Chapter I

Linear algebra

I.1 Free modules revisited

Exercise I.1.1. Prove that $\mathbb{R}$ and $\mathbb{C}$ are isomorphic as $\mathbb{Q}$-*vector spaces.* (In particular, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are isomorphic as groups.)

Solution. Observe that $\dim_{\mathbb{Q}} \mathbb{R}$ is uncountable (and in particular, is the cardinality of the continuum). This is equal to $\dim_{\mathbb{Q}} \mathbb{C}$. Since the two vector spaces have equal dimension, they are isomorphic as $\mathbb{Q}$-vector spaces and hence are isomorphic as groups. □

Exercise I.1.2. Prove that the sets listed in Exercise III.1.4 are all $\mathbb{R}$-vector spaces, and compute their dimensions.

Solution. Recall that we only need to show that each set is a module over $\mathbb{R}$. We start with $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) \mid \operatorname{tr}(M) = 0\}$ and define the action of $\mathbb{R}$ on a matrix as multiplication by each entry. Given $A, B \in \mathfrak{sl}_n(\mathbb{R})$, $r_1, r_2 \in \mathbb{R}$, we have

- $(r_1 + r_2)A = r_1A + r_2A$
- $1A = A$ and $(r_1r_2)A = r_1(r_2A)$
- $r_1(A + B) = r_1A + r_1B$

so $\mathfrak{sl}_n(\mathbb{R})$ is a $\mathbb{R}$-vector space. To find its dimension, we are tasked with finding a basis. First note that the elementary matrices $e_{i,j}$ for $i \neq j$ all have zero trace so they are in $\mathfrak{sl}_n(\mathbb{R})$. For $e_{i,i}$, we require another element on the diagonal to force the trace to be zero. The most convenient choice is to let $h_i = e_{i,i} - e_{i+1,i+1}$. Certainly, this set of matrices generates $\mathfrak{sl}_n(\mathbb{R})$ and it contains $n^2 - n + (n-1) = n^2 - 1$ elements so the dimension of this vector space is $n^2 - 1$. Presumably, we use a similar, if not the same, basis for $\mathfrak{sl}_n(\mathbb{C})$.

We define the action of $\mathbb{R}$ on $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) \mid M + M^t = 0\}$ in exactly the same manner as above. It is easy to verify that this is also a vector space. Again, we are tasked with computing a basis. First, we construct a set of basis matrices with zero entries on the diagonal. Let $g_{i,j}$ denote the matrix with entry 1 at i, j, entry -1 at j, i, and zero everywhere else, where $i \neq j$. Then $g_{i,j} \in \mathfrak{so}_n(\mathbb{R})$. To consider the diagonal, note that if any entry on the diagonal is nonzero, then summing the matrix with its transpose makes a nonzero matrix. Thus, the entries on the diagonal must be zero. This set generates $\mathfrak{so}_n(\mathbb{R})$ and contains $\frac{n(n-1)}{2}$ elements, so this is the dimension of the Lie algebra.

The action of $\mathbb{R}$ on $\mathfrak{su}(n) = \{M \in \mathfrak{sl}_n(\mathbb{C}) \mid M + M^* = 0\}$ is again the same as above. To compute a basis for this vector space, first note that the diagonals must not include reals because the complex transpose matrix will not sum to zero. Therefore, we redefine h_i to use $i, -i$ instead of $1, -1$. Furthermore, the basis matrices with zeros on the diagonals must be separated into real and imaginary components. Therefore, we include the $g_{i,j}$ from above and also define $g^*_{i,j}$ to be matrices with the imaginary unit i at i, j and j, i for $i \neq j$, and zero elsewhere. This is a basis for the vector space and has $n(n-1)+(n-1) = n^2-1$ elements, so this is the dimension of the vector space. □

Exercise I.1.3. Prove that $\mathfrak{su}(2) \cong \mathfrak{so}_3(\mathbb{R})$ as $\mathbb{R}$-vector spaces. (This is immediate, and not particularly interesting, from the dimension computation of Exercise 1.2. However, these two spaces may be viewed as the tangent spaces to $SU(2)$, resp., $SO_3(\mathbb{R})$, at I; the surjective homomorphism $SU(2) \to SO_3(\mathbb{R})$ you constructed in Exercise II.8.9 induces a more 'meaningful' isomorphism $\mathfrak{su}(2) \to \mathfrak{so}_3(\mathbb{R})$. Can you find this isomorphism?)

Solution. Since $\mathfrak{su}(2)$ and $\mathfrak{so}_3(\mathbb{C})$ have the same dimension, namely 3, the two are isomorphic as $\mathbb{R}$-vector spaces. Admittedly, I don't know how to interpret the surjection from $SU(2) \to SO_3(\mathbb{R})$, nor do I have any clue how to work with Lie algebras. □

Exercise I.1.4. Let V be a vector space over a field k. A *Lie bracket* on V is an operation $[\cdot, \cdot] : V \times V \to V$ such that

- $(\forall u, v, w \in V), (\forall a, b \in k)$,

$$[au + bv, w] = a[u, w] + b[v, w], \quad [w, au + bv] = a[w, u] + b[w, v],$$

- $(\forall v \in V), [v, v] = 0$,
- and $(\forall u, v, w \in V), [[u, v], w] + [[v, w], u] + [[w, u], v] = 0$.

(This axiom is called the *Jacobi identity*.) A vector space endowed with a Lie bracket is called a *Lie algebra*. Define a category of Lie algebras over a given field. Prove the following:

- In a Lie algebra V, $[u, v] = -[v, u]$ for all $u, v \in V$.
- If V is a k-algebra (Definition III.5.7), then $[v, w] := vw - wv$ defines a Lie bracket on V, so that V is a Lie algebra in a natural way.
- This makes $\mathfrak{gl}_n(\mathbb{R})$, $\mathfrak{gl}_n(\mathbb{C})$ into Lie algebras. The sets listed in Exercise III.1.4 are all Lie algebras, with respect to a Lie bracket induced from $\mathfrak{gl}$.
- $\mathfrak{su}_2(\mathbb{C})$ and $\mathfrak{so}_3(\mathbb{R})$ are isomorphic as Lie algebras over $\mathbb{R}$.

Solution. First, let $u, v \in V$. We find

$$\begin{aligned} 0 &= [u+v, u+v] \\ &= [u, u+v] + [v, u+v] \\ &= [u,u] + [u,v] + [v,u] + [v,v] \\ &= [u,v] + [v,u] \end{aligned}$$

so $[u, v] = -[v, u]$.

Recall that a k-algebra V is a k-vector space with a compatible ring structure. We merely need to verify that the axioms hold. We find that for $u, v, w \in V$, $a, b \in k$,

$$\begin{aligned} [au + bv, w] &= (au + bv)w - w(au + bv) \\ &= a(uw - wu) + b(vw - wv) \\ &= a[u, w] + b[v, w]. \end{aligned}$$

The other axiom in the first point is easy to verify. Clearly, we have $[v, v] = v^2 - v^2 = 0$. Finally, the Jacobi identity also holds, though it's tedious to typeset. □

Exercise I.1.5. Let R be an integral domain. Prove or disprove the following:

- Every linearly independent subset of a free R-module may be completed to a basis.
- Every generating subset of a free R-module contains a basis.

Solution. The first statement is false. Consider $\mathbb{Z}$ as a module over itself. The set $B = \{2\}$ is linearly independent, yet it cannot be extended to a basis. Indeed, including another element x forces the set to be linearly dependent as $x \cdot 2 - 2 \cdot x = 0$. (Note that we use 2 and x as both elements of the ring and the module.)

The second statement is also false. Consider $\mathbb{Z}$ as a module over itself. The set $B = \{2, 3\}$ is a generating set for $\mathbb{Z}$ because $\gcd(2, 3) = 1$. In particular, every integer is a linear combination of the two. However, neither $\{2\}$ nor $\{3\}$ are a basis for $\mathbb{Z}$. □

Exercise I.1.6. Prove Lemma 1.8.

Lemma 1.8. *Let $R = k$ be a field, and let V be a k-vector space. Let B be a* minimal *generating set for V; then B is a basis of V.*

Every set generating V contains a basis of V.

Solution. Let B be a minimal generating set for V. Suppose B is not linearly independent. That is, there exists a linear combination

$$c_1 b_1 + \cdots c_t b_t = 0.$$

Since k is a field, we can rearrange the above as

$$b_t = (-c_t^{-1} c_1 b_1) + \cdots + (-c_t^{-1} c_{t-1} b_{t-1}).$$

Then $B' = B \setminus \{b_t\}$ is also a generating set for V, contradicting the minimality of B. Thus, our assumption is incorrect and B must be linearly independent, meaning it is a basis of V. The proof details a procedure for reducing a generating set to a basis by repeatedly removing elements contained in the span of existing elements in the set. □

Exercise I.1.7. Let R be an integral domain, and let $M = R^{\oplus A}$ be a free R-module. Let K be the field of fractions of R, and view M as a subset of $V = K^{\oplus A}$ in the evident way. Prove that a subset $S \subseteq M$ is linearly independent in M (over R) if and only if it is linearly independent in V (over K). Conclude that the rank of M (as an R-module) equals the dimension of V (as a K-vector space). Prove that if S generates M over R, then it generates V over K. Is the converse true?

Solution. We prove both directions via the contrapositive. Suppose S is linearly dependent in M. That is, there is a linear combination

$$a_1 s_1 + \cdots + a_t s_t = 0.$$

Since $S \subseteq M \subseteq V$, this linear combination also exists in V so S is linearly dependent in V. Thus, if S is linearly independent in V then it must also be linearly independent in M. Now suppose S is linearly dependent in V. Then there is a linear combination

$$\frac{a_1}{b_1} s_1 + \cdots + \frac{a_t}{b_t} s_t = 0.$$

Multiply this linear combination by $b_1 \cdots b_t$ (this exists since the linear combination must be finite). This yields the equation

$$(b_2 \cdots b_t) a_1 s_1 + \cdots + (b_1 \cdots b_{t-1}) a_t s_t = 0$$

which is a linear combination over R, showing that S is linearly dependent in M. Therefore, if S is linearly independent in M then it must be linearly independent in V.

That is, if B is a maximal linearly independent subset of M then it is also a maximal linearly independent subset of V (AKA a basis) so the rank of M and the dimension of V are equal.

Suppose S generates M over R and let $\frac{a}{b} \in V$. There exists a linear combination

$$r_1 s_1 + \cdots + r_t s_t = a.$$

Since $\frac{r_i}{b} \in K$, we find that

$$\frac{r_1}{b} s_1 + \cdots + \frac{r_t}{b} s_t = \frac{a}{b}$$

so S generates V over K.

The converse is not true. Consider $R = \mathbb{Z}$, $K = \mathbb{Q}$, $M = V = \mathbb{Z}$. Certainly $S = \{2\}$ generates V over K since for any element $n \in \mathbb{Z}$ we have $n = \frac{n}{2} \cdot 2$. However, S does not generate M over R. □

Exercise I.1.8. Deduce Corollary 1.11 from Proposition 1.9.

Corollary 1.11. *Let R be an integral domain, and let A, B be sets. Then*

$$F^R(A) \cong F^R(B) \iff \textit{there is a bijection } A \cong B.$$

Solution. Clearly if $A \cong B$ then the two sets have the same order so $F^R(A)$ and $F^R(B)$ are merely $|A|$ copies of R, so they must be isomorphic. For the other direction, let A be a basis for $F^R(A)$ and let B be a basis for $F^R(B)$. Then A is also a basis for $F^R(B)$, just as B is a basis for $F^R(A)$. But by Proposition 1.9, we have $|A| \leq |B|$ and $|B| \leq |A|$ so $|A| = |B|$ and the two sets are isomorphic. □

Exercise I.1.9. Let R be a commutative ring, and let M be an R-module. Let $\mathfrak{m}$ be a maximal ideal in R, such that $\mathfrak{m}M = 0$ (that is, $rm = 0$ for all $r \in \mathfrak{m}, m \in M$). Define in a natural way a vector space structure over $R/\mathfrak{m}$ on M.

Solution. For M to be a vector space over $R/\mathfrak{m}$, we require multiplication to be well-defined. That is, we should have $rm = (r + \mathfrak{m})m$, or $\mathfrak{m}m = 0$. Since this is the case, M inherits a vector space structure from the module structure on R. In particular, recall that $M/\mathfrak{m}M$ has a module structure over $R/\mathfrak{m}$. However, we also have that $\mathfrak{m}M = 0$ so $M \cong M/\mathfrak{m}M$. □

Exercise I.1.10. Let R be a commutative ring, and let $F = R^{\oplus B}$ be a free module over R. Let $\mathfrak{m}$ be a maximal ideal of R, and let $k = R/\mathfrak{m}$ be the quotient field. Prove that $F/\mathfrak{m}F \cong k^{\oplus B}$ as k-vector spaces.

Solution. Consider the natural homomorphism $\varphi : F \to k^{\oplus B}$ which sends each component to its residue class mod $\mathfrak{m}$. The kernel of this homomorphism is the set of elements in F which are in $\mathfrak{m}$, or $\mathfrak{m}F$. Thus, by the first isomorphism theorem for modules, we have

$$\frac{F}{\mathfrak{m}F} \cong k^{\oplus B}$$

and we are done. □

Exercise I.1.11. Prove that commutative rings satisfy the IBN property. (Use Proposition V.3.5 and Exercise 1.10.)

Solution. Recall that the IBN (Invariant Basis Number) property is the property that $R^m \cong R^n \iff m = n$. One direction is trivial so we only consider the other direction. Let R be a commutative ring and suppose $R^m \cong R^n$. Furthermore, let $\mathfrak{m}$ be a maximal ideal of R^m (its existence is guaranteed by Proposition V.3.5). The isomorphism of modules $R^m \cong R^n$ induces an isomorphism of vector spaces $(R/\mathfrak{m})^m \cong (R/\mathfrak{m})^n$. Since these two finite-dimensional vector fields are isomorphic, it must be the case that $m = n$. □

Exercise I.1.12. Let V be a vector space over a field k, and let $R = \mathrm{End}_{k\text{-Vect}}(V)$ be its ring of endomorphisms (cf. Exercise III.5.9). (Note that R is *not* commutative in general.)

- Prove that $\mathrm{End}_{k\text{-Vect}}(V \oplus V) \cong R^4$ as an R-module.
- Prove that R does not satisfy the IBN property if $V = k^{\oplus \mathbb{N}}$.

(Note that $V \cong V \oplus V$ if $V = k^{\oplus \mathbb{N}}$.)

Solution. The endomorphism ring $\mathrm{End}_{k\text{-Vect}}(V \oplus V)$ may be thought of as the set of 2×2 matrices whose entries are themselves endomorphisms of V. That is, we have the picture

$$\mathrm{End}_{k\text{-Vect}}(V \oplus V) \cong \begin{bmatrix} \mathrm{End}_{k\text{-Vect}}(V) & \mathrm{End}_{k\text{-Vect}}(V) \\ \mathrm{End}_{k\text{-Vect}}(V) & \mathrm{End}_{k\text{-Vect}}(V) \end{bmatrix}$$

and clearly the set of matrices on the right are isomorphic to R^4. This interpretation of the endomorphism of a direct product comes from thinking of mapping the basis of each copy of V, except they can interact with each other.

