

SYMMETRIC POLYNOMIALS AND FINITE FIELDS

APOORVA KHARE

These notes arose out of my teaching the course *Math 370: Fields and Galois Theory* to a strong class of undergraduates at Yale University, in the Spring of 2010. We apply the notions of symmetric polynomials to finite fields. The goal is to answer the following question:

Question. Suppose \mathbb{F} is a finite field, of size $|\mathbb{F}| = q$. Given an integer $k \geq 0$, compute the polynomial

$$S_k(T) := \sum_{a \in \mathbb{F}} (T + a)^k.$$

This is a polynomial that is “translation-invariant”: $S_k(T + a) = S_k(T)$ for all $k \geq 0$ and all $a \in \mathbb{F}$. Our main result reads:

Theorem 1. *Suppose a field \mathbb{F} has size q and characteristic p . For $S_k(T)$ as above,*

$$S_k(T) = \sum_{0 \leq \alpha, \beta \in \mathbb{Z}: (q-1)\alpha + q\beta = k} \frac{(\alpha + \beta - 1)! k}{\alpha! \beta!} (T^q - T)^\beta \in (\mathbb{Z}/p\mathbb{Z})[T].$$

We present an essentially self-contained, elementary introduction to the subject (ending by proving Theorem 1), assuming some basic field theory. Then we present two appendices on translation-invariant rational-functions, ending with the formula for the “only” nontrivial such polynomial.

1. CONSTRUCTION AND PROPERTIES OF FINITE FIELDS

The following are standard results in field theory (and other mathematics), that we may quote without reference, and use without proof.

Proposition 2. *Suppose F is a field, R is a commutative unital ring, $f \in F[T]$ or $R[T]$.*

- (1) *If $f \neq 0$ has degree d , then f has at most d roots in F .*
- (2) *There exists a finite field extension $K : F$, such that f factors into a product of linear factors in $K[T]$.*
- (3) *If $G \subset F^\times$ is a finite subgroup of units in F , then G is cyclic.*
- (4) *If $K : F$ is a field extension, then K is a vector space over F .*
- (5) (Tower Law.) *If $L : K$ and $K : F$ are field extensions, with B, C bases for L over K and K over F respectively, then $\{b \cdot c : b \in B, c \in C\}$ is an F -basis for L .*
- (6) (Factor Theorem.) *If $f \in R[T]$ and $a \in R$, then $f(T) - f(a)$ is divisible by $T - a$.*
- (7) *Given $f(T) = \sum_i a_i T^i \in R[T]$, define the derivative of f to be $f'(T) = \sum_{i>0} i a_i T^{i-1}$. Then the Product Rule holds: $(fg)' = f \cdot g' + f' \cdot g$ for all $f, g \in R[T]$.*

Date: April 13, 2010.

- (8) If f has a multiple root (i.e., $(T - \alpha)^2 \mid f(T)$ for some $\alpha \in F$), then $T - \alpha$ divides f' .
- (9) A splitting field of f over F is defined to be any extension $K : F$ such that f splits over K into a product of linear factors $f(T) = \prod_{i=1}^{\deg f} (T - a_i)$, and $K = F(a_1, \dots, a_{\deg f})$.
- Then for all F and $f \in F[T]$, a splitting field exists, and is unique up to isomorphism.
- (10) Suppose $L : K$ is a field extension, $f \in K[T]$, and $\alpha \in L$ is a root of f . If $\sigma \in \text{Aut}_K(L)$, then $\sigma(\alpha)$ is also a root of f .

1.1. Preliminaries. Let us now start with any finite field \mathbb{F} . Since $0 \neq 1 \in \mathbb{F}$, consider the map $:\mathbb{Z} \rightarrow \mathbb{F}$, sending $1 \mapsto 1$. (We abuse notation and mean, by writing an integer n in \mathbb{F} , its image in \mathbb{F} under this map.) Since \mathbb{F} is finite but \mathbb{Z} is not, there is a nontrivial kernel. Since this is a map of rings into a field, the kernel must be a prime ideal, say (p) .

The following facts are easy to prove:

- For all $f \in \mathbb{F}$, $f + f + \dots + f$ (p times) is zero (using distributivity, and since $p = 0$ in \mathbb{F}).
- \mathbb{F} contains a finite *prime subfield*: the subfield generated by 1 is finite, hence equals $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
- \mathbb{F} is a (finite-dimensional) vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, hence has size p^n for some n .
- By Lagrange's Theorem, since \mathbb{F}^\times is a finite group of units, it is a cyclic group of order $p^n - 1$. Hence $x^{p^n - 1} = 1$ for all $x \in \mathbb{F}^\times$, whence $x^{p^n} - x = 0$ for all $x \in \mathbb{F}$.
- For any prime $p \in \mathbb{Z}$, p divides $\binom{p}{i}$ for all $0 < i < p$.
- (Wilson's Theorem.) $\prod_{a \in \mathbb{F}^\times} a = -1$. This is seen by considering the cyclic generator $g \in \mathbb{F}^\times$. We rewrite \mathbb{F}^\times as $\{g, \dots, g^{q-1}\}$; then

$$\prod_{a \in \mathbb{F}^\times} a = \prod_{i=1}^{q-1} g^i = g^{q(q-1)/2}.$$

If q is even, then this equals

$$(g^{q-1})^{q/2} = 1^{q/2} = 1 = -1$$

as required. Otherwise if q is odd, then it equals

$$(g^q)^{(q-1)/2} = g^{(q-1)/2},$$

which is a nontrivial square root of 1. Thus, it must equal -1 , as claimed.

We will henceforth assume and use these results without reference. Next, we discuss an important map $\phi : \mathbb{F} \rightarrow \mathbb{F}$. Given \mathbb{F} , we fix its characteristic $p > 0$ as above. We use from above, that $\prod_{a \in \mathbb{F}} (T - a) = T^q - T$, where \mathbb{F} is a finite field of size $q = p^n$ (for some $0 < n \in \mathbb{Z}$).

Proposition 3. For every (commutative) unital ring R containing $\mathbb{Z}/p\mathbb{Z}$, define the Frobenius map $\phi : R \rightarrow R$ to be: $\phi(r) := r^p$.

- (1) ϕ is an \mathbb{F}_p -algebra homomorphism.
- (2) If R is an integral domain, ϕ is a ring monomorphism.

- (3) If $|\mathbb{F}| = p^n$, then $\phi : \mathbb{F} \rightarrow \mathbb{F}$ is a field automorphism, and n is the order of ϕ in $\text{Aut}(\mathbb{F})$. Moreover, (for all k ,) $\phi^n : \mathbb{F}(T_1, \dots, T_k) \rightarrow \mathbb{F}(T_1, \dots, T_k)$ sends every $f(T_1, \dots, T_k)$ to $f(T_1^{p^n}, \dots, T_k^{p^n})$.

Proof.

- (1) Since $p \mid \binom{p}{i}$ for $0 < i < p$, hence for all $a, b \in R$, $(a + b)^p = a^p + b^p$ by the Binomial Theorem. Moreover, $(ab)^p = a^p b^p$. This shows that ϕ is a ring homomorphism. Since $\phi(a) = a \ \forall a \in \mathbb{F}_p$, ϕ is \mathbb{F}_p -linear as well.
- (2) If $x^p = y^p$, then $(x^p - y^p) = 0$. If $p = 2$ then $-1 = \pm 1 = (-1)^p$, and if $p > 2$, then $-1 = (-1)^p$. So we get:

$$0 = x^p - y^p = x^p + (-1)^p y^p = (x - y)^p,$$

where the last equality holds because ϕ is an \mathbb{F}_p -algebra homomorphism. But since we are in the integral domain R , $x - y = 0$ as required.

- (3) If $R = \mathbb{F}$ is finite, then ϕ is one-to-one, hence onto as well. Next, consider ϕ^m for various m . Since \mathbb{F}^\times is a cyclic group by Proposition 2, let g be any fixed generator; now g has order $p^n - 1$ in \mathbb{F}^\times . Thus, $g^{p^m} \neq g$ for $0 < m < n$, whence $\phi^m \neq \text{id}$ for $0 < m < n$. But $\phi^n(g) = g^{p^n} = g$, whence the same holds for any power of g (and also for 0). Since \mathbb{F}^\times is generated by g , we get that $\phi^n = \text{id}$ as an automorphism of \mathbb{F} .

Finally, the result for $f \in \mathbb{F}(T_1, \dots, T_k)$ follows if we show it for every $f \in \mathbb{F}[T_1, \dots, T_k]$, since ϕ is a ring homomorphism of $\mathbb{F}(T_1, \dots, T_k)$ by a previous part. Now choose $0 \leq l_i \in \mathbb{Z}$ for all $1 \leq i \leq k$, and $c \in \mathbb{F}$. Since ϕ^n fixes \mathbb{F} , the result is true for every monomial expression $cT_1^{l_1} \dots T_k^{l_k}$. But ϕ is an \mathbb{F}_p -algebra homomorphism, so it is additive, whence the result holds for all multi-variable polynomials, as desired.

□

1.2. Existence and uniqueness. As an aside, we now show the existence and uniqueness of finite fields \mathbb{F} , and classifying all subfields of \mathbb{F} .

Theorem 4.

- (1) *Finite fields of all possible orders exist, and are unique up to isomorphism.*
- (2) *The only subfields of \mathbb{F} are the sets of roots of the polynomials $T^{p^m} - T$, where $m \mid n$. For each such m , there exists a unique subfield of size p^m in \mathbb{F} .*

Proof.

- (1) Given p prime and $n \in \mathbb{N}$, consider the polynomial $f_n(T) = T^{p^n} - T$ over the field $\mathbb{Z}/p\mathbb{Z}$. By Proposition 2, f splits into a product of linear factors over some field extension K of $(\mathbb{Z}/p\mathbb{Z})$.

Now consider the set F of roots of f_n in K . Since $f_n'(T) = -1$, hence f_n does not have any repeated roots by Proposition 2. By another part of that same result, f_n must then have p^n roots in K . We claim that the set F of these roots is a subfield of K .

