Lemma (§2.2)**.** *An order relation $>$ on $\mathbb{Z}_{\geq 0}^n$ is a well-ordering [every nonempty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element] if and only if every strictly decreasing sequence in $\mathbb{Z}_{\geq 0}^n$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

eventually terminates.

Proof. We show the contrapositive:

If $>$ is not a well-ordering then some subset of $\mathbb{Z}_{\geq 0}^n$ does not have a smallest element; from this subset we can form a strictly decreasing sequence $(\alpha(i))$ which does not terminate.

If some strictly decreasing sequence $(\alpha(i))$ does not eventually terminate then $\bigcup_i \alpha(i)$ is a nonempty subset of $\mathbb{Z}_{\geq 0}^n$ which does not have a smallest element; thus $>$ is not a well-ordering. □

Definition (§2.3)**.** *Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{lex} \beta$ if in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive.*

Proposition (§2.4)**.** *$>_{lex}$ on $\mathbb{Z}_{\geq 0}^n$ is a monomial ordering.*

Proof. We show $>_{lex}$ satisfies each monomial ordering requirement:

(i) [$>_{lex}$ is a total ordering]

This can be shown inductively, using the fact that the usual $>$ on $\mathbb{Z}_{\geq 0}$ is a total ordering and that $>_{lex}$ on $\mathbb{Z}_{\geq 0}^n$ can be defined in terms of $>$ on $\mathbb{Z}_{\geq 0}$ (if first entries are unequal) and $>_{lex}$ on $\mathbb{Z}_{\geq 0}^{n-1}$ (if first entries are equal).

(ii) [$\alpha >_{lex} \beta \implies \alpha + \gamma >_{lex} \beta + \gamma$]

$\alpha >_{lex} \beta$ is defined by the value of $\alpha - \beta$ and $\alpha + \gamma >_{lex} \beta + \gamma$ is defined by $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, the same value.

(iii) [$>_{lex}$ is a well-ordering]

If $>_{lex}$ wasn't a well-ordering, by Lemma §2.2 there exists an infinite strictly decreasing $\mathbb{Z}_{\geq 0}^n$-sequence; their first entries will form a decreasing sequence in $\mathbb{Z}_{\geq 0}$. Since $\mathbb{Z}_{\geq 0}$ is well-ordered, it cannot be a strictly decreasing sequence and therefore must eventually stabilize. Afterwards, the other entries will form an infinite strictly decreasing $\mathbb{Z}_{\geq 0}^{n-1}$-sequence; repeatedly applying the above argument will eventually yield a strictly decreasing $\mathbb{Z}_{\geq 0}$-sequence: a contradiction.

□

Lemma (§2.8)**.** *Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials. Then:*

- $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$
- *If $f + g \neq 0$, then*

$$\text{multideg}(f+g) \leq \max(\text{multideg}(f), \text{multideg}(g)).$$

Equality occurs if either

- $\text{multideg}(f) \neq \text{multideg}(g)$
- $\text{multideg}(f) = \text{multideg}(g)$ *and* $\text{LC}(f) \neq -\text{LC}(g)$

Proof. Let $f = \sum_\alpha a_\alpha x^\alpha$ and $g = \sum_\alpha b_\alpha x^\alpha$. Point 1:

$$\begin{aligned}
\text{multideg}(fg) &= \text{multideg}\left(\sum_\alpha \sum_\beta a_\alpha b_\beta x^{\alpha+\beta}\right) \\
&= \max_{a_\alpha b_\beta \neq 0}(\alpha+\beta) = \max_{\substack{a_\alpha \neq 0 \\ b_\beta \neq 0}}(\alpha+\beta) \\
&= \max_{a_\alpha \neq 0}(\alpha + \max_{b_\beta \neq 0}(\beta)) = \max_{a_\alpha \neq 0}(\alpha) + \max_{b_\beta \neq 0}(\beta) \\
&= \text{multideg}(f) + \text{multideg}(g)
\end{aligned}$$

