Noether Normalisation

Daniel Murfet

March 21, 2005

Normalisation is an important tool in modern algebra, and there are many different approaches to the result. The easiest version is for an infinite field, and we give this proof first. Next we give a proof that works for arbitrary fields and gives more information, but requires a lot more work. For yet another version that involves separable algebraic extensions, see our EFT notes.

Lemma 1. *Let R be a domain and $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ a nonzero polynomial. If $Q \subseteq R$ is an infinite set then there exist $a_1, \ldots, a_n \in Q$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Proof. The proof is an easy induction, with the case $n = 1$ being elementary. See our EFT notes. □

Proposition 2. *Let k be an infinite field and A a nonzero finitely generated k-algebra. Either A is integral over k or there are elements $y_1, \ldots, y_r \in A$ which are algebraically independent over k such that A is integral over $k[y_1, \ldots, y_r]$.*

Proof. Let $A = k[s_1, \ldots, s_n]$ where $s_1, \ldots, s_n \in A$. We assume that A is not integral over k, in which case at least one of the s_i is not algebraic over k. If the set $\{s_1, \ldots, s_n\}$ is algebraically independent, then we are done.

Otherwise assume that s_n is algebraic over $k[s_1, \ldots, s_{n-1}]$ (by relabeling if necessary). Let $f(x_1, \ldots, x_n)$ be a nonzero polynomial with $f(s_1, \ldots, s_n) = 0$ and let F be the homogenous part of f of highest degree. If the degree of F is e, then for any constants $\lambda_1, \ldots, \lambda_{n-1} \in k$ the polynomial $f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$ expands to

$$F(\lambda_1, \ldots, \lambda_{n-1}, 1)x_n^e + b_1 x_n^{e-1} + \ldots + b_e \tag{1}$$

where $b_i \in k[x_1, \ldots, x_{n-1}]$ for $1 \leq i \leq e$. Let g be $F(x_1, \ldots, x_{n-1}, 1)$. If F does not involve x_n then $g = F$ and we conclude that g is a nonzero polynomial. If F does involve powers of x_n and $g = 0$ then look at the terms of F involving the highest power of x_n - these become distinct monomials in g, and $g = 0$ implies that the coefficients in F of these terms were all zero, which is impossible. Hence g is a nonzero polynomial, and since k is infinite we can arrange $\lambda_1, \ldots, \lambda_{n-1}$ such that $F(\lambda_1, \ldots, \lambda_{n-1}, 1)$ is nonzero. If we write $t_i = s_i - \lambda_i s_n$ for $1 \leq i \leq n-1$ and evaluate (1) at $t_1, \ldots, t_{n-1}, s_n$ we find

$$\begin{aligned} 0 &= f(s_1, \ldots, s_n) \\ &= f\big(t_1 + \lambda_1 s_n, \ldots, t_{n-1} + \lambda_{n-1} s_n, s_n\big) \\ &= F(\lambda_1, \ldots, \lambda_{n-1}, 1)s_n^e + \sum_{i=1}^{e} b_i(t_1, \ldots, t_{n-1}) s_n^{e-i} \end{aligned}$$

Dividing through by $F(\lambda_1, \ldots, \lambda_{n-1}, 1)$ gives an equation of integral dependence for s_n over $k[t_1, \ldots, t_{n-1}]$. Since $s_i = t_i + \lambda_i s_n$ for $1 \leq i \leq n-1$, this implies that A is integral over $k[t_1, \ldots, t_{n-1}]$. Note that the t_i are linear combinations of $s_1, \ldots, s_n$.

If $\{t_1, \ldots, t_{n-1}\}$ is an algebraically independent set, then we are done. Otherwise we assume t_{n-1} is algebraic over $k[t_1, \ldots, t_{n-2}]$ (if necessary by relabeling) and apply the above argument to produce $q_1, \ldots, q_{n-2} \in A$ which are linear combinations of $t_1, \ldots, t_{n-1}$ with the property that $k[t_1, \ldots, t_{n-1}]$ is integral over $k[q_1, \ldots, q_{n-2}]$. Hence the q_i are linear combinations of $s_1, \ldots, s_n$

and A is integral over $k[q_1,\ldots,q_{n-2}]$. We keep proceeding in this way until we find a set which is algebraically independent. This is guaranteed to happen, since if we reached $k[v]$ with v algebraic over k, then A would be integral over $k[v]$ which is integral over k. But we assumed that A was not integral over k.