Note that $F = K^{\phi^n}$ is precisely the set of fixed points of ϕ^n in K . By Proposition 3, F is a subring. Now if $x \in F \setminus \{0\}$, then $x^{p^n} = x$, whence $x^{-1} = x^{p^n-2}$ is a power of x , hence contained in F (since F is closed under multiplication).

Thus, F is a field of order p^n . Moreover, any such field is clearly a splitting field of the polynomial $f_n(T) \in (\mathbb{Z}/p\mathbb{Z})[T]$; hence by Proposition 2, it is unique up to isomorphism.

- (2) Now fix \mathbb{F} of size p^n . For $F \subset \mathbb{F}$ to be a subfield of size p^m , we must have that $F^\times \subset \mathbb{F}^\times$ is a (cyclic) subgroup. By Lagrange's Theorem, its order divides $|\mathbb{F}^\times|$. Thus, we must have that $(p^m - 1)|(p^n - 1)$.

Since $m \leq n$, let $n = qm + r$, where $0 \leq r < m$ (by the Euclidean algorithm). Then

$$p^n - 1 = p^r(p^{qm} - 1) + (p^r - 1) = (p^m - 1)p^r(1 + p^m + p^{2m} + \cdots + p^{(q-1)m}) + (p^r - 1).$$

Since $(p^m - 1)|(p^n - 1)$, hence $p^r - 1 = 0$, whence $r = 0$. So $m|n$.

Conversely, given any $m|n$, we see that $(p^m - 1)|(p^n - 1)$, whence $T^{p^m-1} - 1$ divides $T^{p^n-1} - 1$ (left to the reader). Thus, $f_m(T)|f_n(T)$. Now since every $f \in \mathbb{F}$ is a root of $f_n(T)$, hence $f_m(T)$ has exactly p^m roots in \mathbb{F} . The set of these roots forms a subfield; thus, we have constructed a subfield of order p^m inside \mathbb{F} . That this is the unique such subfield is clear: the elements of any such subfield are roots of $f_m(T)$; but inside a fixed field \mathbb{F} , there are only p^m such roots, by Proposition 2. These form a unique subfield. □

1.3. Translation-invariant polynomials. For now, we discuss a small result on polynomials in $\mathbb{F}_q[T]$, that are invariant under translating the argument by all $a \in \mathbb{F}_q$. This is a small, special case of a very general result, which we discuss in the appendix.

Proposition 5. *For all finite fields \mathbb{F}_q , a polynomial $f \in \mathbb{F}_q[T]$ is translation-invariant if $f(T + a) = f(T)$ for all $a \in \mathbb{F}_q$. Then f is translation-invariant if and only if $f(T) = g(T^q - T)$ for some $g \in \mathbb{F}_q[T]$.*

Proof. By induction on $\deg f$. If $\deg f = 0$ then we are done. Otherwise given such an f , consider $f(T) - f(0)$; this is still translation-invariant, and has a root at 0, whence every $a \in \mathbb{F}_q$ is also a root. But then $\prod_{a \in \mathbb{F}_q} (T - a) = T^q - T$ (from above) divides $f(T) - f(0)$. The quotient $f_1(T)$ has strictly smaller degree and is also invariant:

$$f_1(T + a) = \frac{f(T + a) - f(0 + a)}{(T + a)^q - (T + a)} = \frac{f(T) - f(0)}{T^q + a^q - T - a} = \frac{f(T) - f(0)}{T^q - T} = f_1(T),$$

using the Frobenius map from Proposition 3 (with $R = \mathbb{F}_q$). But then $f_1(T)$ is a polynomial in $T^q - T$ by the induction hypothesis, whence so is $f(T)$, as claimed. □

2. SYMMETRIC POLYNOMIALS

We now turn to the theory of *symmetric polynomials*. Suppose R is any commutative unital ring. Fix $n \in \mathbb{N}$, and variables x_1, \dots, x_n . Define the *elementary symmetric polynomials*

to be

$$\sigma_k := \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}, \quad 1 \leq k \leq n,$$

and the *power sum symmetric polynomials* for any $k \geq 0$, to be

$$s_k := \sum_{1 \leq i \leq n} x_i^k.$$

Finally, a polynomial $p \in R[x_1, \dots, x_n]$ is *symmetric* if $p \in R[x_1, \dots, x_n]^{S_n}$, where S_n is the symmetric group on n letters, which acts on the polynomial ring by permuting the variables.

Note that the elementary symmetric polynomials appear when expanding a linear factorization of a monic polynomial:

$$\prod_{i=1}^n (T - x_i) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} + \dots + (-1)^n \sigma_n. \quad (6)$$

We now state the following results, which are standard and can be found in a number of textbooks in algebra.

Theorem 7 (Fundamental Theorem of Symmetric Polynomials). *Suppose R is any (commutative unital) ring. The map $p : R[y_1, \dots, y_n] \rightarrow R[x_1, \dots, x_n]$, sending $p(y_1, \dots, y_n) \mapsto p(\sigma_1, \dots, \sigma_n)$, is an isomorphism onto the subring of symmetric polynomials $R[x_1, \dots, x_n]^{S_n}$.*

Theorem 8 (Waring's Formula).¹ *Given $R[x_1, \dots, x_n]$, for all $k > 0$,*

$$s_k = \sum (-1)^{i_2+i_4+i_6+\dots} \frac{(i_1+i_2+\dots+i_n)!k}{i_1!i_2!\dots i_n!} \sigma_1^{i_1} \sigma_2^{i_2} \dots \sigma_n^{i_n} \in \mathbb{Z}[\sigma_1, \sigma_2, \dots, \sigma_n],$$

where we sum over all $(i_1, \dots, i_n) \in \mathbb{Z}^n$ such that all $i_j \geq 0$ and $\sum_j j i_j = k$.

Our next result defines and computes various symmetric, translation-invariant polynomials over \mathbb{F} .

Proposition 9. *Fix \mathbb{F} , and denote $q = |\mathbb{F}|$. Now define, for $k > 0$,*

$$S_k(T) := \sum_{a \in \mathbb{F}} (T + a)^k.$$

Then $S_k(0)$ is the sum of the n th powers of all elements of \mathbb{F} . Next, define

$$\mathcal{F}_k := \{S \subset \mathbb{F} : |S| = k\}, \quad \Sigma_k(T) := \sum_{S \in \mathcal{F}_k} \prod_{a \in S} (T + a), \quad \Sigma_{-k}(T) := \sum_{S \in \mathcal{F}_k} \prod_{a \in S} (T + a)^{-1}.$$

- (1) $S_k(0)$ equals -1 if $(q-1) | k$, and 0 otherwise.
- (2) $S_k(T) \equiv 0$ if $1 \leq k \leq q-2$ or $k = q$, and $S_{q-1}(T) \equiv -1$.

¹I thank Michael Zieve for telling me this result.

$$(3) \text{ For } 1 \leq |k| \leq q, \Sigma_k(T) = \begin{cases} -1, & \text{if } k = q - 1; \\ T^q - T, & \text{if } k = q; \\ -1/(T^q - T) = S_{-1}(T), & \text{if } k = -1; \\ 1/(T^q - T), & \text{if } k = -q; \\ 0, & \text{otherwise.} \end{cases}$$

(4) $S_k(T)$ equals $p_k(\Sigma_1(T), \Sigma_2(T), \dots, \Sigma_q(T))$ for some $p_k \in \mathbb{Z}[x_1, \dots, x_q]$.

Proof.

- (1) Let $g \in \mathbb{F}^\times$ be any fixed cyclic generator, and consider $S_k(0) = \sum_{a \in \mathbb{F}} a^k = \sum_{a \in \mathbb{F}^\times} a^k$, since $k > 0$. This can be rewritten as a geometric series:

$$S_k(0) = \sum_{i=1}^{q-1} (g^i)^k = \sum_{i=1}^{q-1} (g^k)^i.$$

If $(q-1)|k$ then $g^k = 1$, so each summand is 1 and we get $q-1 = -1$. Otherwise $g^k \neq 1$, and we add:

$$S_k(0) = \frac{(g^k)^q - 1}{g^k - 1} = \frac{(g^q)^k - 1}{g^k - 1} = 0.$$

- (2) We use the Binomial Theorem, and exchange the two summations, to compute:

$$S_k(T) = \sum_{i=0}^k \binom{k}{i} T^{k-i} \sum_{a \in \mathbb{F}} a^i = \sum_{i=0}^k \binom{k}{i} T^{k-i} S_i(0),$$

with the understanding that $S_0(0) = \sum_{a \in \mathbb{F}} 1 = q = 0$. By the previous part, most $S_k(T)$'s are identically zero now. The only ones that are possibly not, occur when $k \geq q-1$. Then

$$S_{q-1}(T) = \binom{q-1}{q-1} T^0 S_{q-1}(0) = -1, \quad S_q(T) = \binom{q}{q-1} T^1 S_{q-1}(0) = -qT = 0.$$

Alternatively, Proposition 5 says that $S_k(T)$ is a polynomial of $T^q - T$, being clearly translation invariant. So for $k < q$, $S_k(T)$ is a constant - and the coefficient of T^q in $S_q(T)$ is $S_0(0) = q = 0$. Hence for all $1 \leq k \leq q$, $S_k(T) = S_k(0)$, and we are done by the previous part.

- (3) Since each $\Sigma_k(T)$ is also translation-invariant, it is a polynomial in $T^q - T$ (by Proposition 5), as well as a polynomial of degree at most k , in T . Thus, for $k < q$, $\Sigma_k(T)$ is a constant, hence equals $\Sigma_k(0)$. But now recall Equation (6), and compute:

$$T^q - T = \prod_{a \in \mathbb{F}} (T - a) = T^q - T^{q-1} \Sigma_1(0) + T^{q-2} \Sigma_2(0) - \dots + (-1)^q \Sigma_q(0).$$

(More precisely, replace n by q and apply the homomorphism $:\mathbb{F}[\{x_a : a \in \mathbb{F}\}] \rightarrow \mathbb{F}$, sending $x_a \mapsto a$, to Equation (6).) Thus, $\Sigma_1(0) = \Sigma_2(0) = \dots = \Sigma_{q-2}(0) = 0$, and

$$(-1)^{q-1} \Sigma_{q-1}(0) = -1.$$

If q is even, then $p = 2$, and $(-1)^{q-1} = \pm 1 = 1$ in \mathbb{F} . Otherwise, q is odd, and $(-1)^{q-1} = 1$. In either case, we get: $\Sigma_{q-1}(0) = -1$.

