Monomial ideals, Hilbert Basis Theorem & Gröbner Bases

In the last lecture we saw that one reason why the division algorithm fails to decide ideal membership was because not all the leading monomials of our ideal appeared in the given list of generators of our ideal.
(Recall example $I = (xy-1,\ y^2-1)$ where $x-y \in I$)

Today we will investigate whether adding more polynomials to the list of generators of I (hence we will necessarily have a redundant list of generators) to ensure that our generating set $\{g_1, \dots, g_t\}$ of I satisfies $LM(I) = (LM(g_1), \dots, LM(g_t))$ will fix the issues of the division algorithm.

One issue that we must have in mind is that we haven't proved that ideals in the polynomial ring are finitely generated (a fact that you may know from a previous course, but I'm not sure you have seen a proof of it).

Since our first issue is with monomial ideals, let's study their properties first.

Definition (monomial ideal): an ideal $I \trianglelefteq \mathbb{K}[x_1, \dots, x_n]$ is a monomial ideal if there is a subset $\mathcal{A} \subseteq \mathbb{N}^n$ (possibly infinite) such that $I = (\bar{x}^\alpha \mid \alpha \in \mathcal{A})$.

Monomial ideals have the following nice properties:

Proposition (properties of monomial ideals): Let $I = (\bar{x}^\alpha \mid \alpha \in \mathcal{A})$ be a monomial ideal. Then the following hold:
(1) $\bar{x}^\beta \in I$ iff $\exists\ \alpha \in \mathcal{A}$ s.t. $\bar{x}^\alpha \mid \bar{x}^\beta$.
(2) Let $f \in \mathbb{K}[x_1, \dots, x_n]$. TFAE
  (2.1) $f \in I$
  (2.2) every term of f is in I
  (2.3) f is a $\mathbb{K}$-linear combination of monomials in I.
(3) two monomial ideals are the same iff they contain the same monomials.

The next lemma, whose proof is essentially the same as Hilbert's proof (that any ideal in $\mathbb{K}[\bar{x}]$ is finitely generated), shows that monomial ideals are finitely generated.

Lemma (Dickson's lemma): Let $I = (\bar{x}^\alpha \mid \alpha \in \mathcal{A})$ be a monomial ideal. Then, there are finitely many exponents $\alpha_1, \dots, \alpha_k \in \mathcal{A}$ s.t. $I = (\bar{x}^{\alpha_1}, \dots, \bar{x}^{\alpha_k})$.

Proof: we prove this by induction on the number of variables. When $n = 1$ then $\mathcal{A} \subseteq \mathbb{N}$ which implies that $\mathcal{A}$ has a smallest element $\beta \in \mathbb{N}$ and by the above proposition we have $I = (x^\beta)$.
Now, assume the lemma is true for n variables (where $n \geq 1$) and let's consider $I \trianglelefteq \mathbb{K}[x_1, \dots, x_n, y]$ our monomial ideal (in $n+1$ variables).
Let $J := (\bar{x}^\alpha \mid \exists\ m \in \mathbb{N}$ s.t. $\bar{x}^\alpha y^m \in I)$.
Since J is also a monomial ideal in $\mathbb{K}[x_1, \dots, x_n]$, by inductive hypothesis we know that J is finitely generated, say $J = (\bar{x}^{\alpha_1}, \dots, \bar{x}^{\alpha_k})$.
By definition of J, for each $i \in [k]$, there is $m_i \in \mathbb{N}$ s.t. $\bar{x}^{\alpha_i} y^{m_i} \in I$. Let $M := \max_{i \in [k]} m_i$ and define the ideal

$$H^{(M)} := \left(\bar{x}^{\alpha_1} y^M, \dots, \bar{x}^{\alpha_k} y^M\right).$$