If $V = k^{\oplus \mathbb{N}}$, then we find $R \cong \mathrm{End}_{k\text{-Vect}}(V \oplus V) \cong R^4$ so R does not satisfy the IBN property. □

Exercise I.1.13. Let A be an abelian group such that $\mathrm{End}_{\mathrm{Ab}}(A)$ is a field of characteristic 0. Prove that $A \cong \mathbb{Q}$. (Hint: Prove that A carries a $\mathbb{Q}$-vector space structure; what must its dimension be?)

Solution. Recall that a field of characteristic 0 must contain a copy of $\mathbb{Q}$ (Exercise V.4.17). Thus, A has the structure of a $\mathbb{Q}$-vector space. Recall that $\text{End}(A \oplus B)$ can be thought of as the set of 2×2 matrices of the form

$$\begin{bmatrix} \text{End}(A) & \text{Hom}(B, A) \\ \text{Hom}(A, B) & \text{End}(B) \end{bmatrix}$$

so that homomorphisms from A and B interact with each other. Suppose $\dim(A) > 1$ so we can write $\text{End}(A) = \text{End}(\mathbb{Q}^m \oplus \mathbb{Q}^n)$ with $m, n \geq 1$. Note that the description of $\text{End}(A \oplus B)$ means this ring is not a field. Indeed, consider the matrix

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

which is nilpotent and has determinant zero. It is clearly non-invertible, so this contradicts the assumption that $\text{End}(A)$ is a field. Hence, it must be the case the $\dim(A) = 1$ so $A \cong \mathbb{Q}$. □

Exercise I.1.14. Let V be a finite-dimensional vector space, and let $\varphi : V \to V$ be a homomorphism of vector spaces. Prove that there is an integer n such that $\ker \varphi^{n+1} = \ker \varphi^n$ and $\text{im } \varphi^{n+1} = \text{im } \varphi^n$.

Show that both claims may fail if V has infinite dimension.

Solution. Consider the following chain of vector spaces

$$V \supseteq \varphi(V) \supseteq \varphi^2(V) \supseteq \cdots$$

where each step either preserves or lowers the dimension of the vector space. Since V is finite-dimensional, the dimension cannot keep decreasing. Thus, there exists some integer m such that $\varphi^m(V) = \varphi^{m+1}(V)$.

Similarly, we have the chain of vector spaces

$$0 \subseteq \ker \varphi \subseteq \ker \varphi^2 \subseteq \cdots$$

where each step either preserves or increases the dimension of the vector space. Since V is finite-dimensional, the dimension cannot keep increasing. Thus, there exists some integer m' such that $\ker \varphi^{m'} = \ker \varphi^{m'+1}$. Finally, we only need to set $n = \max\{m, m'\}$.

For a counterexample in the case of infinite dimension, let $V = \mathbb{Q}^{\oplus \mathbb{N}}$ and consider φ which maps a_i to a_{i+1}. Clearly the image of φ is smaller each iteration, but it never terminates for a finite integer. Similarly, the kernel of φ increases each iteration, but it doesn't terminate for a finite integer. □

Exercise I.1.15. Consider the question of Exercise 1.14 for free R-modules F of finite rank, where R is an integral domain that is not a field. Let $\varphi : F \to F$ be an R-module homomorphism.

What property of R immediately guarantees that $\ker \varphi^{n+1} = \ker \varphi^n$ for $n \gg 0$?

Show that there is an R-module homomorphism $\varphi : F \to F$ such that $\operatorname{im} \varphi^{n+1} \subsetneq \operatorname{im} \varphi^n$ for all $n \geq 0$.

Solution. To do. □

Exercise I.1.16. Let M be a module over a ring R. A *finite composition series* for M (if it exists) is a decreasing sequence of submodules

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

in which all quotients M_i/M_{i+1} are *simple* R-modules (cf. Exercise III.5.4). The *length* of a series is the number of strict inclusions. The *composition factors* are the quotients M_i/M_{i+1}.

Prove a Jordan-Hölder theorem for modules; any two finite composition series of a module have the same length and the same (multiset of) composition factors. (Adapt the proof of Theorem IV.3.2.)

We say that M has *length m* if M admits a finite composition series of length m. This notion is well-defined as a consequence of the result you just proved.

Solution. Let

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

be a composition series. We prove this by induction on m. If $m = 0$, then M is trivial so there is nothing to prove. Assume $m > 0$ and let

$$M = M_0' \supsetneq M_1' \supsetneq \cdots \supsetneq M_m' = \langle 0 \rangle$$

be another composition series for M. If $M_1 = M_1'$ then the result follows from the induction hypothesis since M_1 has length $m - 1 < m$.

Thus, we may assume $M_1 \neq M_1'$. Then, since M_1 and M_1' are maximal in M, we must have $M_1 + M_1' = M$. Let $K = M_1 \cap M_1'$ and consider the composition series

$$K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r = \langle 0 \rangle.$$

By the isomorphism theorems for modules, we have

$$\frac{M_1}{K} = \frac{M_1}{M_1 \cap M_1'} \cong \frac{M_1 + M_1'}{M_1'} = \frac{M}{M_1'}, \quad \frac{M_1'}{K} \cong \frac{M}{M_1}$$

are simple modules. Then we can construct new composition series for M, namely

$$M \supsetneq M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \langle 0 \rangle$$

and

$$M \supsetneq M_1' \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \langle 0 \rangle$$

which only differ in the first step. These two series have the same length and the same quotients.

Now we show that the first of these two series has the same length and quotients as the original series. We can see that

$$M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r$$

is a composition series for M_1. By the induction hypothesis, it must have the same length and quotients as

$$M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_m$$

proving our claim.

Similarly, we can show that

$$M_1' \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r$$

has the same length and quotients as

$$M_1' \supsetneq M_2' \supsetneq \cdots \supsetneq M_m'.$$

Thus, the statement follows. □

Exercise I.1.17. Prove that a k-vector space V has finite length as a module over k (cf. Exercise 1.16) if and only if it is finite-dimensional and that in this case its length equals its dimension.

Solution. Suppose V is finite-dimensional and let B be a basis for V. Then we may construct the composition series

$$V = \operatorname{span}(B) \supsetneq \operatorname{span}(B \setminus \{b_1\}) \supsetneq \operatorname{span}(B \setminus \{b_1, b_2\}) \supsetneq \cdots \supsetneq \operatorname{span}(\emptyset) = \langle 0 \rangle$$

which has finite length this B is finite. It is evident from this construction that the length of V is equal to its dimension.

If V has finite length as a module over k, consider a composition series

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_n = \langle 0 \rangle$$

of length n. Suppose V is not finite dimensional and let $B = \{v_1, \ldots, v_n\}$ be a linearly independent set. Then there exists a $v_{k+1} \in V \setminus B$ such that $B \cup \{v_{k+1}\}$ is still linearly independent. But then we may repeat this and construct a composition series for V of infinite length, contradicting our assumption that V has finite length. Thus, V must be finite dimensional (and as shown above, its dimension is equal to its length). □

Exercise I.1.18. Let M be an R-module of finite length m (cf. Exercise 1.16).

- Prove that every submodule N of M has finite length $n \leq m$. (Adapt the proof of Proposition IV.3.4.)

- Prove that the 'descending chain condition' (d.c.c.) for submodules holds in M. (Use induction on the length.)

- Prove that if R is an integral domain that is not a field and F is a free R-module, then F has finite length if and only if it is the 0-module.

Solution. Assume M has a composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

and let N be a submodule of M. Consider the series

$$N = M \cap N \supsetneq M_1 \cap N \supsetneq \cdots \supsetneq M_m \cap N = \langle 0 \rangle.$$

We claim that this is a composition series for N. To verify this, we only need to show that

$$\frac{M_i \cap N}{M_{i+1} \cap N}$$

is either trivial or isomorphic to M_{i+1}/M_i. To see that this is true, consider the homomorphism

$$M_i \cap N \hookrightarrow M_i \twoheadrightarrow \frac{M_i}{M_{i+1}}$$

which clearly has kernel $M_{i+1} \cap N$. By the first isomorphism theorem, we have an injective homomorphism

$$\frac{M_i \cap N}{M_{i+1} \cap N} \hookrightarrow \frac{M_i}{M_{i+1}}$$

which identifies the former with a submodule of the latter. Since the latter is a simple module, our claim follows. Furthermore, removing the trivial quotients forces the length of N to be less than or equal to that of M.

Now we prove that M satisfies the d.c.c. for submodules. We show the much stronger result that every chain of submodules of M can be refined to a composition series for M. Let

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_k = \langle 0 \rangle$$

be a chain of submodules of M. We know $k \leq m$ by the Jordan-Hölder theorem for modules. If $k = m$ then we already have a composition series so suppose $k < n$. Then there exists some i such that M_i/M_{i+1} is not a simple module. That is, there exists a submodule M_i' such that $M_i \supsetneq M_i' \supsetneq M_{i+1}$ and we obtain a chain of length $k + 1$. If $k + 1 = n$, then we are done. Otherwise, we may repeat until we have constructed a chain of length n, at which point we have constructed a composition series for M. This result implies our claim because for any descending chain of submodules of M, we may extend it into a composition series of M. This series is certainly bounded, so the original descending chain must stabilize.

Finally, suppose R is an integral domain that is not a field and let F be a free $R-$ module. Clearly if $F = \langle 0 \rangle$ then it has finite length. Now suppose F has finite length and recall that $F \cong R^n$. Suppose $n \geq 1$. Since F has finite length, it satisfies the d.c.c. for submodules. In particular, it satisfies the d.c.c. for ideals of R, so R is an Artinian ring. However, by Exercise V.1.10, an integral domain is Artinian if and only if it is a field, contradicting our hypothesis. Thus, $F \cong R^0 = \langle 0 \rangle$. □

Exercise I.1.19. Let k be a field, and let $f(x) \in k[x]$ be any polynomial. Prove that there exists a multiple of $f(x)$ in which all exponents of nonzero monomials are *prime* integers. (Example: for $f(x) = 1 + x^5 + x^6$,

$$(1 + x^8 + x^6)(2x^2 - x^3 + x^5 - x^8 + x^9 - x^{10} + x^{11}) \\ = 2x^2 - x^3 + x^5 + 2x^7 + 2x^{11} - x^{13} + x^{17}.)$$

(Hint: $k[x]/(f(x))$ is a finite-dimensional k-vector space.)

Solution. The vector space $V = k[x]/(f(x))$ has finite dimension, say n. Take the monomials

$$x^{p_1}, x^{p_2}, \ldots, x^{p_{n+1}}$$

where p_i is an arbitrary prime integer and consider their remainders mod f as elements of V. Since there are $n+1$ elements, they must be linearly dependent. That is, there exist $a_i \in k$ such that

$$h(x) = a_1 x^{p_1} + a_2 x^{p_2} + \cdots + a_{n+1} x^{p_{n+1}}$$

where $h(x) \in (f(x))$. That is, $h(x)$ is a multiple of $f(x)$ in which all exponents of nonzero monomials are prime integers. □

Exercise I.1.20. Let A, B be sets. Prove that the free groups $F(A), F(B)$ are isomorphic if and only if there is a bijection $A \cong B$. (For the interesting direction: remember that $F(A) \cong F(B) \implies F^{ab}(A) \cong F^{ab}(B)$, by Exercise II.7.12). This extends the result of Exercise II.7.13 to possibly infinite sets A, B.

Solution. It is clear that if $A \cong B$, then the corresponding free groups are isomorphic. Suppose $F(A) \cong F(B)$ and recall that this implies $F^{ab}(A) \cong F^{ab}(B)$. Note that both of these groups are free $\mathbb{Z}$-modules. However, if they are isomorphic, then it must the case that there is a bijection between their bases. That is, $A \cong B$. □

I.2 Homomorphisms of free modules, I

Exercise I.2.1. Prove that the subset of $\mathcal{M}_2(R)$ consisting of matrices of the form

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

is a group under matrix multiplication and is isomorphic to $(R, +)$.

Solution. It is evident that the identity of this group is the identity matrix I_2. Furthermore, it is closed under multiplication:

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ r+s & 1 \end{pmatrix}$$

and since R is closed under addition, this matrix is contained in the group. The multiplication makes it evident that inverse elements have the form

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

where $-r$ is the additive inverse of $r \in R$. The isomorphism is also evident; simply identify

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

and the inverse homomorphism is just as clear. □

Exercise I.2.2. Prove that matrix multiplication is associative.

Solution. Let A be a $m \times n$ matrix, B a $n \times p$ matrix, and C a $p \times q$ matrix. Let $R = AB$ and $S = (AB)C$. We have

$$\begin{aligned} s_{ij} &= \sum_{k=1}^{p} r_{ik} c_{kj} \\ &= \sum_{k=1}^{p} \left(\sum_{l=1}^{n} a_{il} b_{lk} \right) c_{kj} \\ &= \sum_{k=1}^{p} \sum_{l=1}^{n} a_{il} b_{lk} c_{kj} \end{aligned}$$

where the third equality follows from distributivity of multiplication over addition in R. Now let $R = BC$ and $S = A(BC)$. We have

$$\begin{aligned} s_{ij} &= \sum_{l=1}^{n} a_{il} r_{lj} \\ &= \sum_{l=1}^{n} a_{il} \left(\sum_{k=1}^{p} b_{lk} c_{kj} \right) \\ &= \sum_{l=1}^{n} \sum_{k=1}^{p} a_{il} b_{lk} c_{kj} \end{aligned}$$

where the last equality follows from distributivity of multiplication over addition. Finally, the associativity of multiplication and commutativity of addition in R shows that these two sums are equal, so $(AB)C = A(BC)$. □

Exercise I.2.3. Prove that both $\mathcal{M}_n(R)$ and $\mathrm{Hom}_R(R^n, R^n)$ are R-algebras in a natural way and the bijection $\mathrm{Hom}_R(R^n, R^n) \cong \mathcal{M}_n(R)$ of Corollary 2.2 is an isomorphism of R-algebras. In particular, if the matrix M corresponds to the homomorphism $\varphi : R^n \to R^n$, then M is invertible in $\mathcal{M}_n(R)$ if and only if φ is an isomorphism.

Solution. Indeed, $\mathcal{M}_n(R)$ is a ring under component addition and matrix multiplication. It is an R-algebra because for all $r \in R$ and $A, B \in \mathcal{M}_n(R)$, we have

$$r \cdot (AB) = (r \cdot A)B = A(r \cdot B)$$

by the properties of scalar multiplication of matrices. Showing that $\mathrm{Hom}_R(R^n, R^n)$ is an R-algebra amounts to a similar, but more notationally heavy, computation. Recall that the bijection ϕ between the two sets sends a matrix A to the homomorphism φ defined as $\varphi(v) = Av$. To show it is an isomorphism, we only need to show that it is an algebra homomorphism. Indeed, we have (with slight abuse of notation at some points)

- $\phi(I_n)(v) = I_n v = \mathrm{id}$
- $\phi(r \cdot A)(v) = (r \cdot A)(v) = r \cdot (Av) = r \cdot \varphi(A)$
- $\phi(A + B)(v) = (A + B)(v) = Av + Bv = \varphi(A) + \varphi(B)$
- $\phi(AB)(v) = (AB)(v) = A(Bv) = \varphi(A) \circ \varphi(B)$

so the bijection is a homomorphism of R-algebras, making it an isomorphism. The statement regarding when a matrix is invertible follows immediately. I am curious as to how this aligns with the determinant. □

Exercise I.2.4. Prove Corollary 2.2.