Point 2: We have that

$$\text{multideg}(f+g) = \text{multideg}\left(\sum_\alpha (a_\alpha + b_\alpha)x^\alpha\right) = \max_{a_\alpha + b_\alpha \neq 0}(\alpha).$$

Noting that $\{\, \alpha \mid a_\alpha + b_\alpha \neq 0 \,\} \subseteq \{\, \alpha \mid a_\alpha \neq 0 \text{ or } b_\alpha \neq 0 \,\}$, we have

$$\begin{aligned}
\max_{a_\alpha + b_\alpha \neq 0}(\alpha) \leq \max_{\substack{a_\alpha \neq 0 \\ b_\alpha \neq 0}}(\alpha) &= \max(\max_{a_\alpha \neq 0}(\alpha), \max_{b_\alpha \neq 0}(\alpha)) \\
&= \max(\text{multideg}(f), \text{multideg}(g)).
\end{aligned}$$

If $\text{multideg}(f) \neq \text{multideg}(g)$: take $\text{multideg}(f) > \text{multideg}(g)$ without loss of generality. Then we have $a_{\text{multideg}(f)} \neq 0$ and $b_{\text{multideg}(f)} = 0$, so noting that $\text{multideg}(f) \in \{\, \alpha \mid a_\alpha + b_\alpha \neq 0 \,\}$ we have

$$\max_{a_\alpha + b_\alpha \neq 0}(\alpha) \geq \text{multideg}(f) = \max(\text{multideg}(f), \text{multideg}(g)).$$

Which is the opposite inequality from point 2, so

$$\text{multideg}(f+g) = \max(\text{multideg}(f), \text{multideg}(g)).$$

If $\text{multideg}(f) = \text{multideg}(g)$ and $\text{LC}(f) + \text{LC}(g) \neq 0$: then we have $a_{\text{multideg}(f)} + b_{\text{multideg}(f)} \neq 0$ and the same argument as above applies. □

Theorem (§3.3)**.** *The Division Algorithm in $k[x_1, \ldots, x_n]$ works as stated.*

Proof. Correctness: We show that

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{1}$$

holds after every stage (by initialization it holds at the start). Notice that exiting the inner loop can occur in only two ways: in a *division step* or in a *remainder step.*

Division step: redefines p and some a_i:

$$a_i' f_i + p' = (a_i + \operatorname{LT}(p)/\operatorname{LT}(f_i)) f_i + p - f_i \operatorname{LT}(p)/\operatorname{LT}(f_i) = a_i f_i + p$$

Remainder step: redefines p and r:

$$p' + r' = p - \operatorname{LT}(p) + r + \operatorname{LT}(p) = p + r$$

Thus (1) continues to hold following both step types.

Termination: We will show that multideg(p) strictly decreases: in both step types the leading term of p is removed.

Division step: $p' = p - f_i \operatorname{LT}(p)/\operatorname{LT}(f_i)$ and

$$\operatorname{LT}(f_i \operatorname{LT}(p)/\operatorname{LT}(f_i)) = \operatorname{LT}(f_i) \operatorname{LT}(p)/\operatorname{LT}(f_i) = \operatorname{LT}(p)$$

by an extension of Lemma §2.8.

Remainder step: $p' = p - \operatorname{LT}(p)$. Thus in both cases multideg(p) strictly decreases and since $>$ is a well-ordering it cannot strictly decrease indefinitely by Lemma §2.2. Therefore the algorithm must terminate. □

Lemma (§4.2)**.** *Let $I = \langle x^\alpha \mid \alpha \in A \rangle$. Then a monomial $x^\beta \in I$ if and only if there is some $\alpha \in A$ such that x^α divides x^β.*

Proof. Given $x^\beta \in I$, we have $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$ for some $h_i \in k[x_1, \ldots, x_n]$ and $\alpha(i) \in A$. Expand the right-hand side as a linear combination of monomials. Since the left-hand side consists of a single monomial with exponent β, every monomial on the right-hand side which does not have have an exponent of β must cancel off. This leaves a sum of the form $\sum_{i=1}^s h_i' x^{\alpha(i)}$, where $h_i' x^{\alpha(i)} = c_i x^\beta$ and some $c_i \in k$ must be nonzero. Then $x^{\alpha(i)}$ divides x^β, since $x^\beta = (h_i' c_i^{-1}) x^{\alpha(i)}$.

