SMITH NORMAL FORM

BRUNO STONEK

1. Introduction: Elementary operations in linear algebra

An ubiquitous tool in linear algebra are elementary operations, for they allow us to compute different invariants of a matrix or a linear transformation. Let K be a field.

Elementary row operations: To perform an elementary row operation means to multiply on the left by an elementary matrix, which is a special type of invertible matrix. There are three kinds of these, corresponding to the three types of elementary operations. In fact, any invertible matrix is a product of elementary matrices.

Importantly, these operations do not alter the kernel of the matrix (a.k.a. the subspace of solutions of the homogeneous system of equations it defines), nor the row space.

If we interpret a matrix A as a linear transformation $K^n \to K^m$, $v \mapsto Av$, then to perform an elementary row operation amounts to post-composing it with a certain automorphism of K^m: indeed, this does not alter the kernel. The image (a.k.a. the column space), on the other hand, may be altered. But at least the rank is unchanged, as follows e.g. from the rank-nullity theorem.

If we perform elementary row operations judiciously enough (Gaussian elimination), then we can reach a row echelon form (or the reduced row echelon form, which is unique). This is particularly useful because these invariants are easily read off now: the rank r is the number of pivots, i.e. the number of "steps", and accordingly the dimension of the kernel is the number of rows minus r. If the row echelon form is moreover reduced, then the actual kernel is immediately read off this form. The image, in fact, can also be recovered: the columns *of the original matrix* corresponding to the columns with pivots in the echelon form are a basis for it.

Elementary column operations: Similarly, we can perform the same type of operations but on the columns. This amounts to multiplying our matrix by the same type of elementary matrices but on the right. These operations does not alter the image of the matrix (the column space). Interpreting the matrix as a linear transformation $K^n \to K^m$, then to apply an elementary column operation amounts to pre-composing it with a certain automorphism of K^n, so indeed, this does not alter the image. The kernel may be altered, but its dimension is unchanged, again by the rank-nullity theorem.

Using both: If we perform *both* elementary row and column operations, then both the kernel and the image are altered, but the rank (and therefore the dimension of the kernel) stay unchanged, so we can at least determine the isomorphism type of the image and the kernel. Sometimes this is all we want. Notice that doing both types of operations amounts to multiplying our matrix A on the left and on the right by (different) invertible matrices. [1] Two matrices A, B satisfy $B = UAV$ for some U, V invertible matrices if and only if they are matrices of the same linear transformation only on different bases both on the domain and the codomain, if and only if they have the same rank. Let us call this equivalence relation on matrices of a given size simply *equivalence*.

Starting with A, we could first do only row operations to bring it to reduced row echelon form. Then if we allow column operations, it's not hard to see that we can bring to exactly one matrix in block form,

[1] So the determinant is also unchanged when we do both row and column operations.

having an identity matrix in the top left corner, and rectangular zero matrices in the other three corners. For example,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{1.1}$$

corresponding to a linear transformation $K^4 \to K^3$ of rank 1, so the image is isomorphic to K and the kernel is isomorphic to K^3.

So this is another sort of normal form. It is different from the row reduced echelon form, and carries less information. For instance, it changes the kernel, so it is not immediately useful if we are solving systems of linear equations. [2] Indeed it only remembers the rank... But over more general rings, the generalization of this normal form contains more interesting information, as we shall now see.

2. The Smith Normal Form

We would like to generalize the normal form around (1.1) to modules over more general rings.[3] Then we will see how it is useful for different purposes.

We start by considering Euclidean domains such as $\mathbb{Z}$, $k[x]$ or $\mathbb{Z}[i]$, although we will swiftly switch to concentrating on $\mathbb{Z}$.

First of all, we need to understand what are our elementary operations. A different way to say that any invertible matrix over a field can be presented as a product of elementary matrices is to say that the general linear group $GL_n(K)$ is generated by the three types of elementary matrices. We want to say the same when we switch from a field to a general Euclidean domain R, and indeed it is true. First notice that exchanging rows/columns and adding to a row/column a multiple of another one are still invertible operations, but multiplying a row/column by an arbitrary $0 \neq r \in R$ is no longer invertible in general. Instead, we need to take $r \in R^\times$. With this caveat, the elementary matrices corresponding to these elementary operations generate all the invertible matrices:

Theorem 2.1. *If R is a Euclidean domain, then $GL_n(R)$ is generated by the elementary matrices as in linear algebra, only the ones that corresponds to multiplying a row/column by an element must be such that this element is invertible.*

Proof. See [1, App. D "Smith Normal Form over a Euclidean Ring"]. □

Remark 2.2. The matrices of $GL_n(\mathbb{Z})$ are called *unimodular*. Recall that a matrix with coefficients in a commutative ring R is invertible if and only its determinant is invertible in R. Therefore, unimodular matrices are the integer-valued matrices with determinant ± 1.

