Solution to Problem Set 5, Problem 1(a)

**Problem 1(a)** Let $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ be an $m \times n$ matrix with entries in a field $F$. Consider the $m$ linear polynomials

\[
g_1 = a_{11}x_1 + \cdots + a_{1n}x_n, \\
\vdots \\
g_m = a_{m1}x_1 + \cdots + a_{mn}x_n
\]

in $F[x_1, \ldots, x_n]$. Let $E$ be an echelon form of $A$ and $R$ be a reduced echelon form of $A$, and $I \subset F[x_1, \ldots, x_n]$ be the ideal generated by $g_1, \ldots, g_m$. Assume that $I \neq (0)$, i.e., $g_i \neq 0$ for some $i$. Show that the linear polynomials associated to the non-zero rows of $E$ form a minimal Gröbner basis for $I$.

**Solution:** Let $h_1, \ldots, h_t$ be the linear polynomials corresponding to the non-zero rows of $E$. Clearly $(h_1, \ldots, h_t) = I$. We need to show that $h_1, \ldots, h_t$ form a Gröbner basis for $I$. Denote the leading term of each $h_i$ by $LT(h_i) = x_k$ ($h_i$ is monic because $E$ is an echelon form). For $i \neq j$, since $E$ is an echelon form, we have $k_i \neq k_j$, and minimality follows.

To show that $h_1, \ldots, h_t$ form a Gröbner basis for $I$, we use Buchberger’s algorithm. That is, the remainder of dividing $S(h_i, h_j) = x_k h_i - x_k h_j$ by $h_i, h_j$ is zero. I will denote this remainder by $S(h_i, h_j) \mod \{f, g\}$.

For simplicity denote $h_i = f$ and $h_j = g$. Let $\tilde{f} = f - LT(f)$, and $\tilde{g} = g - LT(g)$. Then $S := S(f, g) = (g - \tilde{g})f - (f - \tilde{f})g = \tilde{f}g - \tilde{g}f$. It thus remains to prove the following.

**General claim:** If $LT(f)$ and $LT(g)$ are co-prime, and $LT(f) > LT(\tilde{f})$, $LT(g) > LT(\tilde{g})$, then $\tilde{f}g - \tilde{g}f \equiv 0 \mod \{f, g\}$.

**Proof of the claim:** We argue by induction on $t(\tilde{f}, \tilde{g}) = \text{number of terms in } \tilde{f} + \text{number of terms in } \tilde{g}$. The claim is trivial if $\tilde{f} = 0$ or $\tilde{g} = 0$. In particular, this covers the base case, where $t(\tilde{f}, \tilde{g}) = 0$.

For the induction step, we may assume that $\tilde{f}, \tilde{g} = 0$. Now $LT(\tilde{f}g) = LT(\tilde{f})LT(g) \neq LT(\tilde{g})LT(f) = LT(\tilde{g}f)$. Thus $LT(S) = LT(\tilde{f}g)$ or $LT(S) = -LT(\tilde{g}f)$. By symmetry, we may assume that $LT(S) = LT(\tilde{f}g) = LT(\tilde{f})LT(g)$. Subtracting $LT(\tilde{f})g$ from $S$, we get $S = (\tilde{f} - LT(\tilde{f}))g - \tilde{g}f$. By the induction assumption, $S \equiv 0 \mod \{f, g\}$. □

**Remark:** In order to conclude that the remainder of $S(h_i, h_j)$ by $h_1, \ldots, h_t$ is zero, it is not enough that $S(h_i, h_j) \in I$. $S(h_i, h_j)$ is always an element of $I$, even though not every generating set of $I$ is a Gröbner basis.