m is the rank of m, then for every nonzero $v \in M$, there are some $a, a_1, \ldots, a_m \in A$, not all zero, such that

$$av = a_1u_1 + \cdots + a_mu_m.$$

We must have $a \neq 0$, since otherwise, linear independence of the u_i would imply that $a_1 = \cdots = a_m = 0$, contradicting the fact that $a, a_1, \ldots, a_m \in A$ are not all zero.

Unfortunately, in general, a torsion-free module is not free. For example, $\mathbb{Q}$ as a $\mathbb{Z}$-module is torsion-free but not free. If we restrict ourselves to finitely generated modules over PID's, then such modules split as the direct sum of their torsion module with a free module, and a torsion module has a nice decomposition in terms of cyclic modules.

The following proposition shows that over a PID, submodules of a free module are free. There are various ways of proving this result. We give a proof due to Lang [109] (see Chapter III, Section 7).

Proposition 35.5. *If A is a PID and if F is a free A-module of dimension n, then every submodule M of F is a free module of dimension at most n.*

Proof. Let $(u_1, \ldots, u_n)$ be a basis of F, and let $M_r = M \cap (Au_1 \oplus \cdots \oplus Au_r)$, the intersection of M with the free module generated by $(u_1, \ldots, u_r)$, for $r = 1, \ldots, n$. We prove by induction on r that each M_r is free and of dimension at most r. Since $M = M_r$ for some r, this will prove our result.

Consider $M_1 = M \cap Au_1$. If $M_1 = (0)$, we are done. Otherwise let

$$\mathfrak{a} = \{a \in A \mid au_1 \in M\}.$$

It is immediately verified that $\mathfrak{a}$ is an ideal, and since A is a PID, $\mathfrak{a} = a_1A$, for some $a_1 \in A$. Since we are assuming that $M_1 \neq (0)$, we have $a_1 \neq 0$, and $a_1u_1 \in M$. If $x \in M_1$, then $x = au_1$ for some $a \in A$, so $a \in a_1A$, and thus $a = ba_1$ for some $b \in A$. It follows that $M_1 = Aa_1u_1$, which is free.

Assume inductively that M_r is free of dimension at most $r < n$, and let

$$\mathfrak{a} = \{a \in A \mid (\exists b_1 \in A) \cdots (\exists b_r \in A)(b_1u_1 + \cdots + b_ru_r + au_{r+1} \in M)\}.$$

It is immediately verified that $\mathfrak{a}$ is an ideal, and since A is a PID, $\mathfrak{a} = a_{r+1}A$, for some $a_{r+1} \in A$. If $a_{r+1} = 0$, then $M_{r+1} = M_r$, and we are done.

If $a_{r+1} \neq 0$, then there is some $v_1 \in Au_1 \oplus \cdots \oplus Au_r$ such that

$$w = v_1 + a_{r+1}u_{r+1} \in M.$$

For any $x \in M_{r+1}$, there is some $v \in Au_1 \oplus \cdots \oplus Au_r$ and some $a \in A$ such that $x = v + au_{r+1}$. Then, $a \in a_{r+1}A$, so there is some $b \in A$ such that $a = ba_{r+1}$. As a consequence

$$x - bw = v - bv_1 \in M_r,$$