Q9

Let $(A, \mathbf{b}) \leftarrow \text{LWE}(n, n, q, \chi_e, \chi_s)$. In other words, A is uniformly randomly sampled from all full-rank matrices $\mathbb{F}_q^{n\times n}$, $\mathbf{s} \leftarrow \chi_e^n$, $\mathbf{e} \leftarrow \chi_s^n$, and $\mathbf{b} \leftarrow A\mathbf{s} + \mathbf{e}$.

I claim that matrix inversion $A \mapsto A^{-1}$ on the set of full-rank matrices is a bijection. This is true because the inverse of two distinct matrices is necessarily distinct (injectivity), and every full-rank matrix is the inverse of its inverse (surjectivity).

Because matrix inversion is a bijection from the set of invertible matrices onto itself, if A is uniformly sampled from all full-rank matrices $\mathbb{F}_q^{n\times n}$, then A^{-1} is also a uniformly randomly sampled matrix from the set all full-rank matrices.

Notice that $A^{-1}\mathbf{b} = A^{-1}A\mathbf{s} + \mathbf{e} = A^{-1}\mathbf{e} + \mathbf{s}$. Since $\mathbf{e}$ is sampled from the secret distribution and $\mathbf{s}$ is sampled from the error distribution, A^{-1} is a uniformly random sample, $(A^{-1}, A^{-1}\mathbf{b}) = (A^{-1}, A^{-1}\mathbf{e} + \mathbf{s})$ is a sample from $\text{LWE}(n, n, q, \chi_s, \chi_e)$. If there exists an oracle for $\text{LWE}(n, n, q, \chi_s, \chi_e)$, then this oracle can recover $\mathbf{e}$, and from here we can recover $\mathbf{s}$ in $\text{LWE}(n, n, q, \chi_e, \chi_s)$.

The argument above did not assume anything specific to χ_s or χ_e, so they can be swapped, and we will arrive at the inverse conclusion that $\text{LWE}(n, n, q, \chi_s, \chi_e)$ reduces to $\text{LWE}(n, n, q, \chi_e, \chi_s)$, as well. Therefore, the two problems are equivalent.