On p-polynomials and $\mathbb{F}_p$-vector subspaces of fields

Darij Grinberg

December 9, 2016

Contents

1. The goals

This expository note is devoted to some apocryphal properties of fields of positive characteristic. We shall use the following notations:

Definition 1.1. In the following, rings are always assumed to be associative and with 1. If R is a commutative ring, then an *R-algebra* means a ring A endowed with an R-module structure such that the map $A \times A \to A$, $(a, b) \mapsto ab$ is R-bilinear. The characteristic of a field L is denoted by $\operatorname{char} L$.

The word "prime" always stands for "prime number". Neither 0 nor 1 counts as a prime. The notation $\mathbb{N}$ stands for the set $\{0, 1, 2, \ldots\}$.

Definition 1.2. Let $p \in \mathbb{N}$. Let L be a commutative ring. A polynomial $f \in L[X]$ is said to be a *p-polynomial* if f is an L-linear combination of the monomials $X^{p^0}, X^{p^1}, X^{p^2}, \ldots$. For instance, the polynomial $3X - 7X^2 + X^4 \in \mathbb{Z}[X]$ is a 2-polynomial but not a 3-polynomial.

Our main goal in this note is to demonstrate the following four interrelated facts:

Theorem 1.3. Let V be a finite additive subgroup of a field L. Let $p = \operatorname{char} L$. Then, $\prod_{v \in V} (X + v) \in L[X]$ is a p-polynomial.

Theorem 1.4. Let V be a finite additive subgroup of a field L. Let $t \in L \setminus V$. Then,

$$\sum_{v \in V} \frac{1}{t+v} = \left(\prod_{v \in V} \frac{1}{t+v} \right) \cdot \left(\prod_{v \in V \setminus 0} v \right).$$

Theorem 1.5. Let q be a prime power. Let L be a field extension of the finite field $\mathbb{F}_q$. Let V be a finite $\mathbb{F}_q$-vector subspace of L. Then, $\prod_{v \in V} (X + v) \in L[X]$ is a q-polynomial.

Theorem 1.6. Let q be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Let V be a finite $\mathbb{F}_q$-vector subspace of L. Then, $\prod_{v \in V} (X + v) \in L[X]$ is a q-polynomial.

Note that these four theorems are essentially about fields of positive characteristic. Indeed, it is easy to show that in Theorem 1.3 and in Theorem 1.4, the finite subgroup V must be 0 if $\operatorname{char} L = 0$; thus, the two theorems become fairly trivial if $\operatorname{char} L = 0$, and only the case of positive characteristic is interesting.

Let us first comment on the origins of these results:

Theorem 1.5 is a known fact (e.g., it immediately follows from [Conrad14, Theorem A.1 2) and Corollary A.3], from [Macdon92, (7.7)] or from [Grinbe16, Theorem 3.17]). Theorem 1.3 is a particular case of Theorem 1.5 (obtained by setting $q = p = \operatorname{char} L$ when $\operatorname{char} L \neq 0$), and is due to Oystein Ore ([Ore33, the $\Longrightarrow$ direction of Theorem 8]).

Theorem 1.4 is an auxiliary result from unfinished work [Grinbe16, Proposition 5.3] of mine and James Borger on Carlitz polynomials.

Theorem 1.6 is also not new (it is precisely [Grinbe16, Theorem 3.17], and appears implicitly in [Macdon92]). Clearly, it generalizes Theorem 1.5 (since any field extension of $\mathbb{F}_q$ is a commutative $\mathbb{F}_q$-algebra).

All of the above four theorems are accessible without much preknowledge (basic theory of finite fields should be sufficient), and the purpose of this note is to collect elementary and self-contained proofs.

Theorem 1.3 and Theorem 1.4 were posed as a problem in the PRIMES 2015 application contest[1]. Some of the proofs below were found by students taking part in the contest.

2. Preparations

Before we start proving the above theorems, let us prove some auxiliary facts that will be useful. Some of these facts are actually well-known results.

Lemma 2.1. Let V be a finite additive subgroup of a field L. Let $p = \operatorname{char} L$. Assume that $V \neq 0$.

(a) The number p is prime.

(b) The field L is a field extension of $\mathbb{F}_p$.

(c) The subset V is a finite-dimensional $\mathbb{F}_p$-vector subspace of L.

Proof of Lemma 2.1. **(a)** We have $V \neq 0$. Thus, there exists a nonzero vector $v \in V$. Consider such a v. Every element of the additive group V has finite order (because V is finite). In particular, v has finite order (since v is an element of V). In other words, there exists some positive integer N such that $Nv = 0$. Consider this N.

We have $v \in V \subseteq L$. We can divide the equality $Nv = 0$ by v (since v is a nonzero element of the field L). We thus obtain $N \cdot 1_L = 0$ (where 1_L denotes the one of the field L). Thus, the field L cannot have characteristic 0. In other words, $\operatorname{char} L$ is positive. In other words, p is positive (since $p = \operatorname{char} L$). Hence, p is a prime (since $p = \operatorname{char} L$ is the characteristic of a field, and thus is either prime or 0). This completes the proof of Lemma 2.1 **(a)**.

(b) We know that $\operatorname{char} L = p$ is prime (by Lemma 2.1 **(a)**). Hence, L is a field extension of $\mathbb{F}_p$. This proves Lemma 2.1 **(b)**.

(c) Lemma 2.1 **(b)** shows that L is a field extension of $\mathbb{F}_p$. Hence, L is an $\mathbb{F}_p$-vector space.

Let $\lambda \in \mathbb{F}_p$ and $v \in V$.

We have $\lambda \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Hence, there exists some $n \in \mathbb{Z}$ such that $\lambda = \overline{n}$ (where $\overline{n}$ denotes the residue class of n modulo p). Consider such an n. We have $\lambda = \overline{n}$ and thus $\lambda v = n \underbrace{v}_{\in V} \in nV \subseteq V$ (because V is an additive group).

Now, forget that we fixed λ and v. We thus have shown that $\lambda v \in V$ for every $\lambda \in \mathbb{F}_p$ and $v \in V$. Thus, V is an $\mathbb{F}_p$-vector subspace of L (since we already know that V is an additive subgroup of L). Moreover, V is finite-dimensional (since V is finite). This proves Lemma 2.1 **(c)**. □

[1] See problem M6 in `https://math.mit.edu/research/highschool/primes/materials/2015/entpro2015math.pdf` .

Lemma 2.2. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Any two elements u and v of L satisfy

$$(u+v)^p = u^p + v^p. \tag{1}$$

Proof of Lemma 2.2. For every $i \in \{1, 2, \ldots, p-1\}$, the binomial coefficient $\binom{p}{i}$ is divisible by p (since p is prime), and thus reduces to 0 in L (since L is an $\mathbb{F}_p$-algebra). In other words, for every $i \in \{1, 2, \ldots, p-1\}$, we have

$$\binom{p}{i} = 0 \qquad \text{in } L. \tag{2}$$

But L is commutative. Hence, the binomial formula yields

$$\begin{aligned}(u+v)^p &= \sum_{i=0}^{p} \binom{p}{i} u^i v^{p-i} = u^p + \sum_{i=1}^{p-1} \underbrace{\binom{p}{i}}_{\substack{=0 \text{ in } L \\ \text{(by (2))}}} u^i v^{p-i} + v^p \\ &\qquad \left(\begin{array}{c} \text{here, we have split off the addends for } i=0 \\ \text{and for } i=p \text{ from the sum} \end{array} \right) \\ &= u^p + v^p.\end{aligned}$$

This proves Lemma 2.2. □

Lemma 2.3. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Any two elements u and v of L and any $n \in \mathbb{N}$ satisfy

$$(u+v)^{p^n} = u^{p^n} + v^{p^n}. \tag{3}$$

Proof of Lemma 2.3. Lemma 2.3 follows by induction on n, using (1) and the fact that $w^{p^n} = \left(w^{p^{n-1}}\right)^p$ for every $w \in L$ and every positive integer n. [2] □

[2] Here is the argument in more detail:

Proof of (3): We shall prove (3) by induction on n:

Induction base: Any $u \in L$ and $v \in L$ satisfy

$$\begin{aligned}(u+v)^{p^0} &= (u+v)^1 \qquad \left(\text{since } p^0 = 1\right) \\ &= \underbrace{u}_{\substack{=u^1=u^{p^0} \\ \text{(since } 1=p^0\text{)}}} + \underbrace{v}_{\substack{=v^1=v^{p^0} \\ \text{(since } 1=p^0\text{)}}} = u^{p^0} + v^{p^0}.\end{aligned}$$

In other words, (3) holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$ be positive. Assume that (3) holds for $n = N-1$. We must now

Lemma 2.4. Let p be a prime. Any $\lambda \in \mathbb{F}_p$ satisfies

$$\lambda^p = \lambda. \tag{4}$$

Proof of Lemma 2.4. Let $\lambda \in \mathbb{F}_p$. We must prove (4). If $\lambda = 0$, then (4) is obviously true. Hence, we WLOG assume that $\lambda \neq 0$. Thus, $\lambda \in \mathbb{F}_p \setminus \{0\}$.

