Rep#2: An algebraic proof of an analytic lemma

Darij Grinberg

[not completed, not proofread]

There is a rule of thumb that in 90% of all cases when a proof in algebra or combinatorics seems to use analysis, this use can be easily avoided. For example, when a proof of a combinatorial identity uses power series, it is - in most cases - enough to replace the words "power series" by "formal power series", and there is no need anymore to worry about issues of convergence and well-definedness[1]. When a proof of an algebraic fact works in the field $\mathbb{C}$, it will - in most cases - work just as well in the algebraic closure of $\mathbb{Q}$, or in any algebraically closed field of characteristic zero, and sometimes even the "algebraically closed" condition can be lifted, and it is enough to consider a sufficiently large finite algebraic extension of $\mathbb{Q}$. However, as always when it comes to such rules of thumb, there are exceptions. Here is one lemma that is used in various algebraical proofs, and which seems to be really much simpler to prove using analytical properties of $\mathbb{C}$ than using pure algebra:

Lemma 1. Let $A \diagup \mathbb{Q}$ be a field extension. Let n be a positive integer, and let ζ_1, ζ_2, ..., ζ_n be n roots of unity in A (of course, these roots of unity can be of different orders, and there can be equal roots among them). Assume that $\dfrac{1}{n}\left(\zeta_1 + \zeta_2 + ... + \zeta_n\right)$ is an algebraic integer. Then, either $\zeta_1+\zeta_2+...+\zeta_n = 0$ or $\zeta_1 = \zeta_2 = ... = \zeta_n$.

Remark. An element $s \in A$ is said to be an *algebraic integer* if it is integral over the subring $\mathbb{Z}$ of $\mathbb{Q}$.

This Lemma 1 appears in [1] as Lemma 4.22.

In this note, we will first discuss the standard proof of Lemma 1, which uses complex numbers in a nontrivial way, and then a (much longer and uglier but) purely algebraic-combinatorial one.

Both proofs begin by reducing Lemma 1 to a simpler fact:

Lemma 2. Let $A \diagup \mathbb{Q}$ be a finite-dimensional field extension. Let S be a finite set, and for every $s \in S$, let ξ_s be a root of unity in A. (Of course, these roots of unity can be of different orders, and there can be equal roots among them.) Assume that $\sum\limits_{s \in S} \xi_s \in \mathbb{Q}$ and $\left|\sum\limits_{s \in S} \xi_s\right| \geq |S|$. Then, $\xi_s = \xi_t$ for any two elements s and t of S. (In other words, all the elements ξ_s for various $s \in S$ are equal.)

Let us show how to derive Lemma 1 from this Lemma 2:

[1] This is not entirely correct: For instance, often one needs infinite sums of formal power series, and in this case one still has to worry about their *formal* convergence (i. e. that for any given monomial, only finitely many of the summands have a nonzero coefficient in front of this monomial). However, this is usually much easier than proving analytical convergence.

Proof of Lemma 1. Let $\mathbb{A}$ be the ring of all algebraic integers in A. Then, $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$ [2].

We can WLOG assume that the field extension $A \diagup \mathbb{Q}$ is finite-dimensional (in fact, we can otherwise replace A by the field $\mathbb{Q}(\zeta_1, \zeta_2, ..., \zeta_n)$, which is finite-dimensional over $\mathbb{Q}$ [3]) and normal (in fact, we can otherwise replace A by the normal closure of A). Then, $A \diagup \mathbb{Q}$ is a finite-dimensional Galois extension (since $\operatorname{char} \mathbb{Q} = 0$). Let G be the Galois group of this extension $A \diagup \mathbb{Q}$. Then, the product $\prod\limits_{\sigma \in G} \sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right)$ is the norm of the element $\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n) \in A$, and therefore $\prod\limits_{\sigma \in G} \sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right) \in \mathbb{Q}$. But on the other hand, $\prod\limits_{\sigma \in G} \sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right) \in \mathbb{A}$ [4]. Thus, $\prod\limits_{\sigma \in G} \sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right) \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

Now,

$$n^{|G|} \prod_{\sigma \in G} \underbrace{\sigma\left(\frac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right)}_{\substack{= \frac{1}{n}(\sigma(\zeta_1) + \sigma(\zeta_2) + ... + \sigma(\zeta_n)) \\ \text{(since } \sigma \text{ is a } \mathbb{Q}\text{-algebra homomorphism)}}}$$

$$= n^{|G|} \prod_{\sigma \in G} \left(\frac{1}{n}(\sigma(\zeta_1) + \sigma(\zeta_2) + ... + \sigma(\zeta_n))\right) = \underbrace{n^{|G|} \left(\frac{1}{n}\right)^{|G|}}_{=1} \prod_{\sigma \in G} \underbrace{(\sigma(\zeta_1) + \sigma(\zeta_2) + ... + \sigma(\zeta_n))}_{= \sum\limits_{k=1}^{n} \sigma(\zeta_k)}$$

$$= \prod_{\sigma \in G} \sum_{k=1}^{n} \sigma(\zeta_k) = \sum_{\kappa \in \{1,2,...,n\}^G} \prod_{\sigma \in G} \sigma\left(\zeta_{\kappa(\sigma)}\right) \qquad \text{(by the product rule)}.$$

---

[2] In fact, let $s \in \mathbb{Q} \cap \mathbb{A}$. Then, $s = \dfrac{a}{b}$ for some coprime integers a and b (because $s \in \mathbb{Q} \cap \mathbb{A}$ yields $s \in \mathbb{Q}$), and there exist some $n \in \mathbb{N}$ and integers α_0, α_1, ..., α_n such that $\sum\limits_{k=0}^{n} \alpha_k s^k = 0$ and $\alpha_n = 1$ (because $s \in \mathbb{Q} \cap \mathbb{A}$ yields $s \in \mathbb{A}$, so that s is an algebraic integer; in other words, s is integral over $\mathbb{Z}$). Hence, $0 = \sum\limits_{k=0}^{n} \alpha_k s^k = \sum\limits_{k=0}^{n} \alpha_k \left(\dfrac{a}{b}\right)^k = \sum\limits_{k=0}^{n} \alpha_k \dfrac{a^k}{b^k}$. Multiplying this equation by b^n, we obtain $0 = \sum\limits_{k=0}^{n} \alpha_k a^k b^{n-k} = \sum\limits_{k=0}^{n-1} \alpha_k a^k b^{n-k} + \underbrace{\alpha_n}_{=1} a^n \underbrace{b^{n-n}}_{=b^0=1} = \sum\limits_{k=0}^{n-1} \alpha_k a^k b^{n-k} + a^n$, so that $a^n = -\sum\limits_{k=0}^{n-1} \alpha_k a^k b^{n-k}$. Hence, $b \mid a^n$ (since $b \mid -\sum\limits_{k=0}^{n-1} \alpha_k a^k b^{n-k}$, because $b \mid b^{n-k}$ for every $k \in \{0, 1, ..., n-1\}$). Since a and b are coprime, this yields that either $b = 1$ or $b = -1$. Hence, $s = \dfrac{a}{b}$ must lie in $\mathbb{Z}$. Thus, we have proven that every $s \in \mathbb{Q} \cap \mathbb{A}$ lies in $\mathbb{Z}$. Therefore, $\mathbb{Q} \cap \mathbb{A} \subseteq \mathbb{Z}$, qed. This yields $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$ (since clearly $\mathbb{Z} \subseteq \mathbb{Q} \cap \mathbb{A}$).

[3] because ζ_1, ζ_2, ..., ζ_n are algebraic over $\mathbb{Q}$ (since ζ_1, ζ_2, ..., ζ_n are roots of unity)

[4] In fact, $\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)$ is an algebraic integer, and thus its conjugates $\sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right)$ are algebraic integers for all $\sigma \in G$, and therefore their product $\prod\limits_{\sigma \in G} \sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right)$ is an algebraic integer as well. In other words, $\prod\limits_{\sigma \in G} \sigma\left(\dfrac{1}{n}(\zeta_1 + \zeta_2 + ... + \zeta_n)\right) \in \mathbb{A}$, qed.