The next case is when $k = q$. But then $\mathcal{F}_k = \{\mathbb{F}\}$, so $\Sigma_q(T) = \prod_{a \in \mathbb{F}} (T - a) = T^q - T$. This also shows that $\Sigma_{-q}(T) = 1/(T^q - T)$.

Finally, if $0 < k < q$, then taking common denominators, we get: $\Sigma_{-k}(T) = \Sigma_{q-k}(T)/\Sigma_q(T)$. This concludes the proof of the result.

- (4) Let us consider the variables $\{x_a : a \in \mathbb{F} = \mathbb{F}_q\}$. Then by Theorem 7, $\sum_{a \in \mathbb{F}} x_a^k$ can be written (for all $k > 0$) as a polynomial in the elementary symmetric polynomials in the x_a 's. Now map the ring $\mathbb{F}[\{x_a\}]$ to $\mathbb{F}[T]$ via: $x_a \mapsto T + a$. Then the elementary symmetric polynomials map precisely to the $\Sigma_k(T)$'s, and the elements $\sum_{a \in \mathbb{F}} x_a^k$ map to $S_k(T)$. The relations are preserved in $\mathbb{F}[T]$, and we are done. □

3. THE MAIN RESULT, AND CONSEQUENCES

We now prove the desired formula.

Proof of Theorem 1. Apply Waring's Formula (from Theorem 8) and Proposition 9. Set $R = \mathbb{F}$ and consider the \mathbb{F}_p -algebra homomorphism: $\mathbb{F}[\{x_a : a \in \mathbb{F}\}] \rightarrow \mathbb{F}[T]$, sending $x_a \mapsto T + a$. This sends $\sigma_k \mapsto \Sigma_k(T)$ for all $1 \leq k \leq q$, and $s_k \mapsto S_k(T) \forall k > 0$. Hence we can compute $S_k(T)$ using Waring's Formula.

Note that in that formula, every summand containing a positive power of (the image of) $\sigma_1, \sigma_2, \dots$, or σ_{q-2} automatically vanishes, since $\Sigma_i(T) = 0 \forall 1 \leq i \leq q-2$ by Proposition 9. Thus, changing indices from i_{q-1} and i_q to α and β respectively,

$$S_k(T) = \sum_{0 \leq \alpha, \beta \in \mathbb{Z}: \alpha(q-1) + \beta q = k} (-1)^\epsilon \frac{(\alpha + \beta - 1)! k}{\alpha! \beta!} \Sigma_{q-1}(T)^\alpha \Sigma_q(T)^\beta,$$

with two cases:

- If q is odd, then $\epsilon = \alpha$, and we have

$$(-1)^\alpha \Sigma_{q-1}(T)^\alpha = (-1)^\alpha (-1)^\alpha = 1,$$

which proves the result.

- If q is even, then $\epsilon = \beta$, and

$$(-1)^\beta \Sigma_{q-1}(T)^\alpha = (-1)^{\beta+\alpha} = \pm 1 = 1,$$

and we are again done.

Finally, we note that the coefficients are in $\mathbb{Z}/p\mathbb{Z}$, because in the statement of Waring's Formula, the coefficients are actually integers. □

We end by considering related computations combining the above expressions, that can now be carried out.

Proposition 10. Fix $1 \leq l \leq q$, and $n_1, \dots, n_l \in \mathbb{N}$, and define

$$\Sigma^{n_1, \dots, n_l}(T) := \sum_{(a_1, \dots, a_l): \{a_1, \dots, a_l\} \in \mathcal{F}_l} \prod_{j=1}^l (T + a_j)^{n_j}.$$

Then $\Sigma^{n_1, \dots, n_l}(T)$ is a polynomial in $S_k(T)$ (for $1 \leq k \leq \sum_j n_j$) with integer coefficients, as well as a polynomial in $\Sigma_k(T)$ (for $1 \leq k \leq q$) with “integer” coefficients (i.e., in $\mathbb{Z}/p\mathbb{Z}$) - and hence, also a polynomial in $(T^q - T)$ with “integer” coefficients.

Note that this is a simultaneous generalization of $S_k(T)$ and $\Sigma_k(T)$:

$$\Sigma^{n_1}(T) = S_{n_1}(T), \quad \Sigma^{1, 1, \dots, 1}(T) = \Sigma_l(T),$$

if there are l ones in the superscript.

Proof. The result for $\Sigma_k(T)$ follows by Theorem 7, since $\Sigma^{n_1, \dots, n_l}(T)$ is symmetric in the “variables” $\{x_a = T + a : a \in \mathbb{F}\}$. Next, the result for $T^q - T$ follows from Proposition 9, from the result for $\Sigma_k(T)$ - or from Proposition 5, since it is translation-invariant.

We now show the result for $S_k(T)$ by induction on l . For $l = 1$, this is clear from the above observation: $\Sigma^{n_1}(T) = S_{n_1}(T)$. For the general case, it is not hard to see that

$$\Sigma^{n_1, \dots, n_l}(T) = S_{n_l}(T) \Sigma^{n_1, \dots, n_{l-1}}(T) - \sum_{j=1}^{l-1} \Sigma^{n_1, \dots, n_{j-1}, n_j + n_l, n_{j+1}, \dots, n_{l-1}}(T).$$

We are now done by induction on l . □

Our next result computes the sum of expressions of the form

$$\Sigma_{2,1}(T_1, T_2) = \sum_{(a,b,c): \{a,b,c\} \in \mathcal{F}_3} (T_1 + a)(T_1 + b)(T_2 + c).$$

Thus, we need $q \neq 2$, and we note that a, b, c are pairwise distinct. We now compute such an expression in general. (Note that it is not a translation-invariant polynomial in all T_j 's, but nevertheless, is symmetric in the T_j 's.)

Theorem 11. Fix $k, l_1, \dots, l_k \in \mathbb{N}$ with $l := \sum_i l_i \leq q$. Now define

$$\Sigma_{l_1, \dots, l_k}(T_1, \dots, T_k) := \sum_{((a_{ij})) \in I(l)} \prod_{i=1}^k \prod_{j=1}^{l_i} (T_i + a_{ij}),$$

where $I(l)$ is the set of ordered l -tuples of pairwise distinct elements, which we write as $(a_{11}, \dots, a_{1l_1}, a_{21}, \dots, \dots, a_{kl_k})$. Then $\Sigma_{l_1, \dots, l_k}(T_1, \dots, T_k)$ equals

$$- \sum_{i=1}^k \binom{q-1}{l_1, \dots, l_{i-1}, l_i-1, l_{i+1}, \dots, l_k} T_i$$

if $l = q$, and 0 otherwise.

Note that if $k = 1$, then we recover the expression $\Sigma_{l_1}(T_1)$, which was defined earlier in Proposition 9.

Proof. We note that a general monomial in this expression is of the form

$$b_1 \dots b_{l-n} \prod_i T_i^{n_i},$$

where $0 \leq n_i \leq l_i \forall i$, $l = \sum_i l_i$, $n = \sum_i n_i$, and the b_j 's are pairwise distinct elements of \mathbb{F} . The question is: for a fixed such expression, how many summands in the original sum contribute towards it?

To see this, note that for each fixed subset $\{b_j\} \subset \mathbb{F}$ and given this, for each fixed $\prod_i T_i^{n_i}$, the number of summands contributing towards it is a product of two terms (by ‘‘independence’’ of these two parts):

$$\binom{n}{n_1, \dots, n_k} \cdot \frac{(q-n)(q-n-1)\dots(q-l+1)}{(l_1-n_1)!(l_2-n_2)!\dots(l_k-n_k)!},$$

because we must first remove the repetitions arising within each $\prod_{j=1}^{l_i} (T_i + a_{ij})$ - and given such an expression $b_1 \dots b_{l-n}$, the number of terms from which this arises, comes from choosing $(T_1 - c_1)(T_1 - c_2)\dots(T_1 - c_{l_1-n_1})$ for T_1 , and similarly for the other T_i 's. The number of such choices is $(q-n)(q-n-1)\dots(q-l+1)$, but the repetitions for each T_i must be factored out, and this is precisely what is done above.

Moreover, this above coefficient can be rewritten as

$$\binom{n}{n_1, \dots, n_k} \binom{q-n}{l_1-n_1, \dots, l_k-n_k, q-l}.$$

We are now ready to compute the desired quantity. For each fixed (n_1, \dots, n_k) with $0 \leq n_i \leq l_i \forall i$, we compute the coefficient of $\prod_i T_i^{n_i}$ in $\Sigma_{l_1, \dots, l_k}(T_1, \dots, T_k)$, to be

$$\binom{n}{n_1, \dots, n_k} \binom{q-n}{l_1-n_1, \dots, l_k-n_k, q-l} \Sigma_{l-n}(0).$$

By Proposition 9, this is zero unless $q-1 \leq l-n \leq l \leq q$. Thus, we have only two cases:

- $l = q-1$. Then the only (possible) nonzero contribution occurs when $n = 0$. Thus, we examine the constant term here, and it equals

$$\binom{0}{0, \dots, 0} \binom{q}{l_1, \dots, l_k, 1} = q \cdot \binom{q-1}{l_1, \dots, l_k},$$

where $\sum_i l_i = q-1$. But then q divides this integer, whence the answer is zero.

