Q5

(1)

Denote the columns of A by $A = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$. Without loss of generality, let $\mathbf{a}_n$ be a non-zero linear combination of the other $n-1$ columns: $\mathbf{a}_n = A'\mathbf{z}'$ for some $\mathbf{z} \in \mathbb{Z}^{n-1}$.

It is easy to see that because A' contains only a subset of columns of A, so $A'\mathbb{Z}^{n-1} \subseteq A\mathbb{Z}^n$. It naturally follows that

$$A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m \subseteq A\mathbb{Z}^n + q\mathbb{Z}^m$$

On the other hand, let $\mathbf{v} \in A\mathbb{Z}^n + q\mathbb{Z}^m$, then there exist $\mathbf{x}_1 \in \mathbb{Z}^n, \mathbf{x}_2 \in \mathbb{Z}^m$ such that

$$\begin{aligned}
\mathbf{v} &= A\mathbf{x}_1 + q\mathbf{x}_2 \\
&= \sum_{i=1}^{n} (\mathbf{a}_i \mathbf{x}_{(1,i)}) + q\mathbf{x}_2 \\
&= (\sum_{i=1}^{n-1} \mathbf{a}_i x_{(1,i)}) + \mathbf{a}_n x_{(1,n)} + q\mathbf{x}_2 \\
&= A' \cdot (x_{(1,1)}, x_{(1,2)}, \ldots, x_{(1,n-1)}) + A'\mathbf{z}' x_{(1,n)} + q\mathbf{x}_2 \\
&= A'((x_{(1,1)}, x_{(1,2)}, \ldots, x_{(1,n-1)}) + \mathbf{z}' x_{(1,n)}) + q\mathbf{x}_2 \in A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m
\end{aligned}$$

Therefore we have $A\mathbb{Z}^n + q\mathbb{Z}^m \subseteq A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m$, and the two lattices are indeed equal.

(2)

For the remainder of this problem, we assume that full-rank LWE with parameters (m, n, q, U_s, χ_e) exist, which means that $n \leq m$. To differentiate full-rank LWE with possibly-not-full-rank LWE, we denote full-rank LWE with LWE* and possibly-not-full-rank LWE.

Let $(A, \mathbf{b})$ be a sample from generic (aka potentially not full-rank) LWE(m, n, q, U_s, χ_e). Without loss of generality, assume that $A = [A_1 \mid A_2] \in \mathbb{Z}_q^{m \times (n_1 + n_2)}$ where A_1 is full-rank, and $A_2 = A_1 B$ for some non-zero $B \in \mathbb{Z}_q^{n_1 \times n_2}$. Denote the secret by $\mathbf{s} = [\mathbf{s}_1 \mid \mathbf{s}_2]$ where $\mathbf{s}_1 \leftarrow \chi_s^{n_1}, \mathbf{s}_2 \leftarrow \chi_s^{n_2}$, then:

$$\begin{aligned}
\mathbf{b} &= A\mathbf{s} + \mathbf{e} \\
&= (A_1\mathbf{s}_1 + A_2\mathbf{s}_2) + \mathbf{e} \\
&= A_1\mathbf{s}_1 + A_1 B\mathbf{s}_2 + \mathbf{e} \\
&= A_1(\mathbf{s}_1 + B\mathbf{s}_2) + \mathbf{e}
\end{aligned}$$

Since the secret is sampled from a uniformly random distribution, $\mathbf{s}_1$ and $\mathbf{s}_2$ are both uniformly random. Therefore, $\mathbf{s}_1 + B\mathbf{s}_2$ is also uniformly random. This means that $(A_1, \mathbf{b})$ is a valid sample from LWE$^*(m, n_1, q, U_s, \chi_e)$ where $n_1 < n$. Assuming that there is a unique solution to $(A_1, \mathbf{b})$, if we can solve this instance of full-rank LWE, then the solution must be $\mathbf{s}'$ such that $\mathbf{b} - A_1\mathbf{s}' = \mathbf{e}$ is exactly the error term of the original $(A, \mathbf{b})$. With the error term recovered, the LWE problem $(A, \mathbf{b})$ becomes solving linear equations, which can be efficiently computed using Gaussian eliminations.

It remains to show that given an oracle that solves full-rank LWE of a higher dimension n, we can solve full-rank LWE of a lower dimension $n_1 < n$.

Given $(A_1, \mathbf{b})$ where $A \in \mathbb{Z}_q^{m \times n_1}$ is full-rank, I claim without proof that there exists an efficient algorithm that can output a vector $\mathbf{a}^* \in \mathbb{Z}_q^m$ such that $[A \mid \mathbf{a}]$ is still full-rank (see problem 1). Using this algorithm, we can augment A_1 into a full-rank matrix with n columns $A' = [A_1 \mid A_2']$. We can sample $\mathbf{s}_2'$ from U_s and compute $\mathbf{b}' = \mathbf{b} + A_2'\mathbf{s}_2'$, then $(A', \mathbf{b}')$ is a valid instance of LWE$^*(m, n, q, U_s, \chi_e)$. Assuming that $(A', \mathbf{b}')$ has unique solution, then the solution must be $\mathbf{s}_1 \mid \mathbf{s}_2'$, and we can obtain $\mathbf{s}_1$, which is the solution to $(A_1, \mathbf{b})$. Thus we have solved full-rank LWE of a lower dimension.

P.S. the second reduction is very similar to the reduction in which an oracle for higher dimension LWE (not necessarily full-rank) can be used to solve lower dimension LWE by augmenting the lower dimension

LWE instance. The only difference is that augmenting the lower dimension instance requires sampling linearly independent columns instead of sampling random columns.