Here, we let $\{1,2,...,n\}^G$ denote the set of all maps from the set G to $\{1,2,...,n\}$. Hence,

$$\sum_{\kappa\in\{1,2,...,n\}^G} \prod_{\sigma\in G} \sigma\left(\zeta_{\kappa(\sigma)}\right) = n^{|G|} \underbrace{\prod_{\sigma\in G} \sigma\left(\frac{1}{n}\left(\zeta_1+\zeta_2+...+\zeta_n\right)\right)}_{\in\mathbb{Z}} \in n^{|G|}\mathbb{Z}.$$

If we denote $\prod_{\sigma\in G} \sigma\left(\zeta_{\kappa(\sigma)}\right)$ by ξ_κ for every $\kappa\in\{1,2,...,n\}^G$, then this becomes $\sum_{\kappa\in\{1,2,...,n\}^G} \xi_\kappa \in n^{|G|}\mathbb{Z}$.

Hence, two cases are possible:

Case 1: We have $\sum_{\kappa\in\{1,2,...,n\}^G} \xi_\kappa = 0$.

Case 2: We have $\left|\sum_{\kappa\in\{1,2,...,n\}^G} \xi_\kappa\right| \geq n^{|G|}$.

Let us first consider Case 2. In this case, we notice that for each map $\kappa\in\{1,2,...,n\}^G$, the element $\xi_\kappa = \prod_{\sigma\in G} \sigma\left(\zeta_{\kappa(\sigma)}\right) \in A$ is a root of unity (in fact, $\sigma\left(\zeta_{\kappa(\sigma)}\right)\in A$ is a root of unity for each $\sigma\in G$ [5], and the product of roots of unity is a root of unity again). Also, $\sum_{s\in\{1,2,...,n\}^G} \xi_s = \sum_{\kappa\in\{1,2,...,n\}^G} \xi_\kappa \in n^{|G|}\mathbb{Z}\subseteq\mathbb{Q}$ and

$$\begin{aligned}\left|\sum_{s\in\{1,2,...,n\}^G} \xi_s\right| &= \left|\sum_{\kappa\in\{1,2,...,n\}^G} \xi_\kappa\right| \geq n^{|G|} \qquad \text{(since we are in Case 2)}\\ &= \left|\{1,2,...,n\}^G\right|.\end{aligned}$$

Thus, Lemma 2 (applied to $S=\{1,2,...,n\}^G$) yields that $\xi_s=\xi_t$ for any two elements s and t of S. Consequently, $\zeta_\alpha=\zeta_\beta$ for any two elements α and β of $\{1,2,...,n\}$ (because if we let $s\in\{1,2,...,n\}^G$ be the map defined by $s(\sigma)=\begin{cases}\alpha, & \text{if } \sigma=\text{id};\\ 1, & \text{if } \sigma\neq\text{id}\end{cases}$ for every $\sigma\in G$, and let $t\in\{1,2,...,n\}^G$ be the map defined by $t(\sigma)=\begin{cases}\beta, & \text{if } \sigma=\text{id};\\ 1, & \text{if } \sigma\neq\text{id}\end{cases}$ for every $\sigma\in G$, then

$$\xi_s = \prod_{\sigma\in G} \sigma\left(\zeta_{s(\sigma)}\right) = \prod_{\substack{\sigma\in G;\\ \sigma=\text{id}}} \sigma\left(\underbrace{\zeta_{s(\sigma)}}_{\substack{=\zeta_\alpha\\ (\text{since}\\ \sigma=\text{id}\,)}}\right) \cdot \prod_{\substack{\sigma\in G;\\ \sigma\neq\text{id}}} \sigma\left(\underbrace{\zeta_{s(\sigma)}}_{\substack{=\zeta_1\\ (\text{since}\\ \sigma\neq\text{id}\,)}}\right) = \underbrace{\prod_{\substack{\sigma\in G;\\ \sigma=\text{id}}} \sigma\left(\zeta_\alpha\right)}_{=\text{id}(\zeta_\alpha)=\zeta_\alpha} \cdot \prod_{\substack{\sigma\in G;\\ \sigma\neq\text{id}}} \sigma\left(\zeta_1\right) = \zeta_\alpha \cdot \prod_{\substack{\sigma\in G;\\ \sigma\neq\text{id}}} \sigma\left(\zeta_1\right)$$

and similarly $\xi_t = \zeta_\beta \cdot \prod_{\substack{\sigma\in G;\\ \sigma\neq\text{id}}} \sigma\left(\zeta_1\right)$, and hence [6] $\dfrac{\xi_s}{\xi_t} = \dfrac{\zeta_\alpha \cdot \prod_{\substack{\sigma\in G;\\ \sigma\neq\text{id}}} \sigma\left(\zeta_1\right)}{\zeta_\beta \cdot \prod_{\substack{\sigma\in G;\\ \sigma\neq\text{id}}} \sigma\left(\zeta_1\right)} = \dfrac{\zeta_\alpha}{\zeta_\beta}$, so that $\xi_s=\xi_t$

[5] because $\zeta_{\kappa(\sigma)}$ is a root of unity, and because the map σ sends roots of unity to roots of unity (since σ is a ring automorphism of A)

[6] Here, we use that ξ_t is invertible (since ξ_t is a root of unity)

yields $\zeta_\alpha = \zeta_\beta$). In other words, $\zeta_1 = \zeta_2 = ... = \zeta_n$. Thus, in Case 2, Lemma 1 is proven.

Now let us deal with Case 1. In this case,

$$0 = \sum_{\kappa \in \{1,2,...,n\}^G} \xi_\kappa = \sum_{\kappa \in \{1,2,...,n\}^G} \prod_{\sigma \in G} \sigma\left(\zeta_{\kappa(\sigma)}\right) = n^{|G|} \prod_{\sigma \in G} \sigma\left(\frac{1}{n}\left(\zeta_1 + \zeta_2 + ... + \zeta_n\right)\right).$$

Hence, $0 = \prod_{\sigma \in G} \sigma\left(\frac{1}{n}\left(\zeta_1 + \zeta_2 + ... + \zeta_n\right)\right)$. Thus, there exists some $\sigma \in G$ such that $0 = \sigma\left(\frac{1}{n}\left(\zeta_1 + \zeta_2 + ... + \zeta_n\right)\right)$ (because A is a field, so the product of some elements of A can only be zero if some of the factors is zero). Therefore, $0 = \frac{1}{n}\left(\zeta_1 + \zeta_2 + ... + \zeta_n\right)$ (because σ is an automorphism of the field A and therefore injective), and thus $0 = \zeta_1 + \zeta_2 + ... + \zeta_n$. Thus, Lemma 1 is proven in Case 1.

Altogether, we have thus shown Lemma 1 in both Cases 1 and 2. This completes the proof of Lemma 1 under the assumption that Lemma 2 has been proved.