- $l = q$. Then we need to explore the constant and linear terms. The constant term equals

$$\binom{0}{0, \dots, 0} \binom{q}{l_1, \dots, l_k, 0} \Sigma_q(0),$$

and by Proposition 9, the last factor is zero. The linear term corresponding to a fixed T_i (without loss of generality, assume $i = 1$) equals

$$\binom{1}{1, 0, \dots, 0} \binom{q-1}{l_1-1, l_2, \dots, l_k, 0} \Sigma_{q-1}(0) = -\binom{q-1}{l_1-1, l_2, \dots, l_k}$$

by Proposition 9. We are done. □

We end with a couple of questions, the first of which asks how to compute the common generalization of the previous two results. Given $k, l_1, \dots, l_k \in \mathbb{N}$ such that $l := \sum_i l_i \leq q$, also choose $n_{ij} > 0$ for each $1 \leq i \leq k$ and $1 \leq j \leq l_i$. Now define

$$\Sigma_{l_1, \dots, l_k}^{((n_{ij}))}(T_1, \dots, T_k) = \sum_{((a_{ij})) \in I(l)} \prod_{i=1}^k \prod_{j=1}^{l_i} (T_i + a_{ij})^{n_{ij}}.$$

This is a generalization of various special cases defined above:

$$\Sigma_{l_1, \dots, l_k}^{((1))}(T_1, \dots, T_k) = \Sigma_{l_1, \dots, l_k}(T_1, \dots, T_k), \quad \Sigma_{l_1}^{(n_{1j})}(T_1) = \Sigma^{n_{11}, n_{12}, \dots, n_{1l_1}}(T_1).$$

Question 12. Is it also a polynomial with integer coefficients? Also - compute this expression explicitly!

We also pose a (simpler) question, generalizing our original motivation for this note: Theorem 1.

Question 13. Compute explicitly the expression $\Sigma^{n_1, \dots, n_l}(T)$ as a polynomial in $T^q - T$.

APPENDIX A. TRANSLATION-INVARIANT RATIONAL FUNCTIONS

In this appendix, we discuss the notion of translation-invariant polynomials and rational functions in any number of variables, over any ground field. Given a field F and $k \in \mathbb{N}$, we define \mathbf{T}_k to mean the vector (T_1, \dots, T_k) . Thus, $F[\mathbf{T}_k] = F[T_1, \dots, T_k]$, and $F(\mathbf{T}_k) = F(T_1, \dots, T_k)$. We now have the obvious *translation* map $\tau : F^k \rightarrow \text{Aut}(F(\mathbf{T}_k))$, given by

$$\tau(\mathbf{a})(f)(T_1, \dots, T_k) := f(T_1 + a_1, \dots, T_k + a_k) = f(\mathbf{T}_k + \mathbf{a}),$$

where $\mathbf{a} = (a_1, \dots, a_k) \in F^k$. Now given $Q \subset F^k$, we say f is *Q-translation-invariant*, denoted by $f \in F(\mathbf{T}_k)^{\tau(Q)}$, if $\tau(\mathbf{q})(f) = f$ for all $\mathbf{q} \in Q$. Given $S \subset F$, we say that f is *S-translation-invariant* if $f \in F(\mathbf{T}_k)^{\tau((S \cup \{0\})^k)}$.

We now discuss the notion of *S-translation-invariant* rational functions $f \in F(T_1, \dots, T_k)$. We present some preliminaries, before stating and proving our main result.

Proposition 14. *Given $Q \subset G$ (a group), let $\langle Q \rangle$ be the additive subgroup generated by Q .*

- (1) τ is an isomorphism of groups $: F^k \rightarrow \text{Aut}(F(\mathbf{T}_k))$.
- (2) Given $Q \subset P \subset F^k$ and $S \subset F$, we have

$$F(\mathbf{T}_k)^{\tau(P)} \subset F(\mathbf{T}_k)^{\tau(Q)} = F(\mathbf{T}_k)^{\tau(\langle Q \rangle)}, \quad F(\mathbf{T}_k)^{\tau((S \cup \{0\})^k)} = F(\mathbf{T}_k)^{\tau(\langle S \rangle^k)}.$$

- (3) If $H \subset F$ is infinite, and $f(b_1, \dots, b_k) = 0$ for all $b_i \in H$ (for all i) and some $f \in F(T_1, \dots, T_k)$, then f is identically zero.
- (4) If T_1, \dots, T_k are algebraically independent elements (over a commutative unital ring R), and $f_i \in R[T]$ are nonconstant monic polynomials, then $\{f_i(T_i) : 1 \leq i \leq k\}$ are also algebraically independent over R .
- (5) (Multiple Factor Theorem.) Given $f(T) \in R[T]$, if $f(a_1) = f(a_2) = \dots = f(a_k) = 0$ for $a_i \in R$, and $a_i - a_j$ is not a zerodivisor in R for $i \neq j$, then $\prod_{i=1}^k (T - a_i)$ divides f .

Proof.

- (1) This is easy to verify.
- (2) We first show the first equation. The first inclusion (and the “reverse inclusion” in the equality) are easy to show. To show the “other” inclusion in the equality, if $\mathbf{q}, \mathbf{q}' \in Q$, then by the previous part,

$$\tau(\mathbf{q} + \mathbf{q}')(f) = \tau(\mathbf{q})(\tau(\mathbf{q}')(f)) = f, \quad \tau(-\mathbf{q})(f) = \tau(-\mathbf{q})(\tau(\mathbf{q})(f)) = \tau(-\mathbf{q} + \mathbf{q})(f) = f,$$

whence we are done.

Next, to show the second equality, one inclusion follows from the first equation. Conversely, we claim that $\langle (S \cup \{0\})^k \rangle = \langle S \rangle^k$, which proves the reverse inclusion (again using the first equation). But this claim is easy to check: to obtain all of $\langle S \rangle$ in a given coordinate, use the zero element in all other coordinates.

- (3) Suppose $f = r/s$, with $r, s \in F[T_1, \dots, T_k]$; then $r(b_1, \dots, b_k) = 0 \forall i, b_i \in H$. So it suffices to show the result for r , i.e., when $f \in F[T_1, \dots, T_k]$. The proof is by induction on k . If $k = 1$, then f is a polynomial in one variable with infinitely many roots (in $H \subset F$); hence it vanishes. Now assume the result for $k - 1$. Write a given nonzero polynomial as $f(T_1, \dots, T_k) = \sum_{i=0}^{\infty} f_i(T_1, \dots, T_{k-1})T_k^i$ for some polynomials f_i , say. Fix i_0 such that $f_{i_0} \neq 0$. Now choose $b_1, \dots, b_{k-1} \in H$ by the induction hypothesis, such that $f_{i_0}(b_1, \dots, b_{k-1})$ is nonzero. But then $f(b_1, \dots, b_{k-1}, T_k)$ is a nonzero polynomial in one variable, and we choose $b_k \in H$ that is not a root of this polynomial. This proves the result by induction on k .
- (4) If $0 \neq f \in R[T_1, \dots, T_k]$, then we claim that $f(f_1(T_1), \dots, f_k(T_k))$ is itself a nonzero polynomial in $R[T_1, \dots, T_k]$ (and this will prove the claim). To see this, choose the monomial in f with largest degree in T_1 ; then among these, the largest degree in T_2 ; and so on. Say this monomial is $c \prod_{i=1}^k T_i^{n_i}$. Also define $d_i := \deg f_i$. Then the corresponding “largest” monomial in $f(f_1, \dots, f_k)$ is $c \prod_{i=1}^k T_i^{d_i n_i}$, which is not zero since $c \neq 0$.
- (5) We prove this using the Factor Theorem (a part of Proposition 2), by induction on k . The base case of $k = 1$ follows from the Factor Theorem. Now suppose we know the result for $k - 1$, and let a_1, \dots, a_{k-1}, a_k be pairwise distinct roots of f . Set $g(T) = \prod_{i=1}^{k-1} (T - a_i)$. Thus, $T - a_k$ and $g(T)$ both divide $f(T)$, so using the Euclidean algorithm, suppose that $f(T) = g(T)h(T)$ for some $h \in R[T]$. Evaluating both sides at a (using the Factor Theorem), $f(a_k) = 0$. Since $g(a_k)$ is not a zerodivisor, $h(a_k) = 0$ and $(T - a_k) | h = (f/g)$. We are done by induction. □

Our next result explores some properties of the polynomials $\zeta_{\langle S \rangle}(T)$, when $\langle S \rangle$ is finite.

Proposition 15. *Suppose R is any commutative unital ring, and $\langle S \rangle \subset R$ is finite for some $S \subset R$. If $H \subset R$ is finite, define $\zeta_H(T) := \prod_{s \in H} (T - s) \in R[T]$.*

- (1) *If $\langle S \rangle \neq \{0\}$ and R is an integral domain, then $\langle 1_R \rangle \subset R$ has finite size $p > 0$, and $\langle S \rangle$ is an \mathbb{F}_p -vector-subspace of R . (Here, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)*
- (2) *$\zeta_{\langle S \rangle}(T) \in R[T]$ is S -translation-invariant.*

Now also suppose that $\langle 1_R \rangle \subset R$ has size p .

- (3) $\zeta_{\langle S \rangle}(T)$ is a monic polynomial in $R[T]$, of degree $|\langle S \rangle|$. If T^n is a monomial occurring in $\zeta_{\langle S \rangle}(T)$ with nonzero coefficient, then n is a power of p , between T^{p^0} and $T^{p^{\dim(S)}} = T^{|\langle S \rangle|}$.
- (4) $\zeta_{\langle S \rangle} : R \rightarrow R$ is a map of additive groups, but not necessarily of rings.
- (5) $\zeta_{\langle S \rangle}(aT) = a\zeta_{\langle S \rangle}(T)$ for all $a \in \mathbb{F}_p$.

When $\langle S \rangle \subset F$ is finite, the polynomials $\zeta_{\langle S \rangle}(T)$ give us our first examples of S -translation-invariant polynomials and rational functions. We will see below that these are the *only* nontrivial examples (in some sense).

Proof.