Corollary 2.2. *The correspondence introduced in Lemma 2.1 gives an isomorphism of R-modules*

$$\mathcal{M}_{m,n}(R) \cong \mathrm{Hom}_R(R^n, R^m).$$

Solution. Indeed, the correspondence in Lemma 2.1 is bijective; all matrices $M \in \mathcal{M}_{m,n}(R)$ are mapped to a homomorphism $\varphi \in \mathrm{Hom}_R(R^n, R^m)$ and all homomorphisms are mapped to a matrix. We checked above that the two sets are isomorphic as R-algebras so they must be isomorphic as R-modules. □

Exercise I.2.5. Give a formal argument proving Proposition 2.7.

Proposition 2.7. *Two matrices $P, Q \in \mathcal{M}_{m,n}(R)$ are equivalent if Q may be obtained from P be a sequence of elementary operations.*

Solution. We will only treat the case of elementary row operations. To switch the i- and j-th rows of an $m \times n$ matrix, consider the identity matrix with the i- and j-th rows switched. Similarly, to add a multiple of the i-th row to the j-th row, consider the identity matrix with the entry c at position i, j. To multiply all entries in the i-th row of a matrix by a unit of R, consider the identity matrix with the entry in the i-th row replaced by a unit r. We verify that each of these matrices is invertible.

In the first case, we show the corresponding homomorphism is an isomorphism. Suppose we have two vectors u and v such that $\varphi(u) = \varphi(v)$. Then certainly switching the corresponding rows of these vectors preserves equality. Similarly, all vectors in R^n are in the image of φ by simply switching the rows of the desired elements.

In the second case, we explicitly construct an inverse matrix. Namely, consider the identity matrix with the entry $-c$ at position i, j. Clearly this subtracts the multiple of the i-th row from the j-th row and hence inverts the transformation of the original matrix.

For the third example, we use the fact that r is a unit and hence has an inverse r^{-1}. Then the identity matrix with the entry in the i-th row replaced by r^{-1} is an explicit realization of the inverse.

Since each of these matrices is invertible, the corresponding homomorphisms are all isomorphisms and preserve the "action" of matrices P and Q. □

Exercise I.2.6. A matrix with entries in a field is in *row echelon form* if

- its nonzero rows are all above the zero rows and
- the leftmost nonzero entry of each row is 1, and it is strictly to the right of the leftmost nonzero entry of the row above it.

The matrix is further in *reduced* row echelon form if

- the leftmost nonzero entry of each row is the only nonzero entry in its column.

The leftmost nonzero entries in a matrix in row echelon form are called *pivots*.

Prove that any matrix with entries in a field can be brought into reduced echelon form by a sequence of elementary operations on *rows*. (This is what is more properly called *Gaussian elimination*.)

Solution. Let $A = (a_{ij})$ be a $m \times n$ matrix over a field. We start by appropriately switching all zero rows to the bottom of the matrix. Recalling our elementary row operations, we may multiply the first row by a_{11}^{-1} and subtract necessary multiples of the first row, yielding

$$\begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

From here, we may repeat by multiplying the second row by a_{22}^{-1} and subtracting necessary multiples from all rows below it, switching zero rows to the bottom as they appear. This process eventually terminates and yields a matrix in row echelon form. □

Exercise I.2.7. Let M be a matrix with entries in a field and in reduced row echelon form (Exercise 2.6). Prove that if a row vector $\boldsymbol{r}$ is a linear combination $\sum a_i r_i$ of the nonzero rows of M, then a_i equals the component of $\boldsymbol{r}$ at the position corresponding to the pivot on the i-th row of M. Deduce that the nonzero rows of M are linearly independent.

Solution. Let b_i be the component of $\boldsymbol{r}$ at the position corresponding to the pivot of the i-th row of M. Suppose the pivot of the i-th row is located in the j-th column. Then $b_i = a_i \cdot 1$ because the only nonzero entry in the j-th column is 1 (since M is in reduced echelon form). Thus, $a_i = b_i$.

If $\boldsymbol{r}$ is the zero vector, then it must be the case that each a_i is 0. That is, the nonzero rows of M are linearly independent. Thus, □

Exercise I.2.8. Two matrices M, N are *row-equivalent* if $M = PN$ for an invertible matrix P. Prove that this is indeed an equivalence relation, and that two matrices with entries in a field are row-equivalent if and only if one may be obtained from the other by a sequence of elementary operations on rows.

Solution. Let $M \sim N$ denote row-equivalent matrices. Clearly $M \sim N$ as $M = IM$. If $M \sim N$ then we have $M = PN$ for some invertible matrix P. But then we have $N = P^{-1}M$ so $N \sim P$. Finally, if $M \sim N$ and $N \sim P$, we have

$M = RN$ and $P = SN$. Then $M = RS^{-1}P$, and RS^{-1} is clearly invertible so $M \sim P$. Thus, row-equivalence is an equivalence relation.

The second part of the claim follows from the fact that $GL_n(k)$, the group of invertible matrices of a field, is generated by elementary matrices, which are themselves invertible (obviously). □

Exercise I.2.9. Let k be a field, and consider row-equivalence (Exercise 2.8) on the set of $m \times n$ matrices $\mathcal{M}_{m,n}(k)$. Prove that each equivalence class contains exactly one matrix in reduced row echelon form (Exercise 2.6). (Hint: To prove uniqueness, argue by contradiction. Let M, N be different row-equivalent reduced row echelon matrices; assume that they have the minimum number of columns with this property. If the leftmost column at which M and N differ is the k-th column, use the minimality to prove that M, N may be assumed to be of the form

$$\left(\begin{array}{c|c} I_{k-1} & * \\ \hline 0 & * \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} I_{k-1} & * \end{array}\right).$$

Use Exercise 2.7 to obtain a contradiction.)

The unique matrix in reduced row echelon form that is row-equivalent to a given matrix M is called the *reduced echelon form* of M.

Solution. Certainly each each equivalence class is nonempty as it contains a matrix of the form

$$\left(\begin{array}{c|c} I_{k-1} & * \\ \hline 0 & 0 \end{array}\right)$$

Now suppose M, N are different row equivalent matrices in reduced row echelon form with the minimum number of columns. Suppose the leftmost column at which M and N differ is the k-th column. Construct two matrices M' and N' by selecting all columns with pivot elements to the left of the k-th column, along with the k-th column. Then we have M' and N' are of the form

$$\left(\begin{array}{c|c} I_{k-1} & * \\ \hline 0 & * \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} I_{k-1} & * \end{array}\right)$$

(the case depends on whether $k > n$). Then M' and N' are row equivalent since we are only adjusting columns and we assumed M and N are row equivalent. In either case, the rows of M' and N' are linearly independent so it must be the case that $M' = N'$ and $M = N$. □

Exercise I.2.10. The *row space* of a matrix M is the span of its rows; the *column space* of M is the span of its columns. Prove that row-equivalent matrices have the same row space and isomorphic column spaces.

Solution. Recall that M and N are row-equivalent if there exists an invertible matrix P such that $M = PN$. Then the rows of M are a linear combination of the rows of N. If x is in the span of the rows of M then it is a linear combination of the rows of M. But then it is also a linear combination of the rows of N so the row space of M is a subset of the row space of N. Similarly, since $N = P^{-1}M$, the row space of N is a subset of the row space of M so the two are equal.

By Exercise 2.9, M and N have the same reduced echelon form. Furthermore, the dimension of the column space of a matrix is given by the number of pivot columns in its reduced echelon form since row operations preserve linear relations between columns. Thus, the column space of M and N have the same dimension so they are isomorphic as vector spaces. □

Exercise I.2.11. Let k be a field and $M \in \mathcal{M}_{m,n}(k)$. Prove that the dimension of the space spanned by the rows of M equals the number of nonzero rows in the reduced echelon form of M (cf. Exercise 2.9).

Solution. Note that the reduced echelon form of M can be obtained through a sequence of elementary operations. That is, if N is the reduced echelon form of M, then we have $N = PM$ so the two are row-equivalent. By Exercise 2.10, the two matrices have the same row space. Finally, the dimension of the row space is equal to the number of nonzero rows in the reduced echelon form of M (since the nonzero rows contain pivot elements). Thus, the dimension of the row space of M is equal to the number of nonzero rows in N. □

Exercise I.2.12. Let k be a field, and consider row-equivalence on $\mathcal{M}_{m,n}(k)$ (Exercise 2.8). By Exercise 2.10, row-equivalent matrices have the same row space. Prove that, conversely, there is exactly one row-equivalence class in $\mathcal{M}_{m,n}(k)$ for each subspace of k^n of dimension $\leq m$.

Solution. Given a subspace V of dimension $d \leq n$, we know the row-equivalence class is nonempty since it contains the matrix whose rows are a basis of V, call it A. Suppose we have a second matrix B whose row space is V. Since the two are row-equivalent, we have that for all $x \in k^n$, there exists $y \in k^n$ such that $x^t A = y^t B$. In particular, let $e_i \in k^n$ for $1 \leq i \leq n$ denote the standard basis of k^n and let $y_i \in k^n$ satisfy $e_i^t A = y_i^t B$ (in such a way that the y_i are linearly independent). Construct a matrix P such that the i-th row of P is y_i. Then clearly we have $A = PB$ for an invertible matrix P so the two are row-equivalent. □

Exercise I.2.13. The set of subspaces of given dimension in a fixed vector space is called a *Grassmannian*. In Exercise 2.12 you have constructed a bijection between the Grassmannian of r-dimensional subspaces of k^n and the set of reduced row echelon matrices with n columns and r nonzero rows.

For $r = 1$, the Grassmannian is called the *projective space*. For a vector space V, the corresponding projective space $\mathbb{P}V$ is the set of 'lines' (1-dimensional subspaces) in V. For $V = k^n$, $\mathbb{P}V$ may be denoted $\mathbb{P}_k^{n-1}$, and the field k may be omitted if it is clear from the context. Show that $\mathbb{P}_k^{n-1}$ may be written as a union $k^{n-1} \cup k^{n-2} \cup \cdots \cup k^1 \cup k^0$, and describe each of these subsets 'geometrically'.

Thus, $\mathbb{P}^{n-1}$ is the union of n 'cells', the largest one having dimension $n-1$ (accounting for the choice of notation). Similarly, all Grassmannians may be written as unions of cells. These are called *Schubert cells.*

Prove that the Grassmannian of $(n-1)$-dimensional subspaces of k^n admits a cell decomposition entirely analogous to that of $\mathbb{P}_k^{n-1}$. (This phenomenon will be explained in Exercise VIII.5.17.)

Solution. Think of k^{n+1} as $k^n \times k$. Then each line through the origin either intersects $k^n \times \{1\}$ at a unique point or it lies in the hyperplane $k^n \times \{0\}$. Thus, the lines in k^{n+1} are a union of $k^n \times \mathbb{P}^{n-1}$. Repeating inductively shows that $\mathbb{P}_k^{n-1}$ is a union $k^{n-1} \cup \cdots \cup k^1 \cup k^0$ (where the last set is included for the origin itself). Each of these subsets is the hyperplane of lines in k^m. The most tangible example is $\mathbb{R}^3$ and $\mathbb{RP}^2$.

When working with the Grassmannian of n-dimensional subspaces of k^{n+1}, simply consider the line normal to the n-dimensional hyperplane. Clearly the two are in bijection so the cell decomposition is simply reversed. For a more explicit example, consider $\mathbb{R}^3$ and the Grassmannian of 2-dimensional subspaces, or planes. Each plane through the origin has a normal line, and this set of normal lines is equivalent to $\mathbb{RP}^2$. The lines which intersect $\mathbb{R}^2 \times \{0\}$ correspond to planes which contain the vertical copy of $\mathbb{R}$. The intersection of planes not in this set is $\mathbb{R}^0$, while the intersection of the planes in this set is $\mathbb{R}^1$. Repeating once more with the set of planes whose normal lines intersect $\mathbb{R} \times \{0\}$ yields $\mathbb{R}^2$ since there is only one such plane. □

Exercise I.2.14. Show that the Grassmannian $\mathrm{Gr}_k(2,4)$ of 2-dimensional subspaces of k^4 is the union of 6 Schubert cells: $k^4 \cup k^3 \cup k^2 \cup k^2 \cup k^1 \cup k^0$. (Use Exercise 2.12; list all the possible reduced echelon forms.)

Solution. A 2-dimensional subspace of k^4 corresponds to a reduced echelon matrix of rank 2. There are exactly 6 of these, namely:

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Thus, $\mathrm{Gr}_k(2,4)$ decomposes into exactly 6 Schubert cells. Note that the matrix with m free elements corresponds to the Schubert cell k^m. This is because each subspace is characterized by the values of the free elements. In particular, the sixth matrix corresponds with k^0 while the third matrix corresponds with k^2. □

Exercise I.2.15. Prove that a square matrix with entries in a field is invertible if and only if it is equivalent to the identity, if and only if it is row-equivalent to the identity, if and only if its reduced echelon form is the identity.

Solution. Let M be a square matrix with entires in a field. If M is invertible, then it has an inverse M^{-1} such that $I = M^{-1}M$. Since M^{-1} is invertible, M is row-equivalent to the identity.

If M is row-equivalent to the identity, then there exists an invertible matrix P such that $I = PM$. Since P is invertible, it is a product of elementary matrices. That is, a sequence of row operations on P yields the identity, which is in reduced echelon form.

Finally, suppose the reduced echelon form of M is the identity. Then there is a sequence of row operations which transform M into the identity. This sequence of row operations can be expressed as a product of elementary matrices. This product of elementary matrices is the inverse of M, so M is invertible. □

Exercise I.2.16. Prove Proposition 2.10.

Proposition 2.10. *Over a field, every $m \times n$ matrix is equivalent to a matrix of the form*

$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

(where $r \leq \min(m, n)$ and '0' stands for null matrices of appropriate sizes).

Solution. Let M be an $m \times n$ matrix over a field with rank r. After appropriate row operations, we may assume the first r rows of M are linearly independent. Then we may apply Gaussian elimination to the first r rows to obtain a matrix of the form

$$\left(\begin{array}{c|c} I_r & * \\ \hline * & * \end{array}\right)$$

Add appropriate linear combinations of the first r columns to eliminate the top right block. Since the remaining $m - r$ rows are linearly dependent, they must be a linear combination of the first r rows. Thus, the bottom right block must also be zero. Finally, the proper linear combination of the first r rows will eliminate the bottom left block. What remains is a matrix of the form stated in the problem. □

Exercise I.2.17. Prove Proposition 2.11.

Proposition 2.11. *Let R be a Euclidean domain, and let $P \in \mathcal{M}_{m,n}(R)$. Then P is equivalent to a matrix of the form*

$$\left(\begin{array}{ccc|c} d_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & d_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$$

with $d_1 \mid \cdots \mid d_r$.

Solution. Let M be an $m \times n$ matrix over a Euclidean domain with rank r. After appropriate row operations, we may assume the first r rows of M are linearly independent. Following the Euclidean algorithm, we may add multiples of other rows to ensure that a_{11} is the gcd of the entries in the first column. Adding appropriate multiples of this row to the remaining rows and multiples of this column to the remaining columns yields a matrix of the form

$$\begin{pmatrix} \begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{array} \end{pmatrix}$$

where M' is an $(m-1) \times (n-1)$ matrix with rank $r-1$.

