however, we can only use that $\operatorname{span}(B) = \varphi^{-1}(N)$, implying that $\operatorname{span}(\varphi(B)) = N$, thus finding a (finite) generating set $\varphi(B)$ for N.

□

Remark. Earlier, we noted that linearly independent sets are not necessarily extendable to a basis, and in particular, the basis of a submodule is not necessarily extendable to a basis of the supermodule.

For example, $2\mathbb{Z} \times 2\mathbb{Z} \leq \mathbb{Z} \times \mathbb{Z}$, but we cannot extend the basis $\{(0,2),(2,0)\}$ of $(2\mathbb{Z})^2$ to a basis of $\mathbb{Z}^2$.

However, we can do something close: find a basis for the submodule where each vector is a multiple of a corresponding basis vector of the supermodule.

In this example, with the standard basis $\mathbb{Z}^2 = \langle e_1, e_2 \rangle = \langle (1,0),(0,1) \rangle$, we have a "multiple" basis:

$$(2\mathbb{Z})^2 = \langle 2e_1, 2e_2 \rangle = \langle (2,0),(0,2) \rangle.$$

Definition 10. If M and M' are free modules, $M' \leq M$, and they have bases $\{v_1, \ldots, v_n\}$ and $\{a_1 v_1, \ldots, a_m v_m\}$ respectively, where $a_i \mid a_{i-1}$ $\forall i > 1$, then these bases are called **aligned**.

[11] Since φ is surjective, it is an isomorphism and preserves bases.

With this definition, we can now formulate the main theorem:

Theorem 15. *Over a principal ideal domain, if M is a free module of rank $n \geq 1$ and $M' \leq M$, then M and M' admit aligned bases.*

Remark. It is important to note that the theorem does not state that, given a basis of M, we can find a multiple of it for M'.

Nor does it state that, given a basis of M', we can find a basis of M that is a multiple of it.

What this theorem provides are "new" bases for M and M'.

In fact, such requests are not even reasonable. Consider $M = \mathbb{Z}^2$ with the basis $B = \{(1,0),(0,1)\}$ and its submodule $M' = \langle(1,1)\rangle \times \langle(-1,1)\rangle$ with the basis $B' = \{(1,1),(-1,1)\}$.

Then there is no basis of M for which B' is a multiple, nor is there a basis of M' for which B is a multiple.

However, there exist entirely different bases for the two modules that are aligned:

$$M = \langle(0,1),(1,1)\rangle \quad \text{and} \quad M' = \langle(0,2),(1,1)\rangle.$$

Proof. Let M be a free module of rank n over a principal ideal domain R, and let $M' \leq M$ be its submodule.

Finding aligned bases for these modules, in a sense, means finding such coordinate axes that, pairwise, they are "parallel", and in each subsequent pair, the unit vector of the submodule is proportionally longer than that of the previous pair.

We begin with (one) "shortest" coordinate axis. We examine all possible linear functionals $\mathrm{Hom}(M,R)$ and choose one that "preserves" the most information about the submodule M'.

To do this, we consider the projections $\{\ \varphi(M') \mid \varphi \in \mathrm{Hom}(M,R)\ \}$ of M' onto R. These are submodules, hence ideals, and we can select the largest among them. Let φ be the projection such that $\varphi(M') \leq R$ is maximal. Since R is a principal ideal domain, $\varphi(M')$ is generated by some scalar $a_1 \neq 0$. Denote one of its preimages by v'.

We will check the following:

Mini-proposition 8.1. Every image of v' under a linear functional $\widehat{\varphi}$ is a multiple of a_1.

Proof. On the language of ideals, the statement essentially says that $\langle a_1\rangle \supseteq \langle\widehat{\varphi}(v')\rangle$.