Conversely: If there is some $\alpha \in A$ such that x^α divides x^β then we have $x^\beta = g x^\alpha$ for some $g \in k[x_1, \ldots, x_n]$, but $h x^\alpha \in I$ for all $h \in k[x_1, \ldots, x_n]$. □

Lemma (§4.3)**.** *Let I be a monomial ideal, and let $f \in k[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) $f \in I$

(ii) Every term of f *lies in* I

(iii) f *is a* k*-linear combination of the monomials in* I

Proof. (iii) $\implies$ (ii) $\implies$ (i): Since ideals are closed over addition.

(i) $\implies$ (iii): Say $I = \langle x^\alpha \mid \alpha \in A \rangle$, then any $f \in I$ can be written in the form $f = \sum_{\alpha \in A} h_\alpha x^\alpha$ where $h_\alpha \in k[x_1, \ldots, x_n]$. Write h_α as a k-linear combination of monomials and expand, writing f as a k-linear combination of monomials, all of which must be multiples of monomials in $\{ x^\alpha \mid \alpha \in A \}$ by construction. By Lemma §4.2 this means that these monomials also lie in I and thus f is a k-linear combination of monomials in I. □

Corollary (§4.4)**.** *Two monomial ideals are the same if and only if they contain the same monomials.*

Proof. If two monomial ideals are the same, of course they contain the same monomials.

Conversely: By Lemma §4.3 we know that every element in a monomial ideal can be 'built' out of the monomials of the ideal, so if two monomials ideals contain the same monomials then every other element they contain will also be the same. □

Theorem (§4.5)**.** *Let $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$. Then there exists a finite $A' \subseteq A$ such that $I = \langle x^\alpha \mid \alpha \in A' \rangle$.*

Proof. We already know this is true for $A \subseteq \mathbb{Z}_{\geq 0}$, but we want to show it for $A \subseteq \mathbb{Z}^n_{\geq 0}$. This can be done inductively, with the hypothesis that it is true for all $A \subseteq \mathbb{Z}^{n-1}_{\geq 0}$.

Without getting into the details, it requires 'projecting' the ideal $I \subseteq k[x_1, \ldots, x_n]$ onto $k[x_1, \ldots, x_{n-1}]$ to form ideals which by hypothesis have finite bases. For example, they define the projected ideal J to consist of all monomials in I with their final entry (x_n) removed. The bases for the projected ideals can then be 'augmented' to form a finite $B \subseteq \mathbb{Z}^n_{\geq 0}$ such that $I = \langle x^\beta \mid \beta \in B \rangle$.

However, we want to find a finite $A' \subseteq A$ such that $I = \langle x^\alpha \mid \alpha \in A' \rangle$. By Lemma §4.2, since $x^\beta \in I = \langle x^\alpha \mid \alpha \in A \rangle$, we have that there is some $\alpha' \in A$ such that $x^{\alpha'}$ divides x^β. Finding such an α' for each $\beta \in B$ we construct a finite subset A' such that $\langle x^\beta \mid \beta \in B \rangle \subseteq \langle x^\alpha \mid \alpha \in A' \rangle$.

However, since $A' \subseteq A$ we also have

$$\langle x^\alpha \mid \alpha \in A' \rangle \subseteq \langle x^\alpha \mid \alpha \in A \rangle = \langle x^\beta \mid \beta \in B \rangle,$$

and therefore $I = \langle x^\beta \mid \beta \in B \rangle = \langle x^\alpha \mid \alpha \in A' \rangle$. □