So finally we end up with an algebraically independent family $y_1,\ldots,y_r$ such that A is integral over $k[y_1,\ldots,y_r]$. Moreover the y_i are linear combinations of $s_1,\ldots,s_n$. □

Lemma 3. *Let $A = k[x_1,\ldots,x_n]$ be a polynomial ring over a field k. If $a_1,\ldots,a_n \in A$ are such that A is integral over $k[a_1,\ldots,a_n]$, then $\{a_1,\ldots,a_n\}$ is an algebraically independent set over k.*

Proof. Let $K = k(x_1,\ldots,x_n)$ be the quotient field of A. Then $\{x_1,\ldots,x_n\}$ is a transcendence basis of K/k. Since each x_i is integral over the subfield $k(a_1,\ldots,a_n)$, it follows that the extension $K/k(a_1,\ldots,a_n)$ is algebraic. Hence $\{a_1,\ldots,a_n\}$ contains a transcendence basis - but all such bases have the same number of elements, so the a_i must be algebraically independent. □

Proposition 4. *Let $A = k[x_1,\ldots,x_n]$ be a polynomial ring over a field k, and let $\mathfrak{a}$ be a nonzero proper ideal. There are elements $y_1,\ldots,y_n \in A$ which are algebraically independent over k satisfying the following conditions:*

1. *A is integral over $B = k[y_1,\ldots,y_n]$.*
2. *$\mathfrak{a} \cap B$ is generated as an ideal in B by $y_1,\ldots,y_h$ for some $1 \leq h \leq n$.*

Moreover, given any nonzero $a \in \mathfrak{a}$ we can find $y_1,\ldots,y_n$ satisfying the above conditions with $y_1 = a$.

Proof. First we prove the result in the case where $\mathfrak{a} = (a_1)$ is principal. By assumption $a_1 = g(x_1,\ldots,x_n)$ is a polynomial with coefficients in k. We claim that there are positive integers r_i, $2 \leq i \leq n$ such that A is integral over $B = k[a_1,y_2,\ldots,y_n]$ where for $i \geq 2$ we define

$$y_i = x_i - x_1^{r_i} \tag{2}$$

For the moment let r_i be arbitrary positive integers. Then

$$g(x_1, y_2 + x_1^{r_2},\ldots,y_n + x_1^{r_n}) - a_1 = 0$$

If we write the polynomial g as a sum of monomials $\sum_\alpha g(\alpha)x_1^{\alpha_1}\ldots x_n^{\alpha_n}$ then

$$\sum_\alpha g(\alpha)x_1^{\alpha_1}(y_2 + x_1^{r_2})^{\alpha_2}\ldots(y_n + x_1^{r_n})^{\alpha_n} - a_1 = 0$$

For each α with $g(\alpha) \neq 0$ we pick up a term $x_1^{f(\alpha)}$, where $f(\alpha) = \alpha_1 + r_2\alpha_2 + \ldots + \alpha_n r_n$. There are only finitely many α with $g(\alpha) \neq 0$, and we can find an integer $s > 1$ which is greater than $\alpha_1,\ldots,\alpha_n$ for every such α. If we put $r_i = s^{i-1}$ for $2 \leq i \leq n$ then it is straightforward to check that the $f(\alpha)$ will all be distinct. Hence there will be a unique β with $g(\beta) \neq 0$ that maximises $f(\beta)$, and we can write

$$g(\beta)x_1^{f(\beta)} + \sum_{j<f(\beta)} p_j(a_1,y_2,\ldots,y_n)x_1^j = 0$$

This proves that x_1 is integral over B. Considering (2), we see that $x_2,\ldots,x_n$ are also integral over B, so finally A is integral over B. We apply Lemma 3 to see that $\{a_1,y_2,\ldots,y_n\}$ is an algebraically independent set. Thus the first assertion of the Proposition holds.

Now we show that $\mathfrak{a} \cap B = a_1B$, which will prove the second assertion. Clearly $a_1B \subseteq \mathfrak{a} \cap B$. Let $t = a_1c \in \mathfrak{a} \cap B$, where $c \in A$. Then in K we have $c = t(a_1)^{-1}$ so that $c \in A \cap k(a_1,y_2,\ldots,y_n)$. Since the set $\{a_1,y_2,\ldots,y_n\}$ is algebraically independent, B is isomorphic to a polynomial ring and the subfield $k(a_1,y_2,\ldots,y_n)$ of K is isomorphic to the quotient field of B. Since A is integral over B and any UFD is integrally closed, it follows immediately that $c \in B$ and hence $t = a_1c \in a_1B$ as required. Thus $a_1B = \mathfrak{a} \cap B$ and the proof of the case where $\mathfrak{a}$ principal is complete. Note that we have also shown that in the field K, $A \cap k(a_1, y_2, \ldots, y_n) = B$.