The multiplicative group $\left(\mathbb{F}_p\right)^\times = \mathbb{F}_p \setminus \{0\}$ of the field $\mathbb{F}_p$ has $p-1$ elements (since $\left|\mathbb{F}_p \setminus \{0\}\right| = \underbrace{\left|\mathbb{F}_p\right|}_{=p} - 1 = p-1$). Hence, the order of any element of this group $\left(\mathbb{F}_p\right)^\times$ divides $p-1$ (by Lagrange's theorem). In particular, the order of the element λ of $\left(\mathbb{F}_p\right)^\times$ divides $p-1$ (since $\lambda \in \mathbb{F}_p \setminus \{0\} = \left(\mathbb{F}_p\right)^\times$). Hence, $\lambda^{p-1} = 1$. Now, $\lambda^p = \lambda \underbrace{\lambda^{p-1}}_{=1} = \lambda$. This proves (4). Thus, Lemma 2.4 is proven.

□

Lemma 2.5. Let p be a prime. Any $\lambda \in \mathbb{F}_p$ and any $n \in \mathbb{N}$ satisfy

$$\lambda^{p^n} = \lambda. \tag{5}$$

Proof of Lemma 2.5. Lemma 2.5 follows by induction on n, using (4) and the fact that $\lambda^{p^n} = \left(\lambda^{p^{n-1}}\right)^p$ for every $\lambda \in \mathbb{F}_p$ and every positive integer n. □

Lemma 2.6. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $f \in L[X]$ be a p-polynomial. Then,

$$f(u+v) = f(u) + f(v) \tag{6}$$

show that (3) holds for $n = N$.

Let $u \in L$ and $v \in L$. We have assumed that (3) holds for $n = N-1$. Hence, (3) (applied to $n = N-1$) yields $(u+v)^{p^{N-1}} = u^{p^{N-1}} + v^{p^{N-1}}$. But every $w \in L$ satisfies $w^{p^N} = \left(w^{p^{N-1}}\right)^p$. Applying this to $w = u+v$, we find

$$\begin{aligned}
(u+v)^{p^N} &= \left(\underbrace{(u+v)^{p^{N-1}}}_{=u^{p^{N-1}}+v^{p^{N-1}}}\right)^p = \left(u^{p^{N-1}} + v^{p^{N-1}}\right)^p \\
&= \underbrace{\left(u^{p^{N-1}}\right)^p}_{=u^{p^N}} + \underbrace{\left(v^{p^{N-1}}\right)^p}_{=v^{p^N}} \\
&\qquad \left(\text{by (1), applied to } u^{p^{N-1}} \text{ and } v^{p^{N-1}} \text{ instead of } u \text{ and } v\right) \\
&= u^{p^N} + v^{p^N}.
\end{aligned}$$

Thus, we have shown that (3) holds for $n = N$. This completes the induction step. The proof of (3) is thus finished. In other words, Lemma 2.3 is proven.

for every $u \in L$ and $v \in L$.

Proof of Lemma 2.6. We know that $f \in L[X]$ is a p-polynomial. Thus, f has the form $f = \sum_{n=0}^{d} a_n X^{p^n}$ for some $d \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_d \in L$. Consider this d and these $a_0, a_1, \ldots, a_d$. Every $u \in L$ and $v \in L$ satisfy

$$f(u+v) = \sum_{n=0}^{d} a_n \underbrace{(u+v)^{p^n}}_{\substack{=u^{p^n}+v^{p^n} \\ \text{(by (3))}}} \qquad \left(\text{since } f = \sum_{n=0}^{d} a_n X^{p^n}\right)$$

$$= \sum_{n=0}^{d} a_n \left(u^{p^n} + v^{p^n}\right) = \underbrace{\sum_{n=0}^{d} a_n u^{p^n}}_{=f(u)} + \underbrace{\sum_{n=0}^{d} a_n v^{p^n}}_{=f(v)} = f(u) + f(v).$$

This proves Lemma 2.6. □

Lemma 2.7. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $f \in L[X]$ be a p-polynomial. Then,

$$f(\lambda u) = \lambda f(u) \tag{7}$$

for every $u \in L$ and $\lambda \in \mathbb{F}_p$.

Proof of Lemma 2.7. We know that $f \in L[X]$ is a p-polynomial. Thus, f has the form $f = \sum_{n=0}^{d} a_n X^{p^n}$ for some $d \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_d \in L$. Consider this d and these $a_0, a_1, \ldots, a_d$. Every $u \in L$ and $\lambda \in \mathbb{F}_p$ satisfy

$$f(\lambda u) = \sum_{n=0}^{d} a_n \underbrace{(\lambda u)^{p^n}}_{=\lambda^{p^n} u^{p^n}} \qquad \left(\text{since } f = \sum_{n=0}^{d} a_n X^{p^n}\right)$$

$$= \sum_{n=0}^{d} a_n \underbrace{\lambda^{p^n}}_{\substack{=\lambda \\ \text{(by (5))}}} u^{p^n} = \sum_{n=0}^{d} a_n \lambda u^{p^n} = \lambda \underbrace{\sum_{n=0}^{d} a_n u^{p^n}}_{\substack{=f(u) \\ \left(\text{since } \sum_{n=0}^{d} a_n X^{p^n} = f\right)}} = \lambda f(u).$$

This proves Lemma 2.7. □

Definition 2.8. Let L be a commutative ring. For every polynomial $f \in L[X]$, we let $\mathcal{R}(f)$ be the set of all roots of f (inside L).

Lemma 2.9. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $f \in L[X]$ be a p-polynomial. Then,

$$\mathcal{R}(f) \text{ is a } \mathbb{F}_p\text{-vector subspace of } L. \tag{8}$$

Proof of Lemma 2.9. If $u \in L$ and $v \in L$ are such that $f(u) = 0$ and $f(v) = 0$, then

$$\begin{aligned} f(u+v) &= \underbrace{f(u)}_{=0} + \underbrace{f(v)}_{=0} \qquad \text{(by (6))} \\ &= 0. \end{aligned}$$

In other words, if u and v are two roots of f, then $u+v$ is a root of f. In other words, the set $\mathcal{R}(f)$ of all roots of f is closed under addition. Furthermore, (7) (applied to $\lambda = 0$ and $u = 0$) yields $f(0) = 0f(0) = 0$. Hence, 0 is a root of f. In other words, $0 \in \mathcal{R}(f)$.

Moreover, (7) (applied to $\lambda = -1$) shows that $f(-u) = -f(u)$ for every $u \in L$. Hence, every $u \in \mathcal{R}(f)$ must satisfy $f(-u) = -\underbrace{f(u)}_{\substack{=0 \\ (\text{since } u \in \mathcal{R}(f))}} = 0$ and therefore $-u \in \mathcal{R}(f)$. In other words, the set $\mathcal{R}(f)$ is closed under taking negatives.

Now, we know that the set $\mathcal{R}(f)$ contains 0 (since $0 \in \mathcal{R}(f)$) and is closed under addition and taking negatives. In other words, $\mathcal{R}(f)$ is an additive subgroup of L.

Finally, if $u \in \mathcal{R}(f)$ and $\lambda \in \mathbb{F}_p$, then (7) yields $f(\lambda u) = \lambda \underbrace{f(u)}_{\substack{=0 \\ (\text{since } u \in \mathcal{R}(f))}} = 0$ and therefore $\lambda u \in \mathcal{R}(f)$. Therefore, the set $\mathcal{R}(f)$ is an $\mathbb{F}_p$-vector subspace of L (since we already know that $\mathcal{R}(f)$ is an additive subgroup of L). This proves Lemma 2.9. □

Lemma 2.10. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $f \in L[X]$ be a p-polynomial. Then,

$$\text{the derivative } f' \text{ of } f \text{ equals the coefficient of } f \text{ before } X^1. \tag{9}$$

Proof of Lemma 2.10. We know that $f \in L[X]$ is a p-polynomial. Thus, f has the form $f = \sum_{n=0}^{d} a_n X^{p^n}$ for some $d \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_d \in L$. Consider this d and these $a_0, a_1, \ldots, a_d$. From $f = \sum_{n=0}^{d} a_n X^{p^n}$, we obtain

$$f' = \sum_{n=0}^{d} a_n p^n X^{p^n-1} = a_0 \underbrace{p^0}_{=1} \underbrace{X^{p^0-1}}_{=X^0=1} + \sum_{n=1}^{d} a_n \underbrace{p^n}_{\substack{=0 \text{ in } L \\ (\text{since } p \mid p^n)}} X^{p^n-1} = a_0.$$

But this is clearly the coefficient of f before X^1. Thus, Lemma 2.10 is proven. □

Lemma 2.11. Let L be a field. If $f \in L[X]$ is a polynomial which has more than $\deg f$ roots in L, then $f = 0$.

Proof of Lemma 2.11. This is a general (and well-known) fact about univariate polynomials over a field: If the number of roots of such a polynomial exceeds its degree, then the polynomial is 0. □

3. Proofs of Theorem 1.3

We now come to the proofs of Theorem 1.3.

3.1. First proof

The following proof of Theorem 1.3 was found by Meghal Gupta in the PRIMES 2015 application contest:

First proof of Theorem 1.3. We WLOG assume that $V \neq 0$ (since otherwise, Theorem 1.3 is evident). Lemma 2.1 **(a)** yields that the number p is prime. Lemma 2.1 **(b)** shows that the field L is a field extension of $\mathbb{F}_p$. Lemma 2.1 **(c)** says that the subset V is a finite-dimensional $\mathbb{F}_p$-vector subspace of L.

Now, let W be the polynomial $\prod_{v \in V} (X + v) \in L[X]$. We need to prove that W is a p-polynomial.