We want to use these elementary operations on rows and columns to bring a matrix to a simple form. In other words, we want to find a simple representative of the equivalence class of a matrix. We recall the definition of equivalence:

Definition 2.3. We say $A, B \in M_{m\times n}(R)$ are *equivalent* if there exist invertible matrices U, V such that $B = UAV$.

We now present our normal form:

---

[2] If we take care to keep track of the operations being done, i.e. if we do have the matrices U, V, then we can indeed solve the system of equations in this way. See Remark 2.7.

[3] If you're wondering if the row-reduced echelon form can also be generalized to more general rings like $\mathbb{Z}$, cf. the "Hermite normal form".

Definition 2.4. Let R be a domain and $D \in M_{m\times n}(R)$ be a non-zero matrix. We say D is in *Smith normal form* if it is of the form

$$\begin{pmatrix} a_1 & 0 & \cdots & & & \\ 0 & a_2 & & & & \\ \vdots & & \ddots & & & \\ & & & a_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

with $a_1 \mid a_2 \mid \cdots \mid a_r \neq 0$ in R.

Note that r is the rank of D.

The good news is this form always exists and is essentially unique, at least if we are over a PID. If moreover we are over a Euclidean domain, then a more explicit algorithm exists using elementary operations and the Euclidean algorithm, see the reference at Theorem 2.1.

Theorem 2.5. *If R is a principal ideal domain and $A \in M_{m\times n}(R)$ is a non-zero matrix, then there exist invertible matrices $U \in GL_n(R), V \in GL_m(R)$ such that UAV is in Smith normal form. Moreover, if $a_1 \mid a_2 \mid \cdots \mid a_r$ and $b_1 \mid b_2 \mid \cdots \mid b_r$ are the non-zero elements in the diagonal of two Smith normal forms of A, then a_i and b_i are associate (there exist $r_i \in R^\times$ such that $b_i = r_i a_i$).*

Proof. See [1, Thm. 43.8]. □

The elements $a_1, \ldots, a_r$ are called the *invariant factors* (or *elementary divisors*) of A. They are unique up to units, but if we are e.g. over $\mathbb{Z}$, we might as well take them positive so that they are truly unique. So let us do that from now on.

Remark 2.6. The situation is easier over a Euclidean domain than over a general PID because we then know that we can reach this form via elementary operations. Over $\mathbb{Z}$, this means we can add to a row/column a multiple of another one, we can exchange rows/columns, and we can multiply a row/column by -1. We shall not present the algorithm to reach the Smith normal form, but it is explained in Elman's book. Or you can use Sage to compute it! It even shows you the invertible matrices U, V needed to reach it.

Remark 2.7. One immediate application is the following: if we know not only the Smith normal form D of $A \in M_{m\times n}(\mathbb{Z})$ but also the unimodular matrices U, V such that $UAV = D$, then we can find the integer solutions to a system of linear equations $Ax = b$. Indeed, $Ax = b \iff DV^{-1}x = Ub$. Solving the system $Dy = Ub$ is simple because D is diagonal. Our solutions are then of the form $x = Vy$.

Note how the situation is more complicated than over a field. Over a field, matrices are equivalent if and only if they have the same rank, but over a PID matrices are equivalent if and only if they have the same Smith normal form, and we see that there are lots of non-equivalent matrices with the same rank. The underlying reason is torsion, a phenomenon which is non-existent over a field, where every module is free! We shall see torsion appear very soon.

Example 2.8.

- The Smith normal form of $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in M_{2\times 2}(\mathbb{Z})$ is $\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$. The steps are:

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & -6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

  Note how we used that $3 - 2 = 1$, i.e. there exist $a, b \in \mathbb{Z}$ such that $2a + 3b = 1$, because $2, 3$ are coprime. The above steps generalize to prove that if m, n are coprime, then the Smith normal form of $\begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}$ is $\begin{pmatrix} 1 & 0 \\ 0 & mn \end{pmatrix}$.

- The Smith normal form of $\begin{pmatrix} 1 & 3 & -1 \\ -1 & 2 & 1 \\ 0 & -1 & 1 \\ 2 & -1 & 0 \end{pmatrix} \in M_{4\times 3}(\mathbb{Z})$ is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{pmatrix}$.

