Theorem A1. (Buchberger's Algorithm) Let $I = \langle f_1, \dots, f_s \rangle \subset F[x_1, \dots, x_n]$ be a non-zero ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm:

$$
\begin{aligned}
&\text{Input}: \ F = (f_1, \dots, f_n) \\
&\text{Output}: \ \text{a Gröbner basis } G = (g_1, \dots, g_t) \text{ for } I \text{ with } F \subset G. \\
\\
&G := F \\
&\text{REPEAT} \\
&\qquad G' := G \\
&\qquad \text{FOR each pair } \{p, q\}, \ p \neq q \text{ in } G' \text{ DO} \\
&\qquad\qquad r := \overline{S(p,q)}^{G'} \\
&\qquad\qquad \text{IF } r \neq 0 \text{ THEN } G := G \cup \{r\} \\
&\text{UNTIL } G = G' \\
&\text{RETURN } G
\end{aligned}
$$

Proof. We introduce some notation for convenience. Let $G = \{g_1, \dots, g_n\}$, we define:

$$\langle \mathrm{LT}(G) \rangle := \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_n) \rangle.$$

Firstly it is clear that $G \subset I$ at every stage of the algorithm because initially $G \subset I$ but we only ever append the remainder of each $S(p, q)$. However since $S(p, q) \in I$ and each $f_1, \dots, f_n$ are in I we have the remainder is in I since we can write,

$$r = S(p, q) - q_1 f_1 - \cdots - q_s f_2$$

for some $q_i \in F[x_1, \dots, x_n]$ by the division algorithm. Furthermore we note that G at each step generates I since G contains the generators F.

We show that it eventually terminates. Let us consider two consecutive pass throughs of the algorithm, and name the corresponding sets G and G' where G' is the old set. We of course have $G' \subset G$ and because G contains all the non-zero remainders of $S(p, q)$ we have,

$$\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle. \tag{3.1}$$

Additionally if $G' \neq G$ then it turns out that $\langle \mathrm{LT}(G) \rangle$ is strictly larger than $\langle \mathrm{LT}(G') \rangle$. Indeed take a non-zero remainder $r \in G$ not in G'. Since r is a remainder on division by G', by definition it is not divisible by any of the leading terms of elements in G'. Then by [CLO15, Theorem 2.4.2] we have $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$ however we clearly have $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$ so $\langle \mathrm{LT}(G) \rangle$ is indeed strictly larger than $\langle \mathrm{LT}(G') \rangle$.

Now using (3.1) we have that the algorithm produces an infinite ascending chain of ideals in $F[x_1, \dots, x_n]$, however since F is a field $F[x_1, \dots, x_n]$ is Noetherian so eventually this chain of ideals stablize to achieve $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$. However by the contrapositive of the argument in the previous paragraph this implies that $G' = G$ and the algorithm terminates.

Now we prove that the actual result is indeed a Gröbner basis. Suppose we ran the algorithm until it terminates, then this would necessarily mean that $\overline{S(p,q)}^{G} = 0$ for every $p, q \in G$ so by Theorem 1.3.1 we have that G is a Gröbner basis of I since G generates I. $\square$

Theorem A2. (Improved Buchberger's Algorithm) Let $I = \langle f_1, \ldots, f_s \rangle \subset F[x_1, \ldots, x_n]$ be a non-zero ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm:

Input : $F = (f_1, \ldots, f_n)$
Output : a Gröbner basis $G = (g_1, \ldots, g_t)$ for I with $F \subset G$.

$B := \{(i, j) \mid 1 \leq i < j \leq s\}$
$G := F$
$t := s$
WHILE $B \neq \emptyset$ DO
    Select $(i, j) \in B$
    IF $\text{lcm}(\text{LT}(f_i), \text{LT}(f_j)) \neq \text{LT}(f_i)\text{LT}(f_j)$ AND Criterion$(f_i, f_j, B) =$ false THEN
        $r := \overline{S(f_i, f_j)}^G$
        IF $r \neq 0$ THEN
        $t := t + 1;\ f_t := r$
        $G := G \cup \{f_t\}$
        $B := B \cup \{(i, t) \mid 1 \leq i \leq t - 1\}$
    UNTIL $B := B \backslash \{(i, j)\}$
RETURN G

Here, Criterion(f_i, f_j, B) is true provided that there is some $l \notin \{i, j\}$ for which the pairs $[i, j]$ and $[j, l]$ are not in B and $\text{LT}(f_l)$ divides $\text{lcm}(\text{LT}(f_i), \text{LT}(f_j))$. Where for $i \neq j$, $[i, j] = (i, j)$ if $i < j$ and (j, i) for $j < i$. See [CLO15, Theorem 2.10.9] for a proof of the correctness of this algorithm.