Let $(e_1, e_2, \ldots, e_k)$ be a basis of the $\mathbb{F}_p$-vector space V. Thus, $\dim V = k$, so that $|V| = p^k$.

There exists a nonzero vector $(a_0, a_1, \ldots, a_k) \in L^{k+1}$ satisfying

$$\sum_{j=0}^{k} a_j e_i^{p^{k-j}} = 0 \qquad \text{for every } i \in \{1, 2, \ldots, k\}. \tag{10}$$

(*Proof:* Let us regard (10) as a system of k homogeneous linear equations in the $k+1$ unknowns $a_0, a_1, \ldots, a_k$ over the field L. This system has at least one solution (namely, $(0, 0, \ldots, 0)$), and is underdetermined (since it has more unknowns than it has equations). Hence, it has at least one nonzero solution (where "nonzero" means that at least one of $a_0, a_1, \ldots, a_k$ is nonzero). This means that there exists a nonzero vector $(a_0, a_1, \ldots, a_k) \in L^{k+1}$ satisfying (10), qed.)

So let us fix some nonzero vector $(a_0, a_1, \ldots, a_k) \in L^{k+1}$ satisfying (10) (now that we know that such a vector exists). Define a polynomial $\widetilde{W} \in L[X]$ by $\widetilde{W} = \sum_{j=0}^{k} a_j X^{p^{k-j}}$. Then, (10) rewrites as follows:

$$\widetilde{W}(e_i) = 0 \qquad \text{for every } i \in \{1, 2, \ldots, k\}.$$

In other words,

$$e_i \in \mathcal{R}\left(\widetilde{W}\right) \qquad \text{for every } i \in \{1, 2, \ldots, k\} \tag{11}$$

(since $\mathcal{R}\left(\widetilde{W}\right)$ is the set of all roots of $\widetilde{W}$).

The polynomial $\widetilde{W}$ is not identically 0 (since $(a_0, a_1, \ldots, a_k)$ is a nonzero vector). Notice that "identically 0" means "all coefficients are 0"; this is not the same thing as saying that $\widetilde{W}(x) = 0$ for all $x \in L$. (Actually, $\widetilde{W}(x) = 0$ might hold for all $x \in L$ is small enough!)

Also, $\widetilde{W}$ is a p-polynomial (by its very definition). Hence, (8) (applied to $f = \widetilde{W}$) shows that $\mathcal{R}\left(\widetilde{W}\right)$ is a $\mathbb{F}_p$-vector subspace of L. Since this subspace $\mathcal{R}\left(\widetilde{W}\right)$ contains each vector in the basis $(e_1, e_2, \ldots, e_k)$ of V (by (11)), we can thus conclude that $\mathcal{R}\left(\widetilde{W}\right)$ contains V as a subset. In other words, every $w \in V$ is an element of $\mathcal{R}\left(\widetilde{W}\right)$, thus a root of $\widetilde{W}$. In other words, every $w \in V$ satisfies $\widetilde{W}(w) = 0$.

On the other hand, $W = \prod_{v \in V} (X + v)$. Hence, every $w \in V$ satisfies $W(w) = 0$ [3].

So we conclude that every $w \in V$ satisfies both $\widetilde{W}(w) = 0$ and $W(w) = 0$. Hence, every $w \in V$ satisfies

$$\left(\widetilde{W} - a_0 W\right)(w) = \underbrace{\widetilde{W}(w)}_{=0} - a_0 \underbrace{W(w)}_{=0} = 0.$$

In other words, every $w \in V$ is a root of $\widetilde{W} - a_0 W$. Hence, the polynomial $\widetilde{W} - a_0 W$ has at least p^k roots (since $|V| = p^k$).

The polynomial W is a product of $|V| = p^k$ terms of the form $X + v$, and therefore is a monic polynomial of degree p^k. Hence, both polynomials $\widetilde{W}$ and $a_0 W$ have degree $\leq p^k$, and moreover, their coefficients before X^{p^k} are equal (namely, both are a_0). Therefore, the difference $\widetilde{W} - a_0 W$ is a polynomial of degree $< p^k$ (since the equal coefficients before X^{p^k} cancel out in the subtraction). In other words, $\deg\left(\widetilde{W} - a_0 W\right) < p^k$. But we have just proven that this difference $\widetilde{W} - a_0 W$ has at least p^k roots; thus, it has more than $\deg\left(\widetilde{W} - a_0 W\right)$ roots (since $\deg\left(\widetilde{W} - a_0 W\right) < p^k$). Hence, Lemma 2.11 (applied to $f = \widetilde{W} - a_0 W$)

[3] *Proof.* Let $w \in V$. Then, $-w \in V$ (since V is an additive subgroup of L). Hence, the product $\prod_{v \in V} (w + v)$ contains the factor $w + (-w)$ (this is its factor for $v = -w$), which is 0. Therefore, the whole product $\prod_{v \in V} (w + v)$ must be 0. Now, evaluating both sides of the equality $W = \prod_{v \in V} (X + v)$ at $X = w$, we obtain $W(w) = \prod_{v \in V} (w + v) = 0$. Qed.

shows that $\widetilde{W} - a_0 W = 0$, so that $\widetilde{W} = a_0 W$. Since $\widetilde{W}$ is not identically 0, this shows that $a_0 \neq 0$. Hence, $\widetilde{W} = a_0 W$ becomes $W = \dfrac{1}{a_0}\widetilde{W}$. But $\widetilde{W}$ is a p-polynomial. Hence, W is a p-polynomial (since $W = \dfrac{1}{a_0}\widetilde{W}$). Hence, Theorem 1.3 is proven. $\square$

3.2. Second proof

The following proof of Theorem 1.3 appears in [Macdon92, (7.7)]; it was also found by Jessica Lai in the PRIMES 2015 application contest:

Second proof of Theorem 1.3. We WLOG assume that $V \neq 0$ (since otherwise, Theorem 1.3 is evident). Lemma 2.1 **(a)** yields that the number p is prime. Lemma 2.1 **(b)** shows that the field L is a field extension of $\mathbb{F}_p$. Lemma 2.1 **(c)** says that the subset V is a finite-dimensional $\mathbb{F}_p$-vector subspace of L.

Now, let W be the polynomial $\prod\limits_{v \in V} (X + v) \in L[X]$. We need to prove that W is a p-polynomial.

Let $(e_1, e_2, \ldots, e_k)$ be a basis of the $\mathbb{F}_p$-vector space V. Thus, $\dim V = k$, so that $|V| = p^k$. Also, $e_1, e_2, \ldots, e_k$ are $\mathbb{F}_p$-linearly independent.

For every $n \in \{0, 1, \ldots, k\}$, we let $\mathfrak{m}_n$ be the $n \times n$-matrix

$$\begin{pmatrix} e_1^{p^0} & e_1^{p^1} & \cdots & e_1^{p^{n-1}} \\ e_2^{p^0} & e_2^{p^1} & \cdots & e_2^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ e_n^{p^0} & e_n^{p^1} & \cdots & e_n^{p^{n-1}} \end{pmatrix} \in L^{n \times n},$$

and we let $\mathfrak{M}_n$ be the $(n+1) \times (n+1)$-matrix

$$\begin{pmatrix} e_1^{p^0} & e_1^{p^1} & \cdots & e_1^{p^{n-1}} & e_1^{p^n} \\ e_2^{p^0} & e_2^{p^1} & \cdots & e_2^{p^{n-1}} & e_2^{p^n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ e_n^{p^0} & e_n^{p^1} & \cdots & e_n^{p^{n-1}} & e_n^{p^n} \\ X^{p^0} & X^{p^1} & \cdots & X^{p^{n-1}} & X^{p^n} \end{pmatrix} \in \left(L[X]\right)^{(n+1)\times(n+1)}.$$

These two matrices are related to each other by the following properties:

- The matrix $\mathfrak{m}_n$ consists of the first n rows and the first n columns of $\mathfrak{M}_n$.
- The matrix $\mathfrak{m}_{n+1}$ (for $n < k$) is obtained from $\mathfrak{M}_n$ by substituting e_{n+1} for X.

Now, we shall prove the following[4]:

Lemma 3.1. Let L, V, p, $(e_1, e_2, \ldots, e_k)$, $\mathfrak{m}_n$ and $\mathfrak{M}_n$ be as above.

Let $n \in \{0, 1, \ldots, k\}$. Let V_n be the $\mathbb{F}_p$-vector subspace of V spanned by $e_1, e_2, \ldots, e_n$. (In particular, V_0 is spanned by nothing, and thus equals 0. On the other hand, $V_k = V$.)

(a) We have

$$\det\left(\mathfrak{M}_n\right) = \det\left(\mathfrak{m}_n\right) \cdot \prod_{v \in V_n} \left(X + v\right).$$

(b) The polynomial $\det\left(\mathfrak{M}_n\right) \in L\left[X\right]$ is a p-polynomial of degree $\leq p^n$, and its coefficient before X^{p^n} is $\det\left(\mathfrak{m}_n\right)$.