So from the Smith normal form we can read off the rank r of a matrix $A \in M_{m\times n}(R)$, it is just the number of non-zero columns, but what else? Note that the isomorphism type of the image is not that interesting. The image is a submodule of R^m, but since R is a PID, then submodules of free modules are free, and thus $\mathrm{im}(A) \cong R^r$. But what about the cokernel? Here interesting things happen: torsion may appear, and this is not determined by the rank. But the Smith normal form allows us to obtain the isomorphism type of this cokernel!

From now on, we concentrate on the case $R = \mathbb{Z}$.

Proposition 2.9. *Let $A \in M_{m\times n}(\mathbb{Z})$ with invariant factors $a_1, \dots, a_r$. Then the cokernel of A, defined as the cokernel of the abelian group homomorphism $\mathbb{Z}^n \to \mathbb{Z}^m$ given by left multiplication by A, satisfies:*

$$\mathrm{coker}(A) \cong \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_r \oplus \mathbb{Z}^{m-r}.$$

Proof. Notice that a matrix and its Smith normal form have isomorphic cokernel, since we have just (pre)composed with isomorphisms. But it is clear that the cokernel of the Smith normal form of A is as stated, since its image is spanned by the column vectors. □

In other words, looking at the columns of the Smith normal form: an invariant factor 1 dies in the cokernel, an invariant factor $a \geq 2$ gives a cyclic group $\mathbb{Z}/a$, and a zero column gives a $\mathbb{Z}$. If $m > n$ then we still need to add some copies of $\mathbb{Z}$ to fill up to m. Or we can instead say that in the cokernel there are as many copies of $\mathbb{Z}$ as the number of rows minus the rank, that is, as many copies of $\mathbb{Z}$ as the number of zero rows in the Smith normal form.

Example 2.10. The two examples from Example 2.8 have cokernel $\mathbb{Z}/6$ and $\mathbb{Z}/5$ respectively. Recall that $\mathbb{Z}/6 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$ by the Chinese remainder theorem, but the presentation that the Smith normal form delivers is the former.

A big consequence of the Smith normal form is the fundamental theorem of finitely generated abelian groups:

Theorem 2.11. *Let G be a finitely generated abelian group. Then there exist unique k and unique positive $a_1 \mid a_2 \mid \cdots \mid a_r$ such that $A \cong \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_r \oplus \mathbb{Z}^k$.*

Proof. Since G is finitely generated, it can be generated by m elements for some finite m. A choice of such generators amounts to a choice of an epimorphism $\mathbb{Z}^m \to G$. Now, since a subgroup of a free, finitely generated abelian group is free and finitely generated [1, Prop. 44.1][4], the kernel of this epimorphism is free and finitely generated, say of rank n. [5] Thus we get a short exact sequence (a free resolution of G, actually):

$$0 \to \mathbb{Z}^n \to \mathbb{Z}^m \to G \to 0.$$

Now, a group homomorphism $\mathbb{Z}^n \to \mathbb{Z}^m$ is left multiplication by a matrix $A \in M_{m\times n}(\mathbb{Z})$, and the above short exact sequence presents G as the cokernel of A. We conclude using Proposition 2.9. □

[4] Fun fact: in non-abelian groups, it is also true and non-trivial that the subgroup of a free group is free (Nielsen–Schreier theorem). But it is no longer true that a subgroup of a finitely generated group must be finitely generated!

[5] In other words, a finitely generated abelian group is also finitely presented: not only there are finitely many generators, but finitely many relations between these generators. The previous footnote remarks that a finitely generated non-abelian group may not be finitely presented.

Remark 2.12. These $a_1, \dots, a_r$ are called the *invariant factors* of G, so the terminology coincides with the one from the Smith normal form of a matrix, not by coincidence. This form of the fundamental theorem is perhaps less well-known than the *primary decomposition* that presents G as $\mathbb{Z}^k \oplus \mathbb{Z}/(p_1^{b_1}) \oplus \cdots \oplus \mathbb{Z}/(p_t^{b_t})$ where $p_1, \dots, p_t$ are not-necessarily-distinct prime numbers and $b_1, \dots, b_t \geq 1$.

Remark 2.13. The proof of the fundamental theorem for finitely generated abelian groups G gives an explicit way to find the invariant factor decomposition of G, starting from a presentation of G. Let us spell this out in gory detail. Suppose we have a presentation of G. This means: we have m generators $\{x_1, \dots, x_m\}$ and n relations among the generators of G: $\sum_{j=1}^m a_{ij}x_j = 0$ for all $i = 1, \dots, n$, where $a_{ij} \in \mathbb{Z}$ are some coefficients. This is a linear system of equations with m unknowns and n equations: the coefficients form a matrix $A = (a_{ij}) \in M_{n \times m}(\mathbb{Z})$.