We now prove the Proposition for arbitrary nonzero, proper ideals $\mathfrak{a}$. We proceed by induction on n, where $A = k[x_1, \ldots, x_n]$. We have already done the case $n = 1$, because then A is a PID. So assume $n > 1$ and let a_1 be a nonzero element of $\mathfrak{a}$, and note that since $\mathfrak{a}$ is proper, $a_1 \notin k$. We have just shown that there are elements $t_2, \ldots, t_n \in A$ such that $a_1, t_2, \ldots, t_n$ are algebraically independent over k, A is integral over the polynomial ring $k[a_1, t_2, \ldots, t_n]$. Let $C = k[t_2, \ldots, t_n]$. There are two cases:

Case $\mathfrak{a} \cap C = 0$: Let $B = k[a_1, t_2, \ldots, t_n]$. We claim that $\mathfrak{a} \cap B = a_1 B$. Clearly $a_1 B \subseteq \mathfrak{a} \cap B$. Suppose $t \in \mathfrak{a} \cap B$, so that we can write

$$\begin{aligned} t &= \sum_{\alpha} g(\alpha) a_1^{\alpha_1} t_2^{\alpha_2} \ldots t_n^{\alpha_n} \\ &= \sum_{\alpha, \alpha_1 \neq 0} g(\alpha) a_1^{\alpha_1} t_2^{\alpha_2} \ldots t_n^{\alpha_n} + \sum_{\alpha, \alpha_1 = 0} g(\alpha) t_2^{\alpha_2} \ldots t_n^{\alpha_n} \end{aligned}$$

The first term belongs to $a_1 B \subseteq \mathfrak{a}$, so that the second term belongs to the intersection $\mathfrak{a} \cap k[t_2, \ldots, t_n] = \mathfrak{a} \cap C$, which is zero. Hence $t \in a_1 B$, and the collection $a_1, t_2, \ldots, t_n$ satisfies the required conditions, completing the proof.

Case $\mathfrak{a} \cap C \neq 0$: Since the t_i are algebraically independent, C is isomorphic to a polynomial ring in $n - 1$ variables. By assumption $\mathfrak{a} \cap C$ is a nonzero proper ideal in C. So by the inductive hypothesis, there are elements $y_2, \ldots, y_n$ algebraically independent over k such that C is integral over $k[y_2, \ldots, y_n]$ and $\mathfrak{a} \cap k[y_2, \ldots, y_n]$ is generated as an ideal by $y_2, \ldots, y_h$ for some $h \leq n$.

Let $B = k[a_1, y_2, \ldots, y_n]$. Then A is integral over B since A is integral over $k[a_1, t_2, \ldots, t_n]$ which is integral over B. By Lemma 3, the set $\{a_1, y_2, \ldots, y_n\}$ is algebraically independent. To complete the proof, we show that $\mathfrak{a} \cap B$ is generated as an ideal in B by $a_1, y_2, \ldots, y_h$.

Suppose $t \in \mathfrak{a} \cap B$. Then we can write

$$t = \sum_{\alpha, \alpha_1 \neq 0} g(\alpha) a_1^{\alpha_1} y_2^{\alpha_2} \ldots y_n^{\alpha_n} + \sum_{\alpha, |\alpha| > 0} g(\alpha) y_2^{\alpha_2} \ldots y_n^{\alpha_n} + \ell$$

where $\ell \in k$. Since $t \in \mathfrak{a}$ the sum of the second and third terms belongs to $\mathfrak{a} \cap k[y_2, \ldots, y_n] = (y_2, \ldots, y_h)$. Since the y_i are algebraically independent, this implies that $\ell = 0$ and every monomial in the second summand involves one of $y_2, \ldots, y_h$. Hence $t \in (a_1, y_2, \ldots, y_h)$ as required.

□

We now extend this result to a chain of ideals $\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_m$.