The determinants $\det\left(\mathfrak{m}_n\right)$ are known as the *Moore determinants*, and we will compute them soon enough. First, let us prove the above lemma:

Proof of Lemma 3.1. **(b)** In the matrix $\mathfrak{M}_n$, the indeterminate X appears only in the last row. If we expand $\det\left(\mathfrak{M}_n\right)$ with respect to the last row (Laplace expansion), then we obtain

$$\det\left(\mathfrak{M}_n\right) = \sum_{j=0}^{n} X^{p^j} a_j, \tag{12}$$

where a_j is the appropriate cofactor of $\mathfrak{M}_n$ (namely, $(-1)^{n+j}$ times the determinant of the matrix obtained from $\mathfrak{M}_n$ by removing the $(n+1)$-th row and the $(j+1)$-th column). All of these cofactors $a_0, a_1, \ldots, a_n$ belong to L (since they are determinants of matrices whose entries all lie in L; here we are using the fact that the indeterminate X appears only in the last row of $\mathfrak{M}_n$). Thus, (12) shows that $\det\left(\mathfrak{M}_n\right)$ is a p-polynomial of degree $\leq p^n$. It also shows that its coefficient before X^{p^n} is $a_n = (-1)^{n+n} \det\left(\mathfrak{m}_n\right)$ (because the matrix obtained from $\mathfrak{M}_n$ by removing the $(n+1)$-th row and the $(n+1)$-th column is $\mathfrak{m}_n$). Since $(-1)^{n+n} = 1$, this simplifies to $\det\left(\mathfrak{m}_n\right)$. This concludes the proof of Lemma 3.1 **(b)**.

(a) Let f denote the polynomial $\det\left(\mathfrak{M}_n\right) \in L\left[X\right]$. Lemma 3.1 **(b)** shows that f is a p-polynomial of degree $\leq p^n$, and its coefficient before X^{p^n} is $\det\left(\mathfrak{m}_n\right)$. Thus, (8) shows that $\mathcal{R}\left(f\right)$ is an $\mathbb{F}_p$-vector subspace of L.

Let $i \in \{1, 2, \ldots, n\}$. We have

$$f = \det\left(\mathfrak{M}_n\right) = \det \begin{pmatrix} e_1^{p^0} & e_1^{p^1} & \cdots & e_1^{p^{n-1}} & e_1^{p^n} \\ e_2^{p^0} & e_2^{p^1} & \cdots & e_2^{p^{n-1}} & e_2^{p^n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ e_n^{p^0} & e_n^{p^1} & \cdots & e_n^{p^{n-1}} & e_n^{p^n} \\ X^{p^0} & X^{p^1} & \cdots & X^{p^{n-1}} & X^{p^n} \end{pmatrix}.$$

[4]Lemma 3.1 is a classical result; its part **(a)** is essentially [Goss98, Proposition 1.3.5 2)].

Substituting e_i for X in this equality, we obtain

$$f(e_i) = \det \underbrace{\begin{pmatrix} e_1^{p^0} & e_1^{p^1} & \cdots & e_1^{p^{n-1}} & e_1^{p^n} \\ e_2^{p^0} & e_2^{p^1} & \cdots & e_2^{p^{n-1}} & e_2^{p^n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ e_n^{p^0} & e_n^{p^1} & \cdots & e_n^{p^{n-1}} & e_n^{p^n} \\ e_i^{p^0} & e_i^{p^1} & \cdots & e_i^{p^{n-1}} & e_i^{p^n} \end{pmatrix}}_{\substack{\text{This matrix has two equal rows} \\ \text{(the last row and the } i\text{-th row)}}} = 0.$$

In other words, $e_i \in \mathcal{R}(f)$ (recall that $\mathcal{R}(f)$ denotes the set of all roots of f).

Now, let us forget that we fixed i. We thus have shown that $e_i \in \mathcal{R}(f)$ for every $i \in \{1, 2, \ldots, n\}$. Since $\mathcal{R}(f)$ is an $\mathbb{F}_p$-vector subspace of L, this yields that $\mathcal{R}(f)$ contains the $\mathbb{F}_p$-vector subspace of V spanned by $e_1, e_2, \ldots, e_n$ as a subset. In other words, $\mathcal{R}(f) \supseteq V_n$ (since the $\mathbb{F}_p$-vector subspace of V spanned by $e_1, e_2, \ldots, e_n$ is V_n).

But the vectors $e_1, e_2, \ldots, e_k$ are linearly independent. Hence, so are the vectors $e_1, e_2, \ldots, e_n$. Thus, the $\mathbb{F}_p$-vector subspace V_n spanned by these latter vectors has dimension n. In other words, $\dim(V_n) = n$, so that $|V_n| = p^n$.

Let g denote the polynomial $f - \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v) \in L[X]$. Then, $\deg g < p^n$ [5].

Now, let $w \in V_n$. Then, $w \in \mathcal{R}(f)$ (since $\mathcal{R}(f) \supseteq V_n$) and thus $f(w) = 0$. On the other hand, $-w \in V_n$ (since $w \in V_n$ and since V_n is a vector space). Hence, the product $\prod_{v \in V_n} (w + v)$ contains the factor $w + (-w) = 0$, and therefore vanishes. Hence, $\underbrace{f(w)}_{=0} - \det(\mathfrak{m}_n) \cdot \underbrace{\prod_{v \in V_n} (w + v)}_{=0} = 0$. In other words, w is a root of the polynomial $f - \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v) = g$.

Now, let us forget that we fixed w. We thus have proven that every $w \in V_n$ is a root of the polynomial g. Thus, this polynomial g has at least $|V_n| = p^n$ roots. Hence, this polynomial g has more than $\deg g$ roots (since $\deg g < p^n$).

[5] *Proof.* As we know, the polynomial f has degree $\leq p^n$, and its coefficient before X^{p^n} is $\det(\mathfrak{m}_n)$. On the other hand, $\prod_{v \in V_n} (X + v)$ is a monic polynomial of degree p^n (since it is the product of $|V_n| = p^n$ terms of the form $X + v$), and therefore $\det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v)$ is a polynomial of degree $\leq p^n$ whose coefficient before X^{p^n} is $\det(\mathfrak{m}_n)$.

So both polynomials f and $\det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v)$ have degree $\leq p^n$, and their coefficients before X^{p^n} are $\det(\mathfrak{m}_n)$. Thus, their difference $f - \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v)$ has degree $< p^n$ (since their equal coefficients before X^{p^n} cancel out when they are subtracted). In other words, g has degree $< p^n$ (since $g = f - \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v)$), qed.

Applying Lemma 2.11 to g instead of f, we thus conclude that $g = 0$. Since $g = f - \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v)$, this rewrites as $f - \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v) = 0$. In other words, $f = \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v)$. Since $f = \det(\mathfrak{M}_n)$, this means that Lemma 3.1 **(a)** is proven. □

Now we can compute the Moore determinants[6]:

Corollary 3.2. Let $n \in \{0, 1, \ldots, k\}$. Let L, V, p, $(e_1, e_2, \ldots, e_k)$, $\mathfrak{m}_n$ and $\mathfrak{M}_n$ be as above. Let V_n be as in Lemma 3.1.

(a) We have

$$\det(\mathfrak{m}_n) = \prod_{i=1}^{n} \prod_{v \in V_{i-1}} (e_i + v). \tag{13}$$

(b) We have $\det(\mathfrak{m}_n) \neq 0$.

Proof of Corollary 3.2. **(a)** Corollary 3.2 **(a)** is proven by induction over n.

The *induction base* (i.e., the case $n = 0$) is easy: If $n = 0$, then the left hand side of (13) is 1 (because $\mathfrak{m}_0$ is a 0×0-matrix, and the determinant of a 0×0-matrix is defined to be 1), whereas the right hand side is also 1 (because it is an empty product, and empty products too are defined to be 1).

Induction step: Fix $n \in \{0, 1, \ldots, k-1\}$. Assume that

$$\det(\mathfrak{m}_n) = \prod_{i=1}^{n} \prod_{v \in V_{i-1}} (e_i + v). \tag{14}$$

We now must prove that

$$\det(\mathfrak{m}_{n+1}) = \prod_{i=1}^{n+1} \prod_{v \in V_{i-1}} (e_i + v). \tag{15}$$

Lemma 3.1 **(a)** shows that

$$\det(\mathfrak{M}_n) = \det(\mathfrak{m}_n) \cdot \prod_{v \in V_n} (X + v) \tag{16}$$

Recall that the matrix $\mathfrak{m}_{n+1}$ is obtained from $\mathfrak{M}_n$ by substituting e_{n+1} for X. Hence, $\det(\mathfrak{m}_{n+1})$ is obtained from $\det(\mathfrak{M}_n)$ by substituting e_{n+1} for X. Thus, substituting e_{n+1} for X in the equality (16) yields

$$\begin{aligned}
\det(\mathfrak{m}_{n+1}) &= \underbrace{\det(\mathfrak{m}_n)}_{\substack{= \prod_{i=1}^{n} \prod_{v \in V_{i-1}} (e_i + v) \\ \text{(by (14))}}} \cdot \prod_{v \in V_n} (e_{n+1} + v) \\
&= \left(\prod_{i=1}^{n} \prod_{v \in V_{i-1}} (e_i + v) \right) \cdot \prod_{v \in V_n} (e_{n+1} + v) = \prod_{i=1}^{n+1} \prod_{v \in V_{i-1}} (e_i + v).
\end{aligned}$$

[6] Corollary 3.2 is [Goss98, Corollary 1.3.7].

This proves (15), and thus completes the induction step. Corollary 3.2 **(a)** is thus proven.

(b) We need to prove that $\det(\mathfrak{m}_n) \neq 0$. According to (13), this boils down to showing that $e_i + v \neq 0$ for every $i \in \{1, 2, \ldots, n\}$ and every $v \in V_{i-1}$. So let us fix an $i \in \{1, 2, \ldots, n\}$ and an $v \in V_{i-1}$. We need to show that $e_i + v \neq 0$.