Now, it remains to prove Lemma 2. First, here is the analytic proof:

First proof of Lemma 2. The extension A of the field $\mathbb{Q}$ is finite-dimensional, and therefore can be embedded into the algebraic closure of $\mathbb{Q}$. The algebraic closure of $\mathbb{Q}$, in turn, can be embedded into $\mathbb{C}$. So we can WLOG assume that A is a subfield of $\mathbb{C}$. Then, by the triangle inequality, $\left|\sum_{s \in S} \xi_s\right| \leq \sum_{s \in S} \underbrace{|\xi_s|}_{\substack{=1 \text{ (since } \xi_s \text{ is a} \\ \text{root of unity)}}} = \sum_{s \in S} 1 = |S|$. But this inequality must be an equality (since the opposite inequality $\left|\sum_{s \in S} \xi_s\right| \geq |S|$ also holds), so we must have equality in the triangle inequality $\left|\sum_{s \in S} \xi_s\right| \leq \sum_{s \in S} |\xi_s|$. Hence, all the complex numbers ξ_s for $s \in S$ must have the same argument, i. e., we must have $\arg \xi_s = \arg \xi_t$ for any two elements s and t of S. But this yields $\xi_s = \xi_t$ for any two elements s and t of S (because $\arg \xi_s = \arg \xi_t$ and $|\xi_s| = 1 = |\xi_t|$). This proves Lemma 2.

This proof is short, however it uses the complex numbers in a substantial way. Instead of just relying on their algebraic properties, like most proofs in algebra do, it uses their geometric structure as well (modulus inequalities), and thus cannot be directly translated into a suitably large algebraic extension of $\mathbb{Q}$. But there is a different way to proceed:

Second proof of Lemma 2. We are going to rely on the following lemma:

> **Lemma 3.** Let A be a field. Let n be a positive integer, and for every $i \in \{1, 2, ..., n\}$, let ξ_i be a root of unity in A. Then, there exists some root of unity ζ in A and a sequence $(k_1, k_2, ..., k_n)$ of nonnegative integers such that $\left(\xi_i = \zeta^{k_i} \text{ for every } i \in \{1, 2, ..., n\}\right)$ and $\gcd(k_1, k_2, ..., k_n) = 1$.

The proof of this lemma can be found in [2] (where it appears as Lemma 3). Actually it is a rather easy corollary of the known fact (Theorem 1 in [2]) that any finite subgroup of the multiplicative group of a field is cyclic.

Another simple (but very useful, not only in this context) lemma that we need is:

Lemma 4. Let B be a subfield of a field A. Let $U \in B^{\alpha \times \beta}$ be a matrix, where α and β are nonnegative integers. Then, $\dim \operatorname{Ker}_A U = \dim \operatorname{Ker}_B U$. Here, for any field extension $F \diagup B$, we denote by $\operatorname{Ker}_F U$ the kernel of the linear map $F^\beta \to F^\alpha$ given by $v \mapsto Uv$.

First proof of Lemma 4. It is known that for any field extension $F \diagup B$, we have $\dim \operatorname{Ker}_F U = \beta - \operatorname{Rank}_F U$, where $\operatorname{Rank}_F U$ denotes the rank of the linear map $F^\beta \to F^\alpha$ given by $v \mapsto Uv$. It is also known that $\operatorname{rank}_F U$ is the greatest integer ν such that the matrix U has a $\nu \times \nu$ minor with nonzero determinant. Therefore, $\operatorname{rank}_F U$ does not depend on F, and therefore $\operatorname{rank}_A U = \operatorname{rank}_B U$. Hence, $\dim \operatorname{Ker}_A U = \beta - \operatorname{rank}_A U = \beta - \operatorname{rank}_B U = \dim \operatorname{Ker}_B U$. This proves Lemma 4.

Second proof of Lemma 4. By the Gaussian elimination algorithm (over the field B), we can transform the matrix U into a matrix V which is in row echelon form. In other words, we can find a matrix V in row echelon form and an invertible matrix $E \in B^{\alpha \times \alpha}$ such that $U = EV$ (here, the matrix E is the product of the elementary matrices corresponding to the elementary row operations which constitute the steps of the Gaussian elimination algorithm). Since E is invertible, we have $\operatorname{Ker}_F (EV) = \operatorname{Ker}_F V$ for every field extension $F \diagup B$. But we know that $\dim \operatorname{Ker}_F V = \beta - \operatorname{Rank}_F V$, where $\operatorname{Rank}_F V$ denotes the rank of the linear map $F^\beta \to F^\alpha$ given by $v \mapsto Vv$. The rank $\operatorname{Rank}_F V$ of the matrix V is the number of all nonzero rows of the matrix V (because the matrix V is in row echelon form). Hence, for every field extension $F \diagup B$, we have

$$\begin{aligned}\dim \operatorname{Ker}_F U &= \dim \underbrace{\operatorname{Ker}_F (EV)}_{=\operatorname{Ker}_F V} = \dim \operatorname{Ker}_F V = \beta - \underbrace{\operatorname{Rank}_F V}_{=(\text{the number of all nonzero rows of the matrix } V)} \\ &= \beta - (\text{the number of all nonzero rows of the matrix } V)\,.\end{aligned}$$

Thus, $\dim \operatorname{Ker}_F U$ does not depend on the field F. Hence, $\dim \operatorname{Ker}_A U = \dim \operatorname{Ker}_B U$, and thus Lemma 4 is proven.

Finally, we come to the *proof of Lemma 2:*

First let us WLOG assume that $S \neq \varnothing$ (otherwise, Lemma 2 is vacuously true).

The condition of Lemma 2 yields $\sum\limits_{s \in S} \xi_s \in \mathbb{Q}$. We WLOG assume that $\sum\limits_{s \in S} \xi_s \geq 0$ (because otherwise, we can enforce $\sum\limits_{s \in S} \xi_s \geq 0$ by replacing ξ_s by $-\xi_s$ for every $s \in S$; in fact, this is allowed because $-\xi_s$ is a root of unity for every $s \in S$ [7]). Denote the sum $\sum\limits_{s \in S} \xi_s$ by N. Then, $N = \sum\limits_{s \in S} \xi_s \in \mathbb{Q}$. Also, $N = \sum\limits_{s \in S} \xi_s \geq 0$ yields $N = |N| = \left| \sum\limits_{s \in S} \xi_s \right| \geq |S| > 0$.

We can also WLOG assume that $S = \{1, 2, ..., n\}$ for some $n \in \mathbb{N}$ (because S is a finite set, and we need the set S only as an index set for labeling the roots ξ_s of unity). Consider this n. Then, $n = |S| \neq 0$ (since $S \neq \varnothing$), so that n is a positive integer. Thus, by Lemma 3, there exists some root of unity ζ in A and a sequence $(k_1, k_2, ..., k_n)$ of nonnegative integers such that $\left(\xi_i = \zeta^{k_i} \text{ for every } i \in \{1, 2, ..., n\}\right)$ and $\gcd(k_1, k_2, ..., k_n) = 1$. We WLOG assume that k_1 is the largest of the integers k_1, k_2, ...,

[7] This is because ξ_s is a root of unity for every $s \in S$, and because whenever an element $z \in A$ is a root of unity, the element $-z$ is a root of unity as well.

k_n (otherwise, we can just interchange the roots ξ_1, ξ_2, ..., ξ_n). Then, $k_1 \geq k_s$ for every $s \in \{1, 2, ..., n\}$. Therefore, $k_1 \geq 1$ (because there exists at least one $s \in \{1, 2, ..., n\}$ such that $k_s \geq 1$ [8], and therefore this s satisfies $k_1 \geq k_s \geq 1$).

Now, $N = \sum_{s \in S} \underbrace{\xi_s}_{=\zeta^{k_s}} = \sum_{s \in \{1,2,...,n\}} \zeta^{k_s}$.

Choose a positive integer m such that ζ is a m-th root of unity. (Such m indeed exists, since ζ is a root of unity.) Then, $\zeta^m = 1$.

We need to introduce two notations:

- If $\mathcal{A}$ is an assertion, then we denote by $[\mathcal{A}]$ the truth value of $\mathcal{A}$ (defined by $[\mathcal{A}] = \begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}$).
- If U is a matrix, and u and v are two positive integers, then $U_{u,v}$ denotes the entry of the matrix U at the (u, v)-th place (if such an entry exists). If w is a vector, and i is a positive integer, then w_i denotes the i-th coordinate of the vector w.