Proposition 5. *Let $A = k[x_1, \ldots, x_n]$ be a polynomial ring over a field k, and let $\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_m$ be a chain of nonzero proper ideals. There are elements $y_1, \ldots, y_n \in A$ which are algebraically independent over k satisfying the following conditions:*

1. *A is integral over $B = k[y_1, \ldots, y_n]$.*
2. *There are integers $1 \leq h(1) \leq \ldots \leq h(m) \leq n$ such that $\mathfrak{a}_i \cap B$ is generated as an ideal in B by $y_1, \ldots, y_{h(i)}$ for $1 \leq i \leq m$.*

Moreover, given a sequence of nonzero elements $a_i \in \mathfrak{a}_i$ we can find $y_1, \ldots, y_n$ satisfying the above conditions with the further property that if $1 \leq i \leq m - 1$ and $h(i) < h(i+1)$ then $y_{h(i)+1} = a_{i+1}$ (if $m = 1$ then we can arrange $y_1 = a_1$).

Proof. By induction the number of ideals m. The case $m = 1$ was the subject of the previous Proposition. So assume $m > 1$ and that the result is true for all chains of $m - 1$ nonzero proper ideals. Let $\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_m$ be given. Find $t_1, \ldots, t_n$ satisfying the conditions for the chain $\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_{m-1}$, and let $s = h(m-1)$, and set $C = k[t_1, \ldots, t_n]$.

If $s = n$ then $\mathfrak{a}_{m-1} \cap C = (t_1, \ldots, t_n)$. Since the t_i are algebraically independent, C is a polynomial ring and $\mathfrak{a}_{m-1} \cap C$ is a maximal ideal. Hence $\mathfrak{a}_m \cap C = \mathfrak{a}_{m-1} \cap C = (t_1, \ldots, t_n)$ and we may put $B = C$ and $h(m) = h(m-1)$ to complete the proof.

Otherwise we may assume that $s < n$ and $\mathfrak{a}_m \cap k[t_{s+1}, \ldots, t_n]$ is nonzero, since otherwise we can modify the proof of Proposition (4) (the part dealing with the case $\mathfrak{a} \cap C = 0$) to see that $\mathfrak{a}_m \cap C = \mathfrak{a}_{m-1} \cap C$, and we have already dealt with this situation.

So we may assume $\mathfrak{a}_m \cap k[t_{s+1}, \ldots, t_n]$ is a nonzero proper ideal. There are algebraically independent elements $y_{s+1}, \ldots, y_n$ such that $k[t_{s+1}, \ldots, t_n]$ is integral over $k[y_{s+1}, \ldots, y_n]$ and $\mathfrak{a}_m \cap k[y_{s+1}, \ldots, y_n]$ is generated by $y_{s+1}, \ldots, y_{h(m)}$ for some $s + 1 \leq h(m) \leq n$. Moreover, we may choose $y_{s+1} = a_m$. Let $B = k[t_1, \ldots, t_s, y_{s+1}, \ldots, y_n]$. Then A is integral over C which is integral over B, so A is integral over B. Lemma 3 implies that the set $\{t_1, \ldots, t_s, y_{s+1}, \ldots, y_n\}$ is algebraically independent.

Clearly $h(m-1) = s < h(m) \leq n$. It only remains to check the second condition is satisfied. First we have to check that for $1 \leq i \leq m-1$ the ideal $\mathfrak{a}_i \cap B$ is still generated (as an ideal in B, not C) by the elements $t_1, \ldots, t_{h(i)}$. Clearly the ideal generated by these elements belongs to $\mathfrak{a}_i \cap B$. Now suppose $t \in \mathfrak{a}_i \cap B \subseteq \mathfrak{a}_i \cap C$. Since $\mathfrak{a}_i \cap C$ is the ideal in C generated by $t_1, \ldots, t_{h(i)}$ we can write

$$t = \sum_\alpha g(\alpha) t_1^{\alpha_1} \ldots t_n^{\alpha_n} \tag{3}$$

where each monomial involves a postive power of t_j for some $1 \leq j \leq h(i)$. Since $t \in B$ there is another expression

$$t = \sum_\beta f(\beta) t_1^{\beta_1} \ldots t_s^{\beta_s} y_{s+1}^{\beta_{s+1}} \ldots y_n^{\beta_n} \tag{4}$$