Repeating this process on M' and on subsequent matrices yields a matrix of the form stated in the problem. Now we only need to show that $d_1 \mid \cdots \mid d_r$, for which we take inspiration from the text. Indeed, suppose $d_i \nmid d_{i+1}$. Then we may add the $(i+1)$-th row to the i-th row and repeat the process. Ultimately, we must reach the condition $d_i \mid d_{i+1}$. □

Exercise I.2.18. Suppose $\alpha : \mathbb{Z}^3 \to \mathbb{Z}^2$ is represented by the matrix

$$\begin{pmatrix} -6 & 12 & 18 \\ -15 & 36 & 54 \end{pmatrix}$$

with respect to the standard bases. Find bases of $\mathbb{Z}^3, \mathbb{Z}^2$ with respect to which α is given by a matrix of the form obtained in Proposition 2.11.

Solution. Applying the algorithm described above, we find that applying the following change of basis yields a matrix in the Smith normal form:

$$\begin{pmatrix} 2 & -1 \\ 10 & -4 \end{pmatrix} \begin{pmatrix} -6 & 12 & 18 \\ -15 & 36 & 54 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 3 \\ 0 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}$$

so the above matrices are the bases with which α is given in the Smith normal form. Interestingly, the inverses of these matrices are not elements of $\mathbb{Z}^3$ or $\mathbb{Z}^2$ respectively. □

Exercise I.2.19. Prove Corollary IV.6.5 again as a corollary of Proposition 2.11. In fact, prove the general fact that every *finitely generated* abelian group is a direct sum of cyclic groups.

Solution. Let G be a finitely generated abelian group. Then G is a quotient of $\mathbb{Z}^n$ by a finitely generated free abelian group, say F, and F is a free $\mathbb{Z}$-module. Consider a matrix M whose rows are composed of a basis for F. By Proposition 2.11, M is equivalent to a matrix in the Smith normal form. That is, there is a basis $\{d_1e_1, \dots, d_re_r\}$ for F such that $d_i \mid d_{i+1}$. Then

$$F = d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z}$$

so we find

$$G = \frac{\mathbb{Z}^n}{F} = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}}$$

and G is a direct sum of cyclic groups. □

I.3 Homomorphisms of free modules, II

Exercise I.3.1. Use Gaussian elimination to find all integer solutions of the system of equations

$$\begin{cases} 7x - 36y + 12z = 1, \\ -8x + 42y - 14z = 2. \end{cases}$$

Solution. Transforming the system of equations into a matrix and applying Gaussian elimination yields the factorization

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 6 \\ -8 & -7 \end{pmatrix} \cdot \begin{pmatrix} 7 & -36 & 12 \\ -8 & 42 & -14 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 4 & -3 \end{pmatrix},$$

or $D = M \cdot A \cdot N$. As we are trying to solve $A\boldsymbol{x} = \boldsymbol{b}$, we now can now solve $D\boldsymbol{y} = M\boldsymbol{b}$. Finally, we solve $\boldsymbol{x} = N\boldsymbol{y}$ for a solution of

$$\boldsymbol{x} = \begin{pmatrix} 19 \\ -11 - z \\ -44 - 3z \end{pmatrix}$$

so there are infinitely many solutions based on the free variable z. □

Exercise I.3.2. Provide details for the proof of Lemma 3.2.

Lemma 3.2. *Let A be a square matrix with entries in an integral domain R.*

- *Let A' be obtained from A by switching two rows or two columns. Then* $\det(A') = -\det(A)$.
- *Let A' be obtained from A by adding to a row (column) a multiple of another row (column). Then* $\det(A') = \det(A)$.

- *Let A' be obtained from A by multiplying a row (column) by an element $c \in R$. Then* $\det(A') = c\det(A)$.

In other words, the effect of an elementary operation on $\det A$ *is the same as multiplying* $\det A$ *by the determinant of the corresponding matrix.*

Solution. Switching two rows is equivalent to multiplying each $\sigma \in S_n$ by a fixed transposition. Then the sign of each permutation is switched so we have

$$\det(A') = \sum_{\sigma \in S_n} (-1)^{\sigma+1} \prod_{i=1}^{n} a_{i\sigma(i)} = -\det(A)$$

yielding the desired result.

For the third point, each product has exactly one c in it so we find

$$\det(A') = \sum_{\sigma \in S_n} (-1)^{\sigma} c \prod_{i=1}^{n} a_{i\sigma(i)} = c\det(A)$$

yielding the desired result.

For the second point, note that $A' = (a_1, a_2, \dots, a_i + ka_j, \dots, a_n)$ so A and A' differ at only one row. Then we have

$$\begin{aligned} \det(A') &= \det(A) + \det(a_1, a_2, \dots, ka_j, \dots, a_n) \\ &= \det(A) + k\det(a_1, a_2, \dots, a_j, \dots, a_n). \end{aligned}$$

But then rows i and j are identical in the second matrix so it follows that the determinant of that matrix is 0. Thus, we are left with $\det(A') = \det(A)$. □

Exercise I.3.3. Redo Exercise II.8.8.

Exercise II.8.8. Prove that $\mathrm{SL}_n(\mathbb{R})$ is a *normal subgroup* of $\mathrm{GL}_n(\mathbb{R})$, and 'compute' $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ as a well-known group.

Solution. Recall that $\mathrm{SL}_n(\mathbb{R})$ is the set of $n \times n$ matrices with determinant 1. Certainly this is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$ since it is the kernel of the homomorphism induced by det from $\mathrm{GL}_n(\mathbb{R})$ to $\mathbb{R}^\times$. Then by the first isomorphism theorem, we find that $\mathbb{R}^\times \cong \mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$. □

Exercise I.3.4. Formalize the discussion of 'universal identities': by what cocktail of universal properties is it true that if an identity holds in $\mathbb{Z}[x_1, \dots, x_r]$, then it holds over every commutative ring R, for every choice of $x_i \in R$? (Is the commutativity of R necessary?)

Solution. This holds because $Z[x_1, \dots, x_r]$ is a free object in the category of commutative rings, or commutative $\mathbb{Z}$-algebras. In particular, for every commutative ring R and set function $f : A \to R$, there exists a unique $\mathbb{Z}$-algebra homomorphism from $\mathbb{Z}[x_1, \dots, x_r]$ to R. If the identity is preserved by homomorphisms, then it will hold in every commutative ring. Furthermore, the commutativity of R is not necessary but it is necessary that given a set-function f, we have $f(a)$ commutes with every element of R for all $a \in A$. □

Exercise I.3.5. Let A be an $n \times n$ square invertible matrix with entries in a field, and consider the $n \times (2n)$ matrix $B = (A \mid I_n)$ obtained by placing the identity matrix to the side of A. Perform elementary row operations on B so as to reduce A to I_n (cf. Exercise 2.15). Prove that this transforms B into $(I_n \mid A^{-1})$.

(This is a much more efficient way to compute the inverse of a matrix than by using determinants as in §3.2.)

Solution. Each elementary row operation on B can be encoded as an elementary matrix whose product reduces A to I_n. That is, we have $PA = I_n$. But then $P = A^{-1}$ and since $PI_n = P$, it must be the case that $B = (I_n \mid P) = (I_n \mid A^{-1})$. □

Exercise I.3.6. Let R be a commutative ring and $M = \langle m_1, \dots, m_r \rangle$ a finitely generated R-module. Let $A \in \mathcal{M}_r(R)$ be a matrix such that $A \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Prove that $\det(A)m = 0$ for all $m \in M$. (Hint: Multiply by the adjoint.)

Solution. Denote the adjoint matrix of A by A'. Recall that $A'A = \det(A)I_n$. Multiplying both sides of the equation by the adjoint yields

$$A'A \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = A' \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\det(A)I_n \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

so $\det(A)m_i = 0$ for all $m_i \in \langle m_1, \dots, m_r \rangle$. Since this is a generating set for M, all $m \in M$ are linear combinations of m_i. Thus, we have $\det(A)m = 0$ for all $m \in M$. □

Exercise I.3.7. Let R be a commutative ring, M a finitely generated R-module, and let J be an ideal of R. Assume $JM = M$. Prove that there exists an element $b \in J$ such that $(1+b)M = 0$. (Let $m_1, \dots, m_r$ be generators for M. Find an $r \times r$ matrix B with entries in J such that $\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = B \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$. Then use Exercise 3.6.)

Solution. Let $\langle m_1, \dots, m_r \rangle$ be a set of generators for M. Since $JM = M$, for all m_j in the generating set, there exists a finite sum

$$m_j = \sum_{i=0}^{r} b_i m_i.$$

Thus, we can construct a matrix B with entries in J such that

$$\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = B \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

which can be rearranged to $(I_r - B)(m_i)^T = 0$. Let $d = \det(I_r - B)$. Then $d \in 1 + J$ since $B \equiv 0 \mod J$. By Exercise 3.7, $dm = 0$ for all $m \in M$. That is, there exists $b \in J$ such that $(1+b)M = 0$. □

Exercise I.3.8. Let R be a commutative ring, M be a finitely generated R-module, and let J be an ideal of R *contained in the Jacobson radical* of R (Exercise V.3.14). Prove that $M = 0 \iff JM = M$. (Use Exercise 3.7. This is *Nakayama's lemma*, a result with important applications in commutative algebra and algebraic geometry. A particular case was given as Exercise III.5.16.)

Solution. If $M = 0$, then clearly for all $b \in J$, we have $bM = 0 = M$ so $JM = M$. Now suppose $JM = M$. Recall that the Jacobson radical of a ring is the intersection of its maximal ideals. By Exercise 3.7, there exists some $b \in J$ such that $(1+b)M = 0$. Then $1 + b$ is a unit in R so multiplying both sides by its inverse yields $M = 0$. □

Exercise I.3.9. Let R be a commutative local ring, that is, a ring with a single maximal ideal $\mathfrak{m}$, and let M, N be finitely generated R-modules. Prove that if $M = \mathfrak{m}M + N$, then $M = N$. (Apply Nakayama's lemma, that is, Exercise 3.8, to M/N. Note that the Jacobson radical of R is $\mathfrak{m}$.)

Solution. If $M = \mathfrak{m}M + N$, then $M/N = \mathfrak{m}M/N$. By Nakayama's lemma, $M/N = 0$ so $M = N$. □

Exercise I.3.10. Let R be a commutative local ring, and let M be a finitely generated R-module. Note that $M/\mathfrak{m}M$ is a finite-dimensional vector space over the field $R/\mathfrak{m}$; let $m_1, \dots, m_r \in M$ be elements whose cosets mod $\mathfrak{m}M$ form a basis of $M/\mathfrak{m}M$. Prove that $m_1, \dots, m_r$ generate M.

(Show that $\langle m_1, \dots, m_r \rangle + \mathfrak{m}M = M$; then apply Nakayama's lemma in the form of Exercise 3.9.)

Solution. We have $\langle \bar{m_1}, \dots, \bar{m_r} \rangle = M/\mathfrak{m}M$, where $\bar{m_i} = m_i \mod \mathfrak{m}M$. That is, $\langle m_1, \dots, m_r \rangle + \mathfrak{m}M = M$. Then, by Exercise 3.9, $\langle m_1, \dots, m_r \rangle = M$. □

Exercise I.3.11. Explain how to use Gaussian elimination to find bases for the row space and the column space of a matrix over a field.

Solution. Recall that Gaussian elimination does not change the row space of the matrix. Then reducing a matrix to reduced echelon form yields a matrix whose rows have the same span as the row space of the original matrix and are linearly independent. Thus, they form a basis for the row space. Similarly, applying Gaussian elimination to the transpose of the matrix yields a basis for the column space. □

Exercise I.3.12. Let R be an integral domain, and let $M \in \mathcal{M}_{m,n}(R)$, with $m < n$. Prove that the columns of M are linearly dependent over R.

Solution. Recall that M represents a homomorphism $f : R^n \to R^m$ and the column space of M is equal to the span of im f. If the columns of M are linearly independent, then the standard basis vectors of R^n map to a linearly independent set in R^m. That is, the rank of R^m must be greater than or equal to that of R^n, or $m \geq n$. Thus, if $n < m$, it must be the case that the columns of M are linearly dependent. □

Exercise I.3.13. Let k be a field. Prove that a matrix $M \in \mathcal{M}_{m,n}(k)$ has rank $\leq r$ if and only if there exist matrices $P \in \mathcal{M}_{m,r}(k), Q \in \mathcal{M}_{r,n}(k)$ such that $M = PQ$. (Thus the rank of M is the smallest such integer.)

Solution. Suppose there exist $P \in \mathcal{M}_{m,r}(k), Q \in \mathcal{M}_{r,n}(k)$ such that $M = PQ$. Let $s = \text{rank } P, t = \text{rank } Q$. Then

$$P = \left(\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right), \quad Q = \left(\begin{array}{c|c} I_t & 0 \\ \hline 0 & 0 \end{array}\right).$$

Including zero rows (columns) to the smaller identity matrix to make block multiplication possible yields

$$M = \left(\begin{array}{c|c} I_{\min(s,t)} & 0 \\ \hline 0 & 0 \end{array}\right)$$

and since $\min(s,t) \leq r$, the rank of $M \leq r$.

Now suppose M has rank $r' \leq r$. Consider the matrices

$$P = \left(\begin{array}{c|c} I_{r'} & 0 \\ \hline 0 & 0 \end{array}\right), \quad Q = \left(\begin{array}{c|c} I_{r'} & 0 \\ \hline 0 & 0 \end{array}\right).$$

Note that P and Q can be defined for all $r \geq r'$. Then their product is equivalent to M (up to multiplication by invertible matrices on the left and right, both of which preserve the rank of M). □

Exercise I.3.14. Generalize Proposition 3.11 to the case of finitely generated free modules over any integral domain. (Embed the integral domain in its field of fractions.)

Proposition 3.11. *Let*

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

be a short exact *sequence of finite-dimensional vector spaces. Then*

$$\dim(V) = \dim(U) + \dim(W).$$

Solution. Let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of finitely generated free modules over an integral domain R. Embed R in its field of fractions K. By Exercise 1.7, each module is naturally mapped to a vector space over K. In particular, if A' denotes the vector space corresponding to the module A, we have $\operatorname{rank}(A) = \dim(A')$. Then, by Proposition 3.11, we have $\dim(B') = \dim(A') + \dim(C')$ which translates into $\operatorname{rank}(B) = \operatorname{rank}(A) + \operatorname{rank}(C)$. □

Exercise I.3.15. Prove Proposition 3.13 for the case $N = 1$.

Proposition 3.13. *With notation as above,*

$$\chi(V_\bullet) = \sum_{i=0}^{N} (-1)^i \dim(H_i(V_\bullet)).$$

In particular, if $V_\bullet$ is exact, then $\chi(V_\bullet) = 0$.

Solution. Let

$$V_\bullet : \ 0 \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

be a complex of finite-dimensional vector spaces and linear maps. By definition, we have $\chi(V_\bullet) = \dim(V_0) - \dim(V_1)$. Furthermore, we find

$$H_0(V_\bullet) = \frac{V_0}{\operatorname{im}(\alpha_1)}, \quad H_1(V_\bullet) = \ker(\alpha_1).$$

By Proposition 3.11,

$$\begin{aligned}\dim(H_0(V_\bullet)) &= \dim(V_0) - \dim(\mathrm{im}(\alpha_1)),\\ \dim(H_1(V_\bullet)) &= \dim(\ker(\alpha_1)),\\ \dim(V_1) &= \dim(\ker(\alpha_1)) + \dim(\mathrm{im}(\alpha_1))\end{aligned}$$

so we find

$$\begin{aligned}\sum_{i=0}^{1}(-1)^i \dim(H_i(V_\bullet)) &= \dim(H_0(V_\bullet)) - \dim(H_1(V_\bullet))\\ &= \dim(V_0) - \dim(\mathrm{im}(\alpha_1) - \dim(\ker(\alpha_1))\\ &= \dim(V_0) - \dim(V_1)\\ &= \chi(V_\bullet)\end{aligned}$$

proving the desired result. □

Exercise I.3.16. Prove Claim 3.14.