Now consider the free abelian group $\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_m$, and define the map $T : \mathbb{Z}^n \to \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_m$ via $T(e_i) = \sum_{j=1}^n a_{ij}x_j$ for $i = 1, \dots, n$, where $\{e_i\} \subset \mathbb{Z}^n$ is the standard basis. Then

$$\operatorname{im}(T) = \langle Te_1, \dots, Te_n \rangle = \left\langle \sum_{j=1}^m a_{1j}x_j, \dots, \sum_{j=1}^m a_{nj}x_j \right\rangle$$

so by definition of a presentation, we have $G \cong \frac{\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_m}{\operatorname{im}(T)}$. Identifying $\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_m$ with $\mathbb{Z}^m$ and seeing T as a map $T : \mathbb{Z}^n \to \mathbb{Z}^m$, this amounts to describing G as its cokernel. In other words, G sits in the following short exact sequence:

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{T} \mathbb{Z}^m \longrightarrow G \longrightarrow 0.$$

Note that the matrix of T in the standard bases is $(a_{ij})^T \in M_{m \times n}(\mathbb{Z})$. Notice the transpose: the relations of G are read in the *columns* of the matrix.

Example 2.14. We now give some concrete examples.

- Let $G = \mathbb{Z}^2/\langle(2,0)\rangle$ be the quotient of $\mathbb{Z}^2$ by the subgroup generated by the vector $(2,0)$. This gives a presentation of G: we have two generators and one relation saying that twice the first generator is zero. More abstractly, we have the following short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\left(\begin{smallmatrix} 2 \\ 0 \end{smallmatrix}\right)} \mathbb{Z}^2 \longrightarrow G \longrightarrow 0.$$

  This 2×1 matrix is already in Smith normal form. We immediately get that $G \cong \mathbb{Z}/2 \oplus \mathbb{Z}$.
- Let $G = \mathbb{Z}^2/\langle(2,2),(1,3)\rangle$. That is, our group G is presented by two generators u, v with relations $2u + 2v = 0$, $u + 3v = 0$. We have a short exact sequence

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\left(\begin{smallmatrix} 2 & 1 \\ 2 & 3 \end{smallmatrix}\right)} \mathbb{Z}^2 \longrightarrow G \longrightarrow 0.$$

  Computing the Smith normal form for this matrix, we get that its invariant factors are 1 and 4, so $G \cong \mathbb{Z}/4$.
- Suppose G is an abelian group with generators u, v, w satisfying $2u - 2v + 2w = 0$ and $5u + 3v + 3w = 0$. As explained in Remark 2.13, this means G sits in the following short exact sequence:

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\left(\begin{smallmatrix} 2 & 5 \\ -2 & 3 \\ 2 & 3 \end{smallmatrix}\right)} \mathbb{Z}^3 \longrightarrow G \longrightarrow 0.$$

  The invariant factors are 1 and 4, so $G \cong \mathbb{Z}/4 \oplus \mathbb{Z}$.

There is an additional property of the Smith normal form that may come in handy. It completely identifies the invariant factors, although it involves a lot of computations if the matrix is big.

Proposition 2.15. *Let $A \in M_{m\times n}(\mathbb{Z})$ with invariant factors $a_1 \mid \cdots \mid a_r$. Let Δ_ℓ be the gcd of all the ℓ-order minors of A for $1 \le \ell \le r$, and set $\Delta_0 = 1$. Then*

$$\Delta_0 \mid \Delta_1 \mid \cdots \mid \Delta_r \qquad \text{and} \qquad a_\ell = \frac{\Delta_\ell}{\Delta_{\ell-1}} \quad \text{for all } \ell \ge 1.$$

Proof. See [1, Thm. 43.8]. □

Example 2.16. You can go through the examples in Example 2.8 using the above proposition. The first one concerns a 2×2 matrix, so this gcd method is markedly shorter than using elementary operations.

The following proposition concerns the situation where the cokernel of a square matrix is finite. This happens precisely when the matrix is full rank. In this case, we can very easily determine the order of the cokernel, without having to determine the Smith normal form.

Proposition 2.17. *Let $A \in M_n(\mathbb{Z})$ be a square matrix with non-zero determinant. Then the subgroup index $[\mathbb{Z}^n : \mathrm{im}(A)]$ is $|\det(A)|$. In other words, the cokernel of A has $|\det(A)|$ elements.*

In particular, if $H \le \mathbb{Z}^n$ is a subgroup generated by vectors $v_1, \dots, v_n \in \mathbb{Z}^n$ and $A \in M_n(\mathbb{Z})$ is the square matrix having v_i as its i-th column, then $|\mathbb{Z}^n/H| \cong |\det(A)|$ provided $\det(A) \ne 0$.