Since $y_{s+1}, \ldots, y_n \in k[t_{s+1}, \ldots, t_n]$ for each β involved in (4) we can write

$$y_{s+1}^{\beta_{s+1}} \ldots y_n^{\beta_n} = \sum_\gamma f_\beta(\gamma) t_{s+1}^{\gamma_1} \ldots t_n^{\gamma_{n-s}}$$

Hence (4) becomes

$$t = \sum_\beta \sum_\gamma f(\beta) f_\beta(\gamma) t_1^{\beta_1} \ldots t_s^{\beta_s} t_{s+1}^{\gamma_1} \ldots t_n^{\gamma_{n-s}}$$

Comparing this with (3) and using the algebraic independence of the t_i we conclude that any monomial in (4) involves a positive power of t_j for some $1 \leq j \leq h(i)$. That is, $\mathfrak{a}_i \cap B$ is generated as an ideal in B by $t_1, \ldots, t_{h(i)}$.

Finally, we show that $\mathfrak{a}_m \cap B = (t_1, \ldots, t_s, y_{s+1}, \ldots, y_{h(m)})$ in B. By definition the intersection $\mathfrak{a}_m \cap k[y_{s+1}, \ldots, y_n]$ is generated in $k[y_{s+1}, \ldots, y_n]$ by $y_{s+1}, \ldots, y_{h(m)}$ and $t_1, \ldots, t_s \in \mathfrak{a}_{m-1} \subset \mathfrak{a}_m$, so the right-to-left inclusion is clear. Suppose $t \in \mathfrak{a}_m \cap B$. If $h(m) = n$ then there is nothing to prove (since $\mathfrak{a}_m$ is proper), so assume $h(m) < n$. We can write

$$t = \sum_\beta g(\beta) y_{h(m)+1}^{\beta_1} \cdots y_n^{\beta_n} + \sum_\alpha f(\alpha) t_1^{\alpha_1} \ldots t_s^{\alpha_n} y_{s+1}^{\alpha_{s+1}} \ldots y_n^{\alpha_n}$$

where each monomial in the second summand involves a postive power of one of $t_1, \ldots, t_s$ or $y_{s+1}, \ldots, y_{h(m)}$. Hence the second summand belongs to $\mathfrak{a}_m$, so the first summand belongs to $\mathfrak{a}_m \cap k[y_{s+1}, \ldots, y_n]$ and consequently by algebraic independence each monomial in the first summand must involve a positive power of one of $y_{s+1}, \ldots, y_{h(m)}$. Since this is impossible, the first summand is zero and this implies $t \in (t_1, \ldots, t_s, y_{s+1}, \ldots, y_{h(m)})$, which completes the proof. □

Lemma 6. *Let $A \subseteq B$ be rings, with B integral over A. Let $\mathfrak{b}$ be an ideal of B containing a prime ideal $\mathfrak{p}$ of B. If $\mathfrak{b} \cap A = \mathfrak{p} \cap A$ then $\mathfrak{b} = \mathfrak{p}$.*

Proof. Suppose otherwise that $\mathfrak{p} \subset \mathfrak{b}$ and let $b \in \mathfrak{b} \setminus \mathfrak{p}$. Since b is integral over A, we have an equation

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0 \qquad a_i \in A$$

Clearly $a_n \in \mathfrak{b} \cap A = \mathfrak{p} \cap A$. Hence

$$b(b^{n-1} + a_1 b^{n-2} + \ldots a_{n-1}) \in \mathfrak{p}$$

So $b^{n-1} + a_1 b^{n-2} + \ldots a_{n-1} \in \mathfrak{p}$. Applying the same argument to a_{n-1} and proceeding recursively, we find that $b \in \mathfrak{p}$, a contradiction. Hence $\mathfrak{b} = \mathfrak{p}$. □

Definition 1. For a field k an *affine* k-algebra is a finitely generated k-algebra which is also an integral domain. Since by definition the zero ring is not a domain, any affine k-algebra is nonzero.