Consider the greatest common divisor (GCD) d of a_1 and $\langle\widehat{\varphi}(v')\rangle$. By Bézout's identity, we have:

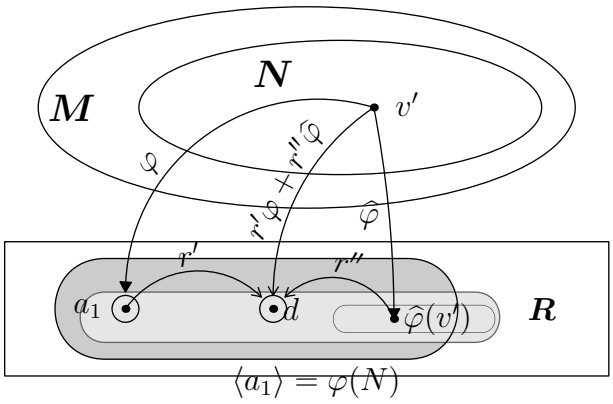
$$d = r'a_1 + r''\widehat{\varphi}(v') = r'\varphi(v') + r''\widehat{\varphi}(v'),$$

meaning d is a linear combination of two images of v' under two linear functionals. Thus, d is itself an image of v' under the linear combination:

$$\psi = r'\varphi + r''\widehat{\varphi} : M' \to R.$$

This leads to the following inclusions:

1. $\langle d\rangle \leq \psi(M')$, because $\operatorname{Im}\psi$ is an ideal of R and is also a principal ideal domain.
2. $\langle d\rangle \supseteq \langle\widehat{\varphi}(v')\rangle \cup \langle a_1\rangle$, since d is the GCD of $\widehat{\varphi}(v')$ and a_1.



We obtained that for any linear functional $\widehat{\varphi}$, $\varphi(N) = \langle a_1 \rangle \leq \langle d \rangle \leq \psi(N)$. Since φ was chosen such that $\varphi(N)$ is maximal, from $\varphi(N) \leq \psi(N)$ it follows that:

$$\varphi(N) = \psi(N),$$

and from the previous inclusions:

$$\langle a_1 \rangle = \langle d \rangle.$$

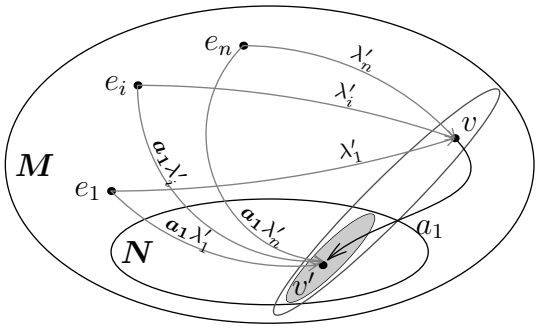
Thus, it turns out that:

$$\langle a_1 \rangle + \langle \widehat{\varphi}(v') \rangle = \langle d \rangle = \langle a_1 \rangle,$$

i.e., $\langle a_1 \rangle \supseteq \langle \widehat{\varphi}(v') \rangle$, and a_1 divides $\widehat{\varphi}(v')$ for any $\widehat{\varphi} : \mathrm{Hom}(M, R)$.

□

Having established that every projection of v' onto the ring is a multiple of a_1, let us examine what happens when we decompose v' in some basis of M.



Let $\{e_i\}$ be a basis of M. Then:

$$v' = \sum_i \lambda_i e_i.$$

Each coordinate $\lambda_i \in R$ of v' is an image under a linear functional projecting the i-th coordinate of any vector in M onto the ring. From the above reasoning, every λ_i is a multiple of a_1, so we can write $\lambda_i = a_1 \lambda'_i$. Therefore:

$$v' = \sum_i \lambda_i e_i = \sum_i a_1 \lambda'_i e_i = a_1 \sum_i \lambda'_i e_i = a_1 v,$$

where $v = \sum_i \lambda'_i e_i$. We have expressed v' as the product of another vector and a_1.

Applying φ to both sides:

$$\begin{aligned} \varphi(v') &= \varphi(a_1 v), \\ a_1 &= a_1 \varphi(v), \\ a_1(1 - \varphi(v)) &= 0 \\ a_1 \neq 0 &\Rightarrow \varphi(v) = 1 \end{aligned}$$

Now we have vectors $v \in M$, $a_1 v \in M'$, and a projection φ such that $v \overset{\varphi}{\mapsto} 1_R$.

