1. $R$-modules

Let $R$ be a commutative ring with 1. An $R$ module is an abelian group $M$ together with a “scalar” multiplication by $R$, satisfying the same axioms as a vector space. In particular, if $R$ is a field, then $M$ is a vector space over $R$. Let $S = (v_1, v_2, \ldots, v_m)$ be an ordered set of elements in $M$. We say that $S$ generates $M$, if every element $v$ in $M$ can be written as a linear combination

$$v = r_1v_1 + \ldots + r_mv_m$$

for some $r_1, \ldots, r_m$ in $R$. We say that $S$ is independent if

$$0 = r_1v_1 + \ldots + r_mv_m$$

implies that $r_1 = \ldots = r_m = 0$. The set $S$ is a basis, if it is both, generates $M$, and is linearly independent. Note that, in general, a module need not have a basis. For example, if $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, then $(1)$ (and nothing else) generates $M$, yet $2 \cdot 1 = 0$. On the other hand, if $M$ has a basis then $M \cong R^m$. 

We can perform the following three operations on any set $S$ of elements in $M$:

- Permute any two elements of $S$.
- Multiply an element in $S$ by an element in $R^\times$.
- Add a multiple of an element to another element.

Note that these operations are reversible, and preserve independent and generating sets.

Assume now that $M$ has a basis $(v_1, \ldots, v_m)$ and $N$ is a submodule generated by $(w_1, \ldots, w_n)$. Then there exist elements $a_{ij}$ in $R$ such that for every $i$,

$$w_i = a_{i1}v_1 + \ldots + a_{mi}v_m.$$ 

In particular, $a_{ij}$ form an $m \times n$-matrix $A$. Now note that the three operations on $(w_1, \ldots, w_n)$ correspond to the standard column operations on the matrix $A$, while on $(v_1, \ldots, v_m)$ they correspond to inverse row operations. More precisely, multiplying $v_i$ by a scalar $r$ corresponds to dividing the $i$-th row by $r$. Similarly, adding a multiple of $v_i$ to $v_j$ corresponds to subtracting the same multiple of the $j$-th row to the $i$-th row. (Hope this is OK). Assume now that the matrix $A$ can be reduced, by row and column operations, to a matrix with zeroes except for the first $k$ entries $d_1, \ldots, d_k$ on the diagonal. This implies that $N \cong R^k$ and

$$M/N \cong R/(d_1) \oplus \ldots \oplus R/(d_k) \oplus R^{m-k}.$$ 

For example, if $R$ is a field, the reduction can be accomplished (Gauss’ elimination procedure), and non-zero diagonal entries can be taken to be one. In fact, this shows that vector spaces are classified by its dimension. Diagonalization can be accomplished for $\mathbb{Z}$ as well, and this is the topic of the next section.
2. \textit{Z-modules}

Here we show that $A$ can be diagonalized, and moreover, diagonal terms satisfy

$$d_1|d_2|\ldots|d_k.$$ 

(to be completed ...)

2.1. \textbf{Example.} Let $M$ be the $Z$-submodule of $Z^2$ spanned by the columns of the matrix

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 3 \end{pmatrix}.$$ 

We illustrate $M$ (black dots) as a submodule of $Z^2$ in the following picture:

We shall now perform row and column operations. First, add the first column to the second. We get the matrix

$$A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix}.$$ 

This column operation corresponds to a change of basis in $M$, and the corresponding figure is:
Second, subtract the first row from the second, and get the matrix

\[ A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}. \]

This row operation corresponds to a change of basis in \( \mathbb{Z}^2 \), and the corresponding figure is:

As a consequence, we obtain \( \mathbb{Z}^2/M \cong \mathbb{Z}/4\mathbb{Z} \). In particular, the index of \( M \) is 4, which, by no accident, is equal to the determinant of \( A_2 \). Since row and column operations only change a sign of the determinant, note that the information about the index can be obtained already from the matrix \( A \), which has determinant \(-4\).
3. Generators of $SL_n(\mathbb{Z})$

Let $A$ be an $n \times n$-matrix. As is well known, the column operations correspond to multiplying $A$ by certain elementary matrices. For example, if $n = 2$, then multiplying $A$ from the right by

$$
\begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}, 
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}
\text{ and } 
\begin{pmatrix}
-1 & 0 \\
0 & 1
\end{pmatrix}
$$

corresponds, respectively, to

- Adding the first column of $A$ to the second.
- Permuting the two columns of $A$.
- Changing signs in the first column of $A$.

Similarly, row operations correspond to multiplying $A$ by the elementary matrices from the left. An inconvenience here is the last two matrices have determinant $-1$. In order to remedy this, we shall replace them by the following matrices of determinant $1$:

$$
\begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}, 
\begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}
\text{ and } 
\begin{pmatrix}
-1 & 0 \\
0 & -1
\end{pmatrix}.
$$

Multiplying $A$ by these three matrices corresponds to so-called strict column operations:

- Adding the first column of $A$ to the second.
- Permuting two columns of $A$, and changing the signs in one.
- Changing the signs in both columns of $A$.

Proposition 3.1. All strict row/column operations can be obtained by repeated application of the first kind of operations: adding a multiple of row/column to another row/column.

Proof. The proof follows from the following identities satisfied by elementary matrices:

$$
\begin{pmatrix}
0 & 1 \\
-1 & 0
\end{pmatrix} = \begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix} \begin{pmatrix}
1 & 0 \\
-1 & 1
\end{pmatrix} \begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix},
$$

and

$$
\begin{pmatrix}
-1 & 0 \\
0 & -1
\end{pmatrix} = \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix} \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}.
$$

Let $x_{ij}$ with $i \neq j$ be the $n \times n$ matrix such that all entries are $0$ except the entry at the position $(i, j)$ which is $1$. Let $e_{ij} = I + x_{ij}$.

Theorem 3.2. The group $SL_n(\mathbb{Z})$ is generated by elementary matrices $e_{ij}$, with $i \neq j$. We have $n^2 - n$ generators in all.

Proof. Let $A$ be in $SL_n(\mathbb{Z})$. Then, using the strict row/column operations, the matrix $A$ can be reduced to a diagonal matrix with integers $d_1, \ldots, d_n$ on the diagonal such that $d_1|d_2| \ldots |d_n$ and $d_2, \ldots, d_n$ positive. Indeed, note that the strict operations allow change of signs in two rows/columns at a time, so we can always arrange that all but one of the diagonal terms is positive. However, since $d_1 \cdot \ldots \cdot d_n = 1$, it follows that $d_1 = \ldots = d_n = 1$. In particular, $A$ can be reduced to the identity matrix using the strict operations only. Since the matrices $e_{ij}$ generate all strict operations, the theorem follows.