We notice a trivial but important fact: If a, b and q are three integers such that $a \leq q \leq b$, and if h_j is an element of A for every $j \in \{a, a+1, ..., b\}$, then

$$\sum_{j=a}^{b} [j = q] \, h_j = h_q. \tag{1}$$

[9]

Now, define a $(k_1 + m) \times (k_1 + m)$-matrix $U \in \mathbb{Q}^{(k_1+m)\times(k_1+m)}$ by

$$\left(U_{i,j} = \begin{cases} [j = i] - [j = i + m], & \text{if } i \leq k_1; \\ \sum_{s \in \{1,2,...,n\}} [j = i - k_s] - N \, [j = i], & \text{if } i > k_1 \end{cases} \right. \\ \left. \text{for every } i \in \{1, 2, ..., k_1 + m\} \text{ and } j \in \{1, 2, ..., k_1 + m\} \right). \tag{2}$$

[10] Hence,

$$U_{i,j} = [j = i] - [j = i + m] \text{ for every } i \in \{1, 2, ..., k_1\} \text{ and } j \in \{1, 2, ..., k_1 + m\} \tag{3}$$

[8] since otherwise, we would have $k_1 = k_2 = ... = k_n = 0$ (because k_1, k_2, ..., k_n are all nonnegative), which would contradict $\gcd(k_1, k_2, ..., k_n) = 1$.

[9] This is because

$$\sum_{j=a}^{b} [j = q] \, h_j = \sum_{j \in \{a,a+1,...,b\}} [j = q] \, h_j = \sum_{\substack{j \in \{a,a+1,...,b\}; \\ j = q}} \underbrace{[j = q]}_{=1 \text{ (since } j=q \text{ is true)}} h_j + \sum_{\substack{j \in \{a,a+1,...,b\}; \\ j \neq q}} \underbrace{[j = q]}_{=0 \text{ (since } j=q \text{ is false)}} h_j$$

$$= \underbrace{\sum_{\substack{j \in \{a,a+1,...,b\}; \\ j = q}} h_j}_{\substack{=h_q \text{ (since } q \in \{a,a+1,...,b\} \\ \text{(because } a \leq q \leq b \text{ and } q \in \mathbb{Z}))}} + \underbrace{\sum_{\substack{j \in \{a,a+1,...,b\}; \\ j \neq q}} 0 h_j}_{=0} = h_q.$$

[10] If you know the theory of resultants, you will recognize this matrix U as the Sylvester matrix of the two polynomials $X^m - 1$ and $\sum_{s \in \{1,2,...,n\}} X^{k_s} - N$ (or as a transposed and, possibly, row-permuted version of this Sylvester matrix - depending on how one defines the Sylvester matrix of two polynomials).

(by (2), because $i \in \{1,2,...,k_1\}$ yields $i \leq k_1$) and

$$U_{i,j} = \sum_{s \in \{1,2,...,n\}} [j = i - k_s] - N\,[j = i] \text{ for every } i \in \{k_1+1, k_1+2, ..., k_1+m\} \text{ and } j \in \{1,2,...,k_1+m\} \tag{4}$$

(by (2), because $i \in \{k_1+1, k_1+2, ..., k_1+m\}$ yields $i > k_1$). Thus, for any vector $h \in A^{k_1+m}$ and every $i \in \{1,2,...,k_1\}$, we have

$$\begin{aligned}
(Uh)_i &= \sum_{j=1}^{k_1+m} U_{i,j} h_j = \sum_{j=1}^{k_1+m} \left([j=i] - [j=i+m]\right) h_j \qquad \text{(by (3))} \\
&= \underbrace{\sum_{j=1}^{k_1+m} [j=i]\, h_j}_{\substack{=h_i \text{ (by (1) (applied to } a=1, \\ q=i \text{ and } b=k_1+m), \text{ since } 1 \leq i \leq k_1+m)}} - \underbrace{\sum_{j=1}^{k_1+m} [j=i+m]\, h_j}_{\substack{=h_{i+m} \text{ (by (1) (applied to } a=1, \\ q=i+m \text{ and } b=k_1+m), \text{ since} \\ 1 \leq i+m \leq k_1+m, \text{ because } i \leq k_1)}} \\
&= h_i - h_{i+m}.
\end{aligned} \tag{5}$$

Besides, for any vector $h \in A^{k_1+m}$ and every $i \in \{k_1+1, k_1+2, ..., k_1+m\}$, we have

$$\begin{aligned}
(Uh)_i &= \sum_{j=1}^{k_1+m} U_{i,j} h_j = \sum_{j=1}^{k_1+m} \left(\sum_{s \in \{1,2,...,n\}} [j = i - k_s] - N\,[j=i] \right) h_j \qquad \text{(by (4))} \\
&= \sum_{s \in \{1,2,...,n\}} \underbrace{\sum_{j=1}^{k_1+m} [j = i-k_s]\, h_j}_{\substack{=h_{i-k_s} \text{ (by (1) (applied to } a=1,\ q=i-k_s \\ \text{and } b=k_1+m), \text{ since } 1 \leq i-k_s \leq k_1+m, \\ \text{because } i > k_1 \geq k_s \text{ yields } i \geq k_s+1)}} - N \underbrace{\sum_{j=1}^{k_1+m} [j=i]\, h_j}_{\substack{=h_i \text{ (by (1) (applied to } a=1, \\ q=i \text{ and } b=k_1+m), \text{ since } 1 \leq i \leq k_1+m)}} \\
&= \sum_{s \in \{1,2,...,n\}} h_{i-k_s} - N h_i.
\end{aligned} \tag{6}$$

Now, let ϑ be *any* m-th root of unity in A; for instance, this means that ϑ may be 1 but may also be ζ or any other m-th root of unity. Then, $\vartheta^m = 1$.

Let us define a vector $\overline{\vartheta} \in A^{k_1+m}$ by $\overline{\vartheta}_i = \vartheta^{k_1+m-i}$ for every $i \in \{1,2,...,k_1+m\}$. Then, for every $i \in \{1,2,...,k_1\}$, we have

$$\begin{aligned}
\left(U\overline{\vartheta}\right)_i &= \underbrace{\overline{\vartheta}_i}_{=\vartheta^{k_1+m-i}} - \underbrace{\overline{\vartheta}_{i+m}}_{=\vartheta^{k_1+m-(i+m)}} \qquad \left(\text{by (5), applied to } h = \overline{\vartheta}\right) \\
&= \underbrace{\vartheta^{k_1+m-i}}_{=\vartheta^{k_1-i+m} = \vartheta^{k_1-i}\vartheta^m} - \underbrace{\vartheta^{k_1+m-(i+m)}}_{=\vartheta^{k_1-i}} = \vartheta^{k_1-i}\left(\underbrace{\vartheta^m}_{=1} - 1\right) = \vartheta^{k_1-i} \underbrace{(1-1)}_{=0} = 0.
\end{aligned} \tag{7}$$

Besides, for every $i \in \{k_1+1, k_1+2, ..., k_1+m\}$, we have

$$\left(U\overline{\vartheta}\right)_i = \sum_{s\in\{1,2,...,n\}} \underbrace{\overline{\vartheta}_{i-k_s}}_{\substack{=\vartheta^{k_1+m-(i-k_s)} \\ =\vartheta^{k_1+m-i+k_s} \\ =\vartheta^{k_1+m-i}\vartheta^{k_s}}} - N \underbrace{\overline{\vartheta}_i}_{=\vartheta^{k_1+m-i}} \qquad \left(\text{by (6), applied to } h=\overline{\vartheta}\right)$$

$$= \sum_{s\in\{1,2,...,n\}} \vartheta^{k_1+m-i}\vartheta^{k_s} - N\vartheta^{k_1+m-i} = \vartheta^{k_1+m-i}\left(\underbrace{\sum_{s\in\{1,2,...,n\}} \vartheta^{k_s}}_{=N} - N\right) = \vartheta^{k_1+m-i}\underbrace{(N-N)}_{=0} = 0. \tag{8}$$

Consequently, $\left(U\overline{\vartheta}\right)_i = 0$ for every $i \in \{1,2,...,k_1+m\}$ [11]. In other words, $U\overline{\vartheta} = 0$, so that $\overline{\vartheta} \in \operatorname{Ker}_A U$. We have thus obtained the result that $\overline{\vartheta} \in \operatorname{Ker}_A U$, where ϑ is any m-th root of unity in A. Applying this result to $\vartheta = 1$ yields $\overline{1} \in \operatorname{Ker}_A U$, while applying the same result to $\vartheta = \zeta$ yields $\overline{\zeta} \in \operatorname{Ker}_A U$.