- (1) If $\langle S \rangle$ is finite and $0 \neq a \in \langle S \rangle$, then $\langle 1_R \rangle \cdot a \subset S$, where $\langle 1_R \rangle$ is the additive subgroup generated by $1 = 1_R$ in R . For this to be a finite set, we need that $\langle 1_R \rangle$ is finite (since R is an integral domain). But then the kernel of the map $:\mathbb{Z} \rightarrow R$ must be a prime ideal, say (p) . Then for all $n \in \mathbb{Z}$ and $a \in \langle S \rangle$, we have: $na = a + a + \dots + a = \bar{n}a \in \langle S \rangle$, where \bar{n} is the image of n in \mathbb{F}_p under the obvious quotient map. That $\langle S \rangle \subset R$ is an \mathbb{F}_p -vector subspace is now easy to prove.
- (2) This is not hard to show, since adding any $s \in \langle S \rangle$ (e.g., $s \in S$) simply rearranges the set $\{T - s' : s' \in \langle S \rangle\}$, and hence preserves their product.
- (3) For the rest of this proposition, we assume that $\langle 1_R \rangle \subset R$ is finite of size p . We show this by induction on the dimension of the \mathbb{F}_p -vector space $\langle S \rangle \subset R$. Suppose v_1, \dots, v_n is a basis. We now work with “universal coefficients”, i.e., in the field $F = \mathbb{F}_p[X_1, \dots, X_n]$. (In his textbook, Michael Artin calls this *permanence of identities*.) The point is that if we can show the result in $F[T]$, then we can show it in $R[T]$, by mapping $\mathbb{F}_p[X_1, \dots, X_n] \rightarrow R$, sending $X_i \mapsto v_i$. (This is because the result actually holds in $\mathbb{F}_p[X_1, \dots, X_n][T]$ inside $F[T]$.)

We show the result in $F[T]$ by induction on n . When $n = 1$, we compute:

$$\prod_{a \in \mathbb{F}_p} (T - aX_1) = X_1^p \prod_{a \in \mathbb{F}_p} (T/X_1 - a) = X_1^p ((T/X_1)^p - (T/X_1)) = T^p - TX_1^{p-1},$$

which is monic of degree p^1 , in $\mathbb{F}_p[T]$, and whose only nonzero terms correspond to T^1 and T^p .

To show the general case, assume that we know the result for $n - 1$. Let S' denote the span of X_1, \dots, X_{n-1} . Then

$$\zeta_{\langle S \rangle}(T) = \prod_{a \in \mathbb{F}_p, s' \in S'} (T - aX_n - s') = \prod_{a \in \mathbb{F}_p} \zeta_{S'}(T - aX_n).$$

By the induction hypothesis, suppose that $\zeta_{S'}(T) = T^{p^{n-1}} + \sum_{i=0}^{n-2} \alpha_i T^{p^i}$. Then since $a^{p^i} = a \forall a \in \mathbb{F}_p$, and the Frobenius “ p -th power map” $\phi : R \rightarrow R$ (sending $r \mapsto r^p$) is an \mathbb{F}_p -algebra homomorphism, hence

$$\zeta_{\langle S \rangle}(T) = \prod_{a \in \mathbb{F}_p} (T^{p^{n-1}} - aX_n^{p^{n-1}} + \sum_{i=0}^{n-2} \alpha_i (T^{p^i} - aX_n^{p^i})) = \prod_{a \in \mathbb{F}_p} (\zeta_{S'}(T) - a\zeta_{S'}(X_n)). \quad (16)$$

By our base case, this equals $\zeta_{S'}(T)^p - \zeta_{S'}(T)\zeta_{S'}(X_k)^{p-1}$. Again using ϕ , we get that $\zeta_{\langle S \rangle}(T) \in R[T]$ is monic of degree $|\langle S \rangle|$, and the only monomials that occur have degrees that are powers of p .

Finally, we remark that not all powers of p need have nonzero coefficient in $\zeta_{\langle S \rangle}(T)$. For instance, let $S = \langle S \rangle = R = \mathbb{F}_q$ for some $q = p^n$. Then $\zeta_{\langle S \rangle}(T) = T^q - T$ from above.

- (4) This result was essentially proved in Equation (16), but we write down a proof here for the convenience of the reader. By the previous part, suppose $\zeta_{\langle S \rangle}(T) = T^{p^n} + \sum_{i=0}^{n-1} \alpha_i T^{p^i}$ for some $\alpha_i \in R$. Then

$$\zeta_{\langle S \rangle}(a+b) = (a+b)^{p^n} + \sum_{i=0}^{n-1} \alpha_i (a+b)^{p^i} = \zeta_{\langle S \rangle}(a) + \zeta_{\langle S \rangle}(b),$$

by applying ϕ^i to $a+b$ for each summand, and ϕ^n to $a+b$ for the first term. Finally, $\zeta_{\langle S \rangle}$ is not a ring map: for instance, consider $R = \mathbb{F}_p[T, U]$ and $S = \langle S \rangle = \mathbb{F}_p$. Then for p odd, one checks that $\zeta_{\langle S \rangle}(T)\zeta_{\langle S \rangle}(U) = (T^p - T)(U^p - U) \neq \zeta_{\langle S \rangle}(TU)$.

- (5) From a previous part, since $\zeta_{\langle S \rangle}(T) = \sum_{i=0}^{\dim \langle S \rangle} \alpha_i T^{p^i}$ for some $\alpha_i \in R$, hence for all $a \in \mathbb{F}_p$,

$$\zeta_{\langle S \rangle}(aT) = \sum_{i=0}^{\dim \langle S \rangle} \alpha_i a^{p^i} T^{p^i} = \sum_{i=0}^{\dim \langle S \rangle} \phi^i(a) \alpha_i T^{p^i} = \sum_{i=0}^{\dim \langle S \rangle} a \cdot \alpha_i T^{p^i} = a \zeta_{\langle S \rangle}(T),$$

since $\phi : \mathbb{F}_p \rightarrow \mathbb{F}_p$ is the identity map. □

We also see from the above proof, that we can inductively write down a formula for $\zeta_{\langle S \rangle}(T)$, where the \mathbb{F}_p -vector space $\langle S \rangle$ has basis $\{X_1, \dots, X_n\}$. Namely, inductively define

$$g_0(T) := T, \quad g_{i+1}(T) = g_i(T)^p - g_i(T)g_i(X_{i+1})^{p-1}.$$

Then $\zeta_{\langle S \rangle}(T) = g_n(T)$. Thus, it makes sense to study $g_n(T)$ - as a function of the X_i 's as well. We do so in a later section.

For now, we end this section by classifying all S -translation-invariant polynomials and rational functions over all fields F , where $S \subset F$.

Theorem 17. *Suppose $S \subset F$ is a subset of a field.*

- (1) *If $\langle S \rangle \subset F$ is infinite, then the only S -translation-invariant rational functions $F(\mathbf{T}_k)^{\tau(\langle S \rangle^k)}$ are constants.*
- (2) *Suppose $\langle S \rangle \subset F$ is finite, and $f \in F(\mathbf{T}_k)$. Then f is S -translation-invariant if and only if $f(\mathbf{T}_k) = g(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_k))$ for some $g \in F(\mathbf{T}_k)$.*
- (3) *Suppose R is an integral domain (with unity), $f \in R[T_1, \dots, T_k]$, and $S \subset R$ is such that $\langle S \rangle \subset R$ is finite. Then f is S -translation-invariant if and only if $f(\mathbf{T}_k) = g(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_k))$ for some $g \in R[\mathbf{T}_k]$.*

Furthermore, if $\langle S \rangle$ is not a singleton, then R contains a unique prime subfield $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and the above implies that f factors to a well-defined function on the \mathbb{F}_p -vector space $R/\langle S \rangle$ - but the converse is false.

Thus, for all fields F and integral domains R containing a finite abelian group $\langle S \rangle$,

$$F(\mathbf{T}_k)^{\tau(\langle S \rangle^k)} = F(\zeta_{\langle S \rangle}(\mathbf{T}_k)), \quad R[\mathbf{T}_k]^{\tau(\langle S \rangle^k)} = R[\zeta_{\langle S \rangle}(\mathbf{T}_k)].$$

For example, suppose that $F = \mathbb{F}_q$ is a finite field and $S = \mathbb{F}_{p^m}$ for some $m|n$, where $q = p^n$ and $p \in \mathbb{N}$ is prime. Then $\zeta_{\langle S \rangle}(T) = T^{p^m} - T$. Here is another example: if $S = \{X\} \subset F = \mathbb{F}_p(X)$, then $\zeta_{\langle S \rangle}(T) = T^p - TX^{p-1}$.

Proof. We first note that if $\langle S \rangle$ is a singleton set, then $\langle S \rangle = \{0\}$ and $\zeta_{\langle S \rangle}(T_i) = T_i \forall i$, which proves the theorem trivially. Thus, we now assume that $|\langle S \rangle| > 1$, whence by Proposition 14, F or $F(R)$ (the quotient field of R) has positive characteristic p , and $\langle S \rangle$ is an \mathbb{F}_p -vector subspace of F (or R).

- (1) We now show this part using Proposition 14. Given $f = u/v$ for $u, v \in F[\mathbf{T}_k]$, choose $a_1, \dots, a_k \in F$ such that $v(a_1, \dots, a_k) \neq 0$ (by the above claim for $H = F$). Now define

$$g(\mathbf{T}_k) := v(a_1, \dots, a_k)u(T_1 + a_1, \dots, T_k + a_k) - u(a_1, \dots, a_k)v(T_1 + a_1, \dots, T_k + a_k).$$

Since $u(T_1, \dots, T_k)/v(T_1, \dots, T_k) - u(T_1 + b_1, \dots, T_k + b_k)/v(T_1 + b_1, \dots, T_k + b_k) = 0$ for all $b_i \in \langle S \rangle$ (by Proposition 14), we now take common denominators, and multiply both sides by these denominators. Evaluating now at $T_i \mapsto a_i$ yields: $g(b_1, \dots, b_k) = 0 \forall b_i \in \langle S \rangle$. By Proposition 14 (for $H = \langle S \rangle$), g is identically zero. If we denote $\mathbf{a} = (a_1, \dots, a_k)$, then we get

$$\frac{u(\mathbf{T}_k)}{v(\mathbf{T}_k)} - \frac{u(\mathbf{a})}{v(\mathbf{a})} = \tau(-\mathbf{a}) \left(\frac{u(\mathbf{T}_k + \mathbf{a})}{v(\mathbf{T}_k + \mathbf{a})} - \frac{u(\mathbf{a})}{v(\mathbf{a})} \right) = \tau(-\mathbf{a})(0) = 0,$$

where the second equality holds because $g(\mathbf{T}_k)$ is identically zero. But then $f = u/v$ equals $u(\mathbf{a})/v(\mathbf{a})$, which is a constant.