Assume the contrary. Thus, $e_i + v = 0$. But V_{i-1} (by definition) is the $\mathbb{F}_p$-vector subspace of V spanned by $e_1, e_2, \ldots, e_{i-1}$. Since $v \in V_{i-1}$, we thus can write v as an $\mathbb{F}_p$-linear combination of $e_1, e_2, \ldots, e_{i-1}$. In other words, $v = a_1 e_1 + a_2 e_2 + \cdots + a_{i-1} e_{i-1}$ for some $a_1, a_2, \ldots, a_{i-1} \in \mathbb{F}_p$. Consider these $a_1, a_2, \ldots, a_{i-1}$. Then, $e_i + v = 0$ becomes $e_i + a_1 e_1 + a_2 e_2 + \cdots + a_{i-1} e_{i-1} = 0$. But this contradicts the fact that $e_1, e_2, \ldots, e_k$ are $\mathbb{F}_p$-linearly independent. This contradiction proves that our assumption was wrong. Hence, $e_i + v \neq 0$ is proven. This completes the proof of Corollary 3.2 **(b)**. □

Now, Lemma 3.1 **(b)** (applied to $n = k$) yields that the polynomial $\det(\mathfrak{M}_k) \in L[X]$ is a p-polynomial of degree $\leq p^k$, and its coefficient before X^{p^k} is $\det(\mathfrak{m}_k)$.

But Lemma 3.1 **(a)** (applied to $n = k$) yields

$$\det(\mathfrak{M}_k) = \det(\mathfrak{m}_k) \cdot \prod_{v \in V_k} (X + v) = \det(\mathfrak{m}_k) \cdot \prod_{v \in V} (X + v)$$

(since $V_k = V$). Since $\det(\mathfrak{m}_k) \neq 0$ (by Corollary 3.2 **(b)**, applied to $n = k$), this yields

$$\prod_{v \in V} (X + v) = \frac{1}{\det(\mathfrak{m}_k)} \cdot \det(\mathfrak{M}_k).$$

Hence, $\prod_{v \in V} (X + v)$ is a p-polynomial (since $\det(\mathfrak{M}_k)$ is a p-polynomial, while $\frac{1}{\det(\mathfrak{m}_k)}$ is just an element of L). This proves Theorem 1.3 again. □

3.3. Third proof

We shall soon give a third proof of Theorem 1.3. This proof is more complicated than the preceding ones, but it is (from certain viewpoints) the most natural, and also possibly the oldest. It appears in [Ore33, proof of Theorem 7] and also (implicitly) in [Macdon92]. In the PRIMES 2015 application contest, it was also found by Mehtaab Sawhney.

Before we come to this proof, let us prove a few more elementary facts:

Lemma 3.3. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Any finitely many elements $u_1, u_2, \ldots, u_k$ of L satisfy

$$(u_1 + u_2 + \cdots + u_k)^p = u_1^p + u_2^p + \cdots + u_k^p. \tag{17}$$

Proof of Lemma 3.3. This follows from (1) by induction over k. □

Lemma 3.4. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $g \in L[X]$ be a p-polynomial. Then, g^p is a p-polynomial as well.

Proof of Lemma 3.4. We know that $g \in L[X]$ is a p-polynomial. Thus, g has the form $g = \sum_{n=0}^{d} a_n X^{p^n}$ for some $d \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_d \in L$. Consider this d and these $a_0, a_1, \ldots, a_d$.

We know that L is a commutative $\mathbb{F}_p$-algebra. Thus, $L[X]$ also is a commutative $\mathbb{F}_p$-algebra. Now, any finitely many elements $u_1, u_2, \ldots, u_k$ of $L[X]$ satisfy

$$(u_1 + u_2 + \cdots + u_k)^p = u_1^p + u_2^p + \cdots + u_k^p. \tag{18}$$

(Indeed, this follows from Lemma 3.3, applied to $L[X]$ instead of L.)

From $g = \sum_{n=0}^{d} a_n X^{p^n} = a_0 X^{p^0} + a_1 X^{p^1} + \cdots + a_d X^{p^d}$, we obtain

$$\begin{aligned} g^p &= \left(a_0 X^{p^0} + a_1 X^{p^1} + \cdots + a_d X^{p^d}\right)^p = \left(a_0 X^{p^0}\right)^p + \left(a_1 X^{p^1}\right)^p + \cdots + \left(a_d X^{p^d}\right)^p \\ &\qquad \left(\text{by (18), applied to } k = d+1 \text{ and } u_i = a_{i-1} X^{p^{i-1}}\right) \\ &= a_0^p \underbrace{X^{p^0 p}}_{=X^{p^1}} + a_1^p \underbrace{X^{p^1 p}}_{=X^{p^2}} + \cdots + a_d^p \underbrace{X^{p^d p}}_{=X^{p^{d+1}}} \\ &= a_0^p X^{p^1} + a_1^p X^{p^2} + \cdots + a_d^p X^{p^{d+1}}. \end{aligned}$$

This is clearly a p-polynomial. Thus, Lemma 3.4 is proven. □

Lemma 3.5. Let p be a prime. We have

$$\prod_{\lambda \in \mathbb{F}_p} (X - \lambda) = X^p - X \tag{19}$$

in the polynomial ring $\mathbb{F}_p[X]$.

Proof of Lemma 3.5. This is a well-known identity, and can be proven, e.g., by comparing the roots and the leading terms of both sides. For the sake of completeness, let us give its proof in more details:

Let G be the polynomial $\prod_{\lambda \in \mathbb{F}_p} (X - \lambda) - (X^p - X) \in \mathbb{F}_p[X]$.

Both polynomials $\prod_{\lambda \in \mathbb{F}_p} (X - \lambda)$ and $X^p - X$ in the ring $\mathbb{F}_p[X]$ are monic polynomials of degree p (in fact, $\prod_{\lambda \in \mathbb{F}_p} (X - \lambda)$ is a product of $\left|\mathbb{F}_p\right| = p$ linear polynomials, and thus has degree p; it is furthermore monic because those linear polynomials all are monic). Hence, their difference $\prod_{\lambda \in \mathbb{F}_p} (X - \lambda) - (X^p - X)$ is a

polynomial of degree $< p$ (because the coefficients of X^p in these two polynomials cancel out when we subtract them). In other words, G is a polynomial of degree $< p$ (since $G = \prod_{\lambda \in \mathbb{F}_p} (X - \lambda) - (X^p - X)$). Thus, $\deg G < p$.

But every $\mu \in \mathbb{F}_p$ satisfies

$$G(\mu) = \underbrace{\prod_{\lambda \in \mathbb{F}_p} (\mu - \lambda)}_{\substack{\text{This product has a zero factor} \\ \text{(indeed, its factor for } \lambda = \mu \text{ is } \mu - \mu = 0\text{),} \\ \text{and thus equals } 0}} - \left(\underbrace{\mu^p}_{\substack{= \mu \\ \text{(by (4), applied} \\ \text{to } \lambda = \mu\text{)}}} - \mu \right)$$

$$\left(\text{since } G = \prod_{\lambda \in \mathbb{F}_p} (X - \lambda) - (X^p - X) \right)$$

$$= 0 - (\mu - \mu) = 0.$$

In other words, each $\mu \in \mathbb{F}_p$ is a root of the polynomial G. Thus, the polynomial G has at least $\left|\mathbb{F}_p\right| = p$ roots. Consequently, the polynomial G has more than $\deg G$ roots (since $\deg G < p$). But if a polynomial Q over a field has more than $\deg Q$ roots, then Q must be 0. Applying this to $Q = G$, we conclude that $G = 0$. Hence, $\prod_{\lambda \in \mathbb{F}_p} (X - \lambda) - (X^p - X) = G = 0$, so that $\prod_{\lambda \in \mathbb{F}_p} (X - \lambda) = X^p - X$. This proves Lemma 3.5. □

Lemma 3.6. Let p be a prime. We have

$$\prod_{\lambda \in \mathbb{F}_p} (X + \lambda Y) = X^p - XY^{p-1} \tag{20}$$

in the polynomial ring $\mathbb{F}_p[X, Y]$.

Proof of Lemma 3.6. Consider the ring $\mathbb{F}_p[X, Y]$ as a subring of the ring $\mathbb{F}_p(X, Y)$ of rational functions in X and Y. We can substitute X/Y for X in (19); as a result, we obtain $\prod_{\lambda \in \mathbb{F}_p} (X/Y - \lambda) = (X/Y)^p - X/Y$. Multiplying both sides of this equality by Y^p, we obtain

$$Y^p \prod_{\lambda \in \mathbb{F}_p} (X/Y - \lambda) = Y^p \left((X/Y)^p - X/Y \right) = X^p - XY^{p-1}.$$

Thus,

$$X^p - XY^{p-1} = Y^p \prod_{\lambda \in \mathbb{F}_p} (X/Y - \lambda) = \prod_{\lambda \in \mathbb{F}_p} \underbrace{(Y (X/Y - \lambda))}_{= X - \lambda Y}$$
$$\left(\text{since the product has } \left|\mathbb{F}_p\right| = p \text{ terms}\right)$$
$$= \prod_{\lambda \in \mathbb{F}_p} (X - \lambda Y) = \prod_{\lambda \in \mathbb{F}_p} (X + \lambda Y)$$

(here, we have substituted λ for $-\lambda$ in the product, since the map $\mathbb{F}_p \to \mathbb{F}_p$, $\lambda \mapsto -\lambda$ is a bijection). This proves Lemma 3.6. □

Lemma 3.7. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $f \in L[X]$ be a p-polynomial. Then,

$$f(u+v) = f(u) + f(v) \tag{21}$$

for every $u \in L[X]$ and $v \in L[X]$.