Now, our goal is to show that $\dim \operatorname{Ker}_A U \leq 1$. In fact, once this is shown, it will follow from $\overline{1} \in \operatorname{Ker}_A U$ and $\overline{\zeta} \in \operatorname{Ker}_A U$ that the vectors $\overline{1}$ and $\overline{\zeta}$ are linearly dependent, which will quickly yield $\zeta = 1$, and Lemma 2 will be proven. In order to prove that $\dim \operatorname{Ker}_A U \leq 1$, we will show that $\dim \operatorname{Ker}_{\mathbb{Q}} U \leq 1$, applying Lemma 4 to see that $\dim \operatorname{Ker}_A U = \dim \operatorname{Ker}_{\mathbb{Q}} U$. But before we delve into the details of this argument, let us prove that $\dim \operatorname{Ker}_{\mathbb{Q}} U \leq 1$.

In fact, let $h \in \operatorname{Ker}_{\mathbb{Q}} U$ be a vector. Then, $h \in \mathbb{Q}^{k_1+m}$ and $0 = Uh$. Consequently, every $i \in \{1,2,...,k_1\}$ satisfies $0 = (Uh)_i = h_i - h_{i+m}$ (by (5)), so that

$$h_i = h_{i+m} \qquad \text{for every } i \in \{1,2,...,k_1\}. \tag{9}$$

Besides, every $i \in \{k_1+1, k_1+2, ..., k_1+m\}$ satisfies

$$\begin{aligned} 0 &= (Uh)_i \qquad (\text{since } 0 = Uh) \\ &= \sum_{s\in\{1,2,...,n\}} h_{i-k_s} - Nh_i \qquad (\text{by (6)}), \end{aligned}$$

so that

$$\sum_{s\in\{1,2,...,n\}} h_{i-k_s} = Nh_i \qquad \text{for every } i \in \{k_1+1, k_1+2, ..., k_1+m\}. \tag{10}$$

The vector $h \in \mathbb{Q}^{k_1+m}$ has k_1+m coordinates: h_1, h_2, ..., h_{k_1+m}. So we have a finite sequence $(h_1, h_2, ..., h_{k_1+m})$ of length k_1+m. We will now extend this sequence in both directions: We define a number $h_i \in \mathbb{Q}$ for every $i \in \mathbb{Z} \setminus \{1,2,...,k_1+m\}$ by setting $h_i = h_{\pi(i)}$, where $\pi : \mathbb{Z} \to \{1,2,...,k_1+m\}$ is the map defined by

$$\pi(i) = (\text{the element } x \text{ of the set } \{1,2,...,k_1+m\} \text{ which satisfies } x \equiv i \bmod k_1+m).$$

[11] In fact, let $i \in \{1,2,...,k_1+m\}$. Then, either $i \in \{1,2,...,k_1\}$ or $i \in \{k_1+1, k_1+2, ..., k_1+m\}$ must hold. But in both cases, $\left(U\overline{\vartheta}\right)_i = 0$ (in fact, in the case $i \in \{1,2,...,k_1\}$, the equation $\left(U\overline{\vartheta}\right)_i = 0$ follows from (7), and in the case $i \in \{k_1+1, k_1+2, ..., k_1+m\}$, the equation $\left(U\overline{\vartheta}\right)_i = 0$ follows from (8)). Thus, $\left(U\overline{\vartheta}\right)_i = 0$ is proven.

Thus, a number $h_i \in \mathbb{Q}$ is defined for every $i \in \mathbb{Z}$, and we get a two-sided infinite sequence $(..., h_{-2}, h_{-1}, h_0, h_1, h_2, ...)$ which extends the sequence $(h_1, h_2, ..., h_{k_1+m})$ of coordinates of the vector h. It is clear that $h_i = h_{\pi(i)}$ for every $i \in \mathbb{Z}$ [12]. Consequently,

$$h_i = h_j \text{ for any two integers } i \text{ and } j \text{ which satisfy } i \equiv j \bmod k_1 + m \tag{11}$$

(because $i \equiv j \bmod k_1 + m$ yields $\pi(i) = \pi(j)$ and thus $h_i = h_{\pi(i)} = h_{\pi(j)} = h_j$). In other words, the sequence $(..., h_{-2}, h_{-1}, h_0, h_1, h_2, ...)$ is periodic with period $k_1 + m$. Thus, $\{h_i \mid i \in \mathbb{Z}\} = \{h_1, h_2, ..., h_{k_1+m}\}$, so that $\{|h_i| \mid i \in \mathbb{Z}\} = \{|h_1|, |h_2|, ..., |h_{k_1+m}|\}$.

Now, let $\nu \in \mathbb{Z}$ be some integer for which $|h_\nu| = \max\{|h_i| \mid i \in \mathbb{Z}\}$. (Such an integer ν exists because the set $\{|h_i| \mid i \in \mathbb{Z}\} = \{|h_1|, |h_2|, ..., |h_{k_1+m}|\}$ is finite and thus has a maximum.) We denote the rational number h_ν by q. Our next goal is to prove that $h_i = q$ for every $i \in \mathbb{Z}$.

First, we note that

$$\text{if an integer } \mu \text{ satisfies } \pi(\mu) \in \{1, 2, ..., k_1\} \text{ and } h_\mu = q, \text{ then } h_{\mu+m} = q. \tag{12}$$

Proof of (12). In fact, if an integer μ satisfies $\pi(\mu) \in \{1, 2, ..., k_1\}$ and $h_\mu = q$, then

$$\begin{aligned} h_{\mu+m} &= h_{\pi(\mu)+m} \qquad \left(\begin{array}{c} \text{by (11) (applied to } \mu+m \text{ and } \pi(\mu)+m \text{ instead of } i \text{ and } j), \\ \text{because } \mu+m \equiv \pi(\mu)+m \bmod k_1+m \text{ (since } \mu \equiv \pi(\mu) \bmod k_1+m) \end{array} \right) \\ &= h_{\pi(\mu)} \qquad \text{(by (9), applied to } i = \pi(\mu)) \\ &= h_\mu = q, \end{aligned}$$

so that (12) is proven.