- (2) We first prove the base case of $k = 1$ by induction on $d := \deg(g) + \deg(h)$, where $f(T) = g(T)/h(T)$. If $d = 0$, then both g and h are constants, and we are done. Now suppose that we know the result for all $d < N$, where $\deg(g) + \deg(h) = N$ and $f = g/h$. If $\zeta_{\langle S \rangle}(T) \mid g(T)$, then $(g(T)/\zeta_{\langle S \rangle}(T))/h(T)$ is S -translation-invariant, and with a smaller value of N . The case when $\zeta_{\langle S \rangle}(T) \mid h(T)$ is similar.

Thus, suppose that $\zeta_{\langle S \rangle}(T)$ divides neither g nor h . If $\deg g < \deg h$, then we can consider $1/f = h/g$, which is also S -translation-invariant. Hence we may restrict ourselves to the case when $\deg g \geq \deg h$. Since $\zeta_{\langle S \rangle}(T) \nmid h(T)$, hence there exists $a \in F$ such that $h(a) \neq 0$. Then $f(T)$ is S -translation-invariant if and only if $f(T) - f(a)$ is. (Note that each such step - replacing $f(T)$ by $1/f(T)$, or by $f(T) - f(a)$ - does not increase the value of $\deg(g) + \deg(h)$.)

But now $f(T) - f(a)$ is S -translation-invariant, and vanishes at a , whence it vanishes at all $b \in F$. Writing it as a fraction $g_3(T)/h_3(T)$, we see that $\zeta_{\langle S \rangle}(T)$ must divide $g_3(T)$. But then $(g_3(T)/\zeta_{\langle S \rangle}(T))/h_3(T)$ is also S -translation-invariant, and has a smaller d -value. By the induction hypothesis, it must equal $r_1(\zeta_{\langle S \rangle}(T))/s_1(\zeta_{\langle S \rangle}(T))$ for some polynomials $r_1, s_1 \in F[T]$. Since we arrived at this polynomial by subtracting constants and multiplying by a (positive or negative) power of $\zeta_{\langle S \rangle}(T)$, hence the same conclusion holds for the original function $f(T)$ as well.

Conversely, every function of the form $r(\zeta_{\langle S \rangle}(T))/s(\zeta_{\langle S \rangle}(T))$ is clearly translation-invariant.

We now prove the general case. Given the result for $k - 1$, write $f(\mathbf{T}_k) = h(T_1, \dots, T_{k-1})$, for some $h \in F(T_k)$. Now replace F by $F(T_k)$, and note that h is S -translation-invariant. Hence by the induction hypothesis, $h(T_1, \dots, T_{k-1}) = h_1(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_{k-1}))$ for some $h_1 \in F(T_k)(T_1, \dots, T_{k-1})$. By Proposition 14, the elements $\zeta_{\langle S \rangle}(T_i)$ are algebraically independent over F . Hence

$$F(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_{k-1})) \cong F(T_1, \dots, T_{k-1}).$$

Now write $h_1(\{\zeta_{\langle S \rangle}(T_i)\})$ in the other way, as

$$h_1(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_{k-1})) = \frac{p(T_k)}{q(T_k)}, \quad p, q \in F(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_{k-1}))[T_k].$$

Since this is S -translation-invariant as a polynomial in T_k alone, hence from above, it is in $F(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_{k-1}))(\zeta_{\langle S \rangle}(T_k))$, and we are done. Conversely, this field is clearly contained in $F(\mathbf{T}_k)^{\tau(\langle S \rangle^k)}$, since $\zeta_{\langle S \rangle}(T_i)$ is S -translation-invariant for all i by Proposition 15.

- (3) Let $F = F(R)$, the quotient field of R . One implication is obvious by the previous part, since every polynomial is also a rational function:

$$R[\zeta_{\langle S \rangle}(\mathbf{T}_k)] \subset F[\zeta_{\langle S \rangle}(\mathbf{T}_k)] \cap R[\mathbf{T}_k] \subset F(\mathbf{T}_k)^{\tau(\langle S \rangle^k)} \cap R[\mathbf{T}_k] = R(\mathbf{T}_k)^{\tau(\langle S \rangle^k)}.$$

Also note that by the first inclusion above, that the $\zeta_{\langle S \rangle}(T_i)$ are algebraically independent over R , since they are algebraically independent over F by Proposition 14.

We now show the converse. If $f \in R[\mathbf{T}_k]^{\tau(\langle S \rangle)}$, then by the previous part, f is a rational function of all $\zeta_{\langle S \rangle}(T_i)$ (over F). We prove that S -translation-invariance implies that f is a polynomial in the $\zeta_{\langle S \rangle}(T_i)$ (with coefficients in R). The base case (wherein $f \in R[T]$) essentially follows from the previous part: if $f \in R[T]$ is S -translation-invariant, it is of the form $r(\zeta_{\langle S \rangle}(T))/s(\zeta_{\langle S \rangle}(T))$ for some r, s . Using the Euclidean algorithm, write $r = sg + h$, where $\deg h < \deg s$ (or $h = 0$). Then

$$(f(T) - g(\zeta_{\langle S \rangle}(T)))s(\zeta_{\langle S \rangle}(T)) = h(\zeta_{\langle S \rangle}(T)).$$

But since $\deg s > \deg h$ or $h = 0$, and $s(\zeta_{\langle S \rangle}(T))$ can never be zero if s is not, hence this is only possible if $h = 0$, whence $f(T) = g(\zeta_{\langle S \rangle}(T))$ as desired. Thus, $f \in R[T] \cap F[\zeta_{\langle S \rangle}(T)] = R[\zeta_{\langle S \rangle}(T)]$.

We now prove the result for general k , by induction on the total degree of $f \in R[T_1, \dots, T_k]$. Given that the result is true for $k - 1$ for polynomials of all total degree, and for k for polynomials of total degree at most d , suppose f has total degree $d + 1$. Now consider $g(T_k) = f(T_1, \dots, T_k) - f(T_1, \dots, T_{k-1}, 0)$. This is S -translation-invariant in the last argument, whence it is divisible by $\zeta_{\langle S \rangle}(T_k)$ (by the ‘‘Multiple Factor Theorem’’ 14).

We now have two cases. The first is that $g(T_k)$ is the zero polynomial - whence f is actually in $F[T_1, \dots, T_{k-1}]$ (and hence in $R[T_1, \dots, T_k]$) and we are done by

induction. Otherwise if $g(T_k) \neq 0$, divide it by $\zeta_{\langle S \rangle}(T_k)$, and consider the quotient $f_1(T_1, \dots, T_k)$. For all $a_i \in S$, we compute:

$$f_1(T_1 + a_1, \dots, T_k + a_k) = \frac{f(T_1 + a_1, \dots, T_k + a_k) - f(T_1 + a_1, \dots, T_{k-1} + a_{k-1}, 0 + a_k)}{\zeta_{\langle S \rangle}(T_k + a_k)}.$$

As above, since f and $\zeta_{\langle S \rangle}$ are both S -translation-invariant, this expression equals $f_1(T_1, \dots, T_k)$. We are now done by the induction hypothesis, since the total degree of f_1 is strictly less than that of f .

We next show the remaining assertions. If $f(T_1, \dots, T_k) = g(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_k))$, then

$$f(\{T_i + a_i\}) = g(\{\zeta_{\langle S \rangle}(T_i + a_i)\}) = g(\{\zeta_{\langle S \rangle}(T_i)\}) = f(\mathbf{T}_k),$$

since $\zeta_{\langle S \rangle}$ is S -translation-invariant and $a_i \in S \forall i$. Hence f is S -translation-invariant.

Finally, if f is S -translation-invariant, find g as above; then for all $a_1, \dots, a_k \in \langle S \rangle$ and $b_i \in R$,

$$f(b_1 + a_1, \dots, b_k + a_k) = g(\{\zeta_{\langle S \rangle}(b_i + a_i)\}) = g(\{\zeta_{\langle S \rangle}(b_i)\}) = f(b_1, \dots, b_k).$$

In particular, this value is independent of the a_i 's, and we get a well-defined function on $R/\langle S \rangle$. However, the converse fails: let $S = R = F = \mathbb{F}_q$ for any fixed finite field \mathbb{F}_q of size q . Then $\zeta_{\langle S \rangle}(T) = T^q - T$, and for any fixed $b \in F$, the polynomial $T_1 \zeta_{\langle S \rangle}(T_1) + b = T_1(T_1^q - T_1) + b$ equals b at all $(a_1, \dots, a_k) \in S^k = \mathbb{F}_q^k$. But it is not a polynomial in the $\zeta_{\langle S \rangle}(T_i)$. □

We now note that there is a more conceptual, and less computational proof of this same result, which uses Galois theory; we mention this now. First, we need a few preliminary definitions from the subject.

Theorem 18. *A finite extension $L : K$ is Galois if L is the splitting field of a polynomial in $K[T]$ with no repeated roots (in any algebraic closure of K). In such a case,*

$$L^{\text{Aut}_K(L)} = K, \quad |\text{Aut}_K(L)| = [L : K],$$

where the first equality describes the elements of L fixed by the Galois group $\text{Aut}_K(L)$.

Alternate proof of Theorem 17. We now show using Galois Theory, that $\tau(G) = \text{Aut}_K(L)$, where

$$L = F(\mathbf{T}_k) \supset K = F(\zeta_{\langle S \rangle}(T_1), \dots, \zeta_{\langle S \rangle}(T_k))$$

is a Galois extension, and $G = \langle S \rangle^k$ is (isomorphic to) its Galois group. Define $U_i := \zeta_{\langle S \rangle}(T_i)$ for all i ; then by Proposition 14, the U_i 's are algebraically independent over F . Now define

$$g(T) = \prod_{i=1}^k \left(\prod_{s \in \langle S \rangle} (T - s) - U_i \right).$$

In $L = F(\mathbf{T}_k)$, the roots of the i th factor of g are precisely the elements $\{T_i - s : s \in \langle S \rangle\}$. These are all pairwise distinct (across all i as well), and generate L over K . Since splitting

fields are unique up to isomorphism (as are algebraic closures), hence $L : K$ is a Galois extension by Theorem 18. But one now checks that $G \cong \tau(G) \subset \text{Aut}_K(L)$: for any $s_i \in \langle S \rangle$, if $\mathbf{s} = (\{s_i\})$, then $\tau(\mathbf{s}) \in \text{Aut}(L)$ from above, and for all i ,

$$\tau(\mathbf{s})(U_i) = \prod_{s \in \langle S \rangle} \tau(s_i)(T_i - s) = \prod_{s \in \langle S \rangle} (T_i - s + s_i) = \prod_{s \in \langle S \rangle} (T_i - s) = U_i,$$

where the penultimate equality follows by reindexing. Hence $\tau(G) \subset \text{Aut}_K(L)$.