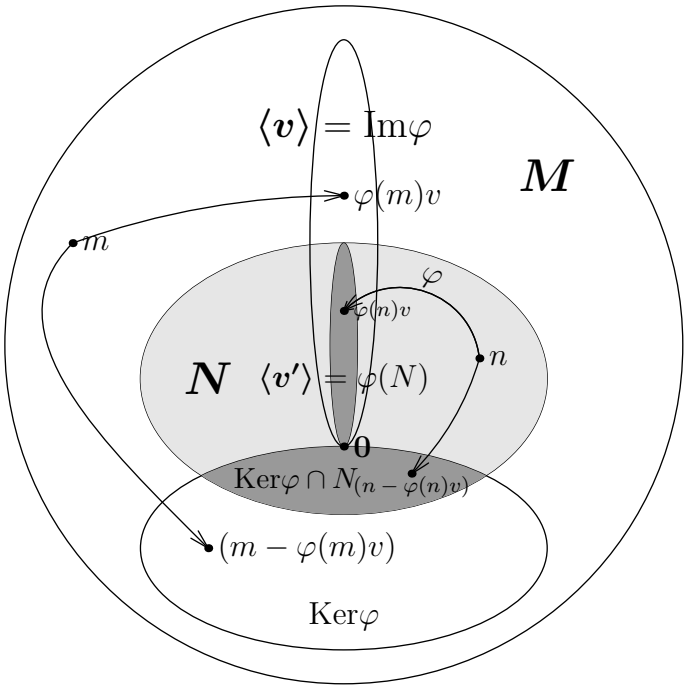
Looking at the entire axis $\langle v \rangle$, the above implies that:

$$\langle v \rangle \overset{\varphi}{\mapsto} \langle 1_R \rangle = R.$$

This suggests that we should take v in the basis of M, and $a_1 v$ in the basis of M'.

Thus, the first aligned axes are $\langle v \rangle$ and $\langle v' \rangle$. Let's find the remaining axes!

1. $M \cong \mathrm{Ker}\, \varphi \oplus \langle v \rangle$, using Lemma 11 for the map $(r \mapsto rv) \circ \varphi$ (here, $r \mapsto rv$ is an isomorphism from R to $\langle v \rangle$).
2. $M' \cong (M' \cap \mathrm{Ker}\, \varphi) \oplus \langle a_1 v \rangle$, again using Lemma 11, but for the restriction $\varphi|_{M'} : M' \to \varphi(M') = \langle a_1 v \rangle = \langle v' \rangle$.



We are now ready to proceed with the inductive step.

From $M \cong \operatorname{Ker}\varphi \oplus \langle v \rangle$, we have:

$$\dim(\operatorname{Ker}\varphi) = \dim M - \dim\langle v \rangle = n - 1.$$

Then we can apply the induction hypothesis to the kernel (which is a free module, as shown in earlier theorems) and its submodule $\operatorname{Ker}\varphi \cap M'$. This gives us aligned bases:

- $\{v_i\}_{i=2}^{n}$ for $\operatorname{Ker}\varphi$, and
- $\{a_i v_i\}_{i=2}^{k}$ for $\operatorname{Ker}\varphi \cap M'$.

Adding v and $v' = a_1 v$ to these, we obtain aligned bases for M and M'.

The base case of the induction is when $n = 1$. Then $M \cong R = \langle 1 \rangle$, and M' is a principal ideal with $M' = \langle a \rangle = \langle a \cdot 1 \rangle$ for some generating element a. □

9 The Theorem

We need one more proposition:

Proposition 16. *Let A_i be modules over the ring R for $i = 1, \ldots, n$, and let $B_i \leq A_i$ be their respective submodules.*

Then:

$$(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n.$$

The proof is purely technical and simply follows the definitions, so it is unnecessary to fill more space here.