Proof. If the determinant of A is not zero, then A has rank n and the Smith normal form is a diagonal matrix without zeros in the diagonal, because the Smith normal form does not change the absolute value of the determinant (it is obtained via multiplication with unimodular matrices). Let $a_1, \dots, a_n$ be the invariant factors: we thus have $|\det(A)| = a_1 \cdots a_n$. Now, $\mathrm{coker}(A) \cong \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_n$, and its order is indeed $a_1 \cdots a_n = |\det(A)|$.

See also [2, Thm. 1.17] for a printed reference. □

Example 2.18. The proposition above determines only the *index* of a subgroup of full rank in $\mathbb{Z}^n$, but sometimes this is enough to determine the quotient group, if one is lucky enough. For example: By the above, the quotient of $\mathbb{Z}^2$ by the subgroup H generated by the vectors $(1,2), (6,6)$ has order 6, but there is only one abelian group of order 6, so $\mathbb{Z}^2/H \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

For a simple example where the determinant does not determine the cokernel: consider the matrices $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$, which are in Smith normal form. They have the same determinant, and yet they have different cokernel. Indeed, they are respectively $\mathbb{Z}^2/\langle(2,0),(0,2)\rangle \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and $\mathbb{Z}^2/\langle(1,0),(0,4)\rangle \cong \mathbb{Z}/4$.

3. Computing homology

The Smith normal form also allows for computing the homology of a chain complex of free, finitely generated abelian groups:

Proposition 3.1. *Let $\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^m \xrightarrow{B} \mathbb{Z}^k$ be a complex of abelian groups, with $A \in M_{m\times n}(\mathbb{Z}), B \in M_{k\times m}(\mathbb{Z})$. Let $a_1, \dots, a_r$ be the invariant factors of A. Then we have an isomorphism of abelian groups:*

$$\frac{\ker(B)}{\mathrm{im}(A)} \cong \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_r \oplus \mathbb{Z}^{m-r-s}$$

where $s = \mathrm{rank}(B)$.

Proof. This proof is adapted from this page. Because $\mathrm{im}(A) \subset \ker(B)$, B descends to the quotient:

$$\bar{B} : \frac{\mathbb{Z}^m}{\mathrm{im}(A)} \to \mathbb{Z}^k$$

and its kernel is $\ker(\bar{B}) = \frac{\ker(B)}{\mathrm{im}(A)}$. By Proposition 2.9, $\frac{\mathbb{Z}^m}{\mathrm{im}(A)} \cong \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_r \oplus \mathbb{Z}^{m-r}$. Since the codomain of $\bar{B}$ is a free abelian group, all torsion in the domain must be in the kernel. Thus

$$\ker(\bar{B}) = \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_r \oplus \ker\big(\bar{B}|_{\mathbb{Z}^{m-r}}\big).$$

But $\ker(\bar{B}|_{\mathbb{Z}^{m-r}})$ is a subgroup of the free group $\mathbb{Z}^{m-r}$, hence is free itself. Note the rank of $\bar{B}|_{\mathbb{Z}^{m-r}}$ is the same as the rank of B, which is s. Therefore, by the rank-nullity theorem,

$$\mathrm{rank}(\ker(\bar{B}|_{\mathbb{Z}^{m-r}})) = m - r - s.$$

Therefore,

$$\frac{\ker(B)}{\mathrm{im}(A)} = \ker(\bar{B}) \cong \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_r \oplus \mathbb{Z}^{m-r-s}$$

as claimed. □

In words, the homology group is like the cokernel of A, only that we must remove as many copies of $\mathbb{Z}$ as the rank of B.

Example 3.2. We compute the homology in the middle of this chain complex:

$$\mathbb{Z}^3 \xrightarrow{\begin{bmatrix} 3 & 12 & 9 \\ 1 & 6 & 5 \\ 2 & 6 & 4 \end{bmatrix}} \mathbb{Z}^3 \xrightarrow{\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -1 & -1 \end{bmatrix}} \mathbb{Z}^4$$

The matrix on the left has invariant factors 1, 6 and rank 2, whereas the matrix on the right has rank 1, so we get that the homology group is $\mathbb{Z}/6$.

References

[1] Richard Elman. *Lectures on Abstract Algebra: Preliminary Version*. Department of Mathematics, University of California, Los Angeles, 2023. Available at https://www.math.ucla.edu/~rse/algebra_book.pdf.

[2] Ian Stewart and David O. Tall. *Algebraic Number Theory and Fermat's Last Theorem*, 3rd ed. A K Peters, Natick, MA, 2002.