Lemma 0.1 *Let $P = \langle X \rangle$ be a finite p-group, and $Q = \langle Y \rangle^P$ be a normal subgroup of P. Let $g \in Y$, and let $R = \langle \{g^p\} \cup Y \setminus \{g\} \cup [g, X] \rangle^P$. Then the index of R in Q is at most p.*

PROOF: Note that $Q = \langle Y \cup [Y, X] \cup [Y, X, X] \cup \ldots \rangle$. Clearly R contains $[Y, X]$, and hence $[Y, X, X]$, $[Y, X, X, X]$ and larger commutators. Also R contains $Y \setminus \{g\}$. So Q/R is cyclic of order at most p, generated by Rg. □

Theorem 0.2 *The algorithm* `PChiefSeriesGenerators` *having as input a list X of upper unitriangular $d \times d$ matrices over a field F, and a list $\bar{X}$ of corresponding SLPs, returns a base for the p-group $P = \langle X \rangle$ such that no two matrices have the same matrix weight.*

PROOF: The algorithm starts by setting $Z := \{(x, \texttt{MatrixWeight}(x)) : x \in X\}$ and $B := \emptyset$, with corresponding sets $\bar{Z}$ and $\bar{B}$ set appropriately. `MatrixWeight` here is defined as in Definition 4.2. We create a list *depth* := $\{\texttt{MatrixWeight}(x) : x \in X\}$ and from it choose a minimum element (j_0, j_1, j_2) with respect to the following total ordering:

$(a_0, a_1, a_2) < (b_0, b_1, b_2)$, if one of the following holds:

1. $a_0 < b_0$;
2. $a_0 = b_0$ and $a_1 < b_1$;
3. $a_0 = b_0, a_1 = b_1$ and $a_2 < b_2$.

We then enter the while-loop. Let $Z_1 = \{a : (a, b) \in Z\}\rangle$ We want to prove that this loop will terminate after finitely many iterations and that, at the end of each iteration, the following induction hypothesis is true: Let Q be the group generated by Z_1 at the beginning of an iteration and R be the group generated by Z_1 at the end of the same iteration.

Suppose that our induction hypothesis is true at the end on an iteration and we are about to start the next iteration of the while loop. Then, Q consists of all the elements of P of weight at least (j_0, j_1, j_2), where (j_0, j_1, j_2) is the minimal weight of an element of Q. We choose an $h \in Z$ such that $h_2 = (j_0, j_1, j_2)$. Set $\alpha = h_{j_0,j_1,j_2}$ (see Section 1.5 for a description of this notation), add h_1 to B and remove h from Z. Now we look for all $z \in Z$ with $z_2 = h_2$. Let $\beta = (z_1)_{j_0,j_1,j_2}$ and replace all such $z \in Z$ with the same matrix weight as h with the pair $(h_1 z_1^{-\alpha/\beta}, \texttt{MatrixWeight}(h_1 z_1^{-\alpha/\beta}))$.

Next, we see if $h_1^p \neq I_d$. If it is not the identity, we add it to Z along with its matrix weight, noting that $h^p_{1j_0,j_1,j_2} = 0$. We then add to Z every non-trivial commutator $[h_1, x]$ such that $x \in X$ (or $x \in B$, if this set is smaller) along with its matrix weight, noting that $[h_1, x]_{j_0,j_1,j_2} = 0, \forall x \in X$. Note that, we can take the commutators with elements of B rather than X because $[h_1, X] = [h_1, Z_1 \setminus \{h_1\}] \cup [h_1, B]$ and, because $\langle Z_1 \rangle^P$ contains $Z_1 \setminus \{h_1\}$, it contains $[h_1, Z_1 \setminus \{h_1\}]$.

Hence, Q and R are as they appear in the above lemma and so $|Q : R| \leq p$. However, R consists of elements of weight strictly greater than (j_0, j_1, j_2) and hence $|Q : R| = p$.

The list Z never contains the identity matrix, which has matrix weight $(d, 1, 1)$. Hence, after at most $d(d-1)/2$ iterations, Z is empty and so the while loop terminates. $\square$