Besides, we note that

$$\begin{aligned} &\text{if an integer } \mu \text{ satisfies } \pi(\mu) \in \{k_1+1, k_1+2, ..., k_1+m\} \text{ and } h_\mu = q, \text{ then} \\ &h_{\mu-k_s} = q \text{ for every } s \in \{1, 2, ..., n\}. \end{aligned} \tag{13}$$

Proof of (13). In fact, let an integer μ satisfy $\pi(\mu) \in \{k_1+1, k_1+2, ..., k_1+m\}$ and $h_\mu = q$. Then, (10) (applied to $i = \pi(\mu)$) yields $\sum\limits_{s \in \{1,2,...,n\}} h_{\pi(\mu)-k_s} = N h_{\pi(\mu)}$. But on the other hand, $\left|\underbrace{h_{\pi(\mu)}}_{=h_\mu}\right| = |h_\mu| = |q| = |h_\nu| = \max\{|h_i| \mid i \in \mathbb{Z}\} \geq \left|h_{\pi(\mu)-k_s}\right|$ for every $s \in \{1, 2, ..., n\}$, so that

$$\begin{aligned} n\left|h_{\pi(\mu)}\right| &= \sum_{s \in \{1,2,...,n\}} \underbrace{\left|h_{\pi(\mu)}\right|}_{\geq \left|h_{\pi(\mu)-k_s}\right|} \geq \sum_{s \in \{1,2,...,n\}} \left|h_{\pi(\mu)-k_s}\right| \geq \left|\underbrace{\sum_{s \in \{1,2,...,n\}} h_{\pi(\mu)-k_s}}_{=N h_{\pi(\mu)}}\right| \qquad \text{(by the triangle inequality)} \\ &= \left|N h_{\pi(\mu)}\right| = \underbrace{|N|}_{\geq n \text{ (since } N \geq n)} \left|h_{\pi(\mu)}\right| \geq n\left|h_{\pi(\mu)}\right|. \end{aligned}$$

[12] In fact, two cases are possible: either $i \in \mathbb{Z} \setminus \{1, 2, ..., k_1+m\}$ or $i \in \{1, 2, ..., k_1+m\}$. But in both cases, we have $h_i = h_{\pi(i)}$ (in fact, in the case $i \in \mathbb{Z} \setminus \{1, 2, ..., k_1+m\}$, we have $h_i = h_{\pi(i)}$ by the definition of h_i; on the other hand, in the case $i \in \{1, 2, ..., k_1+m\}$, we have $h_i = h_{\pi(i)}$ because of $i = \pi(i)$).

This chain of inequalities must be an equality (since the leftmost and the rightmost sides of this chain are equal), so that all inequalities inbetween must be equalities. In particular, the inequality $\left|h_{\pi(\mu)}\right| \geq \left|h_{\pi(\mu)-k_s}\right|$ for every $s \in \{1,2,...,n\}$ must become an equality, and the triangle inequality $\sum\limits_{s\in\{1,2,...,n\}} \left|h_{\pi(\mu)-k_s}\right| \geq \left|\sum\limits_{s\in\{1,2,...,n\}} h_{\pi(\mu)-k_s}\right|$ must become an equality.

Since the inequality $\left|h_{\pi(\mu)}\right| \geq \left|h_{\pi(\mu)-k_s}\right|$ for every $s \in \{1,2,...,n\}$ must become an equality, we must have $\left|h_{\pi(\mu)}\right| = \left|h_{\pi(\mu)-k_s}\right|$ for every $s \in \{1,2,...,n\}$. Thus, $\left|h_{\pi(\mu)-k_s}\right| = \left|h_{\pi(\mu)}\right| = |h_\mu| = |q|$ for every $s \in \{1,2,...,n\}$. Since the triangle inequality $\sum\limits_{s\in\{1,2,...,n\}} \left|h_{\pi(\mu)-k_s}\right| \geq \left|\sum\limits_{s\in\{1,2,...,n\}} h_{\pi(\mu)-k_s}\right|$ must become an equality, the rational numbers $h_{\pi(\mu)-k_1}$, $h_{\pi(\mu)-k_2}$, ..., $h_{\pi(\mu)-k_n}$ must all have the same sign. Hence, of course, the sum $\sum\limits_{s\in\{1,2,...,n\}} h_{\pi(\mu)-k_s}$ of these numbers $h_{\pi(\mu)-k_1}$, $h_{\pi(\mu)-k_2}$, ..., $h_{\pi(\mu)-k_n}$ must also have the same sign as each of these numbers $h_{\pi(\mu)-k_1}$, $h_{\pi(\mu)-k_2}$, ..., $h_{\pi(\mu)-k_n}$. But on the other hand, the sum $\sum\limits_{s\in\{1,2,...,n\}} h_{\pi(\mu)-k_s} = N \underbrace{h_{\pi(\mu)}}_{=h_\mu=q} = Nq$ has the same sign as q (because $N > 0$). Hence, each of the numbers $h_{\pi(\mu)-k_1}$, $h_{\pi(\mu)-k_2}$, ..., $h_{\pi(\mu)-k_n}$ has the same sign as q. But we also know that each of the numbers $h_{\pi(\mu)-k_1}$, $h_{\pi(\mu)-k_2}$, ..., $h_{\pi(\mu)-k_n}$ has the same absolute value as q (because $\left|h_{\pi(\mu)-k_s}\right| = |q|$ for every $s \in \{1,2,...,n\}$). Thus, each of the numbers $h_{\pi(\mu)-k_1}$, $h_{\pi(\mu)-k_2}$, ..., $h_{\pi(\mu)-k_n}$ is equal to q (because if two numbers have the same sign and the same absolute value, then they are equal). In other words, $h_{\pi(\mu)-k_s} = q$ for every $s \in \{1,2,...,n\}$. Since $h_{\pi(\mu)-k_s} = h_{\mu-k_s}$ (because $\pi(\mu) \equiv \mu \bmod k_1 + m$ yields $\pi(\mu) - k_s \equiv \mu - k_s \bmod k_1 + m$, and therefore (11) (applied to $\pi(\mu) - k_s$ and $\mu - k_s$ instead of i and j) yields $h_{\pi(\mu)-k_s} = h_{\mu-k_s}$), this rewrites as $h_{\mu-k_s} = q$ for every $s \in \{1,2,...,n\}$. Thus, (13) is proven.

Next let us prove that

$$\text{if an integer } \mu \text{ satisfies } h_\mu = q, \text{ then } h_{\mu+m} = q. \tag{14}$$

Proof of (14). In fact, let an integer μ satisfy $h_\mu = q$. Then, either $\pi(\mu) \in \{1,2,...,k_1\}$ or $\pi(\mu) \in \{k_1+1, k_1+2, ..., k_1+m\}$ (because $\pi(\mu) \in \{1,2,...,k_1+m\}$). But in both of these cases, $h_{\mu+m} = q$ holds (in fact, in the case when $\pi(\mu) \in \{1,2,...,k_1\}$, we have $h_{\mu+m} = q$ by (12), and in the case when $\pi(\mu) \in \{k_1+1, k_1+2, ..., k_1+m\}$, we have

$$\begin{aligned} h_{\mu+m} &= h_{\mu-k_1} \qquad \left(\begin{array}{c} \text{by (11) (applied to } \mu+m \text{ and } \mu-k_1 \text{ instead of } i \text{ and } j), \\ \text{since } \mu+m \equiv \mu-k_1 \bmod k_1+m \end{array} \right) \\ &= q \qquad \text{(by (13), applied to } s=1) \end{aligned}$$

). Thus, $h_{\mu+m} = q$ must hold, and (14) is proven.

We note that, obviously, (14) is a generalization of (12). But now we will generalize (14) even further (albeit trivially): We will show that

$$\text{if two integers } \delta \text{ and } \varepsilon \text{ satisfy } h_\delta = q \text{ and } \delta \equiv \varepsilon \bmod m, \text{ then } h_\varepsilon = q. \tag{15}$$

Proof of (15). In fact, let an integer δ satisfy $h_\delta = q$. We will first show that $h_{\delta+\rho m} = q$

for every nonnegative integer ρ. In fact, this is clear by induction[13]. Now, for any integer ε satisfying $\delta \equiv \varepsilon \bmod m$, there exists a nonnegative integer ρ satisfying $\varepsilon \equiv \delta + \rho m \bmod k_1 + m$ [14], and thus

$$h_\varepsilon = h_{\delta+\rho m} \qquad \left(\begin{array}{c} \text{by (11) (applied to } \varepsilon \text{ and } \delta+\rho m \text{ instead of } i \text{ and } j\text{),} \\ \text{since } \varepsilon \equiv \delta + \rho m \bmod k_1 + m \end{array} \right)$$
$$= q$$

(because we have proven $h_{\delta+\rho m} = q$ above). This completes the proof of (15).