Proof of Lemma 3.7. The proof of Lemma 3.7 is analogous to the proof of Lemma 2.6 (except that u and v now belong to $L[X]$ instead of L). □

Lemma 3.8. Let p be a prime. Let L be a commutative $\mathbb{F}_p$-algebra. Let $f \in L[X]$ be a p-polynomial. Then,

$$f(\lambda u) = \lambda f(u) \tag{22}$$

for every $u \in L[X]$ and $\lambda \in \mathbb{F}_p$.

Proof of Lemma 3.8. The proof of Lemma 3.8 is analogous to the proof of Lemma 2.7 (except that u now belongs to $L[X]$ instead of L). □

We are now ready to prove Theorem 1.3 again:

Third proof of Theorem 1.3. We WLOG assume that $V \neq 0$ (since otherwise, Theorem 1.3 is evident). Lemma 2.1 **(a)** yields that the number p is prime. Lemma 2.1 **(b)** shows that the field L is a field extension of $\mathbb{F}_p$. Lemma 2.1 **(c)** says that the subset V is a finite-dimensional $\mathbb{F}_p$-vector subspace of L.

Now, we shall prove Theorem 1.3 by induction over $\dim V$.

The *induction base* (that is, the case when $\dim V = 0$) is easy and left to the reader.

Induction step: Let $N \in \mathbb{N}$. Assume (as the induction hypothesis) that Theorem 1.3 is proven in the case when $\dim V = N$. We must then show that Theorem 1.3 holds in the case when $\dim V = N + 1$.

So let us assume that $\dim V = N + 1$. Thus, $\dim V = N + 1 > 0$; hence, V has a nonzero element e. Fix such an e. Then, the $\mathbb{F}_p$-vector subspace $\mathbb{F}_p e$ of V has dimension 1. By a basic fact in linear algebra, there exists a complement to the

subspace $\mathbb{F}_p e$ of the vector space V – that is, there exists an $\mathbb{F}_p$-vector subspace W of V such that $V = W \oplus \mathbb{F}_p e$ (internal direct sum). Fix such a W.

From $V = W \oplus \mathbb{F}_p e$, we obtain $\dim V = \dim W + \underbrace{\dim\left(\mathbb{F}_p e\right)}_{=1} = \dim W + 1$. Thus, $\dim W + 1 = \dim V = N + 1$, so that $\dim W = N$. Hence (by our induction hypothesis) Theorem 1.3 can be applied to W instead of V. As a result, we conclude that $\prod\limits_{v \in W} (X + v) \in L[X]$ is a p-polynomial. Let us denote this p-polynomial by g. Thus,

$$\prod_{v \in W} (X + v) = g. \tag{23}$$

From Lemma 3.4, we conclude that g^p is a p-polynomial as well.

Now, $V = W \oplus \mathbb{F}_p e$. Thus, every $v \in V$ can be uniquely written in the form $w + \lambda e$ for some $(w, \lambda) \in W \times \mathbb{F}_p$. Thus, we can substitute $w + \lambda e$ for v in the product $\prod\limits_{v \in V} (X + v)$. We hence obtain

$$\begin{aligned}
\prod_{v \in V} (X + v) &= \underbrace{\prod_{(w,\lambda) \in W \times \mathbb{F}_p}}_{= \prod\limits_{\lambda \in \mathbb{F}_p} \prod\limits_{w \in W}} \underbrace{(X + w + \lambda e)}_{= X + \lambda e + w} = \prod_{\lambda \in \mathbb{F}_p} \prod_{w \in W} (X + \lambda e + w) \\
&= \prod_{\lambda \in \mathbb{F}_p} \underbrace{\prod_{v \in W} (X + \lambda e + v)}_{\substack{= g(X + \lambda e) \\ \text{(this follows by substituting } X + \lambda e \\ \text{for } X \text{ in (23))}}} \\
&\qquad \left(\text{here, we have renamed the index } w \text{ as } v\right) \\
&= \prod_{\lambda \in \mathbb{F}_p} \underbrace{g\left(X + \lambda e\right)}_{\substack{= g(X) + g(\lambda e) \\ \text{(by (21), applied to } f = g, \\ u = X \text{ and } v = \lambda e)}} = \prod_{\lambda \in \mathbb{F}_p} \left(\underbrace{g\left(X\right)}_{= g} + \underbrace{g\left(\lambda e\right)}_{\substack{= \lambda g(e) \\ \text{(by (22), applied to } f = g \\ \text{and } u = e)}} \right) \\
&= \prod_{\lambda \in \mathbb{F}_p} \left(g + \lambda g\left(e\right)\right) = g^p - g\left(g\left(e\right)\right)^{p-1} \\
&\qquad \left(\text{this follows by substituting } g \text{ and } g\left(e\right) \text{ for } X \text{ and } Y \text{ in (20)}\right).
\end{aligned}$$

But this is clearly a p-polynomial (since both g^p and g are p-polynomials, while $\left(g\left(e\right)\right)^{p-1}$ is just a constant in L). Thus, we have proven that $\prod\limits_{v \in V} (X + v)$ is a p-polynomial. In other words, Theorem 1.3 holds in the case when $\dim V = N + 1$. This completes the induction step, and Theorem 1.3 is proven once again. $\square$

4. Proofs of Theorem 1.4

4.1. First proof

First proof of Theorem 1.4. We WLOG assume that $V \neq 0$ (since otherwise, Theorem 1.4 is evident). Let $p = \operatorname{char} L$. Lemma 2.1 **(a)** yields that the number p is prime. Lemma 2.1 **(b)** shows that the field L is a field extension of $\mathbb{F}_p$. Lemma 2.1 **(c)** says that the subset V is a finite-dimensional $\mathbb{F}_p$-vector subspace of L.

Define a polynomial $W \in L[X]$ by $W = \prod_{v \in V} (X + v)$. Then, Theorem 1.3 yields that the polynomial W is a p-polynomial. Hence, its derivative equals its coefficient before X^1 (by (9), applied to $f = W$). But this coefficient is $\prod_{v \in V \setminus 0} v$. Thus, we know that the derivative of W equals $\prod_{v \in V \setminus 0} v$. Hence, $W'(t) = \prod_{v \in V \setminus 0} v$.

On the other hand, since $W = \prod_{v \in V} (X + v)$, the Leibniz formula yields

$$W' = \sum_{w \in V} \underbrace{(X+w)'}_{=1} \cdot \prod_{\substack{v \in V; \\ v \neq w}} (X+v) = \sum_{w \in V} \prod_{\substack{v \in V; \\ v \neq w}} (X+v) = \sum_{w \in V} \frac{\prod_{v \in V} (X+v)}{X+w}$$
$$= \left(\prod_{v \in V} (X+v) \right) \cdot \left(\sum_{w \in V} \frac{1}{X+w} \right).$$

Applying this to $X = t$, we obtain

$$W'(t) = \left(\prod_{v \in V} (t+v) \right) \cdot \left(\sum_{w \in V} \frac{1}{t+w} \right),$$

so that

$$\sum_{w \in V} \frac{1}{t+w} = \underbrace{\frac{1}{\prod_{v \in V} (t+v)}}_{= \prod_{v \in V} \frac{1}{t+v}} \cdot \underbrace{W'(t)}_{= \prod_{v \in V \setminus 0} v} = \left(\prod_{v \in V} \frac{1}{t+v} \right) \cdot \left(\prod_{v \in V \setminus 0} v \right).$$

Rename the index w as v and obtain the claim of Theorem 1.4. □

4.2. Second proof

The following alternative proof of Theorem 1.4 was found by Meghal Gupta, Mehtaab Sawhney, Brandon Epstein and Girishvar Venkal during the PRIMES application contest 2015:

Second proof of Theorem 1.4. Define a polynomial $f \in L[X]$ by

$$f = \sum_{v \in V} \prod_{w \in V \setminus \{v\}} (X + w) - \prod_{v \in V \setminus \{0\}} v. \tag{24}$$

Clearly, $\deg f \leq |V| - 1$ (since each of the products $\prod_{w \in V \setminus \{v\}} (X + w)$ has at most $|V| - 1$ terms).

Now, let $u \in V$. We shall prove that $f(u) = 0$.

Indeed, substituting u for X in the identity (24), we obtain

$$f(u) = \sum_{v \in V} \prod_{w \in V \setminus \{v\}} (u + w) - \prod_{v \in V \setminus \{0\}} v. \tag{25}$$

Since $u \in V$, we have $-u \in V$ (since V is an additive group). Thus,

$$\sum_{v \in V} \prod_{w \in V \setminus \{v\}} (u + w) = \prod_{w \in V \setminus \{-u\}} (u + w) + \sum_{\substack{v \in V; \\ v \neq -u}} \underbrace{\prod_{w \in V \setminus \{v\}} (u + w)}_{\substack{\text{This product contains the factor } u+(-u) \\ \text{(because } -u \in V \setminus \{v\} \text{ (since } -u \in V \text{ and } -u \neq v)\text{)} \\ \text{and thus is 0 (because this factor is 0)}}}$$

$$= \prod_{w \in V \setminus \{-u\}} (u + w) + \underbrace{\sum_{\substack{v \in V; \\ v \neq -u}} 0}_{\substack{\left(\begin{array}{c} \text{here, we have split off the addend for } v = -u \\ \text{from the sum} \end{array} \right) \\ = 0}} = \prod_{w \in V \setminus \{-u\}} (u + w) = \prod_{v \in V \setminus \{0\}} v$$

(here, we have substituted v for $u + w$ in the product, since the map $V \setminus \{-u\} \to V \setminus \{0\}$, $w \mapsto u + w$ is a bijection[7]). Therefore, (25) rewrites as

$$f(u) = \prod_{v \in V \setminus \{0\}} v - \prod_{v \in V \setminus \{0\}} v = 0.$$

In other words, u is a root of f.