Claim 3.14. *With notation as above, we have the following:*

- χ_K *'is an Euler characteristic', in the sense that it satisfies the formula given in Proposition 3.13:*

  $$\chi_K(V_\bullet) = \sum_i (-1)^i [H_i(V_\bullet)].$$

- χ_K *is a 'universal Euler characteristic', in the following sense. Let* G *be an abelian group, and let* δ *be a function associating an element of* G *to each finite-dimensional vector space, such that* $\delta(V) = \delta(V')$ *if* $V \cong V'$ *and* $\delta(V/U) = \delta(V) - \delta(U)$*. For* $V_\bullet$ *a complex, define*

  $$\chi_G(V_\bullet) = \sum_i (-1)^i \delta(V_i).$$

  Then δ *induces a (unique) group homomorphism*

  $$K(k\text{-}\mathsf{Vect}^f) \to G$$

  mapping $\chi_K(V_\bullet)$ *to* $\chi_G(V_\bullet)$*.*

- *In particular,* $\delta = \dim$ *induces a group homomorphism*

  $$K(k\text{-}\mathsf{Vect}^f) \to \mathbb{Z}$$

  such that $\chi_K(V_\bullet) \mapsto \chi(V_\bullet)$*.*

- *This is in fact an isomorphism.*

Solution. Recall that we define $F(k\text{-}\mathsf{Vect}^f)$ to be the set of isomorphism classes of finite-dimensional vector spaces $[V]$ over a field k. We let E be the subgroup generated by the elements $[V]-[U]-[W]$ for all short exact sequences

$$\begin{tikzcd} 0 \arrow[r] & U \arrow[r] & V \arrow[r] & W \arrow[r] & 0 \end{tikzcd}$$

and define

$$K(k\text{-}\mathsf{Vect}^f) := \frac{F(k\text{-}\mathsf{Vect})}{E}$$

to be the Grothendieck group of the category $k\text{-}\mathsf{Vect}^f$. We also define

$$\chi_K(V_\bullet) := \sum_i (-1)^i [V_i] \in K$$

where summation is the direct sum.

First we prove that χ_k is an Euler characteristic. We adapt the proof by induction used to prove Propositoin 3.11, starting with the case $N=1$. Again, let

$$\begin{tikzcd} V_\bullet : \ 0 \arrow[r] & V_1 \arrow[r, "\alpha_1"] & V_0 \arrow[r] & 0 \end{tikzcd}$$

be a complex of finite-dimensional vector spaces and linear maps. By definition, we have $\chi_K(V_\bullet) = [V_0]-[V_1]$. Recall that, by the definition of homology,

$$H_0(V_\bullet) = \frac{V_0}{\operatorname{im}(\alpha_1)}, \quad H_1(V_\bullet) = \ker(\alpha_1)$$

so we have two exact sequences in $k\text{-}\mathsf{Vect}^f$:

$$\begin{tikzcd} 0 \arrow[r] & H_1(V_\bullet) \arrow[r] & V_1 \arrow[r] & \operatorname{im}(\alpha_1) \arrow[r] & 0 \end{tikzcd}$$

and

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{im}(\alpha_1) \arrow[r] & V_0 \arrow[r] & H_0(V_\bullet) \arrow[r] & 0 \end{tikzcd}$$

so we have the relations $[H_1(V_\bullet)] = [V_1]-[\operatorname{im}(\alpha_1)]$ and $[H_0(V_\bullet)] = [V_0]-[\operatorname{im}(\alpha_1)]$. Thus, we find

$$\begin{aligned} \sum_{i=0}^{1}[H_i(V_\bullet)] &= [H_0(V_\bullet)] - [H_1(V_\bullet)] \\ &= ([V_0]-[\operatorname{im}(\alpha_1)]) - [V_1] - [\operatorname{im}(\alpha_1)] \\ &= [V_0]-[V_1] \\ &= \chi_K(V_\bullet) \end{aligned}$$

so the statement holds in the base case. Now we prove the inductive step. Given a complex

$$\begin{tikzcd} V_\bullet : \ 0 \arrow[r] & V_N \arrow[r, "\alpha_N"] & V_{N-1} \arrow[r, "\alpha_{N-1}"] & \cdots \arrow[r, "\alpha_2"] & V_1 \arrow[r, "\alpha_1"] & V_0 \arrow[r] & 0 \end{tikzcd}$$

we can consider the truncated complex

$$V'_\bullet : \ 0 \longrightarrow V_{N-1} \xrightarrow{\alpha_{N-1}} \cdots \xrightarrow{\alpha_2} V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

where the result is known to hold for $V'_\bullet$. Then

$$\chi_K(V_\bullet) = \chi_K(V'_\bullet) + (-1)^N [V_N]$$

and

$$H_i(V_\bullet) = H_i(V'_\bullet) \text{ for } 0 \leq i \leq N-2$$

while

$$H_{N-1}(V'_\bullet) = \ker(\alpha_{N-1}), \quad H_{N-1}(V_\bullet) = \frac{\ker(\alpha_{N-1}}{\operatorname{im}(\alpha_N)}, \quad H_N(V_\bullet) = \ker(\alpha_N).$$

Then we have exact sequences

$$0 \longrightarrow \ker(\alpha_N) \longrightarrow V_N \longrightarrow \operatorname{im}(\alpha_N) \longrightarrow 0$$

and

$$0 \longrightarrow \operatorname{im}(\alpha_N) \longrightarrow \ker(\alpha_{N-1}) \longrightarrow H_{N-1}(V_\bullet) \longrightarrow 0$$

which yield the relations $[V_N] = [\ker(\alpha_N)] + [\operatorname{im}(\alpha_N)]$ and $[H_{N-1}(V_\bullet)] = [\ker(\alpha_{N-1})] - [\operatorname{im}(\alpha_N)]$. Then we have

$$[H_{N-1}(V'_\bullet)] - [V_N] = [H_{N-1}(V_\bullet)] - [H_N(V_\bullet)]$$

so we find

$$\begin{aligned} \chi_K(V_\bullet) &= \chi_K(V'_\bullet) + (-1)^N [V_N] \\ &= \sum_{i=0}^{N-1} (-1)^i [H_i(V'_\bullet)] + (-1)^N [V_N] \\ &= \sum_{i=0}^{N-2} (-1)^i [H_i(V'_\bullet)] + (-1)^{N-1} \left([H_{N-1}(V'_\bullet)] - [V_N]\right) \\ &= \sum_{i=0}^{N-2} (-1)^i [H_i(V_\bullet)] + (-1)^{N-1} ([H_{N-1}(V_\bullet)] - [H_N(V_\bullet)]) \\ &= \sum_{i=0}^{N} (-1)^i [H_i(V_\bullet)] \end{aligned}$$

which proves the desired result.

For the second part, let $\varphi : K(k\text{-}\mathsf{Vect}^f) \to G$ be the unique group homomorphism induced by δ. We claim that $\varphi([V]) = \delta(V)$ satisfies this universal property. First we check that it is well defined; suppose $[V] = [V']$. Then, since

$V \cong V'$, we have $\delta(V) = \delta(V')$. Now we show that this is a group homomorphism. Let $[U], [V] \in K(k\text{-}\mathsf{Vect}^f)$. Then

$$\varphi([V] - [U]) = \varphi([V/U]) = \delta(V/U) = \delta(V) - \delta(U) = \varphi([V]) - \varphi([U])$$

which verifies that this is a group homomorphism. Finally, let $V_\bullet$ be a complex of finite-dimensional vector spaces. Then

$$\begin{aligned} \varphi(\chi_K(V_\bullet)) &= \varphi\left(\sum_i (-1)^i [V_i]\right) \\ &= \sum_i (-1)^i \varphi([V_i]) \\ &= \sum_i (-1)^i \delta(V_i) \\ &= \chi_G(V_\bullet) \end{aligned}$$

where the second equality follows from φ being a group homomorphism.

The third point follows naturally from the second. Indeed, letting $\delta = \dim$ induces a group homomorphism from $K(k\text{-}\mathsf{Vect}^f)$ to $\mathbb{Z}$ such that $\chi_K(V_\bullet) = \chi(V_\bullet)$, where χ is the natural definition of the Euler characteristic.

To show that this is an isomorphism, we prove it is both injective and surjective. First note that for any non-negative integer n, we may consider the vector space $V = k^n$. Then $\varphi([V]) = n$. If n is negative, consider $V = k^{-n}$ such that $\varphi(-[V]) = -\varphi([V]) = n$. Thus, φ is surjective. Now suppose $\varphi([U]) = \varphi([V])$. That is, $\dim(U) = \dim(V)$. Then $U \cong V$ so $[U] = [V]$ and φ is injective. Thus, φ is an isomorphism and

$$K(k\text{-}\mathsf{Vect}^f) \cong \mathbb{Z}.$$

□

Exercise I.3.17. Extend the definition of Grothendieck group of vector spaces given in §3.4 to the category of vector spaces of *countable* (possibly infinite) dimension, and prove that it is the trivial group.

Solution. Consider the sequence

$$0 \longrightarrow k^{\oplus \mathbb{N}} \longrightarrow k^{\oplus \mathbb{N}} \longrightarrow k^n \longrightarrow 0$$

where $n \in \mathbb{N}$. Certainly, this sequence is exact because $k^{\oplus \mathbb{N}} \cong k^{\oplus \mathbb{N}} \oplus k^n$. But this implies that $[k^{\oplus \mathbb{N}}] = [k^{\oplus \mathbb{N}}] + [k^n]$ or $[k^n] = 0$. Since this also holds for $[k^{\oplus \mathbb{N}}]$, the group $K(k\text{-}\mathsf{Vect})$ is the trivial group. □

Exercise I.3.18. Let Ab^{fg} be the category of finitely generated abelian groups. Define a Grothendieck group of this category in the style of the construction of $K(k\text{-}\mathsf{Vect}^f)$, and prove that $K(\mathsf{Ab}^{fg}) \cong \mathbb{Z}$.

Solution. Note that every object G of Ab^{fg} determines an isomorphism class $[G]$. Let $F(\mathsf{Ab}^{fg})$ be the free abelian group on the set of these isomorphism classes. Furthermore, let E be the subgroup generated by the elements $[B]-[A]-[C]$ for all short exact sequences

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

in Ab^{fg}. Let

$$K(\mathsf{Ab}^{fg}) := \frac{F(\mathsf{Ab}^{fg})}{E}$$

be the Grothendieck group of this category.

Recall that every finitely generated abelian group is isomorphic to a direct sum of cyclic groups (Exercise 2.19). That is, for all finitely generated abelian groups G, we have

$$G \cong \mathbb{Z}^m \oplus \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}}$$

where $d_i \mid d_{i+1}$. Next, note that we may construct the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

so that $[\mathbb{Z}/n\mathbb{Z}] = [\mathbb{Z}] - [\mathbb{Z}] = [0]$ for all $n \in \mathbb{Z}$. Thus, we may construct a homomorphism $\varphi : K(\mathsf{Ab}^{fg}) \to \mathbb{Z}$ which sends $[A]$ to m where $\mathbb{Z}^m$ is in the decomposition of A. Let $\text{rank}(A)$ denote the power of $\mathbb{Z}$ in the decomposition of A. First we verify that this homomorphism is well-defined: if $[A] = [B]$ then $A \cong B$ so
$textrank(A) = \text{rank}(B)$ and $\varphi([A]) = \varphi([B])$. Now we show it is a homomorphism. Let $[A], [B] \in K(\mathsf{Ab}^{fg})$ where $\text{rank}(A) = m$ and $\text{rank}(B) = n$. Then

$$\varphi([A] + [B]) = \varphi(A \oplus B) = m + n = \varphi([A]) + \varphi([B])$$

so φ is in fact a homomorphism. Finally, we verify that it is in fact an isomorphism. Certainly it is surjective since $\varphi([\mathbb{Z}^n]) = n$ for all $n \in \mathbb{Z}^{\geq 0}$ and one can use the additive inverse for negative integers. Lastly, the kernel of the homomorphism is the set of equivalence classes with rank 0. But if A has rank 0 then A is isomorphic to a direct sum of finite cyclic groups which are all isomorphic to $[0]$. That is, $\ker(\varphi) = [0]$ and the mapping is injective. Thus, it is a bijective homomorphism, proving that $K(\mathsf{Ab}^{fg}) \cong \mathbb{Z}$. □

Exercise I.3.19. Let Ab^f be the category of finite abelian groups. Prove that assigning to every finite abelian group its order extends to a homomorphism from the Grothendieck group $K(\mathsf{Ab}^f)$ to the multiplicative group $(\mathbb{Q}^*, \cdot)$.

Solution. First note that the sequence

$$0 \longrightarrow A \xrightarrow{i} A \oplus B \xrightarrow{\pi} B \longrightarrow 0$$

is exact. Let $\varphi : K(\mathsf{Ab}^f) \to \mathbb{Q}$ send a finite abelian group A to its order. To see that this is a homomorphism, let $[A], [B] \in K(\mathsf{Ab}^f)$ with $|A| = m, |B| = n$. Then

$$\varphi([A] + [B]) = \varphi([A \oplus B]) = mn = \varphi([A]) \cdot \varphi([B])$$

so it is in fact a homomorphism. Indeed, $\varphi([0]) = 1$ where 0 is the trivial group, and we can define φ for additive inverses accordingly. □

Exercise I.3.20. Let R-Mod^f be the category of modules of finite *length* (cf. Exercise 1.16) over a ring R. Let G be an abelian group, and let δ be a function assigning an element of G to every *simple* R-module. Prove that δ extends to a homomorphism from the Grothendieck group of R-Mod^f to G.

Explain why Exercise 3.19 is a particular case of this observation.

(For another example, letting $\delta(M) = 1 \in \mathbb{Z}$ for every simple module M shows that length itself extends to a homomorphism from the Grothendieck group of R-Mod^f to $\mathbb{Z}$.)

Solution. Recall that a module M has length m if it admits a composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

where each quotient M_i/M_{i+1} is simple. Let $\varphi : K(R\text{-}\mathsf{Mod}^f) \to G$ be defined as

$$\varphi([M]) = \sum i = 0^{m-1} \delta\left(\frac{M_i}{M_{i+1}}\right)$$

where the sum denotes the operation in G. Certainly this mapping is well-defined as isomorphic modules admit the same composition series (up to a re-ordering of the composition factors). To prove that it is a homomorphism, let $[M], [N] \in K(R\text{-}\mathsf{Mod}^f)$ where M has length m and N has length n. Then

$$\varphi([M] + [N]) = \varphi([M \oplus N]) = m + n = \varphi([M]) + \varphi([N])$$

by properties of the length of a module.