Next, let us generalize (13): Namely, let us show that

$$\text{if an integer } \mu \text{ satisfies } h_\mu = q, \text{ then } h_{\mu - k_s} = q \text{ for every } s \in \{1,2,...,n\}. \tag{16}$$

Proof of (16). In fact, let an integer μ satisfy $h_\mu = q$, and let $s \in \{1,2,...,n\}$. Then, there exists some $\lambda \in \{k_1+1, k_1+2, ..., k_1+m\}$ such that $\lambda \equiv \mu \bmod m$ [15]. Hence, $h_\lambda = q$ (by (15), applied to $\delta = \mu$ and $\varepsilon = \lambda$). But $\lambda \in \{k_1+1, k_1+2, ..., k_1+m\} \subseteq \{1,2,...,k_1+m\}$ yields

$$\pi(\lambda) = (\text{the element } x \text{ of the set } \{1,2,...,k_1+m\} \text{ which satisfies } x \equiv \lambda \bmod k_1 + m) = \lambda$$

(because λ itself is an element of the set $\{1,2,...,k_1+m\}$ and satisfies $\lambda \equiv \lambda \bmod k_1 + m$). Hence, $\lambda \in \{k_1+1, k_1+2, ..., k_1+m\}$ rewrites as $\pi(\lambda) \in \{k_1+1, k_1+2, ..., k_1+m\}$. Thus (13) (applied to λ instead of μ) yields $h_{\lambda - k_s} = q$. Thus, $h_{\mu-k_s} = q$ (by (15), applied to $\delta = \lambda - k_s$ and $\varepsilon = \mu - k_s$) because $\lambda - k_s \equiv \mu - k_s \bmod m$ (since $\lambda \equiv \mu \bmod m$). This proves (16).

We record a trivial generalization of (16): Let us prove that

$$\text{if some } s \in \{1,2,...,n\} \text{ and two integers } \delta \text{ and } \varepsilon \text{ satisfy } h_\delta = q \text{ and } \delta \equiv \varepsilon \bmod k_s, \text{ then } h_\varepsilon = q. \tag{17}$$

Proof of (17). In fact, let some $s \in \{1,2,...,n\}$ and an integer δ satisfy $h_\delta = q$. We will first show that $h_{\delta - \rho k_s} = q$ for every nonnegative integer ρ. In fact, this is clear by induction[16]. Now, for any integer ε satisfying $\delta \equiv \varepsilon \bmod k_s$, there exists a nonnegative

[13] *Induction base:* For $\rho = 0$, we have $h_{\delta+\rho m} = h_{\delta+0m} = h_\delta = q$, and thus $h_{\delta+\rho m} = q$ is proven for $\rho = 0$.

Induction step: Let ϕ be a nonnegative integer. Assume that $h_{\delta+\rho m} = q$ holds for $\rho = \phi$. Then, $h_{\delta+\rho m} = q$ holds for $\rho = \phi+1$ as well (because $h_{\delta+(\phi+1)m} = h_{(\delta+\phi m)+m} = q$ (by (14), applied to $\mu = \delta + \phi m$), because $h_{\delta+\phi m} = q$, since $h_{\delta+\rho m} = q$ holds for $\rho = \phi$). This completes the induction step.

Thus, the induction proof of $h_{\delta+\rho m} = q$ is complete.

[14] In fact, $\dfrac{\varepsilon - \delta}{m} \in \mathbb{Z}$ (since $\delta \equiv \varepsilon \bmod m$). Now, let ρ be the residue of $\dfrac{\varepsilon-\delta}{m}$ modulo $k_1 + m$. Then, $\rho \geq 0$ and $\rho \equiv \dfrac{\varepsilon - \delta}{m} \bmod k_1 + m$, so that $\rho m \equiv \varepsilon - \delta \bmod k_1 + m$ and thus $\varepsilon \equiv \delta + \rho m \bmod k_1 + m$.

[15] In fact, the m integers k_1+1, k_1+2, ..., k_1+m are m consecutive integers, and therefore they leave all possible residues modulo m. Therefore, in particular, one of these m integers leaves the same residue modulo m as μ; in other words, one of these m integers is congruent to μ modulo m. In other words, there exists some $\lambda \in \{k_1+1, k_1+2, ..., k_1+m\}$ such that $\lambda \equiv \mu \bmod m$.

[16] *Induction base:* For $\rho = 0$, we have $h_{\delta-\rho k_s} = h_{\delta-0k_s} = h_\delta = q$, and thus $h_{\delta-\rho k_s} = q$ is proven for $\rho = 0$.

Induction step: Let ϕ be a nonnegative integer. Assume that $h_{\delta-\rho k_s} = q$ holds for $\rho = \phi$. Then, $h_{\delta-\rho k_s} = q$ holds for $\rho = \phi+1$ as well (because $h_{\delta-(\phi+1)k_s} = h_{(\delta-\phi k_s)-k_s} = q$ (by (16), applied to $\mu = \delta - \phi k_s$), because $h_{\delta-\phi k_s} = q$, since $h_{\delta-\rho k_s} = q$ holds for $\rho = \phi$). This completes the induction step.

Thus, the induction proof of $h_{\delta-\rho k_s} = q$ is complete.

integer ρ satisfying $\varepsilon \equiv \delta - \rho k_s \bmod k_1 + m$ [17], and thus

$$h_\varepsilon = h_{\delta - \rho k_s} \qquad \left(\begin{array}{c} \text{by (11) (applied to } \varepsilon \text{ and } \delta - \rho k_s \text{ instead of } i \text{ and } j), \\ \text{since } \varepsilon \equiv \delta - \rho k_s \bmod k_1 + m \end{array} \right)$$
$$= q$$

(because we have proven $h_{\delta - \rho k_s} = q$ above). This completes the proof of (17).

Our next goal is to show that

$$\text{if some } \lambda \in \{1, 2, ..., n\} \text{ and two integers } \delta \text{ and } \varepsilon \text{ satisfy } h_\delta = q \text{ and } \delta \equiv \varepsilon \bmod \gcd(k_1, k_2, ..., k_\lambda), \text{ then } h_\varepsilon = q. \tag{18}$$

Proof of (18). In fact, let us prove (18) by induction over λ.

Induction base: If $\lambda = 1$, then (18) follows from (17), applied to $s = 1$ (because $\lambda = 1$ yields $\gcd(k_1, k_2, ..., k_\lambda) = \gcd(k_1) = k_1 = k_s$ due to $s = 1$). Hence, (18) is proven for $\lambda = 1$, so that the induction base is complete.

Induction step: Let $s \in \{1, 2, ..., n\}$ be such that $s > 1$. Assume that (18) holds for $\lambda = s - 1$. Our aim is then to prove that (18) holds for $\lambda = s$.

In fact, since (18) holds for $\lambda = s - 1$, we have:

$$\text{if two integers } \delta \text{ and } \varepsilon \text{ satisfy } h_\delta = q \text{ and } \delta \equiv \varepsilon \bmod \gcd(k_1, k_2, ..., k_{s-1}), \text{ then } h_\varepsilon = q. \tag{19}$$

Our goal is to prove that (18) holds for $\lambda = s$; in other words, our goal is to prove that

$$\text{if two integers } \delta \text{ and } \varepsilon \text{ satisfy } h_\delta = q \text{ and } \delta \equiv \varepsilon \bmod \gcd(k_1, k_2, ..., k_s), \text{ then } h_\varepsilon = q. \tag{20}$$

In fact, let δ and ε be two integers satisfying $h_\delta = q$ and $\delta \equiv \varepsilon \bmod \gcd(k_1, k_2, ..., k_s)$.

