Proposition. *Given $n+2$ polynomials $g_1, g_2, \dots, g_{n+2}$ in n indeterminates with rational coefficients, construct $n+1$ polynomials $f_1, f_2, \dots, f_{n+1}$ in the same indeterminates with rational coefficients that are zero mod $g_1, g_2, \dots, g_{n+2}$ and have the property that, for each i, some power of g_i is zero mod $f_1, f_2, \dots, f_{n+1}$.*

Proof. Let the indeterminates be $x_1, x_2, \dots, x_n$. Because the g's are elements in the field $\mathbf{Q}(x_1, x_2, \dots, x_n)$ of rational functions in $x_1, x_2, \dots, x_n$ with rational coefficients, and because this field has transcendence degree n, the first $n+1$ of the g's are algebraically dependent. (See Essays.) Therefore there is a nonzero polynomial A in $n+1$ indeterminates with integer coefficients in which substitution of $g_1, g_2, \dots g_{n+1}$ produces the result 0. Let $X_1, X_2, \dots, X_{n+1}$ be the indeterminates in A, and let polynomials A_i and B_i be defined successively by setting $A_{n+1} = A$, by defining k_i to be the number of times that X_i divides A_i, and by setting

$$A_i(X_1, X_2, \dots, X_i) = X_i^{k_i} \cdot A_{i-1}(X_1, X_2, \dots X_{i-1}) + X_i^{k_i+1} B_i(X_1, X_2, \dots, X_{i+1}).$$

Note that $A_i \neq 0$ for $i = n+1, n, \dots, 1, 0$ by the definition of k_i.

Polynomials $f_1, f_2, \dots, f_{n+1}$ with the required properties are found by setting $f_i = g_i - a_i g_{n+2}$, where $a_i = g_i^{-k_i} A_i(g_1, g_2, \dots, g_i)$. Each f_i is obviously zero mod $g_1, g_2, \dots, g_{n+2}$. What is to be shown is that some power of each g_i is zero mod $f_1, f_2, \dots, f_{i+1}$.

Let $\equiv$ denote congruence mod $f_1, f_2, \dots, f_{n+1}$. From $g_{n+1} \equiv a_{n+1} g_{n+2}$, it follows that $g_{n+1}^{k_{n+1}} g_{n+1} \equiv g_{n+1}^{k_{n+1}} a_{n+1} g_{n+2} = A_{n+1}(g_1, g_2, \dots, g_{n+1}) g_{n+2} = 0$, which is to say that a power of g_{n+1} is zero mod $f_1, f_2, \dots, f_{n+1}$.

Suppose now that a power of g_{i+1} is zero mod $f_1, f_2, \dots, f_{n+1}$. From $g_{i+1} \equiv a_{i+1} g_{n+2}$ and $a_{i+1} = g_{i+1}^{-k_{i+1}} A_{i+1}(g_1, g_2, \dots, g_{i+1}) = A_i(g_1, g_2, \dots, g_i) + B_{i+1}(g_1, g_2, \dots, g_{i+1}) g_{i+1} = g_i^{k_i} a_i + B_{i+1}(g_1, g_2, \dots, g_{i+1}) g_{i+1}$, it follows that $g_i^{k_i} \cdot g_i \equiv g_i^{k_i} \cdot a_i \cdot g_{n+2} = g_{n+2}(a_{i+1} - B_{i+1}(g_1, g_2, \dots, g_{i+1}) g_{i+1}) \equiv g_{i+1}(1 - B_{i+1}(g_1, g_2, \dots, g_{i+1}) g_{n+2})$. Thus, $g_i^{\lambda(k_i+1)} \equiv g_{i+1}^{\lambda}(1 - B_{i+1}(g_1, g_2, \dots, g_{i+1}) g_{n+2})^{\lambda} \equiv 0$ for all sufficiently large λ.

Thus, some power of g_i is zero mod $f_1, f_2, \dots, f_{n+1}$ for $i = n+1, n, \dots, 1$.

Finally, $g_1 \equiv a_1 g_{n+2} = g_1^{-k_1} A_1 g_{n+2} = g_{n+2}(A_0 + B_1(g_1) g_1)$ where A_0 is a nonzero integer. Thus, $g_{n+2} = A_0^{-1} g_1(1 - B_1(g_1))$, which shows that some power of g_{n+2} is zero mod $f_1, f_2, \dots, f_{n+1}$ and completes the proof.

Since the Proposition does not assume that all n indeterminates $x_1, x_2, \dots, x_n$ occur in $g_1, g_2, \dots, g_{n+2}$, it can be used to reduce the number of g's whenever there are more than $n+1$ of them. Therefore, iteration of the proposition proves:

Theorem. *Let polynomials $g_1, g_2, \dots, g_m$ in n indeterminates with rational coefficients be given, and let m be greater than $n+1$. Construct $n+1$ polynomials $f_1, f_2, \dots, f_{n+1}$ in the same indeterminates that are zero mod $g_1, g_2, \dots, g_m$ and have the property that, for each $i = 1, 2, \dots, m$, some power of g_i is zero mod $f_1, f_2, \dots, f_{n+1}$.*