We can now prove the main result of this document using the statements formulated so far:

Theorem 17. *Let R be a principal ideal domain, and let M be a finitely generated module over R. Then there exist scalars $\{a_i\}_{i=1}^{m}$ satisfying $a_i \mid a_{i+1}$ for all $i = 1, \ldots, m-1$, and a rank n, such that:*

$$M \cong R^n \oplus (R/a_1) \oplus \cdots \oplus (R/a_m).$$

Proof. Step by step:

- By Proposition 14, there exists a surjective homomorphism:
$$f : R^r \twoheadrightarrow M.$$
- By the homomorphism theorem:
$$R^r / \operatorname{Ker} f \cong M.$$
- Theorem 15 provides aligned bases for the free module R^r and its submodule $\operatorname{Ker} f \leq R^r$:
  - $R^r = \operatorname{span}(\{v_1, \ldots, v_r\})$
  - $\operatorname{Ker} f = \operatorname{span}(\{a_1 v_1, \ldots, a_m v_m\})$,

  where $a_i \mid a_{i+1}$ for $i = 1, \ldots, m-1$.
- Then we can write:
$$M \cong R^r / \operatorname{Ker} f = (\oplus_{i=1}^r R) \,/\, (\langle a_1 v_1 \rangle \oplus \cdots \oplus \langle a_m v_m \rangle).$$
- Noting that $\langle a_i v_i \rangle \cong a_i R$:
$$M \cong (\oplus_{i=1}^r R)/(a_1 R \oplus \cdots \oplus a_m R).$$
- Using the last proposition, we can decompose:
$$M \cong (R/a_1 R) \oplus \cdots \oplus (R/a_m R) \oplus R^{r-m}.$$
- As ideals, $a_i R = \langle a_i \rangle$, and thus we arrive at the desired representation:
$$M \cong R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_m \rangle \oplus R^{r-m}.$$

□

10 Some Notes

- Every finitely generated module over a principal ideal domain decomposes into a torsion module and a free module:
$$M \cong F \oplus T,$$
where $F = R^n$, and $T = \oplus_i (R/\langle a_i \rangle)$.
- In the special case where R is a field, the ideals $(R/\langle a_i \rangle)$ can only be R or $\{0\}$. Thus, in the decomposition, $T \cong \{0\}$, and we obtain that finitely generated vector spaces have the form R^n.
- As a corollary of the theorem for the case $R = \mathbb{Z}$, we obtain the classification of finitely generated abelian groups:

  Proposition 18. *If G is a finitely generated abelian group, there exist numbers $a_1, \ldots, a_m$, each dividing the next, and $n \in \mathbb{N}$, such that:*
$$G \cong \mathbb{Z}^n \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_m}.$$
- The representation of M in the theorem is unique; that is, the rank n and the set $\{a_i\}$ are uniquely determined.
- Using the Chinese Remainder Theorem, any finitely generated module can be expressed in the form:
$$M \cong R^n \oplus (R/\langle p_1^{\alpha_1} \rangle) \oplus \cdots \oplus (R/\langle p_m^{\alpha_m} \rangle),$$
where p_i are prime elements of the ring R.

11 Applications

Jordan Normal Form Let T be a linear operator in the space $V = F^n$ over an algebraically closed field F. We can view V as a *module* over $F[T]$, the ring of polynomials with the variable "operator" T.

In this perspective, for any vector $v \in V$, the scalar $c = a_m T^m + \cdots + a_1 T + a_0 \mathrm{Id}$ acts as:

$$c \cdot v = a_m T^m(v) + \cdots + a_1 T(v) + a_0 v.$$

Viewing V as a module over $F[T]$, its finite dimension as a space implies it is finitely generated as a module. By the theorem on finitely generated modules, we have:

$$V \cong \oplus_i F[T]/(T - \lambda_i)^{k_i},$$

in the form of irreducible factors rather than invariant factors—here, we use the algebraic closure of F to decompose completely into linear factors. It follows that the matrix of T in a basis of V consistent with this decomposition is precisely in Jordan normal form.

Solutions of Linear Homogeneous Differential Equations Similar to the above construction, the solution space of a linear homogeneous differential equation can be viewed as a module over $F[D]$, where D is the differentiation operator. From this perspective, we can derive the "recipe" for solving such equations.

12 Sources

- Keith Conrad, Modules over PID
- Benjamin Levine, Finitely generated modules over a PID
- William Adkins, Steven Weintraub — Algebra. An approach via module theory
- Paul Garrett, Abstract Algebra, #11 Finitely-generated modules
- Dexter Chua, notes on lectures by O. Randal-Williams, Groups, Rings, and Modules
- Numerous Wikipedia pages and questions/answers on math.stackexchange.com