Example:
\[ \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 4 & 6 & 0 \\ 0 & 6 & 0 \\ 0 & 6 & 0 \end{pmatrix} \begin{pmatrix} 4 & 2 & 0 \\ 0 & 6 & 0 \\ 0 & 6 & 0 \end{pmatrix} \]

over \( \mathbb{Z} \)

\[ \begin{pmatrix} 2 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \]

\( \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z} \)

(assuming uniqueness)

What about the case of a PID?
Same "algorithm" applies, if we can find a replacement for the Euclidean algorithm performed on entire columns (rows are analogous).

What I need: Given two vectors

\[ u = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}, \quad v = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \in \mathbb{R}^m \quad (R \neq P \neq P) \]

I would like to have \( R \)-valued linear combinations \( \tilde{u}, \tilde{v} \) of \( u, v \) such that \( u, v \) are also \( R \)-valued linear combinations of \( \tilde{u}, \tilde{v} \) but the first coordinate of \( \tilde{v} \) is 0.
Consequently, the first coordinate of \( \overline{u} \) must be \( \gcd(x_1, y_1) \).

Rephrase this last using some algebra:

The \( \mathbb{R}^m \) is a free \( \mathbb{R} \)-module on a set of \( m \) generators (vectors), \( u, v \in \mathbb{R}^m \), generate a submodule \( \langle u, v \rangle = M \). Now consider projection to the first row coordinate. This is a homomorphism of \( \mathbb{R} \)-modules

\[ M \xrightarrow{\phi} \mathbb{R} \]

This may not be onto. Consider \( \text{Im } \phi < \mathbb{R} \). This is a submodule of \( \mathbb{R} \equiv \text{ an ideal.} \)
But $R$ is a P.I.D. So the ideal $\text{Im} \, \phi$ is principal.

$\text{Im} \, \phi = (a)$.  

But since $R$ is an integral domain,

$a : R \to (a)$ is an isomorphism of $R$-modules.

$0 \to N \to M \xrightarrow{\phi} R \to 0$

Denote the kernel by $N$.

In general, for any commutative ring $R$, if we have a short exact sequence

$0 \to N \xrightarrow{i} M \xrightarrow{\phi} R \to 0$
It is split (by definition, this means that $\sigma$ has a right inverse, an $s$ such that $\sigma \circ s = \text{Id}_{\mathcal{F}(s)}$).

To see this, we know $\sigma$ is onto, but, for $x \in \mathcal{S}$,

$s(x) \in \mathcal{M}$ be any element in such that $\sigma(m) = x$. Use the universal property of a free module.

The significance of a split short exact sequence

$$0 \to M_1 \xrightarrow{i} M \xrightarrow{j} M_2 \to 0 \quad j \circ s = \text{Id}$$

We have an isomorphism

$$M_1 \otimes M_2 \xrightarrow{i} M$$
Given by

\[(m_1, m_2) \mapsto n_1 m_1 + s \cdot m_2\]

Onto: Let \(x \in M\), \(y = s \cdot x - x\) so

\[s \cdot x - x = n \cdot y \quad \text{for some } y \in M\]

\[(y, s \cdot x) \mapsto n \cdot y + s \cdot x = x.\]

Injective: Suppose \(n \cdot m_1 + s \cdot m_2 = 0\).

Apply \(g\): \(x = m_1 + m_2 = 0 \implies m_2 = 0\)

\[n \cdot m_1 = 0 \quad \text{but } n \cdot m_1 \text{ is injective.}\]

In our case, we have

\[0 \to N \hookrightarrow M \overset{\alpha \cdot p}{\to} R \to 0\]
\[ \iota \circ \theta : N \otimes R \to M \]

is an isomorphism. It remains to show that 

\( N \) is generated by a single element.

The key trick for this construction: Apply the

functor

\[ Q \otimes_R \cdot : \text{R-modules} \to \text{Q-modules} \to \text{Q-vector spaces} \]

where \( Q \) is the field of fractions of \( R \).

**Proposition:** For a short exact sequence of

\( \text{R-modules} \)

\[ 0 \to N_1 \overset{i_1}{\to} M \overset{i_2}{\to} N_2 \to 0 \]

the sequence of vector spaces

\[ 0 \to Q \otimes_R N_1 \overset{Q \otimes_R i_1}{\to} Q \otimes_R M \overset{Q \otimes_R i_2}{\to} Q \otimes_R N_2 \to 0 \]
is exact. (All one needs to know that $A \otimes_R \mathfrak{i}$ is injective.)

For $M$ a free module, $i: N_1 \to N_2$ an injection of $R$-modules, $M \otimes_R i$ is injective.

$$
\Pi = R(S) = \bigoplus_{S} i: \bigoplus_{S} N_1 \to \bigoplus_{S} N_2.
$$

The dimension of the $R$-vector space $A \otimes_R M$ for an $R$-module $M$ is called the rank of $M$.

In one case $M = N \oplus R$.

We can argue that $M \cong R^{\aleph_0}$ is free ($R$ PID).

Therefore also $N \cong R$ is free. $N$ has two generators.
so rank $(M) \leq 2$. But rank is additive so rank $N \leq 1$. But then rank of a free module on $k$ generators is $k$. Therefore, $N$ is free on $\leq 1$ generators.

**HW 1.** Prove that when $R$ is an integral domain and $K$ is its fraction field and $\varphi: M \to N$ is an injective homomorphism of $R$-modules, then

$$Q \otimes_R \varphi: Q \otimes_R M \to Q \otimes_R N$$

is injective.
(2) Let $A$ be an abelian group with generators $x, y, z$ and relations

\[ 6x + 8y + 12z = 0 \]
\[ 4x + 8y + 6z = 0. \]

Write $A = \bigoplus \mathbb{Z} \oplus \mathbb{Z}/m_1 \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k \mathbb{Z}$

\($(< m_1 | m_2 | \cdots | m_k \ >)$ \(\text{ (The canonical form).} \)\)