Let $D = \gcd(k_1, k_2, ..., k_{s-1})$. Then, $\gcd(k_1, k_2, ..., k_s) = \gcd\left(\underbrace{\gcd(k_1, k_2, ..., k_{s-1})}_{=D}, k_s \right) = \gcd(D, k_s)$. Hence, $\delta \equiv \varepsilon \bmod \gcd(k_1, k_2, ..., k_s)$ rewrites as $\delta \equiv \varepsilon \bmod \gcd(D, k_s)$. Thus, $\gcd(D, k_s) \mid \delta - \varepsilon$. Hence, there exists an integer Φ such that $\delta - \varepsilon = \Phi \gcd(D, k_s)$.

Now, the two integers $\dfrac{D}{\gcd(D, k_s)}$ and $\dfrac{k_s}{\gcd(D, k_s)}$ are coprime, so that by Bezout's Theorem, there exist integers u and v such that $u\dfrac{D}{\gcd(D, k_s)} + v\dfrac{k_s}{\gcd(D, k_s)} = 1$. In other words, $1 = u\dfrac{D}{\gcd(D, k_s)} + v\dfrac{k_s}{\gcd(D, k_s)} = \dfrac{uD + vk_s}{\gcd(D, k_s)}$, so that $uD + vk_s = \gcd(D, k_s)$. Hence, $\delta - \varepsilon = \Phi \underbrace{\gcd(D, k_s)}_{= uD + vk_s} = \Phi(uD + vk_s) = \Phi uD + \Phi v k_s$. Hence, $\delta - \Phi uD = \varepsilon + \Phi v k_s \equiv \varepsilon \bmod k_s$.

Now, applying (19) to $\delta - \Phi uD$ instead of ε, we obtain $h_{\delta - \Phi uD} = q$ (because $\delta \equiv \delta - \Phi uD \bmod \gcd(k_1, k_2, ..., k_{s-1})$, since $\gcd(k_1, k_2, ..., k_{s-1}) = D$). Therefore, applying (17) to $\delta - \Phi uD$ instead of δ, we obtain $h_\varepsilon = q$ (because $\delta - \Phi uD \equiv \varepsilon \bmod k_s$).

[17] In fact, $\dfrac{\delta - \varepsilon}{k_s} \in \mathbb{Z}$ (since $\delta \equiv \varepsilon \bmod k_s$). Now, let ρ be the residue of $\dfrac{\delta - \varepsilon}{k_s}$ modulo $k_1 + m$. Then, $\rho \geq 0$ and $\rho \equiv \dfrac{\delta - \varepsilon}{k_s} \bmod k_1 + m$, so that $\rho k_s \equiv \delta - \varepsilon \bmod k_1 + m$ and thus $\varepsilon \equiv \delta - \rho k_s \bmod k_1 + m$.

This proves (20). Since (20) is precisely the assertion of (18) for $\lambda = s$, this yields that (18) holds for $\lambda = s$. This completes the induction step, and thus the assertion (18) is proven.

Now, we finally claim that

$$\text{any integer } \varepsilon \text{ satisfies } h_\varepsilon = q. \tag{21}$$

Proof of (21). In fact, we have $h_\nu = q$ (by the definition of q) and $\nu \equiv \varepsilon \bmod \gcd(k_1, k_2, ..., k_n)$ (because $\gcd(k_1, k_2, ..., k_n) = 1$). Hence, (18) (applied to $\lambda = n$ and $\delta = \nu$) yields $h_\varepsilon = q$, and thus (21) is proven.

Now, (21) leads to $h = q \cdot \overline{1}$ [18] (because for every $i \in \{1, 2, ..., k_1 + m\}$, the assertion (21) (applied to $\varepsilon = i$) yields $h_i = q = q \cdot \underbrace{1^{k_1+m-i}}_{=\overline{1}_i} = q \cdot \overline{1}_i = \left(q \cdot \overline{1}\right)_i$), so that $h \in \operatorname{span}\left\{\overline{1}\right\}$. Thus we have proven that every $h \in \operatorname{Ker}_{\mathbb{Q}} U$ satisfies $h \in \operatorname{span}\left\{\overline{1}\right\}$. Consequently, $\operatorname{Ker}_{\mathbb{Q}} U \subseteq \operatorname{span}\left\{\overline{1}\right\}$, and thus $\dim \operatorname{Ker}_{\mathbb{Q}} U \leq \dim \operatorname{span}\left\{\overline{1}\right\} = 1$ (because $\overline{1}$ is not the zero vector, since $\overline{1}_i = 1^{k_1+m-i} \neq 0$ for every $i \in \{1, 2, ..., k_1 + m\}$). Now, Lemma 4 (applied to $B = \mathbb{Q}$) yields $\dim \operatorname{Ker}_A U = \dim \operatorname{Ker}_{\mathbb{Q}} U$, so that $\dim \operatorname{Ker}_{\mathbb{Q}} U \leq 1$ yields $\dim \operatorname{Ker}_A U \leq 1$. Hence, any two vectors in $\operatorname{Ker}_A U$ are linearly dependent. Since we know that $\overline{1} \in \operatorname{Ker}_A U$ and $\overline{\zeta} \in \operatorname{Ker}_A U$, this yields that the vectors $\overline{1}$ and $\overline{\zeta}$ are linearly dependent. Thus, there exist elements u and v of U such that $(u, v) \neq (0, 0)$ and $u\overline{1} + v\overline{\zeta} = 0$. Now, every $i \in \{1, 2, ..., k_1 + m\}$ satisfies

$$\left(u\overline{1} + v\overline{\zeta}\right)_i = u \underbrace{\overline{1}_i}_{=1^{k_1+m-i}=1} + v \underbrace{\overline{\zeta}_i}_{=\zeta^{k_1+m-i}} = u + v\zeta^{k_1+m-i},$$

so that $\left(\underbrace{u\overline{1} + v\overline{\zeta}}_{=0}\right)_i = 0$ becomes $u + v\zeta^{k_1+m-i} = 0$, and therefore

$$u = -v\zeta^{k_1+m-i} \qquad \text{for every } i \in \{1, 2, ..., k_1 + m\}. \tag{22}$$

Applying this to $i = k_1 + m$, we obtain $u = -v\zeta^{k_1+m-(k_1+m)} = -v\zeta^0 = -v$. Thus, $v \neq 0$ (because if v were 0, then we would have $u = -v = -0 = 0$, and thus $(u, v) = (0, 0)$, contradicting $(u, v) \neq (0, 0)$). On the other hand, applying (22) to $i = k_1 + m - 1$ [19], we obtain $u = -v\zeta^{k_1+m-(k_1+m-1)} = -v\zeta^1 = -v\zeta$. Comparing $u = -v$ with $u = -v\zeta$, we obtain $-v = -v\zeta$, which yields $1 = \zeta$ (since $v \neq 0$). Hence, for any two elements s and t of S we have $\xi_s = \zeta^{k_s} = 1^{k_s} = 1$ and $\xi_t = \zeta^{k_t} = 1^{k_t} = 1$, so that $\xi_s = \xi_t$. This completes the proof of Lemma 2.

References

[1] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Elena Udovina and Dmitry Vaintrob, *Introduction to representation theory*, March 9, 2009.
`http://math.mit.edu/~etingof/replect.pdf`

[2] Darij Grinberg, *Rep#2a: Finite subgroups of multiplicative groups of fields.*

[18] where $\overline{\vartheta} \in A^{k_1+m}$ is the vector defined by $\overline{\vartheta}_i = \vartheta^{k_1+m-i}$ for every $i \in \{1, 2, ..., k_1 + m\}$

[19] Here, we use that $k_1 + m - 1 \in \{1, 2, ..., k_1 + m\}$, which is because $k_1 \geq 1$ and $m \geq 1$.