We now claim that $[L : K] = |\langle S \rangle|^k$. Before we prove this, let us see why this finishes the proof of the theorem: by Theorem 18,

$$|\text{Aut}_K(L)| = [L : K] = |\langle S \rangle|^k = |G| = |\tau(G)|,$$

and $\tau(G) \subset \text{Aut}_K(L)$. Hence the two groups are equal, whence $L^{\text{Aut}_K(L)} = L^G = L^{\tau(G)} = K$, as desired.

Thus, it suffices to prove the claim. Let $f_i(T) := \prod_{s \in \langle S \rangle} (T - s) - U_i \in K[T]$. We also set

$$K \subset L_i := F(\{T_1, \dots, \widehat{T}_i, \dots, T_k\})(U_i) \subset L.$$

Note that the elements $T_j (j \neq i)$ and U_i are algebraically independent in L (and hence in L_i) by Proposition 14. We now claim that $L_i[T]/(f_i(T)) \cong L$ for all i . In other words, we are claiming that f_i is the minimal polynomial of T_i over L_i . To see this, since $f_i(T_i) = 0$, it suffices to prove that f_i is irreducible. We now use Proposition 2. Since $G = \langle S \rangle^k \hookrightarrow \text{Aut}_K(L)$, hence $\tau(\mathbf{s})(T_i)$ is a root of $m(T)$ for all $\mathbf{s} \in \langle S \rangle^k$. (Here, $m(T)$ is the minimal polynomial of T_i over K ; thus, $m|f_i$.) The orbit of this on T_i is $\{T_i + s : s \in \langle S \rangle\}$, so $\prod_{s \in \langle S \rangle} (T - T_i - s) = \zeta_{\langle S \rangle}(T - T_i)$ divides $m(T)$. But by Proposition 15,

$$f_i(T) = \zeta_{\langle S \rangle}(T) - U_i = \zeta_{\langle S \rangle}(T) - \zeta_{\langle S \rangle}(T_i) = \zeta_{\langle S \rangle}(T - T_i) \mid m(T) \mid f_i(T),$$

whence $m(T) = f_i(T)$ in $L[T]$. But both polynomials here are in $K[T]$, so we are done.

Finally, since all $T_j (j \neq i)$ and U_i are algebraically independent in L , hence we can now consider the tower of fields:

$$K = K_0 \subset K_1 \subset \dots \subset K_k = L,$$

where $K_i := K(T_1, \dots, T_i)$. We then claim that $K_i[T]/(f_i(T)) \cong K_{i+1}$ for all i ; this follows from the above arguments. Hence

$$[K_{i+1} : K_i] = \deg m = \deg f_i = |\langle S \rangle|$$

from above. But then by the Tower Law for fields,

$$[L : K] = \prod_{i=0}^{k-1} [K_{i+1} : K_i] = \prod_{i=0}^{k-1} |\langle S \rangle| = |\langle S \rangle|^k,$$

and we are done. Moreover, (also by the Tower Law,) $\{T_1^{n_1} \dots T_k^{n_k} : 0 \leq n_i < |\langle S \rangle| \forall i\}$ is a K -basis for L . \square

APPENDIX B. THE GENERATING TRANSLATION-INVARIANT POLYNOMIAL

As seen in Theorem 17, the polynomials $\zeta_{\langle S \rangle}(T)$ are S -translation-invariant, and generate all invariant polynomials (or rational functions) when $\langle S \rangle \subset R$ (or F) is finite. As above, we saw that if $\langle S \rangle$ has finite basis $\{X_1, \dots, X_n\}$ over some finite field $\mathbb{F}_p \subset R$ (or F), then $\zeta_{\langle S \rangle}(T) = g_n(T)$, where

$$g_0(T) := T, \quad g_{i+1}(T) = g_i(T)^p - g_i(T)g_i(X_{i+1})^{p-1}.$$

We now take a closer look at the polynomials g_n . Our first remark is that they should be considered as (symmetric) polynomials $g_n(T, X_1, \dots, X_n)$ in the X_i 's as well. Clearly, they also satisfy the properties mentioned in Proposition 15. In this section, we exhibit some of the large amounts of symmetry that they possess, as well as a formula for them. As earlier, we note that these properties and the formula for

$$g_n(T, X_1, \dots, X_n) \in \mathbb{F}_p[X_1, \dots, X_n][T]$$

can then be applied to computing $\zeta_{\langle S \rangle}(T)$ in any ring R , by evaluating $g_n(T, X_1, \dots, X_n)$ at an \mathbb{F}_p -basis of $\langle S \rangle$ (in place of the X_i 's).

Proposition 19. *Define $g_n(T, X_1, \dots, X_n) \in \mathbb{F}_p[T, X_1, \dots, X_n]$ to be $\prod_{v \in V_n} (T - v)$, where V_n is the \mathbb{F}_p -vector subspace of $\mathbb{F}_p[T, X_1, \dots, X_n]$ with basis $\{X_1, \dots, X_n\}$. (When $n = 0$, define $g_0(T) := T$.) We may also write it as $g_n(T, \mathbf{X}_n)$.*

(1) $g_n(T, \mathbf{X}_n)$ is symmetric in the X_i . More generally,

$$g_n(T + v_0, A(X_1), \dots, A(X_n)) = g_n(T, \mathbf{X}_n) \quad \forall A \in \text{Aut}_{\mathbb{F}_p}(V_n), \quad v_0 \in V_n.$$

(2) $g_n(T, \mathbf{X}_n) = T^{p^n} + \sum_{i=0}^{n-1} \alpha_i T^{p^i}$ for some $\alpha_i \in \mathbb{F}_p[\mathbf{X}_n] = \mathbb{F}_p[X_1, \dots, X_n]$.

(3) For all $a \in \mathbb{F}_p$,

$$g_n(aT, \mathbf{X}_n) = a g_n(T, \mathbf{X}_n), \quad g_n(T, \mathbf{X}_n)^p = g_n(T^p, X_1^p, \dots, X_n^p).$$

(4) If we fix $r_1, \dots, r_n \in R$, a unital commutative ring with $|\langle 1_R \rangle| = p$, then the map $g_n(-, r_1, \dots, r_n) : R \rightarrow R$ is \mathbb{F}_p -linear.

(5) For all $0 \leq m, n \in \mathbb{Z}$,

$$g_{m+n}(T, \mathbf{X}_{m+n}) = g_m(g_n(T, \mathbf{X}_n), g_n(X_{n+1}, \mathbf{X}_n), \dots, g_n(X_{n+m}, \mathbf{X}_n)).$$

Because of the permanence of identities, (suitable analogues of) the above results also hold when one replaces T, X_i by arbitrary elements in a commutative unital ring R with $|\langle 1_R \rangle| = p$.

Proof.

- (1) This follows from the definitions and the fact that the map $v \mapsto v_0 + Av$ (from $V_n \rightarrow V_n$) is actually a bijection.
- (2) This was shown in Proposition 15, with $R = \mathbb{F}_p[\mathbf{X}_n]$.
- (3) The first part was shown in Proposition 15 (where it was formulated using $\zeta_{\langle S \rangle}(T)$). To show the second part, use Proposition 3 for $n = 1$ and $\mathbb{F} = \mathbb{F}_p$, replacing the T_i 's by T, X_1, \dots, X_n , and f by g_n .

- (4) Consider the evaluation map π from $R' := \mathbb{F}_p[\mathbf{X}_n]$ to R , sending $X_i \mapsto r_i$. This extends to an \mathbb{F}_p -algebra homomorphism $\pi : R'[T] \rightarrow R[T]$. We now have to prove that $\pi \circ g_n : R \rightarrow R$ is \mathbb{F}_p -linear. But by the previous part (evaluated at $T = r$),

$$\pi(g_n(ar, \mathbf{X}_n)) = \pi(ag_n(r, \mathbf{X}_n)) = a\pi(g_n(r, \mathbf{X}_n)).$$

Moreover, that $\pi(g_n(-, \mathbf{X}_n))$ is additive was shown in Proposition 15. We are done.

- (5) We show this by induction on m . The base cases follow from Proposition 15, where we showed that

$$g_0(T) = T, \quad g_1(T, X_1) = T^p - TX_1^{p-1}, \quad g_{n+1}(T, \mathbf{X}_{n+1}) = g_1(g_n(T, \mathbf{X}_n), g_n(X_{n+1}, \mathbf{X}_n)).$$

Thus, we have shown the statement for $m = 0, 1$. Given the statement for general m , we compute:

$$\begin{aligned} g_{m+1+n}(T, \mathbf{X}_{m+n+1}) &= g_1(g_{m+n}(T, \mathbf{X}_{m+n}), g_{m+n}(X_{m+n+1}, \mathbf{X}_{m+n})) \\ &= g_1(g_m(g_n(T, \mathbf{X}_n), g_n(X_{n+1}, \mathbf{X}_n), \dots, g_n(X_{n+m}, \mathbf{X}_n)), \\ &\quad g_m(g_n(X_{n+m+1}, \mathbf{X}_n), g_n(X_{n+1}, \mathbf{X}_n), \dots, g_n(X_{n+m}, \mathbf{X}_n))) \\ &= g_{m+1}(g_n(T, \mathbf{X}_n), g_n(X_{n+1}, \mathbf{X}_n), \dots, g_n(X_{n+m+1}, \mathbf{X}_n)), \end{aligned}$$

where the last equality follows from the statement for $m = 1$, replacing n by m , T by $g_n(T, \mathbf{X}_n)$, and X_j (for $1 \leq j \leq m + 1$) by $g_n(X_{j+n}, \mathbf{X}_n)$ respectively. \square

To present a formula/expansion for (the coefficients α_i of) g_n , we now define another multivariate polynomial in $\mathbb{F}_p[T, \mathbf{X}_n]$, and explore its properties.