Now note that if $\bar{x}^\beta y^m \in I$ and $m \geq M$ then by definition of J and $\alpha_1, \dots, \alpha_k$ we have that $\bar{x}^\beta y^m \in H^{(M)}$. Thus all we have left to capture all monomials in I is to prove that the monomials $\bar{x}^\beta y^m \in I$ with $m < M$ are finitely generated.
For that, let $J^{(\ell)} := (\bar{x}^\alpha \mid \bar{x}^\alpha y^\ell \in I)$ where $0 \leq \ell < M$. By induction, since $J^{(\ell)}$ is a monomial ideal in $\mathbb{K}[\bar{x}]$, we have that each $J^{(\ell)}$ is finitely generated.
Letting $\alpha_{\ell 1}, \dots, \alpha_{\ell r_\ell}$ be s.t. $J^{(\ell)} = (\bar{x}^{\alpha_{\ell 1}}, \dots, \bar{x}^{\alpha_{\ell r_\ell}})$ and defining $H^{(\ell)} := (\bar{x}^{\alpha_{\ell 1}} y^\ell, \dots, \bar{x}^{\alpha_{\ell r_\ell}} y^\ell)$ we have

$$I = H^{(0)} + H^{(1)} + \cdots + H^{(M)}$$

$\therefore$ I finitely generated since the RHS is finitely generated

A corollary of Dickson's lemma is the equivalence between well-ordering and every exponent being larger than 0 in any monomial ordering.

Corollary [CLO'15, Chapter 2.4, Corollary 6]: Let $\prec$ be a relation on $\mathbb{N}^n$ satisfying
(1) $\prec$ is a total ordering on $\mathbb{N}^n$
(2) if $\alpha \prec \beta$ and $\gamma \in \mathbb{N}^n$ then $\alpha + \gamma \prec \beta + \gamma$
Then $\prec$ is a well-ordering iff $\alpha \succ 0$ for all $\alpha \in \mathbb{N}^n$.

Corollary [CLO'15, chapter 2.4, Proposition 7]: Let $I \trianglelefteq \mathbb{K}[\bar{x}]$ be a monomial ideal. Then I has a minimal basis, i.e., $I = (\bar{x}^{\alpha_1}, \dots, \bar{x}^{\alpha_k})$ with the property that $\bar{x}^{\alpha_i} \nmid \bar{x}^{\alpha_j}\ \forall\ i \neq j \in [k]$.

We are now ready to prove Hilbert's basis theorem:

Theorem [Hilbert basis theorem]: every ideal $I \trianglelefteq \mathbb{K}[x_1, \dots, x_n]$ is finitely generated. Moreover, for any set $\{g_1, \dots, g_t\}$ s.t. $I \supseteq (g_1, \dots, g_t)$ and $LM(I) = (LM(g_1), \dots, LM(g_t))$, we have that $I = (g_1, \dots, g_t)$.
Remark: we make a convention that if $t = 0$ (i.e. the set is $\emptyset$) then $I = (\emptyset) = (0)$.

Proof: If $I = (0)$ then it is finitely generated. Else, we have that $LM(I) := \{\bar{x}^\alpha \mid \bar{x}^\alpha = LM(f)$ where $f \in I\setminus\{0\}\}$ is finitely generated by Dickson's lemma.
Let $g_1, \dots, g_t \in I$ be s.t. $LM(I) = (LM(g_1), \dots, LM(g_t))$.
By definition of g_i's, we have $(g_1, \dots, g_t) \subseteq I$.
Let $f \in I$. By the division algorithm, we have

$$f = g_1 h_1 + \cdots + g_t h_t + r \quad \text{where no term of } r$$

is divisible by any $LM(g_i)$, $i \in [t]$.
Since $r = f - g_1 h_1 - \cdots - g_t h_t \in I$ the above implies that $r = 0$, otherwise $LM(r) \neq 0$ and thus it must be in $LM(I) = (LM(g_1), \dots, LM(g_t)) \Rightarrow LM(r)$ is divisible by the leading monomial of some g_i, which is a contradiction. Hence $f \in (g_1, \dots, g_t)$, which proves that $I = (g_1, \dots, g_t)$. $\square$

The above theorem shows us that any basis for an ideal which captures all the leading monomials make the division algorithm work as originally intended. This motivates the following definition:

Definition (Gröbner basis): Given a polynomial ring $\mathbb{K}[x_1, \dots, x_n]$ with a monomial ordering $\prec$, a set $G = \{g_1, \dots, g_t\}$ of I is a Gröbner basis of an ideal $I \trianglelefteq \mathbb{K}[\bar{x}]$ if:
(1) $g_i \in I \quad \forall\ i \in [t]$
(2) $LM(I) = (LM(g_1), \dots, LM(g_t))$
By our convention, we will denote $\emptyset$ as the Gröbner basis of the zero ideal (0).