In particular, let $R = \mathbb{Z}$ and $G = (\mathbb{Q}^*, \cdot)$. Since simple finite abelian groups are cyclic groups of prime order $\mathbb{Z}/p\mathbb{Z}$, let $\delta(\mathbb{Z}/p\mathbb{Z}) = p$. Then φ is the extension of δ from $K(\mathbb{Z}\text{-}\mathsf{Mod}^f) \to \mathbb{Q}$. Indeed, given a finite abelian group

$$G = \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p_r^{n_r}\mathbb{Z}}$$

we find

$$\begin{aligned}\varphi([G]) &= \prod_i \delta\left(\frac{\mathbb{Z}}{p_i\mathbb{Z}}\right)^{n_i} \\ &= \prod_i p_i^{n_i} \\ &= |G|\end{aligned}$$

which aligns with the definition given in Exercise 3.19. □

I.4 Presentations and resolutions

Exercise I.4.1. Prove that if R is an integral domain and M is an R-module, then $\mathrm{Tor}(M)$ is a submodule of M. Give an example showing that the hypothesis that R is an integral domain is necessary.

Solution. Clearly $\mathrm{Tor}(M) \neq \emptyset$ since $0 \in \mathrm{Tor}(M)$. Now suppose $a, b \in \mathrm{Tor}(M)$. Then $\exists r, s \in R$ such that $ra = sb = 0$. Therefore, $rs(a + b) = s(ra) + r(sb) = 0$ so $a + b \in \mathrm{Tor}(M)$. Similarly, for all $s \in R$, we have $r(sa) = s(ra) = 0$ so $sa \in \mathrm{Tor}(M)$. Thus, $\mathrm{Tor}(M)$ is a submodule of M.

To see that R is an integral domain is necessary, consider $R = M = \mathbb{Z}/6\mathbb{Z}$. Then $\mathrm{Tor}(M) = \{0, 2, 3, 4\}$. But then $2 + 3 = 5 \notin \mathrm{Tor}(M)$ so $\mathrm{Tor}(M)$ is not a submodule of M. □

Exercise I.4.2. Let M be a module over an integral domain R, and let N be a torsion-free module. Prove that $\mathrm{Hom}_R(M, N)$ is torsion-free. In particular, $\mathrm{Hom}_R(M, R)$ is torsion-free. (We will run into this fact again; see Proposition VIII.5.16.)

Solution. Let $f \in \mathrm{Hom}_R(M, N)$ and suppose $r \cdot f = 0$ for some $r \in R$. That is, for all $m \in M$,

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

But since $f(m) \in N$, $f(m)$ is not a torsion element and $r = 0$. Thus, $\mathrm{Hom}_R(M, N)$ is torsion-free. □

Exercise I.4.3. Prove that an integral domain R is a PID if and only if every submodule of R itself is free.

Solution. Note that the submodules of R are its ideals. If R is a PID, then every submodule of R is generated by a single element. That is, every submodule of R has a basis, making it free. Now suppose every submodule of R is free. Recall that if M is a submodule of R, then $\dim(M) \leq \dim(R)$. In particular, $\dim(M) \leq 1$. Thus, every ideal of R is generated by at most one element so R is a PID. □

Exercise I.4.4. Let R be a commutative ring and M an R-module.

- Prove that $\mathrm{Ann}(M)$ is an ideal of R.
- If R is an integral domain and M is finitely generated, prove that M is torsion if and only if $\mathrm{Ann}(M) \neq 0$.
- Give an example of a torsion module M over an integral domain, such that $\mathrm{Ann}(M) = 0$. (Of course this example cannot be finitely generated!)

Solution. Let $a, b \in \operatorname{Ann}(M)$. That is, for all $m \in M$, we have $am = bm = 0$. Then $(a+b)m = am + bm = 0$ so $a + b \in \operatorname{Ann}(M)$. Similarly, for all $r \in R$, we find $(ra) \cdot m = r \cdot (am) = r \cdot 0 = 0$ so $ra \in \operatorname{Ann}(M)$, proving that it is an ideal.

If $\operatorname{Ann}(M) \neq 0$, there exists an $r \in R$ such that $rm = 0$ for all $m \in M$. Thus, every element of M is torsion. Now suppose M is torsion. That is, for every element $m_i \in M$, there exists an $r_i \in R, r_i \neq 0$ such that $r_i m_i = 0$. In particular, there is such an r_i for each generator of M. Then we may consider s to be the product of these r_i. Since R is an integral domain, $s \neq 0$. Furthermore, since all $m \in M$ is a linear combination of these generators, we have $sm = 0$ for all $m \in M$. Thus, $s \in \operatorname{Ann}(M)$.

Let $R = \mathbb{Z}$ and consider the $\mathbb{Z}$-module

$$M = \bigoplus_{i=1}^{\infty} \frac{\mathbb{Z}}{2^i \mathbb{Z}}.$$

Then each element of M has the form

$$a = (a_1 + \mathbb{Z}/2\mathbb{Z}, a_2 + \mathbb{Z}/2^2\mathbb{Z}, \dots, a_k + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \dots)$$

so $2^k a = 0$ which makes M a torsion module. Now suppose $r \in \operatorname{Ann}(M)$. Choose $k \in \mathbb{Z}$ such that $r < 2^k$ and consider the element

$$a = (0, 0, \dots, 1 + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \dots).$$

Then $ra = 0$, but since $r < 2^k$, it must be the case that $r = 0$. Thus, $\operatorname{Ann}(M) = 0$. □

Exercise I.4.5. Let M be a module over a commutative ring R. Prove that an ideal I of R is the annihilator of an element of M if and only if M contains an isomorphic copy of R/I (viewed as an R-module).

The *associated primes* of M are the prime ideals among the ideals $\operatorname{Ann}(m)$, for $m \in M$. The set of the associated primes of a module M is denoted $\operatorname{Ass}_R(M)$. Note that every prime in $\operatorname{Ass}_R(M)$ contains $\operatorname{Ann}_R(M)$.

Solution. Let I be the annihilator of an element $m \in M$. That is, for all $r \in I$, $rm = 0$. Consider the map $\varphi : R \to M$ which sends r to rm. The kernel of this map is the set of r such that $rm = 0$. That is, $\ker(\varphi) = I$ so, by the isomorphism theorem,

$$\frac{R}{I} \cong \operatorname{im}(\varphi) \subseteq M.$$

Now suppose M contains a submodule $N \cong R/I$ for an ideal $I \subseteq R$ and let $\varphi : R \to M$ be the composition of the natural projection and inclusion. We claim that I is the annihilator of $m = \varphi(1)$. Indeed, if $r \in I$ then

$$rm = r\varphi(1) = \varphi(r) = i(\pi(r)) = i(0) = 0$$

so $r \in \operatorname{Ann}(m)$ and $I \subseteq \operatorname{Ann}(m)$. Similarly, if $r \in \operatorname{Ann}(m)$ then

$$rm = 0 \Longrightarrow \varphi(r) = 0 \Longrightarrow \pi(r) = 0$$

so $r \in I$ and $\operatorname{Ann}(m) = I$. □

Exercise I.4.6. Let M be a module over a commutative ring R, and consider the family of ideals $\operatorname{Ann}(m)$, as m ranges over the nonzero elements of M. Prove that the maximal elements in this family are prime ideals of R. Conclude that if R is Noetherian, then $\operatorname{Ass}_R(M) \neq \emptyset$ (cf. Exercise 4.5).

Solution. Let $\mathfrak{m}$ be a maximal element in this family of ideals, say $\mathfrak{m} = \operatorname{Ann}(m)$. Suppose $rs \in \mathfrak{m}$. If $r \in \mathfrak{m}$ then there is nothing to prove so suppose otherwise. We know $rs \cdot m = 0$ but $rm \neq 0$. Thus, $s \in \operatorname{Ann}(rm)$. Furthermore, it is clear that $\operatorname{Ann}(m) \subseteq \operatorname{Ann}(rm)$ since if $am = 0$ then $a(rm) = 0$. Then, by the maximality of $\operatorname{Ann}(m)$, we have $\operatorname{Ann}(m) = \operatorname{Ann}(rm)$ so $s \in \mathfrak{m}$ and the ideal is prime.

If R is Noetherian, then every family of ideals has a maximal element. In particular, given a module M, the family of ideals $\operatorname{Ann}(m)$ as m ranges over the nonzero elements of M has a maximal element which is a prime ideal. Such prime ideals are elements of $\operatorname{Ass}_R(M)$, meaning the set is nonempty. □

Exercise I.4.7. Let R be a commutative Noetherian ring, and let M be a finitely generated module over R. Prove that M admits a finite series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

in which all quotients M_i/M_{i+1} are of the form $R/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of R. (Hint: Use Exercises 4.5 and 4.6 to show that M contains an isomorphic copy M' of $R/\mathfrak{p}_1$ for some prime $\mathfrak{p}_1$. Then do the same with M/M', producing an $M'' \supsetneq M'$ such that $M''/M' \cong R/\mathfrak{p}_2$ for some prime $\mathfrak{p}_2$. Why must this process stop after finitely many steps?)

Solution. By Exercise 4.6, $\operatorname{Ass}_R(M) \neq \emptyset$ so let $\mathfrak{p}_1 \in \operatorname{Ass}_R(M)$. Then by Exercise 4.5, M contains a submodule $M' \cong R/\mathfrak{p}_1$. Now consider M/M', which is also an R-module. Thus, $\operatorname{Ass}_R(M/M') \neq \emptyset$ and there is a submodule $M'' \supsetneq M'$ of M such that $M''/M' \cong R/\mathfrak{p}_2$ for some prime $\mathfrak{p}_2$. That is, we have a chain

$$M \supsetneq M'' \supsetneq M' \supsetneq \langle 0 \rangle$$

such that $M''/M' \cong R/\mathfrak{p}_2$ and $M'/0 \cong R/\mathfrak{p}_1$ for prime ideals of R. Since M is finitely generated over a Noetherian ring, it is a Noetherian module and all chains of submodules eventually stabilize. Thus, iterating this process yields a finite series whose quotients are isomorphic to $R/\mathfrak{p}$ for prime ideals. □

Exercise I.4.8. Let R be a commutative Noetherian ring, and let M be a finitely generated module over R. Prove that every prime in $\operatorname{Ass}_R(M)$ appears in the list of primes produced by the procedure presented in Exercise 4.7. (If $\mathfrak{p}$ is an associated prime, then M contains an isomorphic copy N of $R/\mathfrak{p}$. With notation as in the hint in Exercise 4.7, prove that either $\mathfrak{p}_1 = \mathfrak{p}$ or $N \cap M' = 0$. In the latter case, N maps isomorphically to a copy of $R/\mathfrak{p}$ in M/M'; iterate the reasoning.)

In particular, if M is a finitely generated module over a Noetherian ring, then $\operatorname{Ass}(M)$ is *finite*.

Solution. Let $\mathfrak{p} \in \operatorname{Ass}_R(M)$ and suppose $R/\mathfrak{p} \cong N \subseteq M$. In particular, if $x \in M$ such that $\operatorname{Ann}_R(x) = \mathfrak{p}$, then $N = Rx$. If $Rx \cap M' \neq 0$, say $rx = m$ is a nonzero element, then $\operatorname{Ann}_R(m) \subseteq \mathfrak{p}$. But by definition, $\operatorname{Ann}_R(m) = \mathfrak{p}_1$ so $\mathfrak{p}_1 \subseteq \mathfrak{p}$. The reverse inclusion can be shown similarly. Thus, if M' and N have nontrivial intersection, $\mathfrak{p} = \mathfrak{p}_1$. Otherwise, $M' \cap N = 0$. In the latter case, N is isomorphic to some $R/\mathfrak{p}$ in $M/M' \cong R/\mathfrak{p}_2$. Thus, we may repeat the above reasoning which eventually terminates. □

Exercise I.4.9. Let M be a module over a commutative Noetherian ring R. Prove that the union of all annihilators of nonzero elements equals the union of all associated primes of M. (Use Exercise 4.6)

Deduce that the *union* of the associated primes of a Noetherian ring R (viewed as a module over itself) equals the set of zero-divisors of R.

Solution. Certainly every associated prime is the annihilator of some element $m \in M$, so we only need to show the other direction. If $I \in \operatorname{Ann}_R(m)$ for some $m \in M$, then $I \subseteq \mathfrak{p}$ for some maximal element in the family of annihilators of elements of M. By Exercise 4.6, $\mathfrak{p}$ is prime in R so I is in the union of all associated primes, proving the result. □

Exercise I.4.10. Let R be a commutative Noetherian ring. One can prove that the minimal primes of $\operatorname{Ann}(M)$ (cf. Exercise V.1.9) are in $\operatorname{Ass}(M)$. Assuming this, prove that the *intersection* of the associated primes of a Noetherian ring R (viewed as a module over itself) equals the nilradical of R.

Solution. Recall that the nilradical of R is the set of elements $r \in R$ such that $r^n = 0$ for some $n > 0$. If $x \in \operatorname{nil}(R)$ then x is in the intersection of all prime ideals of R, particularly the intersection of associated primes of R. Now suppose x is in the intersection of the associated primes of R. Then it is in the minimal primes of $\operatorname{Ann}(R)$. Since every prime ideal contains a minimal prime ideal, the intersection of all prime ideals equals the intersection of all minimal prime ideals. Thus, $x \in \operatorname{nil}(R)$. □

Exercise I.4.11. Review the notion of presentation *of a group*, and relate it to the notion of presentation introduced in §4.2.

Solution. Recall that a presentation of a group G is an explicit isomorphism

$$G \cong \frac{F(A)}{R}$$

for a set A and a subgroup R of relations. A presentation of an R-module M is an exact sequence

$$R^n \longrightarrow R^m \longrightarrow M \longrightarrow 0$$

In particular, if G is an abelian group, then we have the exact sequence

$$R \longrightarrow F(A) \longrightarrow G$$

where R is also a free module since it is a submodule of $F(A)$. □

Exercise I.4.12. Let $\mathfrak{p}$ be a prime ideal of a polynomial ring $k[x_1, \ldots, x_n]$ over a field k, and let $R = k[x_1, \ldots, x_n]/\mathfrak{p}$. Prove that every finitely generated module over R has a finite presentation.

Solution. Let M be a finitely generated module over R. Then there is a surjection $\pi : R^a \to M$ for some $a \in \mathbb{Z}$ where $\ker(\pi)$ is a submodule of R^a. Since k is a field, by Hilbert's basis theorem, $k[x_1, \ldots, x_n]$ is also Noetherian. But then R is a quotient of a Noetherian ring and is Noetherian itself. Thus, $\ker(\pi)$ is finitely generated and there is an exact sequence

$$R^b \longrightarrow \ker(\pi) \longrightarrow 0$$

which yields the exact sequence

$$R^b \longrightarrow R^a \longrightarrow M \longrightarrow 0$$

so M is finitely presented. □

Exercise I.4.13. Let R be a commutative ring. A tuple $(a_1, a_2, \ldots, a_n)$ of elements of R is a *regular sequence* if a_1 is a non-zero-divisor in R, a_2 is a non-zero-divisor modulo (a_1), a_3 is a non-zero-divisor modulo (a_1, a_2), and so on.

For a, b in R, consider the following complex of R-modules:

$$(*) \qquad 0 \longrightarrow R \xrightarrow{d_2} R \oplus R \xrightarrow{d_1} R \xrightarrow{\pi} \frac{R}{(a,b)} \longrightarrow 0$$

where π is the canonical projection, $d_1(r, s) = ra + sb$, and $d_2(t) = (bt, -at)$. Put otherwise, d_1 and d_2 correspond, respectively, to the matrices

$$\begin{pmatrix} a & b \end{pmatrix}, \quad \begin{pmatrix} b \\ -a \end{pmatrix}.$$

- Prove that this is indeed a complex, for every a and b.
- Prove that if (a,b) is a regular sequence, this complex is *exact*.