Proposition 20. *Given elements r_1, \dots, r_n of a commutative unital ring R with $|\langle 1_R \rangle| = p$ prime, define their p -alternator to be 1 if $n = 0$, and otherwise,*

$$\Lambda_p(r_1, \dots, r_n) := \sum_{\sigma \in S_n} (-1)^{\ell(\sigma)} r_{\sigma(1)}^{p^0} \cdots r_{\sigma(n)}^{p^{n-1}} = \sum_{\sigma \in S_n} (-1)^{\ell(\sigma)} \prod_{i=1}^n r_{\sigma(i)}^{p^{i-1}}.$$

- (1) Λ_p is the determinant of the $n \times n$ Van der Monde-type matrix $((r_i^{p^{j-1}}))$.
- (2) Λ_p is \mathbb{F}_p -linear and antisymmetric in its arguments. If A is any $n \times n$ matrix with entries in \mathbb{F}_p , and we define $Ar_i := \sum_{j=1}^n a_{ij} r_j$, then

$$\Lambda_p(A(r_1), \dots, A(r_n)) = \det(A) \cdot \Lambda_p(r_1, \dots, r_n).$$

- (3) $\Lambda_p(r_1, \dots, r_n)^p = \Lambda_p(r_1^p, \dots, r_n^p)$.

Proof. Once again, it suffices to show the result in $\mathbb{F}_p[\mathbf{X}_n]$ for X_i , since we can then map this ring to R , via $\pi : X_i \mapsto r_i \forall i$.

- (1) This follows from the definition of the determinant.
- (2) We use the basics of elementary row operations and Gaussian elimination. By the previous part, the p -alternator satisfies the usual properties of determinants (since the Frobenius map $\phi : \mathbb{F}_p[\mathbf{X}_n] \rightarrow \mathbb{F}_p[\mathbf{X}_n]$ is an \mathbb{F}_p -algebra homomorphism). In particular, it is \mathbb{F}_p -linear in each argument, and changes sign when two arguments are reversed. But then Λ_p is well-behaved under the three *elementary Gaussian*

(row/column) operations: $\Lambda_p(A(r_1), \dots, A(r_n)) = \det(A)\Lambda_p(r_1, \dots, r_n)$ for all elementary Gaussian matrices A .

Thus, it remains to proving the claim for all $A_{n \times n}$ in reduced row echelon form. If A is nonsingular, then A is the identity matrix, and the claim is trivial. Otherwise the last row of A is zero, which makes $A(r_n) = 0$, whence $\Lambda_p(A(r_1), \dots, A(r_n)) = 0$ by definition. Once again, we are done.

(3) This follows from Proposition 3, since $\Lambda_p(\mathbf{X}_n) \in \mathbb{F}_p[\mathbf{X}_n]$. □

We can now state and prove our main result, which relates these two polynomials.

Theorem 21. *For all $0 < n \in \mathbb{Z}$, and commutative unital rings R with $|\langle 1_R \rangle| = p$ prime,*

$$g_n(T, \mathbf{X}_n) = (-1)^n \frac{\Lambda_p(T, \mathbf{X}_n)}{\Lambda_p(\mathbf{X}_n)} \in \mathbb{F}_p[T, \mathbf{X}_n].$$

Moreover, define $I := \{1, \dots, n\}$, and for $J = \{1 \leq j_1 < \dots < j_i \leq n\}$, define

$$|J| := i, \quad \ell(J) := \sum_{l=1}^i j_l, \quad \mathbf{X}_J := (X_{j_1}, \dots, X_{j_i}).$$

Then for all n ,

$$\begin{aligned} \Lambda_p(T, \mathbf{X}_n) &= \sum_{i=0}^n (-1)^{\binom{i}{2}} T^{p^i} \sum_{J \subset I, |J|=i} (-1)^{\ell(J)} \Lambda_p(\mathbf{X}_J) \Lambda_p(\mathbf{X}_{I \setminus J})^{p^{i+1}} \\ &= \sum_{J \subset I} (-1)^{\ell(J) + \binom{|J|}{2}} T^{p^{|J|}} \Lambda_p(\mathbf{X}_J) \Lambda_p(\mathbf{X}_{I \setminus J})^{p^{|J|+1}}. \end{aligned}$$

Thus, the coefficient of X_0 is $\Lambda_p(\mathbf{X}_I)^p = \Lambda_p(\mathbf{X}_n)^p$, and the coefficient of $X_0^{p^n}$ is $(-1)^n \Lambda_p(\mathbf{X}_n)$. Moreover, $g_n(T, \mathbf{X}_n)$ is monic in T , with linear coefficient $\Lambda_p(\mathbf{X}_n)^{p-1}$. More generally, the coefficient in $g_n(T, \mathbf{X}_n)$ of T^{p^i} is

$$\frac{\sum_{J \subset I, |J|=i} (-1)^{\ell(J) + \binom{i}{2}} \Lambda_p(\mathbf{X}_J) \Lambda_p(\mathbf{X}_{I \setminus J})^{p^{i+1}}}{(-1)^n \Lambda_p(\mathbf{X}_n)} \in \mathbb{F}_p[\mathbf{X}_n],$$

and this is symmetric in the X_j , for all i .

Proof. For this proof, fix $R = \mathbb{F}_p[\mathbf{X}_n] \subset F = F(R) = \mathbb{F}_p(\mathbf{X}_n)$. Also define

$$h(T) := (-1)^n \frac{\Lambda_p(T, \mathbf{X}_n)}{\Lambda_p(\mathbf{X}_n)} \in F[T].$$

For the first part, we are to show two assertions: $h \in R[T]$, and $h(T) = g_n(T, \mathbf{X}_n)$ (for all n). First, one easily shows that $\Lambda_p(T, \mathbf{X}_n) \in \mathbb{F}_p[T, \mathbf{X}_n]$ is a polynomial in T of degree p^n , with leading coefficient $(-1)^n \Lambda_p(\mathbf{X}_n)$. Moreover, if V_n denotes the \mathbb{F}_p -vector space with basis X_1, \dots, X_n , then for all $v_0 \in V_n$,

$$\Lambda_p(T + v_0, \mathbf{X}_n) = \Lambda_p(T, \mathbf{X}_n) + \Lambda_p(v_0, \mathbf{X}_n) = \Lambda_p(T, \mathbf{X}_n) + 0 = \Lambda_p(T, \mathbf{X}_n),$$

using Proposition 20. This easily implies that $h(T)$ is S -translation-invariant (where $S = \langle S \rangle = V_n \subset R$). Applying Theorem 17 to $h(T)$ (using $k = 1$ and R replaced by F),

$h(T) \in F[T]$ is a polynomial in $\zeta_{(S)}(T) = g_n(T, \mathbf{X}_n)$. Since both these polynomials (in $F[T]$) have degree p^n and are monic, and since F is an integral domain, hence they are one and the same. But then $h(T) = g_n(T, \mathbf{X}_n)$ must lie in $R[T]$ as well.

For the second part, we refer to F. R. Gantmacher's book, *The theory of matrices, Volume 1*. More specifically, consider the *Laplace expansion formula* for computing determinants (in Chapter 1). Suppose $A_{n \times n}$ is a square matrix with entries in a commutative unital ring R , and for $J', J'' \subset I = \{1, \dots, n\}$ subsets of size i (for some i), $A \binom{J'}{J}$ denotes the appropriate *minor* (i.e., the determinant of the $i \times i$ submatrix formed out of the rows and columns corresponding to J' and J'' respectively). Then

$$\sum_{J \subset I, |J|=i} (-1)^{\ell(J)+\ell(J'')} A \binom{J'}{J} A \binom{I \setminus J''}{I \setminus J} = \begin{cases} \det A, & \text{if } J' = J''; \\ 0, & \text{otherwise.} \end{cases}$$

We now apply this result to the Van der Monde type matrix $A = ((X_i^{p^j-1})_{i=0}^n)_{j=1}^{n+1}$, where $X_0 = T$. Now expand this matrix along the first column (i.e., along the powers of T). The coefficient of T^{p^i} is $(-1)^i$ times the $n \times n$ minor, whose first i rows are $((X_l^{p^j-1})_{j=1}^i)_{l=1}^n$, and whose remaining $n-i$ rows are $((X_l^{p^j-1})_{l=1}^n)_{j=i+2}^{n+1}$. Now apply the Laplace expansion formula, using $J' = J'' = \{1, \dots, i\}$. Then

$$A \binom{J'}{J} = \Lambda_p(\mathbf{X}_J), \quad A \binom{I \setminus J''}{I \setminus J} = \Lambda_p(\mathbf{X}_{I \setminus J}^{p^{i+1}}) = \Lambda_p(\mathbf{X}_{I \setminus J})^{p^{i+1}},$$

where we have slightly abused notation (and used Proposition 20 for the last equality). The only thing left to verify is the sign attached to this expression (together with the $(-1)^i$ obtained above). By the Laplace expansion formula, we get

$$(-1)^i (-1)^{\ell(J)+(1+2+\dots+i)} = (-1)^{\ell(J)+\binom{i}{2}},$$

and hence we are done. □

We end with an easy consequence of this result.

Corollary 22. $\Lambda_p(\mathbf{X}_n) = g_0(X_1)g_1(X_2, \mathbf{X}_1) \dots g_{n-1}(X_n, \mathbf{X}_{n-1})$.

Proof. This is shown inductively. The statement clearly holds if $n = 1$. Now for general n , we use Theorem 21 to compute:

$$\Lambda_p(\mathbf{X}_n) = (-1)^{n-1} \Lambda_p(X_n, \mathbf{X}_{n-1}) = (-1)^{n-1} (-1)^{n-1} g_{n-1}(X_n, \mathbf{X}_{n-1}) \Lambda_p(\mathbf{X}_{n-1}),$$

whence we are done by the induction hypothesis for $n - 1$. □