2. Fix an ideal I of $\mathbb{F}[x_1, \ldots, x_n]$ and a monomial order.

Lemma 1: Let I' be an ideal generated by monomials $m_1, \ldots, m_k$. Then $f \in \mathbb{F}[x_1, \ldots, x_n]$ is in I' if and only if every monomial term f_i of f is a multiple of one of the m_j.

$\Rightarrow$ If $f \in I'$, $f = a_1 m_1 + \cdots a_k m_k$ for $a_i \in \mathbb{F}[x_1, \ldots, x_n]$. Each a_i is the sum of monomial terms, so for each $1 \leq i \leq k$, if we distribute m_i over the monomial terms of a_i, f is a sum of monomial terms, each of which has a factor of at least one of the m_i. $\Leftarrow$ If every monomial term of f is a multiple of one of the m_i, for each $1 \leq i \leq k$, we can "collect" all the monomials that are multiples of that m_i and factor m_i out, thereby expressing f in the form $f = b_1 m_1 + \cdots b_k m_k$ for $b_i \in \mathbb{F}[x_1, \ldots, x_n]$. which implies that $f \in I'$.

Lemma 2: Let $\{m_1, \ldots, m_n\}$ be a minimal set of monomials that generate monomial ideal I' in $\mathbb{F}[x_1, \ldots, x_n]$. Then each m_i is unique, $1 \leq i \leq k$.

Let $f \in I'$. From Lemma 1, every monomial term of f is a multiple of one of the m_i. Suppose the m_i are not unique, ie suppose that $m_j = m_k$ for some $j \neq k$. Then we can rewrite each monomial term of f, replacing each occurence of m_k with m_j, so that each monomial term of f is not a multiple m_k. (Note that we replace any m_k that appear as monomial coefficients from $\mathbb{F}[x_1, \ldots, x_n]$ as well). Then as above, we "collect like terms", factor out the m_i, and express f in the form $f = b_1 m_1 + \cdots b_n m_n$ for $b_i \in \mathbb{F}[x_1, \ldots, x_n]$, but f will have no term that is a multiple of m_k, which contradicts that $m_1, \ldots, m_n$ is minimal. Therefore each m_i is unique.

(a) Prove that $\{g_1, \ldots, g_m\} \subset I$ is a minimal Gröbner basis for I if and only if the multiset $\{\mathbf{in}(g_1), \ldots, \mathbf{in}(g_m)\}$ is a minimal generating set for $\mathbf{in}(I)$.

Let $\{g_1, \ldots, g_m\}$ be a minimal Gröbner basis for I. Then by the definition of Gröbner basis, $\text{in}(I) = \langle \text{in}(g_1), \ldots, \text{in}(g_m) \rangle$. Suppose $\{\text{in}(g_1), \ldots, \text{in}(g_m)\}$ is not a minimal generating set for $\text{in}(I)$. Then $\{\text{in}(g_1), \ldots, \text{in}(g_m)\} \setminus \text{in}(g_i)$ generates $\text{in}(I)$ for some $\text{in}(g_i) \in \{\text{in}(g_1), \ldots, \text{in}(g_m)\}$. Then since $g_i \in I$, $\text{in}(g_i) \in \text{in}(I)$ and in particular, note that $\text{in}(g_i)$ is a monomial. Then from Lemma 1 above, $\text{in}(g_i)$ is a multiple of some $\text{in}(g_j)$, $i \neq j$ from the generating set of $\text{in}(I)$. But this contradicts the definition of a minimal Gröbner basis. Therefore $\{\text{in}(g_1), \ldots, \text{in}(g_m)\}$ must be a minimal generating set.

Now let $\{\text{in}(g_1), \ldots, \text{in}(g_m)\}$ be a minimal generating set for $\text{in}(I)$ and suppose that $\{g_1, \ldots, g_m\}$ is not a minimal Gröbner basis for I. Then there is some $\text{in}(g_j)$ that is a multiple of some $\text{in}(g_k)$, $j \neq k$. But this implies that $\{\text{in}(g_1), \ldots, \text{in}(g_m)\}$ is not minimal, which is a contradiction. Therefore $\{g_1, \ldots, g_m\}$ is a minimal Gröbner basis for I.

(b) Prove that any two minimal Gröbner bases for I have the same size and the same set of leading terms

Let $\{g_1, \ldots, g_m\}$ and $\{h_1, \ldots, h_n\}$ be two minimal Gröbner bases for I. Then from part a, $\{\text{in}(g_1), \ldots, \text{in}(g_m)\}$ and $\{\text{in}(h_1), \ldots, \text{in}(h_n)\}$ are minimal monomial generating sets for $\text{in}(I)$. Then by lemma 1, $\text{in}(g_i) = m_1 \text{in}(h_j)$ and $\text{in}(h_j) = m_2 \text{in}(g_k)$ for some monic monomials $m_1, m_2 \in \mathbb{F}[x_1, \ldots, x_n]$, $1 \leq i, k \leq m$, and $1 \leq j \leq n$. This implies $\text{in}(g_i) = m_1 m_2 \text{in}(g_k)$. From the definition of minimal Gröbner basis, we know that $\text{in}(g_i)$ is not a multiple of $\text{in}(g_k)$, $i \neq k$. This implies that $m_1 m_2 = 1$ and $i = k$. And since m_1 and m_2 are monic monomials, this implies that $m_1 = m_2 = 1$. Thus we know that $\text{in}(g_i) = \text{in}(h_j)$. From lemma 2, we know that the $\text{in}(g_i)$, $1 \leq i \leq m$, and $\text{in}(h_j)$, $1 \leq j \leq n$ are unique. Therefore there is a bijection between $\{\text{in}(g_1), \ldots, \text{in}(g_m)\}$ and $\{\text{in}(h_1), \ldots, \text{in}(h_n)\}$. This implies that $m = n$, and so any two minimal Gröbner bases for I have the same size and the same set of leading terms.