The complex (*) is called the *Koszul complex* of (a,b). Thus, when (a,b) is a regular sequence, the Koszul complex provides us with a free resolution of the module $R/(a,b)$.

Solution. First we verify that this is a complex for all a and b. Certainly the image of the zero map is a subset of $\ker(d_2)$. Let $(r,s) \in \operatorname{im}(d_2)$. Then $(r,s) = (bt, -at)$ for some $t \in R$ and

$$d_1(bt, -at) = bta - bta = 0$$

so $\operatorname{im}(d_2) \subseteq \ker(d_1)$. Furthermore, let $ra + sb \in \operatorname{im}(d_1)$. Then $\pi(ra+sb) = 0 \in R/(a,b)$ so $\operatorname{im}(d_1) \subseteq \ker(\pi)$. Finally, the image of π is clearly a subset of the kernel of the zero map. Thus, we have verified that this is in fact a complex.

Now suppose (a,b) is a regular sequence. Let $t \in \ker(d_2)$. That is, $(bt, -at) = (0,0)$. Since $a \neq 0$, it must be the case that $t = 0$ so t is in the image of the zero map, proving the two are equal.

Now suppose $(r,s) \in \ker(d_1)$. Then $ra + sb = 0$. Consider the equation mod a: $sb = 0$. Since b is not a zero-divisor in $R/(a)$, $s \in (a)$ so $s = at$ for some $t \in R$. Then we have $ra + atb = 0$, or $(r + tb)a = 0$. Since a is not a zero-divisor in R, it must be the case that $r + tb = 0$, or $r = -tb$. That is, $(r,s) = (-tb, at) \in \operatorname{im}(d_2)$ so the two sets must be equal.

Now let $x \in \ker(\pi)$ so $\pi(x) = 0 \implies x = ra + sb$ for $r, s \in R$. Then $x = d_1(r,s) \in \operatorname{im}(d_1)$ and the two sets are equal.

Finally, the projection is surjective and the kernel of the zero map is all of its domain so the last map is exact. □

Exercise I.4.14. A Koszul complex may be defined for any sequence $a_1, \dots, a_n$ of elements of a commutative ring R. The case $n = 2$ seen in Exercise 4.13 and the case $n = 3$ reviewed here will hopefully suffice to get a gist of the general construction; the general case will be given in Exercise VIII.4.22.

Let $a, b, c \in R$. Consider the following complex:

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "d_3"] & R \oplus R \oplus R \arrow[r, "d_2"] & R \oplus R \oplus R \arrow[r, "d_1"] & R \arrow[r, "\pi"] & \frac{R}{(a,b,c)} \arrow[r] & 0 \end{tikzcd}$$

where π is the canonical projection and the matrices for d_1, d_2, d_3 are, respectively,

$$\begin{pmatrix} a & b & c \end{pmatrix}, \quad \begin{pmatrix} 0 & -c & -b \\ -c & 0 & a \\ b & a & 0 \end{pmatrix}, \quad \begin{pmatrix} a \\ -b \\ c \end{pmatrix}.$$

- Prove that this is indeed a complex, for every a, b, c.

- Prove that if (a, b, c) is a regular sequence, this complex is *exact*.

Koszul complexes are very important in commutative algebra and algebraic geometry.

Solution. Clearly the image of the zero map is in the kernel of d_3. Let $(ar, -br, cr) \in \operatorname{im}(d_3)$. Then

$$\begin{pmatrix} 0 & -c & -b \\ -c & 0 & a \\ b & a & 0 \end{pmatrix} \cdot \begin{pmatrix} ar \\ -br \\ cr \end{pmatrix} = \begin{pmatrix} bcr - bcr \\ -acr + acr \\ abr - abr \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

so $(ar, -br, cr) \in \ker(d_2)$. Now let $(-cs - bt, -cr + at, br + as) = d_2(r, s, t) \in \operatorname{im}(d_2)$. Then

$$\begin{pmatrix} a & b & c \end{pmatrix} \cdot \begin{pmatrix} -cs - bt \\ -cr + at \\ br + as \end{pmatrix} = -acs - abt - bcr + abt + bcr + acs = 0$$

so $\operatorname{im}(d_2) \subseteq \ker(d_1)$. Now consider $ra + sb + ct = d_1(r, s, t) \in \operatorname{im}(d_1)$. We have

$$\pi(ra + sb + ct) = 0$$

by definition of the projection to a quotient so $\operatorname{im}(d_1) \subseteq \ker(\pi)$. The image of projection is obviously a subset of the kernel of the zero map. Thus, this is indeed a complex.

Now suppose (a, b, c) is a regular sequence. If $r \in \ker(d_3)$ then $d_3(r) = (0, 0, 0)$. In particular, $ar = 0$ and since a is not a zero-divisor, we must have $r = 0$ so r is in the image of the zero map, hence it equals the image of d_3.

If $(r_1, r_2, r_3) \in \ker(d_2)$, then

$$\begin{pmatrix} 0 & -c & -b \\ -c & 0 & a \\ b & a & 0 \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} -cr_2 - br_3 \\ -cr_1 + ar_3 \\ br_1 + ar_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

The third equation mod a yields $br_1 = 0$ in $R/(a)$. Since b is not a zero-divisor in this ring, we must have $r_1 = at$ for some $t \in R$. Substituting this back into the third equation, we have $abt + ar_2 = 0$, or $r_2 = -bt$ (since a is not a zero-divisor in R). Substituting this into the second equation yields $-act + ar_3 = 0$ so $r_3 = ct$ by the same reasoning as above. But then

$$(r_1, r_2, r_3) = (at, -bt, ct) = d_3(t)$$

so $\operatorname{im}(d_3) = \ker(d_2)$.

If $(r_1, r_2, r_3) \in \ker(d_1)$, then

$$\begin{pmatrix} a & b & c \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = ar_1 + br_2 + cr_3 = 0.$$

Considering this equation mod (a, b) yields $cr_3 = 0$ in $R/(a, b)$ and since c is not a zero-divisor in this ring, we must have $r_3 \in (a, b)$ or $r_3 = ar + bs$ for $r, s \in R$. Substituting this into the equation yields

$$ar_1 + br_2 + acr + bcs = 0$$

which we can consider mod a to yield $br_2 + bcs = 0$ in $R/(a)$, or $r_2 + cs = at$ for some $t \in R$. That is, $r_2 = at - cs$, which we can again substitute into the equation to obtain

$$ar_1 + abt - bcs + acr + bcs = 0$$

which yields $a(r_1 + bt + cs) = 0$ so $r_1 = -bt - cs$. But then

$$(r_1, r_2, r_3) = (-bt - cs, at - cs, ar + bs) = d_2(r, s, t)$$

so $\mathrm{im}(d_2) = \ker(d_1)$.

Finally, suppose $x \in \ker(\pi)$. That is, $x \in (a, b, c)$. Then $x = ra + bs + ct = d_1(r, s, t)$ and $\mathrm{im}(d_1) = \ker(\pi)$. The last equality is obvious. Thus, the complex is exact. □

Exercise I.4.15. View $\mathbb{Z}$ as a module over the ring $R = \mathbb{Z}[x, y]$, where x and y act by 0. Find a free resolution of $\mathbb{Z}$ over R.

Solution. Recall that a free resolution of an R-module M is an exact complex

$$\cdots \longrightarrow R^{m_3} \longrightarrow R^{m_2} \longrightarrow R^{m_1} \longrightarrow R^{m_0} \longrightarrow M \longrightarrow 0.$$

Consider the complex

$$0 \longrightarrow R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0$$

where d_1 and d_2 correspond to the matrices

$$\begin{pmatrix} x & y \end{pmatrix}, \quad \begin{pmatrix} y \\ -x \end{pmatrix}$$

and π is the natural projection to the constant term. It is easy to see that this is in fact a complex. To see that it is exact, let $f(x, y) \in \ker(\pi)$. That is, f has no constant term, so it may be written as

$$f = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} f_1(y) \\ f_2(x) \end{pmatrix}$$

so $f \in \mathrm{im}(d_1)$. Similarly, if $(f, g) \in \ker(d_1)$ then $fx + gy = 0$. Gathering terms, this is only possible if $f = hy$ and $g = -hx$ for some $h \in R$. That is, $(f, g) = d_2(h)$ so $\ker(d_1) = \mathrm{im}(d_2)$ and the sequence is exact. Thus, this is a free resolution of $\mathbb{Z}$ over R. □

Exercise I.4.16. Let $\varphi : R^n \to R^m$ and $\psi : R^p \to R^q$ be two R-module homomorphisms, and let

$$\varphi \oplus \psi : R^n \oplus R^p \to R^m \oplus R^q$$

be the morphism induced on direct sums. Prove that

$$\operatorname{coker}(\varphi \oplus \psi) = \operatorname{coker}\varphi \oplus \operatorname{coker}\psi.$$

Solution. First note that

$$\operatorname{im}(\varphi \oplus \psi) = \operatorname{im}(\varphi) \oplus \operatorname{im}(\psi).$$

Now consider the map

$$R^m \oplus R^q \to \frac{R^m}{\operatorname{im}\varphi} \oplus \frac{R^q}{\operatorname{im}\psi}.$$

The kernel of this map is $\operatorname{im}(\varphi) \oplus \operatorname{im}(\psi)$ so by the first isomorphism theorem, we have

$$\frac{R^m \oplus R^q}{\operatorname{im}(\varphi \oplus \psi)} \cong \frac{R^m}{\operatorname{im}\varphi} \oplus \frac{R^q}{\operatorname{im}\psi}$$

and $\operatorname{coker}(\varphi \oplus \psi) = \operatorname{coker}(\varphi) \oplus \operatorname{coker}(\psi)$. □

Exercise I.4.17. Determine (as a better known entity) the module represented by the matrix

$$\begin{pmatrix} 1+3x & 2x & 3x \\ 1+2x & 1+2x-x^2 & 2x \\ x & x^2 & x \end{pmatrix}$$

over the polynomial ring $k[x]$ over a field.

Solution. We perform Gaussian elimination to reduce the matrix to a simpler but equivalent form. Subtracting three times the third row from the first yields a unit in the 1, 1 position so we are reduced to the 2×2 matrix

$$\begin{pmatrix} 1+2x-x^2 & 2x \\ x^2 & x \end{pmatrix}.$$

Adding the second row to the first and subtracting $\frac{2}{3}$ times the second column from the first yields another unit in the 1, 1 position so we have reduced the matrix to

$$\begin{pmatrix} x \end{pmatrix}.$$

The module represented by the original matrix is isomorphic to the cokernel of the homomorphism

$$\varphi : k[x] \to k[x]$$

which maps 1 to x. That is,

$$M \cong \operatorname{coker}\varphi \cong \frac{k[x]}{(x)} \cong k.$$

□

I.5 Classification of finitely generated modules over PID

Exercise I.5.1. Let N, P be submodules of a module M, such that $N \cap P = \{0\}$ and $M = N + P$. Prove that $M \cong N \oplus P$. (This is a word-for-word repetition of Proposition IV.5.3 for modules.)

Solution. Consider the mapping

$$\varphi : N \oplus P \to N + P$$

defined by $\varphi(n, p) = n + p$. Certainly this is an R-module homomorphism. It is surjective since for all $m = n + p \in N + P$, we have $m = \varphi(n, p)$. Furthermore, the kernel of this mapping is

$$\ker \varphi = \{(n, p) \in N \oplus P \mid n + p = 0\}.$$

If $n + p = 0$ then $n = -p \in P$ so $n \in N \cap P$ and $n = 0$. Similarly, $p = 0$ so $\ker \varphi = \{0\}$ and the map is injective. Thus, this is an isomorphism and $M = N + P \cong N \oplus P$. □

Exercise I.5.2. Let R be an integral domain, and let M be a finitely generated R-module. Prove that M is torsion if and only if $\operatorname{rk} M = 0$.

Solution. The rank of M is 0 if and only if for all $m \in M$, the set $\{m\}$ is linearly dependent. This occurs if and only if there exists $r \in R$ such that $rm = 0$, but this is true if and only if M is torsion. □

Exercise I.5.3. Complete the proof of Corollary 5.3.

Corollary 5.3. *Let R be a PID, let F be a finitely generated free module over R, and let $M \subseteq F$ be a submodule. Then there exists a basis $(x_1, \ldots, x_n)$ of F and nonzero elements $a_1, \ldots, a_m$ of R ($m \leq n$) such that $(a_1x_1, \ldots, a_mx_m)$ is a basis of M. Further, we may assume $a_1 \mid a_2 \mid \cdots \mid a_m$.*

Solution. We only need to show the existence of the bases. By Lemma 5.2, there exists $x \in F$ such that

$$F = \langle x_1 \rangle \oplus F^{(1)}.$$

If $F^{(1)} = 0$, then (x_1) is a basis for F. Otherwise we may repeat this process. Since F is a finitely generated free module, this process terminates and yields a basis $(x_1, \ldots, x_n)$ for F. Lemma 5.2 also guarantees the existence of $y_1 = a_1x_1$ such that

$$M = \langle y_1 \rangle \oplus M^{(1)}.$$

If $M^{(1)} = 0$, then $(y_1) = (a_1x_1)$ is a basis for M. Otherwise we may repeat this process. Since M is a submodule of F, $\operatorname{rk} M \leq \operatorname{rk} F$ so this process also terminates at some $m \leq n$. □

Exercise I.5.4. Let R be an integral domain, and assume that $a, b \in R$ are such that $a \neq 0$, $b \notin (a)$, and $R/(a), R/(a,b)$ are both integral domains.

- Prove that the Krull dimension of R is at least 2.
- Prove that if R satisfies the finiteness condition discussed in §5.2 for some n, then $n \geq 2$.

You can prove this second point by appealing to Proposition 5.4. For a more concrete argument, you should look for an R-module admitting a free resolution of length 2 which cannot be shortened.

- Prove that (a, b) is a regular sequence in R. (Exercise 4.13).
- Prove that the R-module $R/(a,b)$ has a free resolution of length exactly 2.

Can you see how to construct analogous situations with $n \geq 3$ elements $a_1, \dots, a_n$?

Solution. Since $R/(a)$ and $R/(a,b)$ are integral domains, (a) and (a,b) are both prime ideals. Thus, we may construct the chain of prime ideals

$$(0) \subsetneq (a) \subsetneq (a,b)$$

in R, so the Krull dimension of R is at least 2.

Now suppose every finitely generated R-module M admits a free resolution of finite length n. To show that $n \geq 2$, it suffices to construct a free resolution of length 2 which cannot be shortened. Consider the R-module $M = R/(a,b)$. Then we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "d_2"] & R^2 \arrow[r, "d_1"] & R \arrow[r, "\pi"] & M \arrow[r] & 0 \end{tikzcd}$$

where $d_2(r) = (-br, ar)$, $d_1(r,s) = ra + sb$, and π is the natural projection. It is easy to check that this is an exact sequence, and it cannot be shortened to $n = 1$. To see this, note that $\ker \pi = (a,b)$. Any morphism whose image is (a,b) must have domain R^2 since there are two degrees of choice in the image. Since the kernel of a map from $R^2 \to R$ must be nontrivial, there must be another copy of R before R^2 in the free resolution and the free resolution cannot be shortened. It also follows from the fact that the Krull dimension of a PID is at most 1.