Lemma 7. *Let A be an affine k-algebra. Then A is integral over k if and only if A is a finite algebraic extension of k.*

Proof. The condition is clearly sufficient. To that it is necessary, suppose that A is integral over k. By Corollary 5.24 of A & M it suffices to show that A is a field. If $\mathfrak{m}$ is a maximal ideal of A, then $\mathfrak{m}$ and 0 both contract to 0 in $k \subseteq A$, so by the previous Lemma $\mathfrak{m} = 0$ and A is a field. □

Theorem 8. *Let k be a field, A an affine k-algebra, and $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_m$ a chain of nonzero proper ideals in A. Suppose A can be generated over k by n elements. Then either A is integral over k or there is an integer $1 \leq r \leq n$ and elements $y_1, \ldots, y_r \in A$ which are algebraically independent over k satisfying the following conditions:*

1. *A is integral over $B = k[y_1, \ldots, y_r]$.*
2. *There are integers $1 \leq h(1) \leq \ldots \leq h(m) \leq r$ such that $\mathfrak{a}_i \cap B$ is generated as an ideal in B by $y_1, \ldots, y_{h(i)}$.*

Proof. Let A be an affine k-algebra with a chain of nonzero proper ideals $\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_m$. Assume that A is not integral over k. If A can be generated by n elements then there is an isomorphism of k-algebras

$$\phi : k[x_1, \ldots, x_n]/\mathfrak{p} \longrightarrow A$$

with $\mathfrak{p}$ a nonzero prime ideal (If $\mathfrak{p} = 0$ then by Proposition 5 we are done). Let $\mathfrak{a}'_i$ be ideals of $k[x_1, \ldots, x_n]$ containing $\mathfrak{p}$ such that ϕ identifies $\mathfrak{a}'_i$ and $\mathfrak{a}_i$. Then $\mathfrak{p} \subset \mathfrak{a}'_1 \subset \ldots \subset \mathfrak{a}'_m$ is a chain of nonzero proper ideals in $k[x_1, \ldots, x_n]$. By Proposition 5 there exist elements $z_1, \ldots, z_n$ which are algebraically independent such that $k[x_1, \ldots, x_n]$ is integral over $B' = k[z_1, \ldots, z_n]$, $\mathfrak{a}'_i \cap B'$ is generated by $z_1, \ldots, z_{h(i)}$ and $\mathfrak{p} \cap B'$ is generated by $z_1, \ldots, z_{h(0)}$. Lemma 6 implies that $1 \leq h(0) < h(1) \leq n$.

Let $a \in A$ and $\phi(g + \mathfrak{p}) = a$. Let $g^n + f_1 g^{n-1} + \ldots + f_n = 0$ be an equation of integral dependence for g, where $f_i \in k[z_1, \ldots, z_n]$ for each i. Mapping to the quotient ring and applying ϕ we find an equation of integral dependence for a over $k[\phi(z_1 + \mathfrak{p}), \ldots, \phi(z_n + \mathfrak{p})]$.

Let $r = n - h(0)$ and set $y_1 = \phi(z_{h(0)+1} + \mathfrak{p}), \ldots, y_r = \phi(z_n + \mathfrak{p})$. It is still true that A is integral over $B = k[y_1, \ldots, y_r]$ and we now show that these elements are algebraically independent (in particular, they are all nonzero and distinct). For if a polynomial in the $z_{h(0)+1}, \ldots, z_n$ belonged to $\mathfrak{p}$, then since $\mathfrak{p} \cap B' = (z_1, \ldots, z_{h(0)})$ we could apply algebraic independence of the z_i to see that the polynomial was zero.

Consider the integers $f(i) = h(i) - h(0)$ for $1 \leq i \leq m$. Clearly $1 \leq f(1) \leq \ldots \leq f(m) \leq r$ and our next task is to show that $\mathfrak{a}_i \cap B$ is generated as an ideal in B by $y_1, \ldots, y_{f(i)}$. Clearly the ideal generated by these elements is contained in $\mathfrak{a}_i \cap B$. To prove the reverse inclusion, let $a \in \mathfrak{a}_i \cap B$ and $g \in k[x_1, \ldots, x_n]$ be such that $\phi(g + \mathfrak{p}) = a$. Then $g \in \mathfrak{a}'_i$ and modulo $\mathfrak{p}$, g is equal to a polynomial $v(z_{h(0)+1}, \ldots, z_n)$. Thus $v(z_{h(0)+1}, \ldots, z_n) \in \mathfrak{a}'_i \cap B'$ and consequently

$$v(z_{h(0)+1}, \ldots, z_r) = d_1 z_1 + \ldots + d_{h(i)} z_{h(i)}$$

for $d_j \in B' = k[z_1, \ldots, z_n]$. Using the fact that $a = \phi(g + \mathfrak{p})$ we find that a belongs to the ideal generated in B by $y_1, \ldots, y_{f(i)}$, which completes the proof. □