and so $x = x - bw + bw$ with $x - bw \in M_r$, which shows that

$$M_{r+1} = M_r + Aw.$$

On the other hand, if $u \in M_r \cap Aw$, then since $w = v_1 + a_{r+1}u_{r+1}$ we have

$$u = bv_1 + ba_{r+1}u_{r+1},$$

for some $b \in A$, with $u, v_1 \in Au_1 \oplus \cdots \oplus Au_r$, and if $b \neq 0$, this yields the nontrivial linear combination

$$bv_1 - u + ba_{r+1}u_{r+1} = 0,$$

contradicting the fact that $(u_1, \ldots, u_{r+1})$ are linearly independent. Therefore,

$$M_{r+1} = M_r \oplus Aw,$$

which shows that M_{r+1} is free of dimension at most $r + 1$. $\square$

The following two examples show why the hypothesis of Proposition 35.5 requires A to be PID. First consider $6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ as a free $6\mathbb{Z}$-module with generator $\overline{1}$. The $6\mathbb{Z}$-submodule $\{\overline{0}, \overline{2}, \overline{4}\}$ is not free, even though it is generated by $\overline{2}$ since $\overline{3} \cdot \overline{2} = \overline{0}$. Proposition 35.5 fails since $6\mathbb{Z}$ is not even an integral domain. Next consider $\mathbb{Z}[X]$ as a free $\mathbb{Z}[X]$-module with generator 1. We claim the ideal

$$(2, X) = \{2p(X) + Xq(X) \mid p(X), q(X) \in \mathbb{Z}[X]\},$$

is not a free $\mathbb{Z}[X]$-module. Indeed any two nonzero elements of $(2, X)$, say $s(X)$ and $t(X)$, are linearly dependent since $t(X)s(X) - s(X)t(X) = 0$. Once again Proposition 35.5 fails since $\mathbb{Z}[X]$ is not a PID. See Example 32.1.

Proposition 35.5 implies that if M is a finitely generated module over a PID, then any submodule N of M is also finitely generated.

Indeed, if $(u_1, \ldots, u_n)$ generate M, then we have a surjection $\varphi\colon A^n \to M$ from the free module A^n onto M. The inverse image $\varphi^{-1}(N)$ of N is a submodule of the free module A^n, therefore by Proposition 35.5, $\varphi^{-1}(N)$ is free and finitely generated. This implies that N is finitely generated (and that it has a number of generators $\leq n$).

We can also prove that a finitely generated torsion-free module over a PID is actually free. We will give another proof of this fact later, but the following proof is instructive.

Proposition 35.6. *If A is a PID and if M is a finitely generated module which is torsion-free, then M is free.*

Proof. Let $(y_1, \ldots, y_n)$ be some generators for M, and let $(u_1, \ldots, u_m)$ be a maximal subsequence of $(y_1, \ldots, y_n)$ which is linearly independent. If $m = n$, we are done. Otherwise, due to the maximality of m, for $i = 1, \ldots, n$, there is some $a_i \neq 0$ such that such that