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 $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) \mid M + M^t = 0\}$ 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 $\mathfrak{su}(n) = \{M \in \mathfrak{gl}_n(\mathbb{C}) \mid M + M^* = 0\}$ 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 $\mathrm{End}(A \oplus B)$ can be thought of as the set of 2×2 matrices of the form

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

so that homomorphisms from A and B interact with each other. Suppose $\dim(A) > 1$ so we can write $\mathrm{End}(A) = \mathrm{End}(\mathbb{Q}^m \oplus \mathbb{Q}^n)$ with $m, n \geq 1$. Note that the description of $\mathrm{End}(A \oplus B)$ 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 $\mathrm{End}(A)$ 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 $\mathrm{im}\ \varphi^{n+1} = \mathrm{im}\ \varphi^n$.

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 addi-

tion 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 $x^tA = y^tB$. 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 $e_i^tA = y_i^tB$ (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

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

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 $\{d_1e_1, \ldots, d_re_r\}$ 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. □