2.6.1(a). Show that f can be written in the form $f = g + r$ where $g \in I$ and no term of r is divisible by any element of $LT(I)$.

Proof. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I. By the division algorithm, we can divide f by g and obtain an expression

$$f = q_1 g_1 + \cdots + q_t g_t + r$$

where no term of r is divisible by any of $LT(g_1), \ldots, LT(g_t)$. Since $g_1, \ldots, g_t \in I$ and I is an ideal, we know that $g = q_1 g_1 + \cdots + q_t g_t \in I$. Also, since r is a Gröbner basis, we know that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Since no term of r is divisible by any of the $LT(g_i)$, we also know that no term of r is divisible by any element of $LT(I)$. $\square$

(b). Suppose $f = g + r$ and $f = g' + r'$ are two expressions as in part (a). Prove that $r = r'$ and $g = g'$.

Proof. Observe that $g + r = g' + r'$. Moving terms around, we see that

$$r - r' = g' - g.$$

Since $g, g' \in I$ and I is an ideal, we have $g' - g \in I$, so $r - r' \in I$.

We want to show that $r = r'$, so suppose for a contradiction that $r \neq r'$, which means that $r - r'$ is a nonzero element of I. Then $LT(r - r') \in LT(I)$. But $LM(r - r')$ must be a monomial of either r or r', and we know that no term of either r or r' is divisible by any element of $LT(I)$. This means that $LT(r - r')$ is both an element of $LT(I)$ and not divisible by any element of $LT(I)$, which is of course a contradiction. Thus $r = r'$.

Now, since $g + r = g' + r'$ and $r = r'$, we see that $g = g'$ as well. $\square$

Discussion. Suppose $\{g_1, g_2\}$ is a Gröbner basis for an ideal I. If you take a polynomial f and divide it by (g_1, g_2), you get some expression of the form

$$f = q_1 g_1 + q_2 g_2 + r$$

where no term of r is divisible by any element of $LT(I)$. We can set $g = q_1 g_1 + q_2 g_2$ to get an element of I such that $f = g + r$.

On the other hand, if we divide f by (g_2, g_1), we might get different quotients as you showed in exercise 2.6.2. In other words, you get some expression of the form

$$f = q_1' g_2 + q_2' g_1 + r'$$

where no term of r' is divisible by any element of part $LT(I)$, where the quotients are different. But, *even though the quotients are different*, the polynomial $g' = q_1' g_2 + q_2' g_1$ will be the same as the polynomial g that we computed the first time around! This is what the uniqueness assertion of 2.6.1(b) is saying.

More concretely, in 2.6.2, we have $g_1 = x + z$ and $g_2 = y - z$ and $f = xy$. If we do the division in the order (g_1, g_2), we get

$$f = \underbrace{y}_{q_1} \cdot (x + z) \underbrace{-z}_{q_2} \cdot (y - z) \underbrace{-z^2}_{r}$$

so we have $g = y(x + z) - z(y - z) = xy + z^2$. On the other hand, if we do the division in the other order (g_2, g_1), we get

$$f = \underbrace{x}_{q_1'} \cdot (y - z) + \underbrace{z}_{q_2'} \cdot (x + y) \underbrace{-z^2}_{r'}$$

so we have $g' = x(y - z) + z(x + z) = xy + z^2$, which is the same as g. Notice also that $r = r'$.