Now, let us forget that we fixed u. We thus have proven that every $u \in V$ is a root of f. Thus, f has at least $|V|$ roots. Since $|V| > \deg f$ (because $\deg f \leq |V| - 1$), this shows that f has more than $\deg f$ roots. According to Lemma 2.11, this entails that $f = 0$. Because of (24), this yields

$$\sum_{v \in V} \prod_{w \in V \setminus \{v\}} (X + w) = \prod_{v \in V \setminus \{0\}} v.$$

Substituting t for X in this equality, we obtain

$$\sum_{v \in V} \prod_{w \in V \setminus \{v\}} (t + w) = \prod_{v \in V \setminus \{0\}} v.$$

[7] Check this!

Dividing both sides by $\prod\limits_{w\in V}(t+w)$, we obtain

$$\frac{\sum\limits_{v\in V}\prod\limits_{w\in V\setminus\{v\}}(t+w)}{\prod\limits_{w\in V}(t+w)} = \frac{\prod\limits_{v\in V\setminus\{0\}} v}{\prod\limits_{w\in V}(t+w)} = \left(\prod_{w\in V}\frac{1}{t+w}\right)\cdot\left(\prod_{v\in V\setminus\{0\}} v\right)$$
$$= \left(\prod_{v\in V}\frac{1}{t+v}\right)\cdot\left(\prod_{v\in V\setminus\{0\}} v\right).$$

Comparing this with

$$\frac{\sum\limits_{v\in V}\prod\limits_{w\in V\setminus\{v\}}(t+w)}{\prod\limits_{w\in V}(t+w)} = \sum_{v\in V}\underbrace{\frac{\prod\limits_{w\in V\setminus\{v\}}(t+w)}{\prod\limits_{w\in V}(t+w)}}_{=\frac{1}{t+v}} = \sum_{v\in V}\frac{1}{t+v},$$

we obtain

$$\sum_{v\in V}\frac{1}{t+v} = \left(\prod_{v\in V}\frac{1}{t+v}\right)\cdot\left(\prod_{v\in V\setminus\{0\}} v\right).$$

This proves Theorem 1.4 again. □

4.3. A generalization

The second proof of Theorem 1.4 shown above can be easily adapted to the following generalization:

Theorem 4.1. Let V be a finite additive subgroup of a field L. Let $s\in L[X]$ be a polynomial of degree $\leq |V|-1$. Let $t\in L\setminus V$. Then,

$$\sum_{v\in V}\frac{s(v)}{t+v} = \left(\prod_{v\in V}\frac{1}{t+v}\right)\cdot\left(\prod_{v\in V\setminus 0} v\right)\cdot s(-t).$$

Proof of Theorem 1.4. The polynomial $s(-X)$ has degree $\leq |V|-1$ (since the polynomial s has degree $\leq |V|-1$).

Define a polynomial $f\in L[X]$ by

$$f = \sum_{v\in V} s(v)\prod_{w\in V\setminus\{v\}}(X+w) - \left(\prod_{v\in V\setminus\{0\}} v\right)\cdot s(-X). \tag{26}$$

Clearly, $\deg f \leq |V| - 1$ (since each of the products $\prod_{w \in V \setminus \{v\}} (X + w)$ has at most $|V| - 1$ terms, and since the polynomial $s(-X)$ has degree $\leq |V| - 1$).

Now, let $u \in V$. We shall prove that $f(u) = 0$.

Indeed, substituting u for X in the identity (26), we obtain

$$f(u) = \sum_{v \in V} s(v) \prod_{w \in V \setminus \{v\}} (u + w) - \left(\prod_{v \in V \setminus \{0\}} v \right) \cdot s(-u). \tag{27}$$

Since $u \in V$, we have $-u \in V$ (since V is an additive group). Thus,

$$\begin{aligned}
&\sum_{v \in V} s(v) \prod_{w \in V \setminus \{v\}} (u + w) \\
&= s(-u) \prod_{w \in V \setminus \{-u\}} (u + w) + \sum_{\substack{v \in V; \\ v \neq -u}} s(v) \underbrace{\prod_{w \in V \setminus \{v\}} (u + w)}_{\substack{\text{This product contains the factor } u+(-u) \\ \text{(because } -u \in V \setminus \{v\} \text{ (since } -u \in V \text{ and } -u \neq v)) \\ \text{and thus is 0 (because this factor is 0)}}} \\
&\quad \left(\begin{array}{c} \text{here, we have split off the addend for } v = -u \\ \text{from the sum} \end{array} \right) \\
&= s(-u) \prod_{w \in V \setminus \{-u\}} (u + w) + \underbrace{\sum_{\substack{v \in V; \\ v \neq -u}} s(v) \, 0}_{=0} \\
&= s(-u) \prod_{w \in V \setminus \{-u\}} (u + w) = s(-u) \prod_{v \in V \setminus \{0\}} v
\end{aligned}$$

(here, we have substituted v for $u + w$ in the product, since the map $V \setminus \{-u\} \to V \setminus \{0\}$, $w \mapsto u + w$ is a bijection[8]). Therefore, (27) rewrites as

$$f(u) = s(-u) \prod_{v \in V \setminus \{0\}} v - \left(\prod_{v \in V \setminus \{0\}} v \right) \cdot s(-u) = 0.$$

In other words, u is a root of f.

Now, let us forget that we fixed u. We thus have proven that every $u \in V$ is a root of f. Thus, f has at least $|V|$ roots. Since $|V| > \deg f$ (because $\deg f \leq |V| - 1$), this shows that f has more than $\deg f$ roots. According to Lemma 2.11, this entails that $f = 0$. Because of (26), this yields

$$\sum_{v \in V} s(v) \prod_{w \in V \setminus \{v\}} (X + w) = \left(\prod_{v \in V \setminus \{0\}} v \right) \cdot s(-X).$$

[8] Check this!

Substituting t for X in this equality, we obtain

$$\sum_{v\in V} s(v) \prod_{w\in V\setminus\{v\}} (t+w) = \left(\prod_{v\in V\setminus\{0\}} v\right)\cdot s(-t).$$

Dividing both sides by $\prod\limits_{w\in V}(t+w)$, we obtain

$$\begin{aligned}\frac{\sum\limits_{v\in V} s(v) \prod\limits_{w\in V\setminus\{v\}} (t+w)}{\prod\limits_{w\in V}(t+w)} &= \frac{\left(\prod\limits_{v\in V\setminus\{0\}} v\right)\cdot s(-t)}{\prod\limits_{w\in V}(t+w)} \\ &= \left(\prod_{w\in V}\frac{1}{t+w}\right)\cdot\left(\prod_{v\in V\setminus\{0\}} v\right)\cdot s(-t) \\ &= \left(\prod_{v\in V}\frac{1}{t+v}\right)\cdot\left(\prod_{v\in V\setminus\{0\}} v\right)\cdot s(-t).\end{aligned}$$

Comparing this with

$$\frac{\sum\limits_{v\in V} s(v) \prod\limits_{w\in V\setminus\{v\}} (t+w)}{\prod\limits_{w\in V}(t+w)} = \sum_{v\in V} s(v) \underbrace{\frac{\prod\limits_{w\in V\setminus\{v\}}(t+w)}{\prod\limits_{w\in V}(t+w)}}_{=\frac{1}{t+v}} = \sum_{v\in V}\frac{s(v)}{t+v},$$

we obtain

$$\sum_{v\in V}\frac{s(v)}{t+v} = \left(\prod_{v\in V}\frac{1}{t+v}\right)\cdot\left(\prod_{v\in V\setminus\{0\}} v\right)\cdot s(-t).$$

This proves Theorem 4.1. □

Theorem 1.4 is the particular case of Theorem 4.1 for $s = 1$.