Recall that a regular sequence is a tuple $(a_1, a_2, \dots, a_n)$ where a_1 is not a zero-divisor of R, a_2 is not a zero-divisor of $R/(a_1)$, a_3 is not a zero-divisor of $R/(a_1, a_2)$ and so on. Since R is an integral domain, a is a non-zero-divisor of R. Furthermore, $b \notin (a)$ so $b \neq 0 \in R/(a)$. Then, since $R/(a)$ is an integral domain, b is not a zero divisor in $R/(a)$. Thus, (a,b) is a regular sequence in R.

The sequence constructed in part 2 of this exercise proves that $R/(a,b)$ has a free resolution of length 2. □

Exercise I.5.5. Recall (Exercise V.4.11) that a commutative ring is *local* if it has a single maximal ideal $\mathfrak{m}$. Let R be a local ring, and let M be a *direct summand* of a finitely generated free R-module: that is, there exists an R-module N such that $M \oplus N$ is a free R-module.

- Choose elements $m_1, \ldots, m_r \in M$ whose cosets mod $\mathfrak{m}M$ are a basis of $M/\mathfrak{m}M$ as a vector space over the field $R/\mathfrak{m}$. By Nakayama's lemma, $M = \langle m_1, \ldots, m_r \rangle$ (Exercise 3.10).
- Obtain a surjective homomorphism $\pi : F = R^{\oplus r} \to M$.
- Show that π splits, giving an isomorphism $F \cong M \oplus \ker \pi$. (Apply Exercise III.6.9 to the surjective homomorphism π and the free module $M \oplus N$ to obtain a splitting $M \to F$; then use Proposition III.7.5.)
- Show $\ker \pi / \mathfrak{m} \ker \pi = 0$. Use Nakayama's lemma (Exercise 3.8) to deduce that $\ker \pi = 0$.
- Conclude that $M \cong F$ is in fact free.

Summarizing, over a *local ring*, every *direct summand* of a finitely generated free R-module is free. Using the terminology we will introduce in Chapter VIII, we would say that 'projective modules over local rings are free'. This result has strong implications in algebraic geometry, since it underlies the notion of vector bundle.

Contrast this fact with Proposition 5.1, which shows that, over a *PID*, *every* submodule of a finitely generated free module is free.

Solution. The first point follows from Exercise 3.10.

Define $\pi : R^{\oplus r} \to M$ which sends e_i to m_i where e_i is an elementary basis vector. Certainly this is surjective as a projection.

There is a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker \pi \arrow[r] & F \arrow[r, "\pi"] & M \arrow[r] & 0 \end{tikzcd}$$

and since π has a right-inverse (sending the basis of M to the basis of F), Proposition III.7.5 implies that this sequence is split and $F \cong M \oplus \ker \pi$.

Note that

$$\left(\frac{R}{\mathfrak{m}}\right)^r \cong \frac{M}{\mathfrak{m}M} \oplus \frac{\ker \pi}{\mathfrak{m} \ker \pi}$$

as vector spaces over $R/\mathfrak{m}$. Since the dimension of $M/\mathfrak{m}M$ is r, we must have $\ker \pi / \mathfrak{m} \ker \pi = 0$. Then, by Nakayama's lemma, $\ker \pi = 0$.

Thus, $F \cong M$ and M is a free module. □

Exercise I.5.6. Let R be an integral domain, and let $M = \langle m_1, \ldots, m_r \rangle$ be a finitely generated module. Prove that $\operatorname{rk} M \leq r$. (Use Exercise 3.12.)

Solution. Assume for the sake of contradiction that $k = \operatorname{rk} M > r$. There are surjections $f : R^r \to M$ and $g : R^k \to M$. Let $N \in \mathcal{M}_{r,k}(R)$ such that g maps the columns of N to a maximal linearly independent subset of M. By Exercise 3.12, the columns of N are linearly dependent. In particular, there exist $\{r_1, \ldots, r_k\}$ such that $r_1 n_1 + \cdots + r_k n_k = 0$ where the $n_i \in R^r$. Then

$$g(r_1 n_1 + \cdots + r_k n_k) = r_1 g(n_1) + \cdots + r_k g(n_k) = 0,$$

which contradicts the assumption that the image of the columns of N is linearly independent. Thus, $k = \operatorname{rk} M \leq r$. □

Exercise I.5.7. Let R be an integral domain, and let M be a finitely generated module over R. Prove that $\operatorname{rk} M = \operatorname{rk}(M/\operatorname{Tor}(M))$.

Solution. First note that $\operatorname{rk}(M/\operatorname{Tor}(M)) \leq \operatorname{rk} M$ because any linearly independent subset of the former induces a linearly independent subset of the latter. Suppose $\operatorname{rk} M = r$ and let $S = \{m_1, \ldots, m_r\}$ be a maximal linearly independent subset of M. Consider $S + \operatorname{Tor}(M) = \{m_1 + \operatorname{Tor}(M), \ldots, m_r + \operatorname{Tor}(M)\}$. If this set is linearly dependent, then there exist $r_1, \ldots, r_r \in R$ such that $r_1 m_1 + \cdots + r_r m_r \in \operatorname{Tor}(M)$. That is, there exists an $s \in R, s \neq 0$ such that

$$s(r_1 m_1 + \cdots + r_r m_r) = 0.$$

Since R is an integral domain, this implies $r_1 m_1 + \cdots + r_r m_r = 0$ and S is linearly dependent in M, a contradiction. Thus, $S + \operatorname{Tor}(M)$ is also linearly independent and we have $\operatorname{rk} M = \operatorname{rk}(M/\operatorname{Tor}(M))$. □

Exercise I.5.8. Let R be an integral domain, and let M be a finitely generated module over R. Prove that $\operatorname{rk} M = r$ if and only if M has a *free* submodule $N \cong R^r$, such that M/N is torsion.

If R is a PID, then N may be chosen so that $0 \to N \to M \to M/N \to 0$ splits.

Solution. Suppose $\operatorname{rk} M = r$ and let $S = \{m_1, \ldots, m_r\}$ be a linearly independent subset. Consider the free submodule $N = \langle S \rangle \cong R^r$. Indeed, an isomorphism is given by mapping corresponding basis elements $m_i \mapsto e_i$. Now let $x + N \in M/N$. If $x + N$ is not a torsion element then there is no $r \in R$ such that $rx \in N$. That is, x is linearly independent of S, but this contradicts that S is a maximal linearly independent set. Thus, $x + N$ is a torsion element and M/N is torsion.

Now suppose M has a free submodule $N \cong R^r$ such that M/N is torsion. Choose a linearly independent set $S = \{m_1, \ldots, m_r\}$ such that S is a basis for N. Let $x + N \in M/N$. Since this module is torsion, there exists an $r \in R$ such that $rx \in N$. That is, x is a linear combination of the elements of S. Since this holds for all elements of M, S is a maximal linearly independent subset of M and $\operatorname{rk} M = r$. □

Exercise I.5.9. Let R be an integral domain, and let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be an exact sequence of finitely generated R-modules. Prove that $\operatorname{rk} M_2 = \operatorname{rk} M_1 + \operatorname{rk} M_3$.

Deduce that 'rank' defines a homomorphism from the Grothendieck group of the category of finitely generated R-modules to $\mathbb{Z}$.

Solution. Let $r_i = \operatorname{rk} M_i$. By the isomorphism theorems, $M_3 \cong M_2/M_1$. Let $\{u_1, \ldots, u_{r_1}\}$ be linearly independent in M_1 and $\{v_1 + M_1, \ldots, v_{r_3} + M_1\}$ be linearly independent in M_3. If

$$a_1u_1 + \cdots + a_{r_1}u_{r_1} + b_1v_1 + \cdots + b_{r_3}v_{r_3} = 0$$

in M_2, then reducing the equation modulo M_1 yields

$$b_1(v_1 + M_1) + \cdots + b_{r_3}(v_{r_3} + M_1) = 0 + M_1$$

so $b_1 = \cdots = b_{r_3} = 0$ by linear independence in M_3. But then $a_1 = \cdots = a_{r_1} = 0$ by linear independence in M_1 so $r_2 \geq r_1 + r_3$.

To show the other inequality, let N be a linearly independent subset of M_2. Let $X \subset N$ be maximal with respect to the property that $f(X)$ is linearly independent in M_3 (where f is the surjection from $M_2 \to M_3$). Now let $m \in N \setminus X$. The set $f(\{m\} \cup X)$ is linearly dependent in M_3 so there exist $r_m, s_{m,x} \in R$ such that

$$0 = r_m f(m) + \sum_{x \in X} s_{m,x} f(x) = f\left(r_m m + \sum_{x \in X} s_{m,x} x\right),$$

hence $r_m m + \sum_{x \in X} s_{m,x} x \in M_1$. Note that $r_m \neq 0$ since $f(X)$ is linearly independent. Now let $t_m \in R$ such that

$$\sum_{m \in N \setminus X} t_m(r_m m + \sum x \in X s_{m,x} x) = 0$$

and rearrange to yield

$$0 = \sum_{m \in N \setminus X} t_m r_m m + \sum_{x \in X} \sum_{m \in N \setminus X} t_m s_{m,x} x.$$

The linear independence of N shows that $t_m r_m = 0$, so $t_m = 0$ since $r_m \neq 0$ and R is an integral domain. Thus, the elements $(r_m m + \sum_{x \in X} s_{m,x} x)_{m \in N \setminus X}$ are linearly independent. This shows that N can be split into a disjoint union $N = (N \setminus X) \cup X$ such that the elements of $N \setminus X$ are linearly independent in M_1 and the elements of X are linearly independent in M_3. That is, $r_2 \leq r_1 + r_3$. Combining this with the above inequality yields $\operatorname{rk} M_2 = \operatorname{rk} M_1 + \operatorname{rk} M_3$. □

Exercise I.5.10. Let R be an integral domain, M an R-module, and assume $M \cong R^r \oplus T$, with T a torsion module. Prove directly (that is, without using Theorem 5.6) that $r = \operatorname{rk} M$ and $T \cong \operatorname{Tor}_R(M)$.

Solution. We have an exact sequence

$$0 \longrightarrow R^r \longrightarrow M \longrightarrow T \longrightarrow 0$$

and by the above exercise, $\operatorname{rk} M = \operatorname{rk} R^r + \operatorname{rk} T$. Since the rank of a torsion module is 0 (every element is linearly dependent), we have $\operatorname{rk} M = r$. We also have an isomorphism $T \cong M/R^r$. Note that $\operatorname{Tor}(M) = \{(s,t) \in M \mid \exists r \in R, (rs, rt) = (0,0)\}$. Since R^r is a free module, if $rs = 0$ with $s \in R^r$, we must have $r = 0$. Thus, $\operatorname{Tor}(M) = \{(0,t) \mid t \in T\}$, and clearly this is isomorphic to T. □

Exercise I.5.11. Let R be an integral domain, let M, N be R-modules, and let $\varphi : M \to N$ be a homomorphism. For $m \in M$, show that $\operatorname{Ann}(\langle m \rangle) \subseteq \operatorname{Ann}(\langle \varphi(m) \rangle)$.

Solution. Let $a \in \operatorname{Ann}(\langle m \rangle)$ and consider $r\varphi(m) \in \langle \varphi(m) \rangle$. We have $a \cdot r\varphi(m) = r\varphi(am) = r\varphi(0) = 0$ so $a \in \operatorname{Ann}(\langle \varphi(m) \rangle)$. □

Exercise I.5.12. Complete the proof of uniqueness in Theorem 5.6. (The hint in Exercise IV.6.1 may be helpful.)

Solution. Let R be a PID and suppose M_1, M_2 are isomorphic R-modules. In particular, we have $\operatorname{Tor}(M_1) \cong \operatorname{Tor}(M_2)$ and $\operatorname{rk} M_1 = \operatorname{rk} M_2$. It suffices to show that the decomposition of the torsion submodule is equivalent. We have

$$\operatorname{Tor}(M_1) \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)} \cong \frac{R}{(b_1)} \oplus \cdots \oplus \frac{R}{(b_n)} \cong \operatorname{Tor}(M_2).$$

Since R is a PID and in particular a UFD, the decomposition of $\operatorname{Tor}(M_1)$ is unique up to associates so $m = n$. Thus, we can rearrange the factors such that the p_i are associate to the q_i for $i = 1, \ldots, n$. The uniqueness for form of elementary divisors follows easily. □

Exercise I.5.13. Let M be a finitely generated module over a Noetherian ring R.

Prove that if R is a PID, then M is torsion-free if and only if it is free. Prove that this property characterizes PIDs. (Cf. Exercise 4.3.)

Solution. If M is torsion-free, then the structure theorem yields $M \cong R^{\operatorname{rk} M}$ so M is free. If M is free, then it has a basis E. Let $m = a_1 e_1 + \cdots a_n e_n \in M$. Then for $r \neq 0$ in R

$$rm = (ra_1)e_1 + \cdots + (ra_n)e_n \neq 0$$

since $a_i \neq 0 \Rightarrow ra_i \neq 0$. Thus, M is torsion-free.

Now suppose that R is merely a Noetherian domain and every finitely generated module M is torsion-free if and only if it is free. Clearly every ideal $I \subseteq R$ is torsion-free and finitely generated, so I must be free. Assume I is generated by more than one element, say a_1, a_2. Then $a_2a_1 - a_1a_2 = 0$ is a dependence relation in R so $a_1 = a_2 = 0$, contradicting the fact that they form a basis for I. Thus, I is generated by one element and R is a PID. □

Exercise I.5.14. Give an example of a finitely generated module over an integral domain which is *not* isomorphic to a direct sum of cyclic modules.

Solution. Consider the integral domain $R = \mathbb{Z}[x]$ and the module $M = (2, x)$. Suppose M is a direct sum of cyclic $\mathbb{Z}[x]$ modules. If (N_a) is a family of cyclic submodules of M such that $M = \sum_{a\in A} N_a$ and $N_b \cap \sum_{a\neq b} N_a = 0$ for all $b \in A$, then each N_a is a principal ideal in $\mathbb{Z}[x]$. But clearly if $x_a \in N_a$ and $x_b \in N_b$ then $x_a x_b \in N_a \cap N_b$ so $N_a \cap N_b \neq 0$ and $|A| = 1$, which implies that M is a principal ideal, a contradiction. □

Exercise I.5.15. Prove that the prime ideals appearing in the elementary divisor version of the classification theorem for a torsion module M over a PID are the prime ideals containing the characteristic ideal of M, as defined in Remark 5.8.

Solution. Recall that given a torsion module

$$M \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)}$$

with $a_1 \mid \cdots \mid a_m$, we define

$$(a_1 \cdots a_m)$$

to be the characteristic ideal of M. To do. □

Exercise I.5.16. Prove that the prime ideals appearing in the elementary divisor version of the classification theorem for a module M over a PID are the associated primes of M, as defined in Exercise 4.5.

Solution. To do. □

Exercise I.5.17. Let R be a PID. Prove that the Grothendieck group of the category of finitely generated R-modules is isomorphic to $\mathbb{Z}$.

Solution. Let M be an R-module. By the structure theorem, we have $M \cong R^{\operatorname{rk} M} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$. Next note that we may construct the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "a"] & R \arrow[r] & \frac{R}{(a)} \arrow[r] & 0 \end{tikzcd}$$

which implies that $[R/(a)] = [0]$ for all $a \in R$. Then we consider the homomorphism $\varphi : K(R\text{-}\mathsf{Mod}^{fg}) \to \mathbb{Z}$ which sends a module M to $\operatorname{rk} M$. It is easy to check that this morphism is well-defined, it is surjective, and the kernel is $[0]$, so it is injective. Thus, φ is an isomorphism. □