Cor 3 Let $L \subset \mathbb{R}^n$ be a lattice, and let $u_1, \dots, u_k$ be linearly independent vectors in L. Then the following are equivalent:

(a) there are $u_{k+1}, \dots, u_n \in L$ s.t. $u_1, \dots, u_k, \dots, u_n$ are a basis of L (i.e., $(u_1, \dots, u_k)$ is a primitive k-tuple)

(b) $\mathrm{span}_{\mathbb{Z}}(u_1, \dots, u_k) = L \cap \mathrm{span}_{\mathbb{R}}(u_1, \dots, u_k)$.

Pf (a) $\Rightarrow$ (b). It is clear that any $u \in \mathrm{span}_{\mathbb{Z}}(u_1, \dots, u_k)$ belongs to both L and $\mathrm{span}_{\mathbb{R}}(u_1, \dots, u_k)$. For the reverse inclusion, let $u \in L \cap \mathrm{span}_{\mathbb{R}}(u_1, \dots, u_k)$ and write $u = \sum_{i=1}^{k} b_i u_i = \sum_{i=1}^{n} a_i u_i$, where $b_1, \dots, b_k \in \mathbb{R}$,

$a_1, \dots, a_n \in \mathbb{Z}$, and $u_{k+1}, \dots, u_n$ are as in (a).

Since the u_i are a basis of $\mathbb{R}^n$, there is a unique way to write u as a linear combination of $u_1, \dots, u_n$, so $a_1 = b_1, \dots, a_k = b_k$, $a_{k+1} = \dots = a_n = 0$. Thus $u \in \mathrm{span}_{\mathbb{Z}}(u_1, \dots, u_k)$.

(b) $\Rightarrow$ (a) By a corollary from the lecture, there is a basis $v_1, \dots, v_n$ of L, ~~so that~~ and $m_{ij} \in \mathbb{Z}$ s.t.

(*)
$$u_1 = m_{11} v_1 \qquad k \geq i \geq j \geq 1$$
$$\vdots \qquad m_{kk} > 0$$
$$u_k = m_{k1} v_1 + \dots + m_{kk} v_k \qquad 0 \leq m_{ij} < m_{ii}$$

Each of $v_1, \dots, v_k$ is in $\mathrm{span}_{\mathbb{R}}(u_1, \dots, u_k) \cap L$ by (*) and so by (b), in $\mathrm{span}_{\mathbb{Z}}(u_1, \dots, u_k)$.

Considering (*) and u_1, this gives $m_{11} = 1$, $u_1 = v_1$.

Moving to 2nd line in (*), we have

$$u_2 = m_{21} v_1 + m_{22} v_2 = m_{21} u_1 + m_{22} v_2$$
$$= m_{21} u_1 + m_{22} (\alpha u_1 + \beta u_2) \quad \text{where } \alpha, \beta \in \mathbb{Z}$$

Since u_1, u_2 are linearly independent:
$1 = m_{22} \beta$, and since $m_{22} \in \mathbb{N}$, $m_{22} = \beta = 1$

$\Rightarrow$ (since $0 \leq m_{21} < m_{22} = 1$) $m_{21} = 0 \Rightarrow u_2 = v_2$.

Continuing inductively in this way we get

$u_1 = v_1, \ldots, u_k = v_k$, and to derive ⓐ we take $u_{k+1} = v_{k+1}, \ldots, u_n = v_n$.