5. Proofs of Theorem 1.5

Many of the facts shown in Section 2 have analogues in which $\mathbb{F}_p$ is replaced by $\mathbb{F}_q$. In preparation for the proof of Theorem 1.5, we shall now prove some of these analogues:

Lemma 5.1. Let $q > 1$ be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Any two elements u and v of L satisfy

$$(u+v)^q = u^q + v^q. \tag{28}$$

Proof of Lemma 5.1. We know that $q > 1$ is a prime power. In other words, $q = p^N$ for some prime p and some positive integer N. Consider these p and N. Now, $\mathbb{F}_q$ is a $\mathbb{F}_p$-algebra (since $q = p^N$). Hence, L is a commutative $\mathbb{F}_p$-algebra. Let $u \in L$ and $v \in L$. Applying (3) to $n = N$, we obtain $(u+v)^{p^N} = u^{p^N} + v^{p^N}$. Since $q = p^N$, this rewrites as $(u+v)^q = u^q + v^q$. This proves Lemma 5.1. □

Lemma 5.2. Let $q > 1$ be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Any two elements u and v of L and any $n \in \mathbb{N}$ satisfy

$$(u+v)^{q^n} = u^{q^n} + v^{q^n}. \tag{29}$$

Proof of Lemma 5.2. To obtain a proof of Lemma 5.2, just replace every "p" by a "q" in the proof of Lemma 2.3, and replace the reference to (1) by a reference to (28). □

Lemma 5.3. Let $q > 1$ be a prime power. Any $\lambda \in \mathbb{F}_q$ satisfies

$$\lambda^q = \lambda. \tag{30}$$

Proof of Lemma 5.3. To obtain a proof of Lemma 5.3, just replace every "p" by a "q" in the proof of Lemma 2.4. □

Lemma 5.4. Let $q > 1$ be a prime power. Any $\lambda \in \mathbb{F}_q$ and any $n \in \mathbb{N}$ satisfy

$$\lambda^{q^n} = \lambda. \tag{31}$$

Proof of Lemma 5.4. To obtain a proof of Lemma 5.4, just replace every "p" by a "q" in the proof of Lemma 2.5, and replace the reference to (4) by a reference to (30). □

Lemma 5.5. Let $q > 1$ be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Let $f \in L[X]$ be a q-polynomial. Then,

$$f(u+v) = f(u) + f(v) \tag{32}$$

for every $u \in L$ and $v \in L$.

Proof of Lemma 5.5. To obtain a proof of Lemma 5.5, just replace every "p" by a "q" in the proof of Lemma 2.6, and replace the reference to (3) by a reference to (29). □

Lemma 5.6. Let $q > 1$ be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Let $f \in L[X]$ be a q-polynomial. Then,

$$f(\lambda u) = \lambda f(u) \tag{33}$$

for every $u \in L$ and $\lambda \in \mathbb{F}_q$.

Proof of Lemma 5.6. To obtain a proof of Lemma 5.6, just replace every "p" by a "q" in the proof of Lemma 2.7, and replace the reference to (5) by a reference to (31). □

Lemma 5.7. Let $q > 1$ be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Let $f \in L[X]$ be a q-polynomial. Then,

$$\mathcal{R}(f) \text{ is a } \mathbb{F}_q\text{-vector subspace of } L. \tag{34}$$

Proof of Lemma 5.7. To obtain a proof of Lemma 5.7, just replace every "p" by a "q" in the proof of Lemma 2.9, and replace the references to (6) and (7) by references to (32) and (33). □

Lemma 5.8. Let $q > 1$ be a prime power. Let L be a commutative $\mathbb{F}_q$-algebra. Let $f \in L[X]$ be a q-polynomial. Then,

$$\text{the derivative } f' \text{ of } f \text{ equals the coefficient of } f \text{ before } X^1. \tag{35}$$

Proof of Lemma 5.8. To obtain a proof of Lemma 5.8, just replace every "p" by a "q" in the proof of Lemma 2.10, and then replace the words "(since $q \mid q^n$)" by "(since $\operatorname{char}\left(\mathbb{F}_q\right) \mid q \mid q^n$ and thus $q^n = 0$ in $\mathbb{F}_q$)". □

Proof of Theorem 1.5. We know that $q > 1$ is a prime power. In other words, $q = p^N$ for some prime p and some positive integer N. Consider these p and N. We have $\operatorname{char}\left(\mathbb{F}_q\right) = p$ (since $q = p^N$).

In order to obtain a proof of Theorem 1.5, it suffices to take any of our three proofs of Theorem 1.3, and replace every appearance of "p" by "q" while simultaneously replacing all references to (1), (3), (4), (5), (6), (7), (8), (9), Lemma 2.6 and Lemma 2.7 by references to (28), (29), (30), (31), (32), (33), (34), (35), Lemma 5.5 and Lemma 5.6.[9] Thus, three different proofs of Theorem 1.5 can be obtained. □

[9] Here we are regarding Lemma 3.3, Lemma 3.4, Lemma 3.5, Lemma 3.6, Lemma 3.7, Lemma 3.8 (as well as the proofs of these lemmas) as parts of the proof. So the same replacements must be made inside these lemmas and inside their proofs.

6. Proofs of Theorem 1.6

First proof of Theorem 1.6. As we have seen above, each of our three proofs of Theorem 1.3 can be turned into a proof of Theorem 1.5 by certain replacements. In particular, applying these replacements to the third proof of Theorem 1.3, we obtain a proof of Theorem 1.5. It is straightforward to observe that the latter proof of Theorem 1.5 doubles as a proof of Theorem 1.6 (i.e., it works just as well if L is a commutative $\mathbb{F}_q$-algebra instead of being a field extension of $\mathbb{F}_q$). Thus, Theorem 1.6 is proven. □

Second proof of Theorem 1.6. We can also derive Theorem 1.6 from Theorem 1.5 as follows:

The $\mathbb{F}_q$-vector space V is finite, and thus finite-dimensional. Hence, it has a basis $(e_1, e_2, \ldots, e_n)$. Fix such a basis.

Let M be the $\mathbb{F}_q$-algebra $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ (the polynomial ring over $\mathbb{F}_q$ in n indeterminates $X_1, X_2, \ldots, X_n$). Then, the universal property of the polynomial ring M shows that there exists a unique $\mathbb{F}_q$-algebra homomorphism $\Phi : M \to L$ satisfying

$$(\Phi(X_i) = e_i \qquad \text{for every } i \in \{1, 2, \ldots, n\}). \tag{36}$$

Consider this Φ.

Let $N = \mathbb{F}_q(X_1, X_2, \ldots, X_n)$ be the fraction field of M. This N is clearly a field extension of $\mathbb{F}_q$. Let W be the $\mathbb{F}_q$-vector subspace of M spanned by $X_1, X_2, \ldots, X_n$. Then, $W \subseteq M \subseteq N$. Also, the $\mathbb{F}_q$-vector space W is finite-dimensional, and thus finite. Hence, Theorem 1.5 (applied to N and W instead of L and V) yields that $\prod_{v \in W} (X + v) \in N[X]$ is a q-polynomial. In other words, $\prod_{v \in W} (X + v) \in M[X]$ is a q-polynomial (since $\prod_{v \in W} (X + v)$ belongs to $M[X]$ (because $W \subseteq M$)).

The $\mathbb{F}_q$-vector space W has basis $(X_1, X_2, \ldots, X_n)$, whereas the $\mathbb{F}_q$-vector space V has basis $(e_1, e_2, \ldots, e_n)$. The map $\Phi : M \to L$ sends the former basis to the latter basis (because of (36)). Hence, the map Φ restricts to an $\mathbb{F}_q$-vector space isomorphism $W \to V$. In other words, the map $W \to V$, $v \mapsto \Phi(v)$ is well-defined and is an $\mathbb{F}_q$-vector space isomorphism. In particular, this map is a bijection.

But the $\mathbb{F}_q$-algebra homomorphism $\Phi : M \to L$ canonically induces an $\mathbb{F}_q[X]$-algebra homomorphism $\Phi[X] : M[X] \to L[X]$ [10]. This latter homomorphism $\Phi[X]$ clearly sends q-polynomials to q-polynomials. In other words, if $f \in M[X]$

[10] Explicitly, this homomorphism $\Phi[X]$ is given by

$$(\Phi[X])\left(\sum_{i \geq 0} a_i X^i\right) = \sum_{i \geq 0} \Phi(a_i) X^i$$

for every polynomial $\sum_{i \geq 0} a_i X^i \in M[X]$ (with $a_i \in M$).

is a q-polynomial, then $(\Phi[X])(f) \in L[X]$ is a q-polynomial. Applying this to $f = \prod_{v \in W} (X+v)$, we conclude that $(\Phi[X]) \left(\prod_{v \in W} (X+v) \right) \in L[X]$ is a q-polynomial. Since

$$(\Phi[X]) \left(\prod_{v \in W} (X+v) \right) = \prod_{v \in W} (X + \Phi(v)) = \prod_{v \in V} (X+v)$$
$$\left(\begin{array}{c} \text{here, we have substituted } v \text{ for } \Phi(v) \text{ in the} \\ \text{product, since the map } W \to V,\ v \mapsto \Phi(v) \\ \text{is a bijection} \end{array} \right),$$

this rewrites as follows: $\prod_{v \in V} (X+v) \in L[X]$ is a q-polynomial. Thus, Theorem 1.6 is proven again. □

We note in passing that Lemma 3.1 and Corollary 3.2 **(a)** can also be generalized to the situation where L is just a commutative $\mathbb{F}_p$-algebra (not necessarily a field). Again, the generalizations can be derived from the original statements using the same trick that we used in our second proof of Theorem 1.6.

References

[Conrad14] Keith Conrad, *Carlitz extensions*.
`http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/carlitz.pdf`

[Goss98] David Goss, *Basic Structures of Function Field Arithmetic*, Springer, 1st edition 1998.

[Macdon92] I. G. Macdonald, *Schur functions: Theme and variations*, Séminaire Lotharingien de Combinatoire 28, B28a (1992).
`http://www.emis.de/journals/SLC/opapers/s28macdonald.html`

[Grinbe16] Darij Grinberg, *Do the symmetric functions have a function-field analogue?*, draft, 4 November 2016.
`http://www.cip.ifi.lmu.de/~grinberg/algebra/schur-ore.pdf`

[Ore33] Oystein Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), pp. 559–584.
`http://www.ams.org/journals/tran/1933-035-03/S0002-9947-1933-1501703-0/`